Written Testimony of:

Daniel Sergile
Senior Consulting Director, Unit 42
Palo Alto Networks

Before the:

Committee on Financial Services
Subcommittee on National Security, Illicit Finance, and International Financial Institutions

Regarding:

*“Held for Ransom: How Ransomware Endangers our Financial System”*

April 16, 2024
10:00 AM

Chairman Luetkemeyer, Ranking Member Beatty, and distinguished members of the committee:

Thank you for the opportunity to testify on the ransomware threat landscape. Your committee's interest in better understanding the role of incident responders in ransomware investigations is greatly appreciated. My name is Daniel Sergile, and I am Senior Consulting Director of Unit 42, the threat intelligence and incident response division of Palo Alto Networks. On behalf of my company, I offer our commitment to work in partnership with you and your staffs as you continue to examine the ransomware landscape and its impact on the financial services sector.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the global cybersecurity leader – protecting businesses, people, and governments across more than 150 countries. We support 95 of the Fortune 100, 8 of the 10 largest U.S. banks, critical infrastructure operators of all shapes and sizes, the U.S. federal government, universities, educational institutions, and a wide range of state and local partners.

Practically speaking, this means we have a unique vantage point into the cyber threat landscape. This information, paired with the insights we develop from helping organizations respond on a daily basis to complex cybersecurity incidents, puts us on the front lines of the cyber defense battle. We are committed to using this mantle to be good cyber citizens and trusted security partners.

**Ransomware Actors Are Becoming More Sophisticated**

The scourge of ransomware has taken cybersecurity from what was seen as an "IT issue" to something with day-to-day relevance for many Americans and reputational, operational, and financial risk for organizations of all sizes. Every member of this committee has likely had a business, bank, school, or local government entity in their district victimized by a ransomware attack. These attacks affect our daily lives – from the hospitality industry to disruptions of public services like healthcare or emergency services, interruptions in supply chains, to critical gas pipelines being taken offline.

This threat is not subsiding. Instead, adversaries continue to enhance their techniques and increase their sophistication. They are more knowledgeable and able to use IT, cloud, and security tools as offensive weapons – and are using proven processes and playbooks to achieve their goals more efficiently. In the recent *Ransomware and Extortion Report* from Unit 42, we specifically highlight three alarming trends – 1) an increase in harassment activity, 2) an increase in multi-extortion techniques, and 3) continued evolution in the attack vectors used for initial compromise.

Cyber adversaries are already leveraging AI to advance their tradecraft and will continue to do so going forward. For example, we see evidence that adversaries are using AI to enhance what we call social engineering attacks – phishing emails and voice calls designed to lure users to "click the link" or provide access. Cybercriminals now have AI-driven methods to combine both legitimate and fraudulent voice and data to evade Know Your Customer (KYC) and Anti-Money

Laundering (AML) authentication processes from account origination through credit, lending, payments, and trading activities.

Additionally, bad actors are innovating with AI to accelerate and scale attacks and find new attack vectors. If they successfully take over an organization's network, AI enables them to move laterally with increased speed and identify an organization's critical assets for exfiltration and extortion. Bad actors can now execute numerous attacks simultaneously against one company, leveraging multiple vulnerabilities.

In addition to increasing the scale and volume of ransomware attacks, ransomware threat actors are becoming more aggressive with their tactics, with the ultimate goal of increasing their chances of getting paid. These bad actors now target specific individuals in an organization, often in the C-suite, with extortion threats and unwanted communications. This harassment is now involved in 27% of ransomware cases Unit 42 investigates, compared to just 1% a few years ago. It is not uncommon for threat actors to leverage customer information that has been stolen to try to force the organization's hand into payment.

Threat actors have also come to realize that they are more likely to get paid if they put additional layers of pressure on their victims. We call these tactics multi-extortion. Threat actors may use ransomware to lock up an organization's networks or data, and since many organizations now have viable backups, the attackers will also steal data and threaten to leak it to the dark web or other channels to increase their chances of getting paid. The use of multi-extortion tactics continues to rise, with ransomware threat actors currently engaged in data theft in about 70% of cases on average, compared to only about 40% of cases as of mid-2021.

Every day, Unit 42 researchers see about seven new ransomware victims posted on leak sites. That is one *every four hours*. In 2023, Unit 42 observed an average ransom demand of $4 million per attack, with peaks reaching as high as $35 million. We have also seen certain groups become more aggressive at targeting specific sectors and industries, with professional and legal services, technology, manufacturing, healthcare, and financial services being the most targeted, as outlined in Unit 42's *Ransomware Retrospective 2024*.

