KROLL

The Monitor

Volume 6

ISSUE 16

Growing Threat of DDoS Attacks by Extortionist Threat Actors

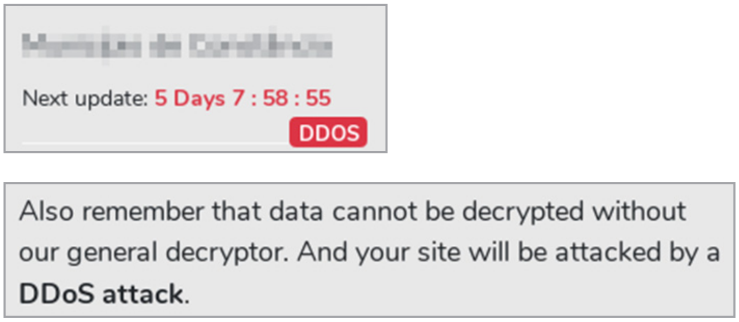
Kroll experts have noticed an increase in distributed denial of service (DDoS) attacks by cybercriminals seeking to turn a profit in two distinct incident types. First, many ransomware operators are now threatening and conducting DDoS attacks as an additional pressure tactic during the ransom negotiation process. Second, also known as ransom denial of service (RDoS), attackers threaten DDoS attacks that will take down an organization's public-facing services unless a ransom is paid.

What Is DDoS?

DDoS attacks are designed to take advantage of bottlenecks within an organization's systems. If a website or other internet-facing service is flooded with more data, traffic or requests than it can handle, the system may be unable to respond to legitimate requests and ultimately crash. Attackers often use this method as a means of causing confusion within an organization's systems to prevent regular business activity and distract employees while data is exfiltrated.

Attacker Insights and Motivations

Multiple ransomware gangs have added DDoS attacks as another pressure tactic during the ransom negotiation process. Figure 1 highlights a DDoS threat posted to the Avaddon ransomware group's actor-controlled site. Such activity frequently occurs when negotiation discussions stall as a means for the ransomware gangs to force the victim to resume discussions.



Next update: 5 Days 7 : 58 : 55

Also remember that data cannot be decrypted without our general decryptor. And your site will be attacked by a **DDoS attack**.

Figure 1 Avaddon DDoS Threats

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticetext

RDoS Attack Patterns

An RDoS attack adds an extortion element to a standard DDoS attack. In these instances, a cybercriminal may threaten to perform a DDoS attack against an organization unless a ransom is paid. In these scenarios, the actors will perform a “teaser” DDoS attack, sending anywhere from 50–100 gigabytes per second (Gbps) against an IP address associated with the target to prove their ability to perform the attack.

After the initial “teaser” attack, threat actors will often threaten higher-volume attacks that may cause more damage to public-facing services unless the ransom is paid. In order to provide legitimacy to this threat, actors may masquerade as well-known advanced persistent threat (APT) groups. In reality, the groups sending the extortion letters commonly lack the ability to actually carry out the DDoS attacks they threaten. These letters typically come in waves following news reports of major DDoS attacks or the discovery of a new vector for carrying out DDoS attacks. Sometimes, the attacker may not carry out the follow-on attack, even if the target does not pay the ransom demand.

On occasion, an organization may not experience a “teaser” attack at all but rather just receive a letter threatening such activity. Receiving an RDoS extortion threat via letter does not mean that an organization is under threat of an attack. In fact, most legitimate RDoS attackers work under the radar and will not provide any warning before carrying out their sample attack.

Some common features of attempted RDoS attacks identified by Kroll analysts include:

- **Protocols:** RDoS attackers use a variety of different network protocols to flood a target system with traffic. These attacks can take advantage of DDoS amplification, where spoofed traffic sent to a particular service results in much larger responses being sent to the target system.
- **Volume:** RDoS attacks can achieve high bandwidths of malicious traffic. The largest attack observed by Kroll reached a peak of approximately just under 200 Gbps.
- **Targets:** The IP addresses targeted in these attacks are located in different places. Often, these are systems with a single public-facing SSH, RDP, NetBIOS, or HTTP port open to the internet.
- **Botnets:** DDoS attackers commonly use a network of compromised computers to generate the malicious traffic in their attacks. In general, many of these systems are internet of things (IoT) devices and other computers that are compromised due to their use of weak usernames and passwords.

These RDoS attacks can easily take down under-protected public-facing services. However, a DDoS mitigation solution with robust traffic scrubbing capabilities can easily handle attacks of this volume.

ILLUSTRATIVE CASE STUDY

In a recent Kroll engagement, a victim was the target of an RDoS attack performed by a group claiming to be an advanced persistent threat (APT) group. The DDoS attack took down the company's internet-facing assets.

