WEBINAR SUMMARY

August 19, 2020

DARKReading

Building and Refining Threat Hunting Practices in Your Enterprise

Stacey Halota, Vice President – Information Security and Privacy, Graham Holdings Company
David Wolpoff, Co-Founder, CTO, Randori

KEY TAKEAWAYS

- Threat hunting reduces the risk of cyberattacks and security breaches.
- Companies need to better understand themselves to know potential threats.
- Start with the basics when developing a threat hunting program.
- When threat hunters understand how attackers think, they better predict threats.
- To help businesses defend against attacks, Randori prioritizes the most important, most likely targets.

in partnership with

Randori

OVERVIEW

Data breaches cost companies money, customers, and their reputation. To mitigate the risk of cyber-attacks and breaches, organizations need to become "threat hunters" by proactively searching for threats that lurk on the network.

Building an effective threat hunting program can seem daunting and complex, but organizations can start hunting for threats with many of the basics they already have in place—like logs and automated alerts—and can build up their threat hunting capabilities from there.

Tools like Randori Recon can play a key role in helping businesses detect threats by looking at the likelihood of attack.

CONTEXT

Stacey Halota discussed the importance of threat hunting and how businesses can create a threat hunting program. David Wolpoff described improving an organization's defenses by understanding how attackers think and identifying potential targets.

KEY TAKEAWAYS

Threat hunting reduces the risk of cyberattacks and security breaches.

Threat hunting—the practice of proactively searching for cyber threats lurking undetected on the network—can dramatically reduce the risk of costly cyberattacks and security breaches.

How Threat Hunting Reduces the Risks of an Attack

- Proactively identifies issues
- Improves incident response times
- Enables the security team to understand the company better
- Reveals control gaps that can be used for attacks
- Minimizes the impact of a security breach or attack on the organization

Companies need to better understand themselves to know potential threats.

Random attacks happen, but many attacks are targeted to a specific company or industry. Companies that take the time to understand their profile, potential attacker motivations, and target information and personnel are more likely to identify and thwart attacks.

Industry, location, company size, data processed, mergers and acquisitions activity, and other factors make up a company's profile.

Within a company are its "crown jewels," the information that attackers are after when breaching a system for profit, spying, or hacktivism.

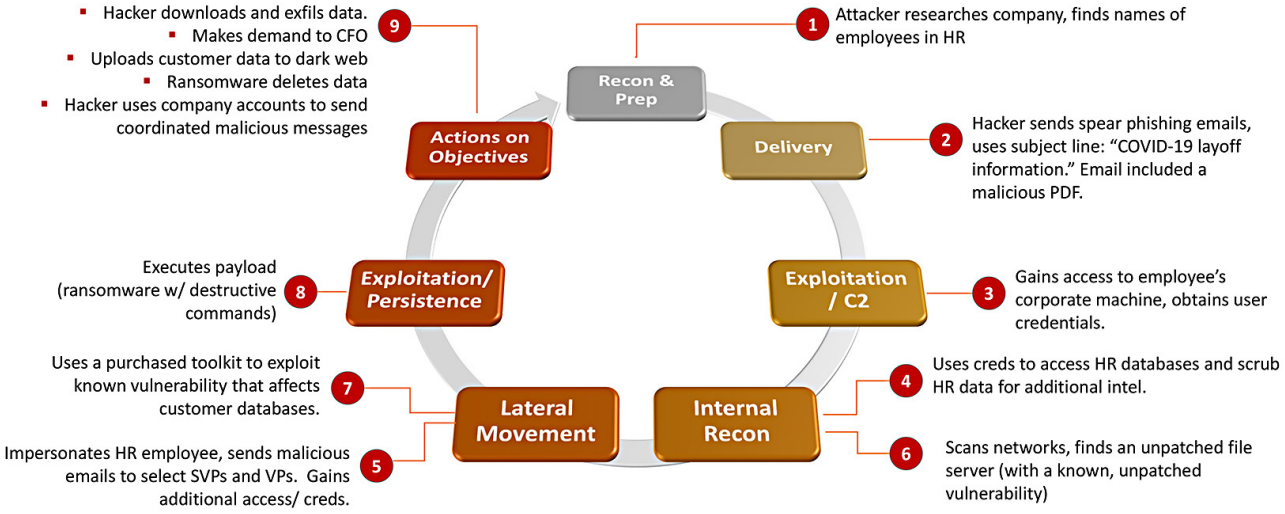
To gain access to the company, its network, and its data, attackers typically target the workforce. This includes the C-suite, as well as employees with access to valuable data, such as the finance or treasury department, human resources, legal, and IT. Remote workers have increasingly become a target, as the pandemic has driven most employees to work from home.

