WEBINAR SUMMARY

August 19, 2021

New Trends in Ransomware Response

Sherri Davidoff, CEO, LMG Security
Matt Durrin, Director of Response and Research, LMG Security
Don Shin, Security Marketing Strategist, ExtraHop

KEY TAKEAWAYS

- Ransomware is big business, with an increasing focus on data theft.
- Since attack techniques are scalable, response planning must be scalable as well.
- Threat hunting allows organizations to identify and eradicate persistent threats.
- Threat intelligence monitoring is a critical part of a successful response process.
- Ransomware risk assessments allow organizations to be proactive in their response.
- ExtraHop identifies intruders using network detection and response.

in partnership with

OVERVIEW

Ransomware has evolved into big business, as ransomware practitioners are now offering ransomware-as-a-service (RaaS) platforms to franchise and affiliate organizations, increasing the footprint of ransomware gangs. These criminal organizations are doing more than holding data hostage; they are stealing intellectual property (IP) and sensitive data, which they threaten to release unless the ransom is paid.

Alongside these evolving, more mature ransomware trends are new trends in business responses. Organizations are shifting their approaches to ransomware attacks, ensuring they can identify and eradicate persistent threats quickly and effectively.

CONTEXT

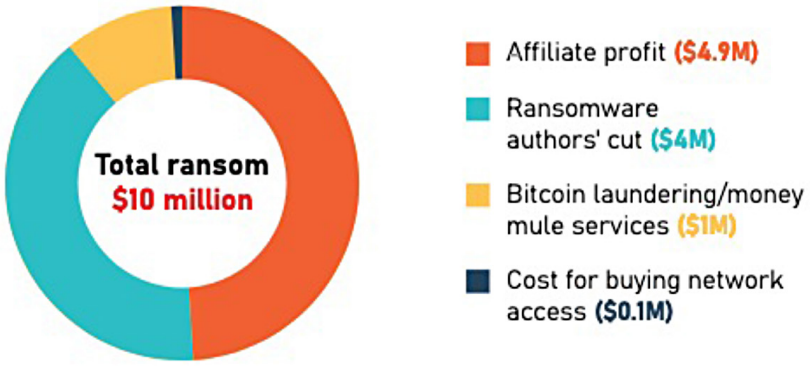
Sherri Davidoff and Matt Durrin shared current trends in both ransomware and ransomware response. Don Shin discussed ExtraHop's network detection and response (NDR) solution.

KEY TAKEAWAYS

Ransomware is big business, with an increasing focus on data theft.

Today's ransomware attacks are not just focused on just holding data hostage; 81% of all ransomware cases now involve data theft. With this double extortion approach and the potential for large pay days, many ransomware gangs are acting like corporations, employing staff for software development, customer service, IT support, and public relations, and even working with other attackers in an affiliate/franchise model, where they offer ransomware-as-a-service platforms (RaaS) for license.

Figure 1: Example: Where the profits go on a $10 million ransom



> Ransomware is big business, and these guys operate just like corporations because they kind of are.
>
> *Sherri Davidoff, CEO, LMG Security*

Since attack techniques are scalable, response planning must be scalable as well.

The most prolific ransomware strains are scalable, allowing these cybercriminals to go after bigger targets and make more money, which they then invest into development and staffing to effectively scale out to attack even bigger, more lucrative targets. To combat this, organizations need to ensure that their response planning is scalable as well.

Increasingly, ransomware gangs like Conti, which is the second most prolific ransomware strain with 14.4% of the market, offer a RaaS platform to franchisees and affiliates, as well as standardized playbooks, shared tools, and community support. This enables more attacks and more revenue earned; between 2019 and 2020, payments tracked across several cryptocurrency platforms rose 344% to more than $416 million.

Ransomware is no longer relegated to isolated incidents on workstations or to locking down data until a ransom is paid. With scalable, business-wide attacks that include data theft that criminals are threatening to share if ransoms are not paid, organizations need scalable response planning.