A few employees received a ransom note via email that had supposedly come from the criminals, with instructions on when and how the company could make payments to prevent a future attack from occurring.

The organization reached out to Kroll to help with managing the incident. Kroll analysts took several steps to improve the company's security posture and protection against DDoS attacks:

- **Compromise assessment:** DDoS attacks commonly originate from outside the victim's network and may not indicate the organization had been compromised, but it's important to confirm whether the criminals had established any sort of foothold within the impacted organization.
- **Gap analysis:** Kroll analysts began with an analysis of the organization's defenses against different types of DDoS events. This included evaluating the current protective technologies that were in place, reviewing the company's overall network architecture, and identifying vulnerabilities that could be exploited by a DDoS attacker.
- **Risk management recommendations:** Based on the results of the gap analysis, Kroll analysts provided recommendations on steps that the organization should take to both mitigate the short-term threat of the RDoS attack and manage their cyber security risks in general.
- **Threat intelligence research:** Kroll's threat intelligence research helped the organization better understand the common tactics, techniques and procedures used by the criminal group and assess which other threats posed the highest risk, based on the organization's footprint.

KROLL EXPERTS CORNER

James McLeary
Managing Director
Cyber Risk

Protecting Against DDoS Attacks

The following recommendations, provided by Kroll expert James McLeary, should be taken into consideration to protect against the threat of DDoS attacks:

- Consider implementation of DDoS scrubbing (cloud-based DDoS mitigation) solutions to give additional protection but ensure multi-layered overall approach across cloud protection, CDN, DNS and application-based appliances
- Contact your incident response partners and consider methods such as rate limiting, port blocking and blocking specific servers, if under such an attack
- Provide indicators of compromise to your internet service providers (ISPs) so they can also action responsive measures
- Ensure good cyber hygiene in your environment—identify prioritized assets that require extra protection and ensure your vulnerability and patch management is up to date
- Develop a DDOS incident response playbook and test it to solidify what to do during detection, response and recovery
- Consider the use of out-of-band communication channels for crisis handling that do not rely on ordinary corporate infrastructure. For example, if your corporate email, messaging and Active Directory services are affected by DDoS, the team can quickly switch to using temporary webmail, instant messaging or group chat applications, whilst being aware of the risks that this may pose

To adequately protect your organization from a DDoS attack, it is important to implement good cyber hygiene to ensure you're covered. In the event of an attack, Kroll experts can help respond. For further guidance, contact a Kroll expert at one of our 24x7 cyber incident response hotlines or connect with us through our Contact Us page.

ISSUE 17

Initial Access Brokers: Fueling the Ransomware Threat

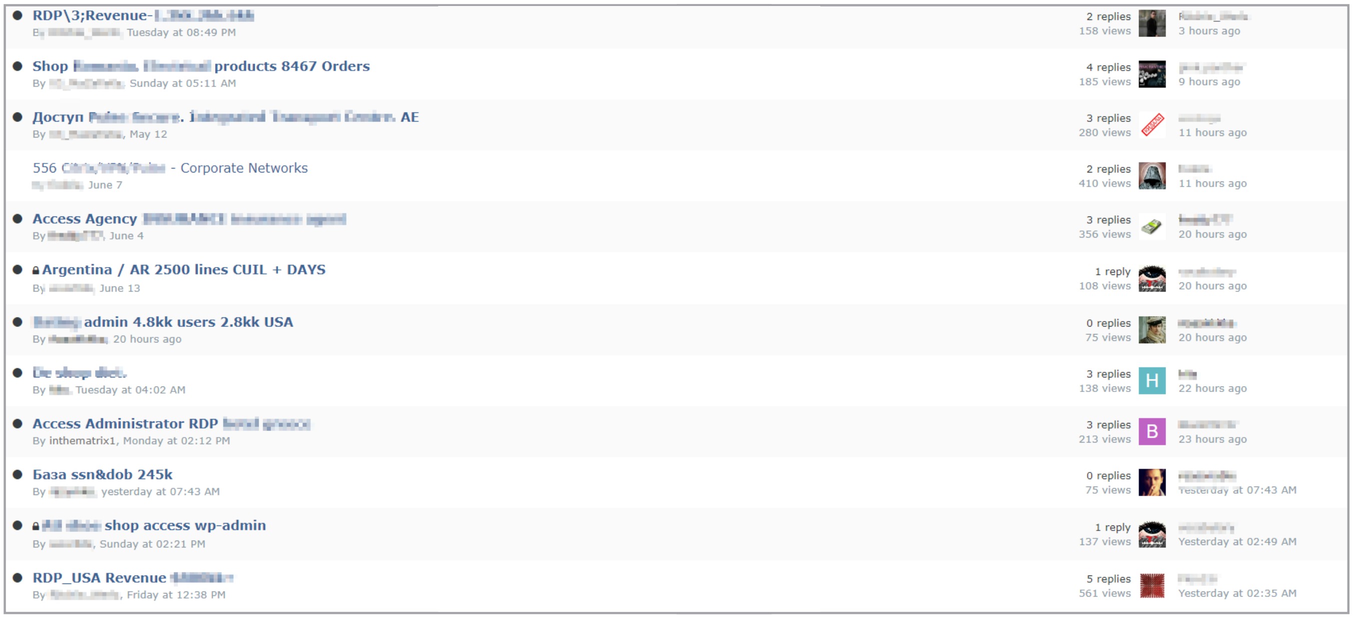
Kroll has observed an uptick in actors offering network access on the dark web, particularly in the wake of recent disruptions to the ransomware-as-a-service (RAAS) ecosphere such as the ban on ransomware discussions in notorious underground criminal forums.

