DARKReading

WEBINAR SUMMARY

September 23, 2021

Detecting and Stopping Online Attacks

Dmitriy Ayrapetov, Vice President of Platform Architecture, SonicWall
John Sawyer, Director of Services, Red Team, IOActive, Inc.

KEY TAKEAWAYS

- Protection and defense begin with understanding the environment and identifying risks.
- Organizations can limit successful attacks by proactively taking defensive measures.
- Ransomware and malware are increasingly evasive as attacks become more targeted.
- SonicWall's solutions offer advanced threat protection.

in partnership with

SONICWALL®

OVERVIEW

Attackers have evolved, making it increasingly difficult for defenders to protect against, detect, and stop attacks from happening on their systems. Not only has the pace of attacks increased, but the methods for how attackers breach and infiltrate systems are also changing, becoming more targeted and increasingly evasive.

In this challenging and rapidly changing environment, security operations teams need to have a thorough understanding of the landscape so they can adapt and shift, just as the attackers have, and can quickly detect and stop online attacks.

CONTEXT

John Sawyer and Dmitriy Ayrapetov discussed how online attacks are changing and steps organizations can take to improve detection and response.

KEY TAKEAWAYS

Protection and defense begin with understanding the environment and identifying risks.

Organizations can take significant steps toward protecting and defending their environment against attacks by understanding their environment and identifying risks. This includes understanding both internal and external risks as well as understanding where data lives and how it moves.

Areas of risk in an organization can be external and systemic, related to the supply chain, or company specific. For example, the pandemic increased risks to organizations as they rapidly shifted business models from in-building to remote work.

Table 1: Areas of risk to an organization are internal and external

Area of risk	Factors to consider
External and systemic risks	– Societal – Global – Economic – Geopolitical
Supply chain risks	– Suppliers to consumers – Upstream/downstream – Hardware/software
Company-specific risks	– Business partners – 3rd and 4th parties

Organizations also need to understand where their data is stored and where and how it is transmitted. This includes understanding which other organizations and vendors may be storing this data, including cloud vendors, and how they approach security.

Understanding the environment and risks is critical for managing prevention and early detection. Faster threat defense across endpoints, networks, systems, and applications bolsters incident response. Businesses need to learn what the incident response plan is when vendors—or vendors' vendors—experience a security incident, including how these businesses will notify the organization.

Organizations can limit successful attacks by proactively taking defensive measures.

Preventing attacks is extremely difficult. Keeping up with threat intelligence around attacker tactics, techniques, and processes can help organizations close gaps and improve security, but it won't stop an attack. Organizations, instead, need to focus on defensive measures to identify and stop attacks before they become successful. These measures include:

- **Threat hunting:** A proactive, human-driven search through the organization's environment to detect threats that evade existing security controls.
- **Endpoint protection:** Automated tools that look for indicators of compromise (IOCs) and can protect the system when potential threats are identified.
- **Blocking intersystem communications:** Using private virtual local area networks (VLANs), Windows Firewall, and other host-based firewalls and network access control (NAC) solutions, limits lateral movement and isolates machines on the network.
- **User awareness:** Developing security policies and educating users about how they can prevent attacks from happening play a key role in limiting successful attacks.

> Don't balk at user awareness training; these people are the first line of defense.
>
> *John Sawyer, Director of Services, Red Team, IOActive, Inc.*

A threat hunting team can identify security gaps before they become a problem and can stop attacks before they occur. This team must have a deep understanding of the organization's environment, strong forensics and incident response skills, significant offensive security experience, and research capabilities.

While such a team can be extremely beneficial to an organization, having a team with the necessary expertise and with a full-time focus on threat hunting is challenging for many organizations.

