Written Testimony of:

Sam Rubin
Vice President – Global Operations, Unit 42
Palo Alto Networks

Before the:

Committee on Oversight and Accountability
Cybersecurity, Information Technology, and Government Innovation Subcommittee
Economic Growth, Energy Policy, and Regulatory Affairs Subcommittee
United States House of Representatives

Regarding:

"Combating Ransomware Attacks"

September 27, 2023
1:00 PM

Chairs Mace and Fallon, Ranking Members Connolly and Bush, and distinguished members of the committee:

Thank you for the opportunity to testify on combating ransomware attacks. Your subcommittees' continued commitment to advancing thoughtful, bipartisan cybersecurity policy is greatly appreciated. My name is Sam Rubin, and I am Vice President and the Global Head of Operations for 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 address a range of critical cybersecurity issues.

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, critical infrastructure operators of all shapes and sizes, the U.S. federal government, universities and other educational institutions, and a wide range of state and local partners.

Practically speaking, this means that we see a lot. This expansive 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 cyber defense battles. 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. Every member of this committee has likely had a business, school, or local government entity in their district victimized by a ransomware attack. These attacks affect our daily lives – from disruptions to needed public services, like hospitals or first responders, to 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. In our 2023 Ransomware and Extortion Report, we specifically illuminate 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.

In addition to increasing the scale and volume of ransomware attacks, ransomware threat actors are 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 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 harass them and try to force the organization's hand into payment.

Threat actors have also come to a realization that they're more likely to get paid if they put additional layers of pressure on their victims. We call this multi-extortion. Threat actors may use ransomware to lock up an organization, and since many organizations have viable backups, the attackers will also steal data and threaten to leak it to increase their odds of getting paid. Multi-extortion tactics continue to rise, with ransomware threat actors engaged currently 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's one *every four hours*. Our most recent Ransomware and Extortion Report puts the median monetary demand per attack at $650,000, with the median ransomware payment at $350,000. We have also seen certain groups become more aggressive at targeting specific sectors and industries. For example, a group called Vice Society has been especially prolific at targeting educational institutions, with at least 145 victims since 2021 and more than half of their attacks impacting the education, government, and healthcare sectors.

More recently, we've seen a group called Muddled Libra look for strategic points of leverage to scale the impact of their malicious activity. By targeting Business Process Outsourcing (BPO) providers, they've proven adept at compromising these widely used third party services to gain access to BPO customers across multiple sectors. Among other tactics, threat actors frequently use social engineering or text messages to lure employees into providing credentials to gain access to organizations.

Attack Surfaces Remain Vulnerable to Ransomware and Other Attacks

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 cyber breach. Entities of all sizes, public and private, have historically struggled to understand and manage the digital infrastructure – phones, laptops, servers, and all the rest – they have exposed on 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.

Leveraging a capability that indexes the public-facing internet through the eyes of the adversary to discover systems, vulnerabilities, and misconfigurations, we publish an annual Attack Surface Threat Research Report. This report essentially provides a detailed analysis of the digital infrastructure that adversaries may try to exploit.

The results indicate that far too many "digital doors" remain open. A particularly concerning finding is the ubiquity of poor configurations around a remote access method called Remote Desktop Protocol (RDP), a prime target for ransomware attacks. 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. Additionally, over 85% of organizations we observed with these exposures left them unaddressed for at least 25% of a typical month, leaving the organizations open to ransomware attacks or unauthorized login attempts for sustained periods of time.

The report underscores that while many organizations are understandably focused on transitioning to cloud infrastructure, they cannot afford to neglect security. In fact, over 80% of the exposures we observed were based in the cloud.

Bottom line – the global attack surface looks extremely porous to a cyber adversary. It is incumbent on all of us in the cybersecurity community to flip that paradigm.

Meeting the Moment – Out-Innovating Attackers With AI and Automation

Despite the evolving ransomware threat landscape, we remain confident that we are well-equipped to combat the cyber incursions of today and tomorrow. Advances in artificial intelligence and automation enable us to ingest and analyze security data in real-time to prevent, detect, and respond rapidly to incidents.

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.

Perhaps 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. In fact, a recent Unit 42 report that analyzed real-world cloud breach incident response cases from 2022 found that, on average, security teams take nearly *six days* to resolve an alert. In contrast, the average amount of time it takes adversaries to move from compromise to data exfiltration is 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, using AI-driven data analysis, 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.

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. To ensure we 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 tools 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 future is simple: enable organizations to have comprehensive, real-time visibility across their digital estate, 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. Simply put, policymakers are telling all of us that it is time to collectively step up.

The Executive Order on Improving the Nation’s Cybersecurity (EO 14028) from May 2021 and the National Cyber Strategy released just a few months ago promote key themes we applaud – more real-time visibility across enterprises, rapid adoption of zero trust network architecture, and secure software development.

The Cybersecurtity 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.

Bipartisan and bicameral efforts to modernize the *Federal Information Security Management Act (FISMA)* represent another important policy initiative in this arena. We support this committee’s efforts to push that legislation across the finish line.

Cybersecurity resilience does, of course, require investment. To that end, we applaud 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. The deadline for states to apply for a grant under the program’s year two funding is October 6, and we encourage widespread participation.

Partnership Remains 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, we have found substantial value in participating in the Ransomware Task Force, 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.

We are also proud to be a founding Alliance member of CISA's Joint Cyber Defense Collaborative (JCDC). On a daily basis, we share technical threat intelligence through partnerships with the Department of Homeland Security, the Intelligence Community, private sector coalitions, and other allied nations to support global prevention and response to significant cyber incidents.

In forums like these, commercial competitors become threat intelligence *partners*. Our collective defense depends upon maintaining that spirit. We continue to see productive collaboration take place across a range of cybersecurity-focused convening bodies, including the National Security Telecommunications Advisory Committee (NSTAC), the Information Technology Sector Coordinating Council (IT-SCC), and the newly created Federal Secure Cloud Advisory Committee (FSCAC).

Preparing the Cyber Workforce of Tomorrow

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 staying ahead of all cyber threats, including ransomware.

To that end, we have been encouraged to see the impact of several initiatives aimed at broadening access to cybersecurity education. Of note, the *Palo Alto Networks Cybersecurity Academy* offers free and accessible curriculum and hands-on labs to academic institutions from middle school through college, and an annual competition for college students to address cyber threats in vulnerable industries has successfully sparked interest in the cybersecurity field from all corners of the country.

Palo Alto Networks also offers several accelerated onboarding programs to help diversify the workforce, including the *Unit 42 Academy*, which welcomes at least 10 new participants each August as full-time members of our incident response and cyber risk management teams. Each cohort represents a highly diverse group of early career professionals with both university and military service backgrounds who spend 15 months growing skills through highly specialized, instructor-led courses, on-the-job training, and mentorship. This early career program affords Unit 42 the opportunity to build world class security consultants. We are proud to report that our 2023 class is 80% female.

Conclusion – 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.
2. Ensure complete visibility of your attack surface: 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 resilience for the entire cybersecurity ecosystem.

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