Understanding the Initial Access Broker Process

Threat actors who offer network access, known as initial access brokers, operate at the beginning of the intrusion lifecycle by conducting reconnaissance to identify networks with vulnerable applications or devices, including Virtual Private Network (VPN) appliances, servers with exposed software vulnerabilities or open Remote Desktop Protocol (RDP). During the last year, multiple VPN providers have announced critical vulnerabilities, many of which could be exploited by attackers to access sensitive data such as login credentials. Open RDP instances are often exploited by actors testing credentials via brute-force attacks such as password spraying or by actors testing credentials related to the target network which are publicly exposed in credential dumps on the dark web.

Once access is achieved, access brokers advertise their network access on dark web forums, seeking to sell the validated credentials to ransomware operators, affiliates or other criminals who leverage the initial access to conduct a number of different cyber attacks such as data theft or encryption. In particular, ransomware operators are known to purchase such listings and provide them to their affiliate distributors who then engage in the intrusion lifecycle to execute code on the target network for lateral movement, conduct privilege escalation and ultimately, mission execution in the form of data theft, data destruction or ransomware deployment.

This segmented approach of RAAS operators creates more layers of intermediaries between the operators and the actors on the ground who carry out the attack, decreasing the risk of exposure and law enforcement apprehension.



- RDP\3;Revenue-[redacted]
  By [redacted] Tuesday at 08:49 PM — 2 replies, 158 views — [redacted] 3 hours ago
- Shop [redacted] products 8467 Orders
  By [redacted] Sunday at 05:11 AM — 4 replies, 185 views — [redacted] 9 hours ago
- Доступ [redacted]. [redacted]. AE
  By [redacted], May 12 — 3 replies, 280 views — [redacted] 11 hours ago
- 556 [redacted] - Corporate Networks
  [redacted] June 7 — 2 replies, 410 views — [redacted] 11 hours ago
- Access Agency [redacted]
  By [redacted], June 4 — 3 replies, 356 views — [redacted] 20 hours ago
- 🔒Argentina / AR 2500 lines CUIL + DAYS
  By [redacted] June 13 — 1 reply, 108 views — [redacted] 20 hours ago
- [redacted] admin 4.8kk users 2.8kk USA
  By [redacted] 20 hours ago — 0 replies, 75 views — [redacted] 20 hours ago
- [redacted]
  By [redacted] Tuesday at 04:02 AM — 3 replies, 138 views — [redacted] 22 hours ago
- Access Administrator RDP [redacted]
  By inthematrix1, Monday at 02:12 PM — 3 replies, 213 views — [redacted] 23 hours ago
- База ssn&dob 245k
  By [redacted] yesterday at 07:43 AM — 0 replies, 75 views — [redacted] Yesterday at 07:43 AM
- 🔒[redacted] shop access wp-admin
  By [redacted], Sunday at 02:21 PM — 1 reply, 137 views — [redacted] Yesterday at 02:49 AM
- RDP_USA Revenue [redacted]
  By [redacted], Friday at 12:38 PM — 5 replies, 561 views — [redacted] Yesterday at 02:35 AM

Figure 1 illustrates an auction page in a dark web marketplace advertising RDP/VPN credentials.