Know the company's "crown jewels" and where they live	
Common data & information	– Personally Identifiable Information (PII), including Social Security numbers, medical information, and passport and driver's license details – Credit card numbers – Intellectual property – User IDs and passwords – Email addresses
Where data and information often reside	– System infrastructures, including cloud, hybrid, on-premise, and legacy systems – Paper records – Applications – Mobile devices

Start with the basics when developing a threat hunting program.

Threat hunting doesn't have to be complex to be effective. Organizations looking to start a threat hunting program can start with the basics, looking at threat trends and areas where detection can be automated. These alerts help identify threat actors early in Lockheed Martin's Cyber Kill Chain.

Figure 1: Identify threat actors early in the Cyber Kill Chain



> Start threat hunting where you are and use the resources that you have.
>
> *Stacey Halota, VP – Information Security and Privacy, Graham Holdings Company*

Next, organizations need to survey and analyze the information they have and apply threat intelligence to better understand the risk.

Next steps in developing a threat hunting program	
Survey what information is available	– Endpoint data – Operating system event logs – Antivirus logs – Database logs – Proxy and firewall log information – Other relevant logs and data
Analyze the data	– Security information and event management (SIEM) solutions – Machine learning – Other analysis tools
Use threat intelligence	– Look at threat research – Use different intelligence sources – Follow security news sources on social media – Review and understand internal and previous incidents – Identify indicators of attack (IOA) and indicators of compromise (IOC)

The Hypothesis is Critical to Threat Hunting

A hypothesis, which looks at possible threats to the business, is the best place to start when threat hunting. From the hypothesis, the threat hunter can step through what has happened and look for indicators that the threat exists. Using this model, the hypothesis can be executed, tested, and fine-tuned as more information is understood.

Example: A healthcare company began with the hypothesis that an adversary emulation plan could threaten its business. Knowing that PowerShell can be a source of these kinds of threats, they began exploring and testing against PowerShell and fine-tuned the hypothesis as they looked for threats.

When threat hunters understand how attackers think, they better predict threats.

When threat hunters can predict threats to their organization, it leads to more effective prioritization of threats, optimization of resources to defend against the threat, and ultimately, reduced risk.

Understanding where an attacker is going to spend their time, money, and resources to attack allows defenders to better spend their own time, money, and resources to disrupt the attacks. Organizations that goes through this process become more difficult and costly to attack, which discourages attackers and causes them to look elsewhere.

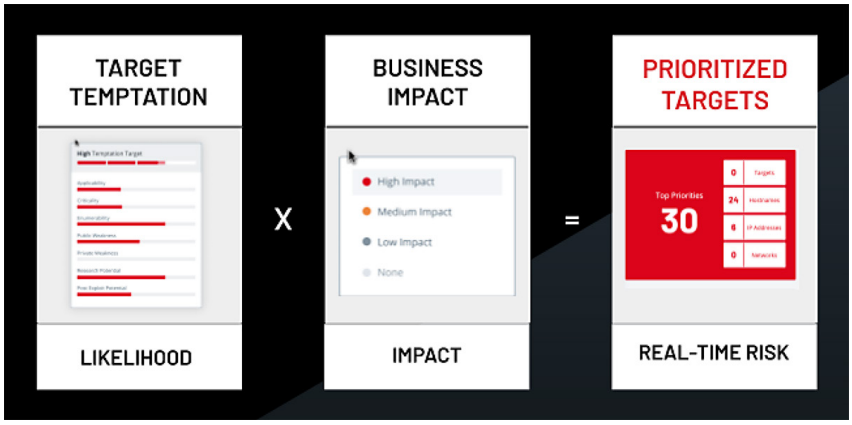
> If you can predict where [an attacker] is going to spend their time and money, you can, as a threat hunter, disrupt the attacker's actions in ways that make the attack more expensive or disruptive to the attacker.
>
> *David Wolpoff, Co-Founder and CTO, Randori*

Threat hunters have the home field advantage; attacks are taking place on their own turf. Threat hunters can identify the things that matter most to the business—the crown jewels—and can assume that these crown jewels are what also matters most to the adversary. With that knowledge, defenders can take extra steps to protect those areas.