Attackers are often in the systems of organizations long before those organizations become aware of an intrusion. Dwell time is the time between the first detection of attacker activity and the earliest evidence of the attacker's presence. The median dwell time in 2023 was 13 days, but attackers are increasingly getting faster at exfiltrating data once they have gained access to a network or system. In 45% of Unit 42 incident response cases last year, attackers exfiltrated data in less than a day after compromise.

Certain threat actors are increasingly creative at evading detection. Nation states in particular use sophisticated techniques that include outsourcing key parts of their offensive operations to proxies. While nation state attacks are typically conducted with the primary goal of intellectual property theft or espionage, we have recently seen nation states leverage ransomware to disguise this activity as criminal hacktivism. This dynamic has increased demand for “ransomware-as-a-service” operators, often blurring the lines between state actors and criminal groups and making attribution and accountability much more difficult. Cybercriminals also use cryptocurrency for anonymity via blockchain technology, which can make tracing the payments challenging.

**Attack Surfaces Remain Vulnerable to Ransomware Attacks**

A sobering yet persistent reality of our connected world is that far too many “digital doors” are left open for adversaries to walk through with relative ease.

It is often said the internet looks very small to an attacker but massive to a defender. After all, an enterprise that closes 99% of its digital doors but leaves one open inadvertently may well be destined for a breach. Entities of all sizes, public and private, have historically struggled to understand and manage their digital infrastructure, including phones, laptops, servers, and applications that have been exposed to the internet. In fact, we have found that even sophisticated enterprises actually have twice the number of systems exposed on the internet than what they were internally monitoring – a visibility gap that gives adversaries the upper hand.

Complementing our insights from incident response cases, we also leverage a capability that indexes the public-facing internet through the eyes of the adversary to discover exposed systems, vulnerabilities, and misconfigurations.

Data points from this capability highlight the ubiquity of poor configurations around a remote access method called Remote Desktop Protocol (RDP), a prime target for ransomware attacks. While RDP provides the ability to work from anywhere, if not properly configured and controlled, this protocol can grant adversaries extensive access to administrative privileges within a network, thereby amplifying the potential impact of a network intrusion.

RDP misconfigurations make up 20% of all the exposures we observe on the public-facing internet, according to our annual attack surface threat report. Additionally, over 85% of organizations we observed with these exposures left them unaddressed for at least 25% of a typical month. Much of this can likely be explained by legacy security postures that do not appropriately incorporate automation and AI into vulnerability discovery and remediation. Such a posture too often leaves organizations open to ransomware attacks or unauthorized login attempts for sustained periods of time.

In addition to unpatched vulnerabilities on internet-facing systems, partial or incomplete deployment of an organization’s security controls and poor identity and access management allows attackers to access and move around networks. We are also increasingly seeing cloud infrastructure as an inviting attack vector for adversaries. In fact, over 80% of the exposures we observed were cloud-based, and Unit 42 similarly saw a 115% increase in cloud-related incidents in 2023 compared to 2022.

In summary, global attack surfaces can look porous to cyber adversaries. This concern is often exacerbated by the prevalence of legacy IT, which has proven problematic in the financial services sector due to the geographic distribution of branches and personnel.

**Incident Response: Helping Organizations in Their Times of Need**

Rapidly deployable incident response teams like Unit 42 at Palo Alto Networks often get the proverbial 3:00 AM phone call from an organization that has been compromised. Helping these organizations during moments of great vulnerability and duress is both challenging and rewarding. When Unit 42 becomes involved in an incident response case, we move quickly to assess the breadth, severity, and nature of an attack.

The four widely recognized stages of cyber incident response are: 1) preparation and prevention, 2) detection and analysis, 3) containment and eradication, and 4) recovery.

Ransomware attacks may originate from unmanaged devices, such as employees working remotely on a personal device while still accessing critical resources or sensitive corporate data. Accordingly, understanding an organization's preparation and prevention baseline is important when calibrating subsequent incident response efforts. For example, an entity's awareness of where various data assets reside, its access control posture across its networks, and its deployment of visibility and continuous monitoring of tools across its digital estate, provide critical context for incident responders when initially assessing the severity of a breach.