Kroll Observations

In incident response investigations, our digital forensic examiners often identify a single suspicious VPN or RDP log-in that predates the ransomware activity by several days, weeks or, at times, months. That first suspicious log-in is likely to be the initial access broker testing credentials and identifying a "match" for a username and password combination. The user account or internal user's computer that the unauthorized actor first lands on as a result of the log in success is what investigators associate with "patient zero" for the incident investigation. Subsequent analysis of the target organization domain has frequently identified that the credentials related to "patient zero" were readily available in various credentials dumps posted to the dark web.

EXAMPLE ENGAGEMENT

Multiple times in the past year, Kroll has observed threat actors in dark web forums sharing large datasets related to confirmed credentials for various VPN applications. In August 2020, a technology company experienced a ransomware attack. That same month, a large dataset of VPN credentials was briefly posted on a dark web forum. Kroll's identification and review of that dataset identified multiple account credentials available from the organization's employees, matching up nearly 100% with the accounts that the threat actors had accessed during the attack. This illustrated the likelihood that actors conducting ransomware attacks have access to initial lists of legitimate credentials, highlighting how dark web postings assist ransomware threat actor groups and organized crime affiliates to repeat their intrusion lifecycles against victims.

KROLL EXPERTS CORNER

Keith Novak
Managing Director,
Cyber Risk

Keith Novak provides best practices to mitigate against the effectiveness of initial access brokers:

1 Awareness Training

Training employees to identify and report phishing emails remains a critical component of every organization's security defenses. An organization should build on employee training with technical response procedures that guide the IT or InfoSec teams on the investigation and response to phishing attempts.

2 Multi-Factor Authentication (MFA)

MFA pairs a username and password with a unique second factor which can include a PIN or biometric that prevents an attacker who obtained user credentials from logging in as a legitimate employee. MFA should be required for all remote access, cloud services, and privileged access accounts and remains one of the top recommendations for any organization.

3 Vulnerability Management

Actor groups don't always rely on phishing to obtain their access. In fact, many threat actor groups exploit unpatched public facing systems and services to gain their initial foothold and exfiltrate usernames and passwords from internal systems that have been compromised. A mature vulnerability management program should include routine scanning of all external and internal systems, devices, and applications for vulnerable software and the timely application of patches from the vendors to remediate them.

4 Public Facing Systems

Reducing an organization's public facing systems and services is a great way to reduce the risk of initial compromise. For example, attackers routinely target Microsoft RDP services for both vulnerabilities as an entry point using phished user credentials. Moving all remote access services behind a corporate remote access VPN connection, requiring MFA, and posture-checking the users' device can be very effective at defending against unauthorized access.

5 Passwords

When it comes to password best practices, a few concepts continue to be proven true including: requiring the use of MFA, the longer the password the better, utilizing password managers, preventing the caching of passwords on user systems and browsers, and not sharing credentials with others.

6 Digital Risk Protection (DRP)

Proactive monitoring of dark web forums and other remote corners of the internet can help spot when corporate credentials are exposed in a new auction, or if attackers are impersonating your domains for phishing campaigns. Consider incorporating DRP in your security program.

To protect your access credentials and prevent them from possibly appearing on the dark web for auction, it is important to set up proper precautions including ensuring good password hygiene and enabling MFA. Kroll's Digital Risk Protection services can be used to monitor the deep and dark web for any exposures including any access credentials from your organization. Our experts will monitor for any threats, and provide assessments of exposure and vulnerabilities, delivered with actionable advice for how to protect your organization. For further guidance, contact one of our Kroll experts at one of our 24x7 cyber incident response hotlines or connect with us through our Contact Us page.

ISSUE 18

Deep Dive Into PYSA Ransomware

PYSA is the most recent ransomware variant known distributed by the Mespinoza Ransomware as a Service (RaaS) gang, which has been infecting victims since 2019. Kroll has consistently observed PYSA in our incident response engagements since 2020 and has noted an increase in frequency of this variant since the second quarter of 2021.

Our analysis shows PYSA is opportunistic and not restricted to one sector or geographical area. PYSA primarily leverages exposed Remote Desktop Protocol (RDP) to gain a foothold into a network. Once inside a network, PYSA deploys several tools, including custom-built scripts written in GO language to maintain persistence. During their time in a network, the group focuses on exfiltration of data followed by encryption. Victims are then extorted for decryption services and to ensure that confidential information is not leaked.

Initial Access

Similarities across PYSA investigations such as tactics, infrastructure and the steady development of capabilities, suggests that the group is operated manually by a single group of actors. Initial access is usually gained through internet exposed RDP by using active, valid accounts. These accounts are accessed by brute force or previously exposed credentials from other breaches.