To help businesses defend against attacks, Randori prioritizes the most important, most likely targets.

Understanding the attacker's perspective allows threat hunters to rank potential targets and prioritize the likelihood of attack. Randori Recon helps organizations identify and prioritize targets based on the temptation to the attacker and the business impact. The result is that organizations have greater insight into where to focus their defense efforts.

Figure 2: How Randori Recon enables risk-based attack surface management



In providing insights to users and enabling risk-based attack surface management, Randori looks at six factors of temptation. The result is a determination of the likelihood that a target will be attacked.

Six Factors of Temptation

Factor	Ranking examples
1. Enumerability Precision of detection	– High: Detecting an exact version, patch level, and configuration – Medium: Detecting a major and minor version – Low: Detecting only the software name
2. Public/Private Weakness Known disclosures and exploits	– High: Critical, reliable, unauthenticated remote code execution with proof of concept (POC) – Medium: Local privilege escalation, post-authentication – Low: Possible information disclosure vulnerability
3. Criticality Importance of function	– High: Services that inherently define a critical security boundary – Medium: Services infrequently but possibly on a security boundary – Low: Services not commonly on a security boundary
4. Applicability Level of adoption	– High: A ubiquitous service found in most enterprises – Medium: A service found in limited segments – Low: An unusual service with few users
5. Post-Exploitation Potential Usefulness after compromise	– High: Well-known environment where few defenses exist – Medium: Common environment with likely defenses – Low: Esoteric or highly defended environment
6. Research Potential Ease of development	– High: Tooling, research, POCs, and exemplars exist – Medium: Some prior research, but may lack development tools – Low: Difficult to obtain hardware, no tools, no prior research

ADDITIONAL INFORMATION

For a free 14-day trial of Randori Recon, visit Randori.com/DR.

BIOGRAPHIES

Stacey Halota

Vice President – Information Security and Privacy, Graham Holdings Company

Stacey Halota joined Graham Holdings Company (then The Washington Post Company) in 2003. Graham Holdings is a diversified education and media company whose operations include educational services, television broadcasting, online, print and local TV news, home health and hospice care, manufacturing, car dealerships, and restaurants. She leads the development and implementation of information security and privacy programs, including Sarbanes-Oxley, privacy law, Payment Card Industry compliance, and other data protection efforts. Stacey has more than 25 years of experience in the information technology, security, and privacy field. Before joining Graham Holdings, she served as the federal government and southeast region leader of Guardent (now part of Verisign), a security and privacy consulting and managed security services company. Prior to Guardent, she worked at PricewaterhouseCoopers in the Technology Risk Services consulting practice working with federal government and Fortune 500 clients.

Stacey is a past recipient of *Secure Computing Magazine's* Chief Security Officer of the Year award and was also named Mid-Atlantic Information Security Executive of the Year (Commercial Category) by the Executive Alliance. She is a Certified Information Systems Security Professional (CISSP), a Certified Information Privacy Professional (CIPP), and a Certified Information Systems Auditor (CISA). Stacey is a frequent speaker on information security and privacy topics and is on the strategic advisory boards of CyberVista and Y/L Ventures.

David Wolpoff

Co-Founder, CTO, Randori

David Wolpoff (Moose) is co-founder and CTO of Randori. David is a recognized expert in digital forensics, vulnerability research, and embedded electronic design. Prior to founding Randori, David held executive positions at Kyrus Tech, a leading defense contractor, and ManTech where he oversaw teams conducting vulnerability research, forensics, and offensive security efforts on behalf of government and commercial clients. David holds a Bachelor of Science and Master of Science degrees in Electrical Engineering from the University of Colorado.

© 2020 Informa. All rights reserved.