SANS Institute 2020 Threat Hunting Survey: Top 5 Threat Hunting Hurdles

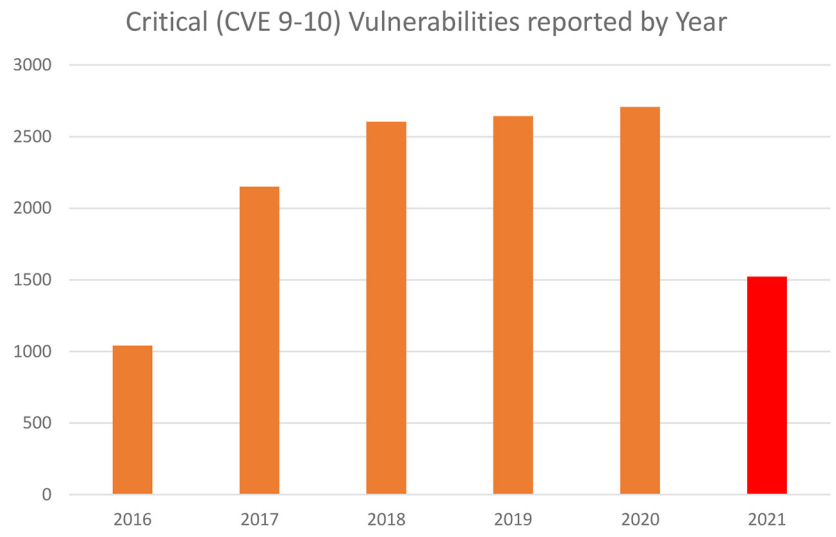
1. **Lack of skilled staff** within the organization; lack of properly trained staff and staff lacking critical skill sets.
2. **Little or no budget** to support threat hunting staff or activities.
3. **No** defined threat hunting **process**.
4. **Limited data** of the quantity and/or quality needed to look for issues.
5. **Lack of management support** for threat hunting tasks and team.

Ransomware and malware are increasingly evasive as attacks become more targeted.

Ransomware groups have shifted their strategies to become more targeted, often focusing on common vulnerabilities and exposures (CVEs) in software. At the same time, ransomware and malware have become more evasive, making it extremely difficult for organizations to detect attacks until it is too late.

While phishing is still used by attackers with the hopes that a user will click on a link or file to launch malicious code, many attackers are focusing on the many CVEs that organizations leave unpatched. Attackers use scanning tools like Shodan.io to find vulnerable hosts and then target their attacks at those unpatched systems.

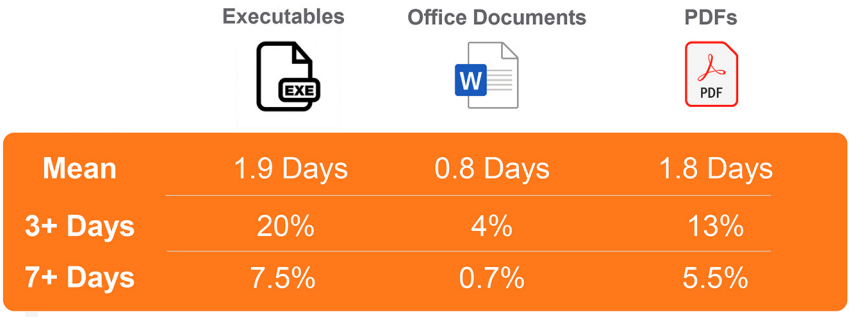
Figure 1: 2021 is on path to exceed previous years in highest-scored (CVE 9-10) vulnerabilities



> All software has vulnerabilities. People who don't patch them become victims.
>
> *Dmitriy Ayrapetov, Vice President Platform Architecture, SonicWall*

The attack surface is also shifting; web browsers are becoming a less popular vector as modern browsers no longer use vulnerability-rich plugins like Flash and Java. Instead, executables, Microsoft Office documents, and Adobe PDFs are being used to deliver malware and ransomware payloads and evade common detection methods.