Once they have accessed a network, PYSA threat actors use discovery tactics to identify admins and other systems on the network. Tools such as AdvancedIPScanner and AdvancedPortScanner are commonly used during this process. PYSA will dump Local Security Authority Subsystem Service (LSASS) in order to gain enhanced privileges or further access to other privileged accounts before using Mimikatz to extract account information and passwords. Precursor PowerShell scripts are often run to disable anti-virus and other security mechanisms, the deletion of volume shadow copies, disable services and to identify documents of interest prior to encryption.

In our observation, loiter time for PYSA is longer than the average ransomware event, likely due to the manual nature of the attack. Earlier activity relied on maintaining access to valid accounts, however the group has recently been observed using a Golang tool known as Chisel to maintain command and control. The tool operates a tunnel over HTTP secured by Secure Shell (SSH)to pass through firewalls, allowing “hands-on” access to the target environment.

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticetext

The main goal of a PYSA attack is extortion for data encryption and data leakage. They typically offer to decrypt and not leak stolen information if the victims pays the requested ransom. Once a network is encrypted, PYSA drops a ransom note (Readme.Read) and locks files with the extension .<domain> or .pysa. The ransomware binary writes the note to the registry key below, which displays the ransom note on logon.

SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticetext

PYSA Exfiltration Tactics, Techniques and Procedures

To locate documents for exfiltration, PYSA uses automated scanning of systems with PowerShell by using a script that searches 123 keywords. Files can contain personal identifiable information (PII), tax and financial information, login credentials, legal documents, incriminating evidence and other sensitive information. Exfiltration has been achieved through the mounting of file shares on adversary infrastructure and the use of tools such as WinSCP.

PSYA will post these files on their actor-controlled site, the home page of which advertises the slogan "Protect Your System Amigo." (Figure 1) PYSA typically adds new victims 1-2 times per month with each "update" possibly including 5 to 20+ victims. Recently, the threat actors have implemented CAPTCHAs to the shaming site in order to view published exfiltrated data.

We have observed that the time lag between encryption and data publication is longer for PYSA than other ransomware variants. In some instances, Kroll has identified victims posted to the actor-controlled site upwards of three months past the date of encryption.

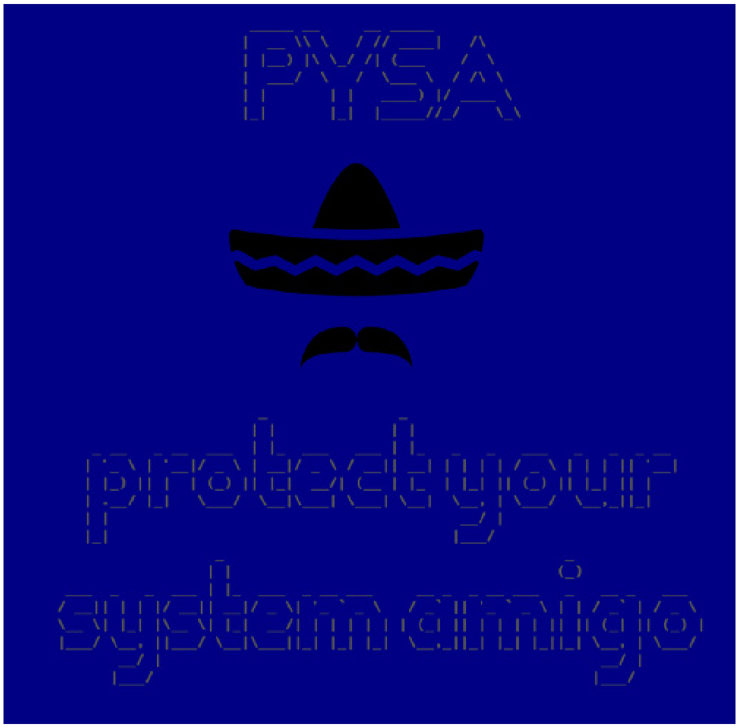


Figure 1 - PYSA Actor-Controlled Site Home Page (SOURCE: Kroll)

Victim Trends

Although the most common sector targeted is education, PYSA targeting includes a wide spectrum of sectors such as medical, manufacturing, construction, local government, transport and retail. This is not an all-inclusive list.