We act quickly to answer key questions such as how an incident was identified, what data and assets were impacted, and what indicators of compromise exist. We use this information to determine the threat actor behind the attack. The close partnership between an organization and its trusted incident response firm helps to identify the size, scope, and severity of the incident during this critical time.

Incident response teams maintain careful documentation through the analysis phase. They work expeditiously to safeguard and restrict access to case data because it often contains sensitive information, such as data on exploited vulnerabilities, recent security breaches, and users that may have performed inappropriate actions. Combining the functional impact to the organization's systems and the impact to the organization's information determines the aggregate business impact of the attack.

As we support entities during the incident response process, we discover compromised systems by rapidly deploying specialized technology to identify and contain malicious activity. The incident response team works closely with individuals at the impacted entity and its partners assisting in the response. These individuals vary by organization, and may change based on the nature and scope of the attack, but often include the chief information officer, head of information security, human resources leaders, legal departments, outside counsel, cyber insurance companies, communications, and law enforcement.

Once an investigation is complete, the victim organization receives a detailed report as well as guidance in implementing additional security controls to get back on its feet now that the threat actor is out of its environment. Data is recovered, and systems are patched and reconfigured so business operations can resume securely. Incident responders offer lessons learned and recommend specific improvements to transform an organization's security profile.

**Repelling Attackers With AI and Automation**

AI and automation are transformative for network defenders, enabling organizations not only to recover more quickly, but also more nimbly ingest and analyze security data to harden their networks against future attacks.

One of the most promising applications of AI and automation for cyber defense is to significantly uplevel and enhance the capabilities within Security Operation Centers (SOCs). For too long, our community's most precious cyber resources – people – have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of "whack-a-mole," while vulnerabilities remain exposed and critical alerts are missed.

Two of the most important metrics for any security operations team are Mean Time to Detect and Mean Time to Respond. As the terms suggest, these metrics provide quantifiable data points for network defenders about how quickly they discover potential security incidents and then how quickly they can contain them.

Historically, organizations have struggled to execute against these metrics. A recent Unit 42 report that analyzed real-world cloud-related incident response cases found that, on average, security teams take nearly *six days* to resolve an alert. In contrast, we now see many adversaries moving from compromise to data exfiltration in just hours.

Giving defenders the upper hand requires a new approach that leverages AI-driven SOCs. This technology will be a force multiplier for our cybersecurity professionals and substantially reduce detection and response times.

Early results from deploying this technology on our own company networks have been particularly promising. On average, we ingest 36 billion events daily and use AI-driven data analysis to automatically triage that number down to just eight that require manual analysis. In addition, we have reduced our Mean Time to Detect to just 10 seconds and our Mean Time to Respond to just one minute for high priority alerts.

Early customer benefits have been similarly encouraging. We have already seen a reduction in mean response times from weeks and days to hours and minutes. Such a reduction is critical to stopping ransomware threat actors before they can encrypt systems or steal sensitive information, and for minimizing the impact of an incident. This tool has dramatically improved incident close-out rates from 20% pre-deployment to 100% post-deployment.

Both increased adversarial speed to steal or encrypt data and policy developments requiring cyber incidents to be reported within days of determining their severity demand rapid detection and response. In order to stay a step ahead of sophisticated adversaries, we must also detect never-before-seen anomalous behavior, not just previously identified attack patterns. AI now gives us the capability to do so – putting network defenders back in the driver's seat, not a step behind.

**A Shared Vision for the Future of Cyber Defense**

Our vision for a more secure digital future is simple: enable organizations to have comprehensive, real-time visibility across their networks, and the ability to prevent, detect, and respond to cyber attacks quickly and effectively with automated capability.

The U.S. government has recently taken a number of policy steps that endorse and promote this vision. The Executive Order on Improving the Nation's Cybersecurity (EO 14028) from May 2021, and the National Cybersecurity Strategy and its related implementation plan released last year, promote key themes we support – more real-time visibility across enterprises, rapid adoption of zero trust network architecture, and secure software development.

The Cybersecurity and Infrastructure Security Agency (CISA) recently launched a Ransomware Vulnerability Warning Pilot to provide critical infrastructure entities with advance notice of vulnerabilities and exposures present on their networks before an adversary exploits them. We appreciate CISA's efforts to continue maturing this capability and encourage all critical infrastructure entities and state and local governments to contact their nearest CISA regional office to take advantage of the free services the agency offers.

Cybersecurity resilience does, of course, require investment. To that end, we commend the progress of the State and Local Cybersecurity Grant Program, a byproduct of the bipartisan *Infrastructure Investment and Jobs Act*, for the critical role it is already playing in catalyzing cyber resilience across all corners of the country.