Figure 2: Malware mean detection times and longevity on systems in 2020

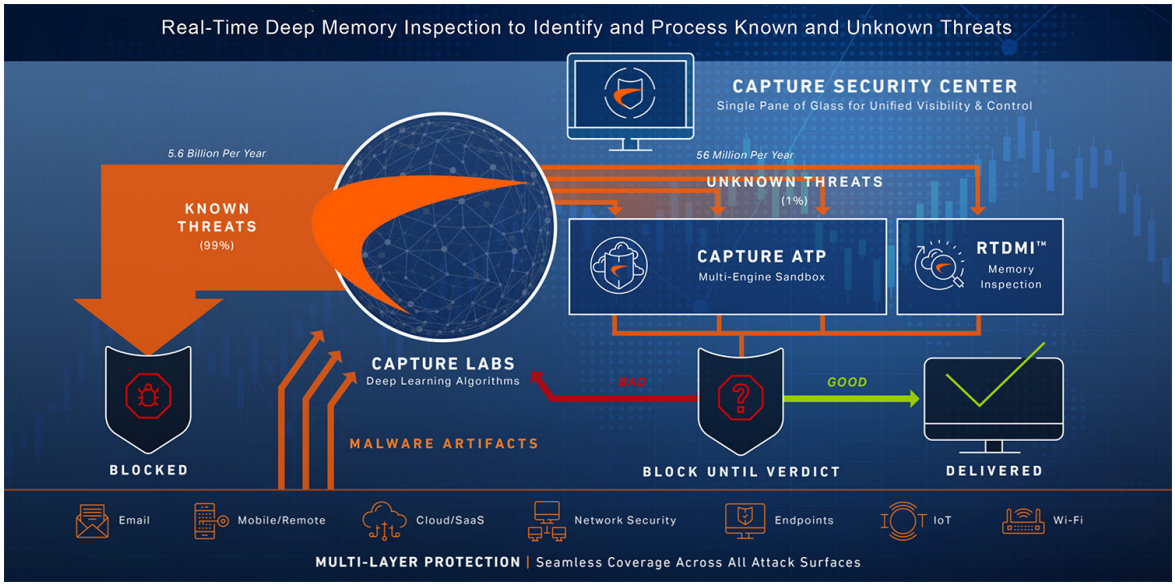


	Executables	Office Documents	PDFs
Mean	1.9 Days	0.8 Days	1.8 Days
3+ Days	20%	4%	13%
7+ Days	7.5%	0.7%	5.5%

SonicWall's solutions offer advanced threat protection.

SonicWall offers security across numerous attack surfaces, including the network, mobile, endpoint, wireless, and email. The SonicWall Capture ATP Protection technology, which is built into all SonicWall products, offers advanced threat protection (ATP) that allows organizations to defend against the complex, changing attack environment.

Figure 3: SonicWall solutions include Capture ATP Protection technology



ADDITIONAL INFORMATION

- **MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) framework.** The free MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations and is a useful tool for organizations looking to develop more effective cybersecurity.

BIOGRAPHIES

Dmitriy Ayrapetov

Vice President Platform Architecture, SonicWall

Dmitriy Ayrapetov is VP of Platform Architecture at SonicWall working to solve cybersecurity issues facing organizations around the world by helping to guide product development at SonicWall. Dmitriy is also working on bringing SonicWall's Real Time Deep Memory Inspection threat detection technology to broader markets. Prior to this position, Dmitriy held engineering roles and product management leadership roles at SonicWall. Before SonicWall, Dmitriy worked as a software engineer at several startups, one of which was acquired by SonicWall in 2005. As a cybersecurity expert, he speaks at industry conferences including RSA and Gartner Security Summit and is a regular voice with analysts, the press, and SonicWall's channel partners. Dmitriy holds an MBA from the Haas School of Business at U.C. Berkeley and a BA in Cognitive Science at U.C. Berkeley.

John Sawyer

Director of Services, Red Team, IOActive, Inc.

John has more than two decades of IT experience including an extensive background in offensive security, intrusion analysis, and forensics. He's earned numerous certifications and two DEF CON Capture the Flag black badges, and co-founded the University of Florida Student Infosec Team. John has a passion for helping others dig deeper into the complex world of security.