Mespinoza (PYSA) Doxxing Victims by Sector

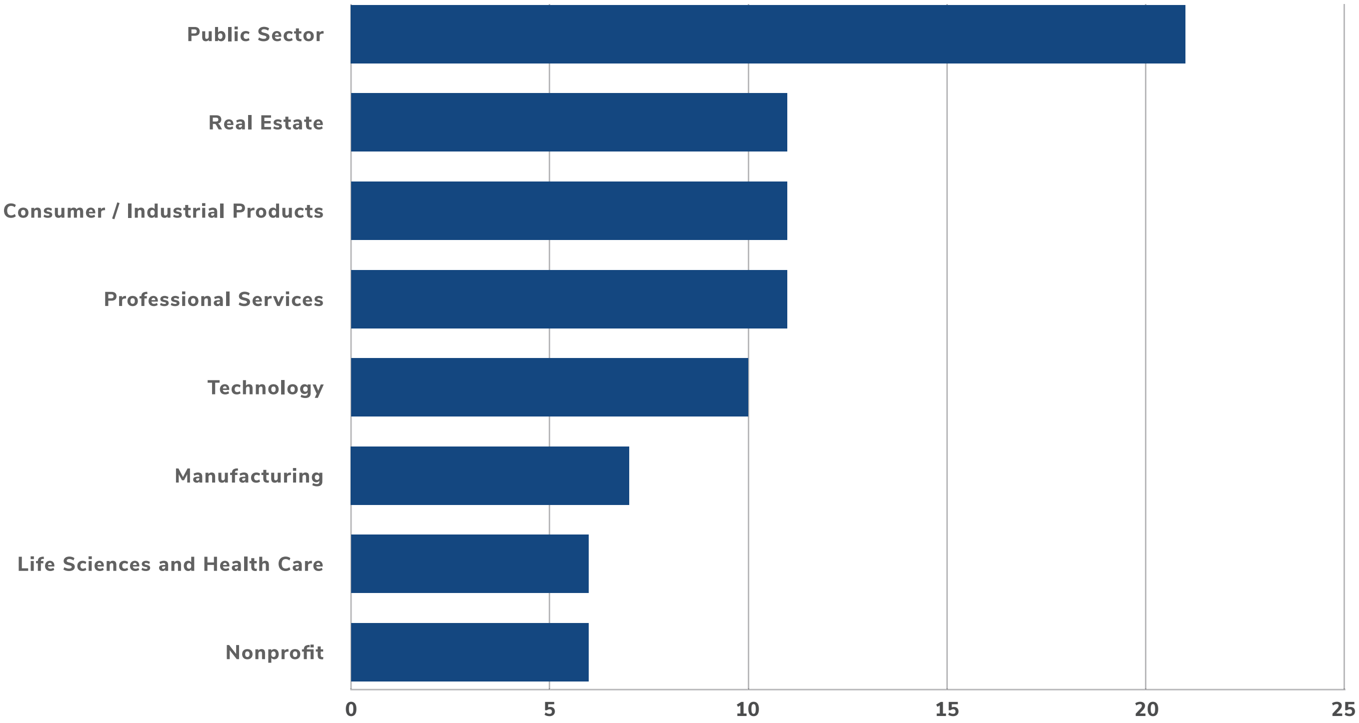


Figure 2 - PYSA Victims by Sector (Data Source: Intel471)

55% of victims are located within the United States. However, companies in other countries such as the United Kingdom, Brazil, Italy, Canada, and France have all faced numerous attacks.