Policymakers continue pushing cyber incident report requirements, most recently highlighted by CISA's release of its proposed rulemaking pursuant to the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA), which will eventually require covered entities to report certain cyber incidents and ransom payments. We see CIRCIA, the recently enacted SEC cyber rules, and other similar rules and requirements around the world as part of a broader signaling by policymakers concerning the need to intensify efforts to increase cyber awareness and resilience.

We urge all cyber stakeholders to look at meeting these requirements not simply as a compliance exercise, but rather as an opportunity to reimagine defense of our digital ecosystem using modern, AI-powered cyber and incident response capabilities.

**Partnerships and People Remain Critical**

It is often said that cybersecurity is a team sport, and partnership is very much in our DNA at Palo Alto Networks – and across the entire cybersecurity industry.

Of particular relevance to this hearing, executives at our company find value participating in the Ransomware Task Force (RTF) in their personal capacity. The RTF is a group of over 60 experts from industry, government, law enforcement, and civil society that has created and helped execute a comprehensive framework for public-private action to combat ransomware. As a Financial Services Information Sharing and Analysis Center (FS-ISAC) sector advisor, Palo Alto Networks contributes to a number of timely reports analyzing the current threat landscape and trends facing financial institutions.

Palo Alto Networks is also proud to be a founding Alliance member of CISA's Joint Cyber Defense Collaborative (JCDC). In forums like these, we share technical threat intelligence on a daily basis through partnerships with U.S. government entities, private sector entities, and other allied nations to support global prevention and response to significant cyber incidents.

With AI and automation central to modern cyber defenses, it is critical we educate and train the cyber workforce of tomorrow with the advanced skills required for meaningful jobs that complement technological innovation. This approach is foundational to improving our collective cyber defense and staying ahead of all cyber threats, including ransomware.

To that end, Palo Alto Networks offers several accelerated onboarding programs to diversify the workforce, including the *Unit 42 Academy*, which welcomes new early career participants each August as full-time members of our incident response and cyber risk management teams. We are pleased to report that our 2023-2024 class is 80% female.

**Five Key Recommendations to Reduce Risk**

With so much information from countless sources about the cyber threat landscape, it can be difficult for organizations to prioritize cyber risk management efforts where they matter most. With that in mind, we recommend organizations focus on the following actions to increase their cyber resilience:

1. Maintain an incident response plan to prepare for and respond to cyber incidents, including emerging ransomware tactics like extortion, multi-extortion, and harassment. Organizations that continuously review, update, and test their incident response plans – ideally with input from cybersecurity experts – are much more likely to effectively respond to and contain an active attack. Organizational leadership must elevate cybersecurity as a core part of their overall enterprise risk management strategy.
2. Ensure complete visibility of attack surfaces: 75% of ransomware attacks and breaches fielded by Unit 42's incident response team result from a common culprit – internet-facing attack surface exposures. Deploying solutions that provide centralized,

near real-time visibility can help organizations identify and mitigate vulnerabilities before they can be exploited.

3. Leverage the power of AI and automation to modernize security operations and reduce the burden on overworked analysts. The latest technology can help organizations drive down key cybersecurity metrics like Mean Time to Detect and Mean Time to Respond, denying attackers the time they need to compromise an organization's systems or exfiltrate its data. Additionally, technique-based protections mapped to the MITRE ATT&CK Framework can help defenses nimbly evolve in response to adversarial tactics.
4. Implement enterprise-wide zero trust network architecture: This is a fundamental security principle that assumes the network is already compromised and implements processes that continuously validate the user, device, application, and data in a controlled manner. Zero trust network architecture creates layers of security that prevent or limit an attacker from successfully moving laterally around the network. This provides victims with more time to detect, properly contain, and remediate the threat.
5. Protect cloud infrastructure and applications: With cloud migration accelerating, threat actors will continue to develop tactics, techniques, and procedures designed to target and compromise cloud workloads. Organizations leveraging cloud infrastructure should implement a cloud security program and platform that offers comprehensive cloud-native security.

While there is no silver bullet in cybersecurity, prioritizing these recommendations will materially reduce the risk of falling victim to an attack, more effectively contain an attack, if one does occur, and help increase the resilience of financial institutions and the entire cybersecurity ecosystem.

Thank you for the opportunity to testify. I look forward to your questions.