Mespinoza (PYSA) Doxxing Victims by Region

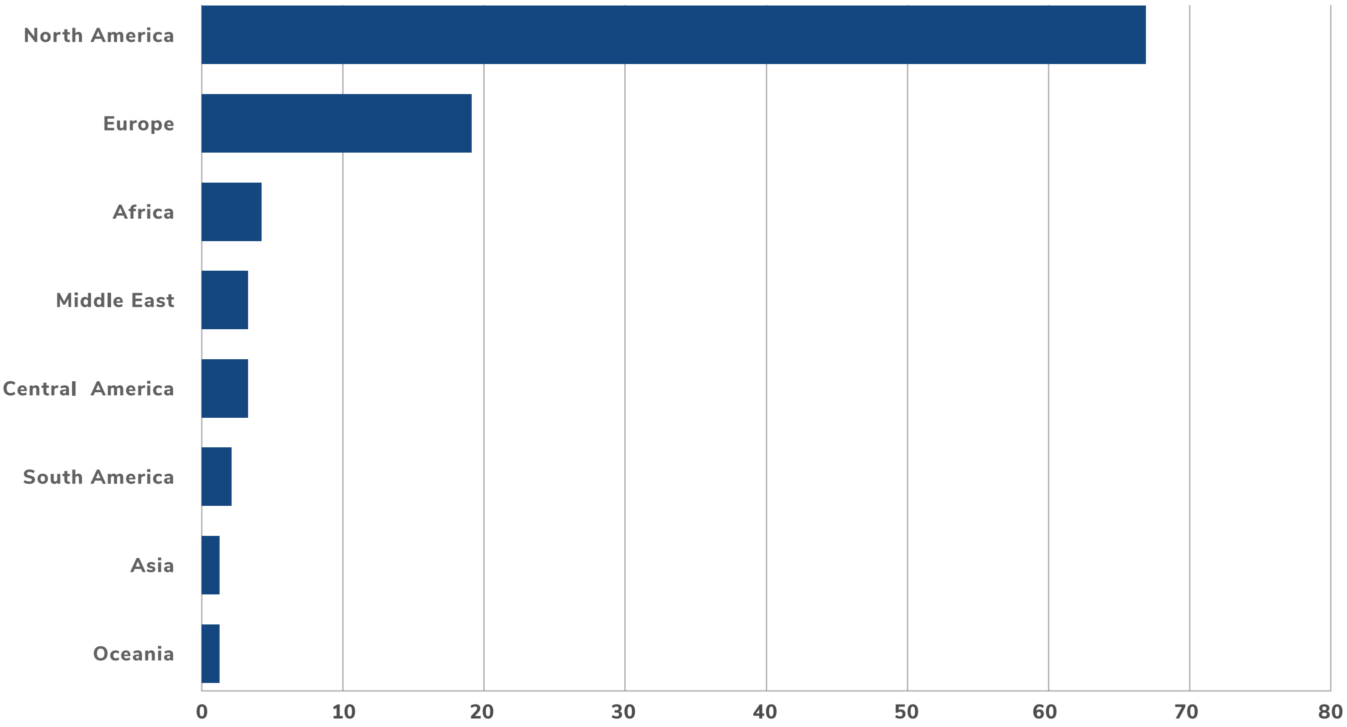


Figure 3 - PYSA Victims by Region (Data Source: Intel471)

EXAMPLE ENGAGEMENT

In a recent Kroll engagement, a multinational company in the food and beverage industry was targeted by PYSA and had their data exfiltrated and a ransom demanded. The initial access point for the threat actors was the organizations' exposed RDP. One month after the initial access, ransomware was executed. Data exfiltration was conducted via a Server Message Block (SMB) protocol-based share to an internally hosted web server, where the adversary left the remote share over-exposed. This allowed the exfiltrated files to be viewed on PYSA's server for a short while.

KROLL EXPERTS CORNER

Paul Wells
Vice President, Cyber Risk

James Thoburn
Senior Vice President, Cyber Risk

Paul Wells and James Thoburn in our practice provide recommendations to keep your network secure and prevent PYSA from being able to access your data.

We observed PYSA exploiting exposed RDP services. This is not a tactic unique to this group and is used by many threat actors as a quick method to get an easy foothold into an environment. Securing RDP connections is important for all organizations, but it can be challenging for geographically dispersed and complex IT infrastructures.

- **Understand your internet footprint.** External RDP services are often enabled to solve short term issues or for a development environment. These can fly under the radar of the usual security controls and may present an unexpected weak spot attractive to attackers. Conducting regular assessments of what services are exposed to the internet can be an effective method of identifying whether your exposure has changed. Ideally this should be conducted by an independent third party to ensure a thorough check.
- **Secure RDP connections.** RDP systems exposed to the internet will be vulnerable to brute force attacks, credential stuffing and potential vulnerabilities within the service. Best practice is to ensure all RDP services run within a virtual private network (VPN) solution to restrict external access.
- **Enable Network Level Authentication (NLA) for RDP.** NLA requires authentication prior to a session being established. If NLA is not enabled, threat actors may be able to enumerate user accounts and fingerprint the Windows version. Vital intelligence for any motivated adversary.

PYSA is dependent on PowerShell scripts for reconnaissance, disruption and in some cases even encryption. Modern Windows operating systems include the Anti-Malware Scan Interface (AMSI) to enable anti-virus agents to detect and block malicious scripts. However, older operating systems, such as Windows 2012, do not include AMSI, so malicious scripts are unlikely to be detected and blocked. Therefore, it is important to assess the operating systems deployed within your environment and to make sure mitigation strategies are in place for any machines that do not conform to the hardening policy. Restricting the number of accounts that can run PowerShell may also reduce the ability of PYSA to operate as effectively within the network during their intrusion lifecycle.

Contacts

Keith Wojcieszek
Managing Director, Cyber Risk
+1 443 295 5082
keith.wojcieszek@kroll.com

Based in Washington, D.C., Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security.

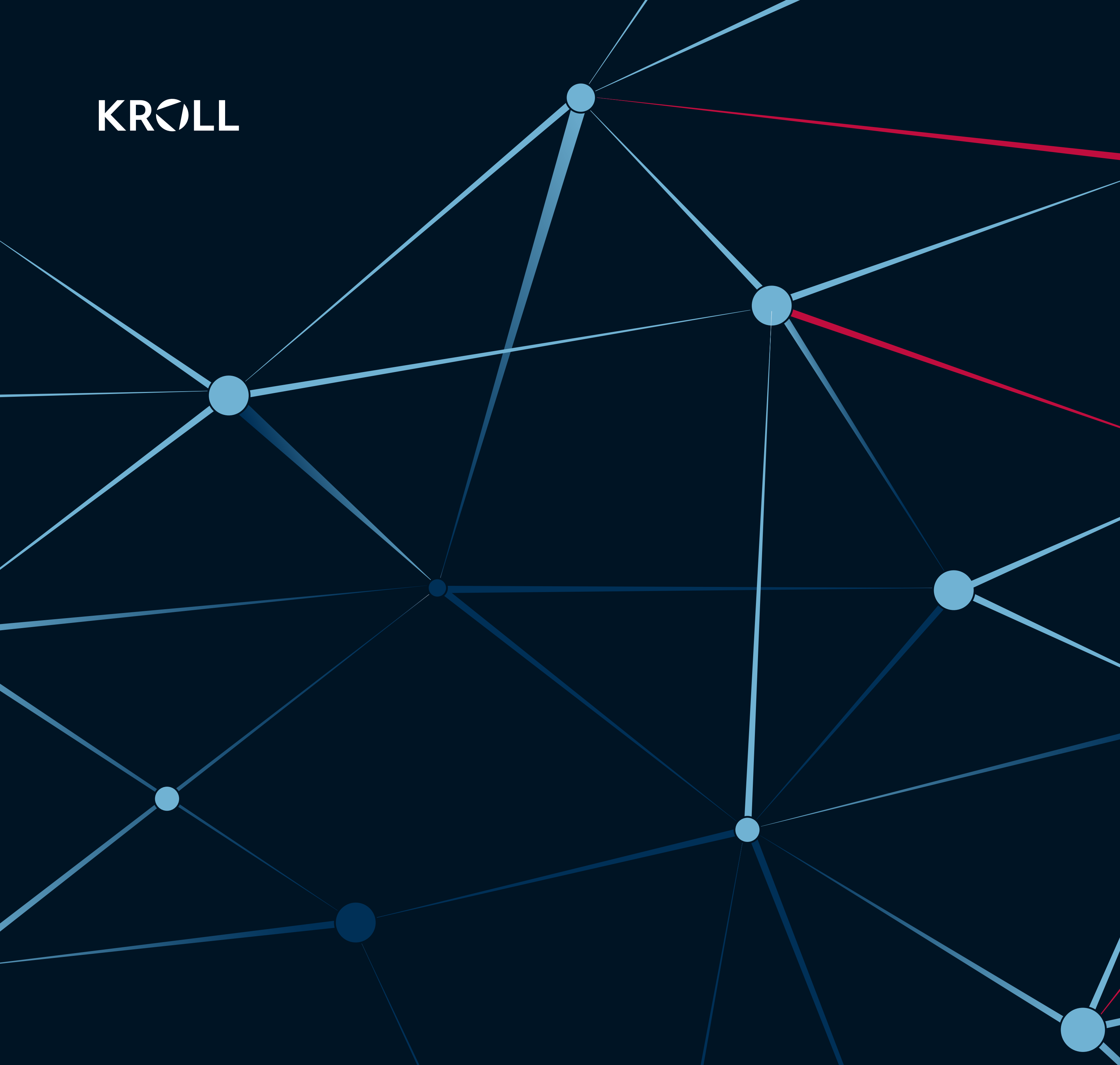
Nicole Sette
Senior Vice President, Cyber Risk
+1 609 514 8225
nicole.sette@kroll.com

Based in the Secaucus office. Nicole is a highly accomplished security professional, who brings unique insight to the multiple dimensions inherent in client challenges from her years of federal law enforcement and military experience. Nicole served as a Cyber Intelligence Analyst with the Federal Bureau of Investigation for nearly 10 years, and was an Intelligence Specialist with the U.S. Army Communications-Electronics Command for four years.

Laurie Iacono
Senior Vice President, Cyber Risk
+1 412 588 4337
laurie.iacono@kroll.com

Based in the Secaucus office, Laurie is an experienced cyber intelligence professional with a focus on tracking threat actor groups affiliated with ransomware-as-a-service operations. Laurie joined Kroll from the NCFTA where she led a team of intelligence analysts focusing on cybercrime and dark web investigations across multiple industries.

KROLL



Browse the latest editions of *The Monitor* and subscribe free at kroll.com/themonitor

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.