Scalable response planning is necessary to combat today's scalable ransomware attacks

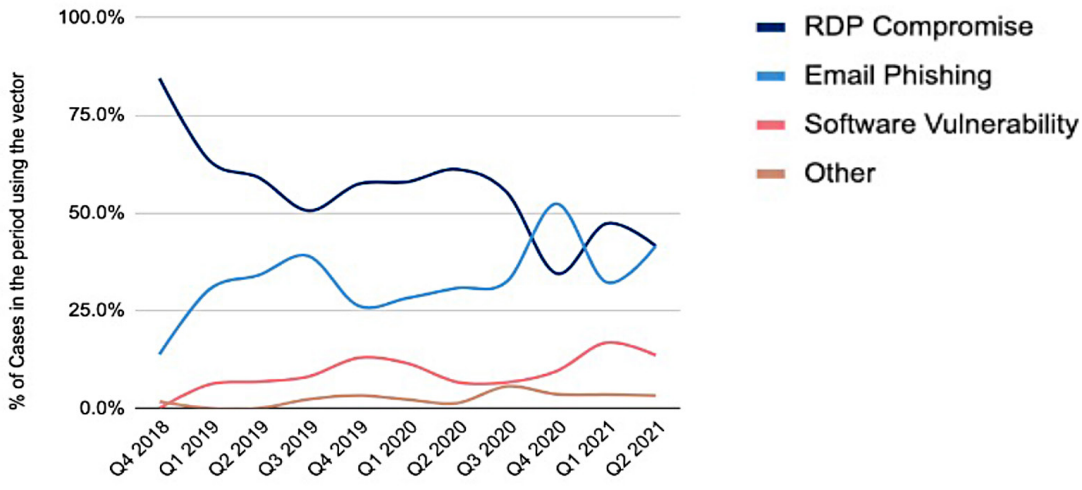
- Tie response planning into business continuity plans and disaster recovery plans.
- Build response playbooks that provide the information necessary to develop a quick and effective response that matches the attack. Playbooks include:
  - Data inventory to identify what data was stolen
  - List of obligations to understand regulatory and other requirement that can impact the response
  - Technical documentation, including dependencies and credentials information
  - Communication plans, including out-of-band, after hours, escalation guidance, and third part contacts
- Train the team to ensure everyone can respond and adapt quickly in a crisis.

Threat hunting allows organizations to identify and eradicate persistent threats.

Organizations can take steps to reduce the risk of unauthorized entry into their network and systems. They also need to conduct threat hunting to catch and stop attacks that managed to get in.

Remote desktop protocol (RDP) compromises, email phishing, and software vulnerabilities are the most common entry paths for attackers. Businesses can take steps to reduce the risk of unauthorized entry by deploying multi-factor authentication, defending against phishing, restricting remote login interfaces, and ensuring systems are patched and up to date.

Figure 2: RDP compromises and email phishing are the top initial entry vectors for ransomware



Even with the best prevention techniques in place, some criminals will find their way in. Most lurk on the network to gain as much information they can on the business, including passwords, intellectual property, client data, financial information, and insurance details. Proactive, human-driven threat hunting enables organizations to find and eradicate persistent threats and prevent repeat ransomware infections.

> [Threat hunting] allows us to save a minor network event from turning into a catastrophic network failure if an adversary is not caught in the correct amount of time.
>
> *Matt Durrin, Director of Response and Research, LMG Security*

Threat intelligence monitoring is a critical part of a successful response process.

Threat intelligence monitoring can help organizations identify and prepare for potential attacks, allowing them to respond to issues efficiently, regardless of when they occur.

Organizations need to identify their key software products and suppliers so they can be sure to keep an eye on areas of concerns, like zero-day exploits, with those products. They should also be working with suppliers to ensure they are also monitoring threat intelligence and preparing for attacks.

Businesses also need to identify and follow threat intelligence sources, assign responsibility for responding to alerts, review and triage alerts, and feed them into response processes. They also need to practice responses, such as running through tabletop exercises.

Threat intelligence sources to follow

- Vendor alerts
- Social media
- Threat intelligence sources like the SANS Institute, Critical Stack, CrowdStrike, and others
- Cybersecurity news, including Bleeping Computer, ZDNet, Wall Street Journal, and others

As part of threat intelligence, organizations need to be acutely aware of known vulnerabilities in their systems, as cyber attackers can take advantage of these at any time.

Ransomware risk assessments allow organizations to be proactive in their response.

Organizations can reduce their risk and limit business impact of an attack by working with experts to conduct ransomware risk assessments. A ransomware risk assessment conducted by experts includes:

- Review security controls related to ransomware.
- Determine incident response preparedness, including the backup strategy and the offline storage, testing, and recovery process.
- Actional recommendations to reduce risk.
- Policy and strategy recommendations to limit the business impact.

Businesses also need to work with their suppliers to proactively manage supplier risks, including involving key suppliers in the organization's response planning.

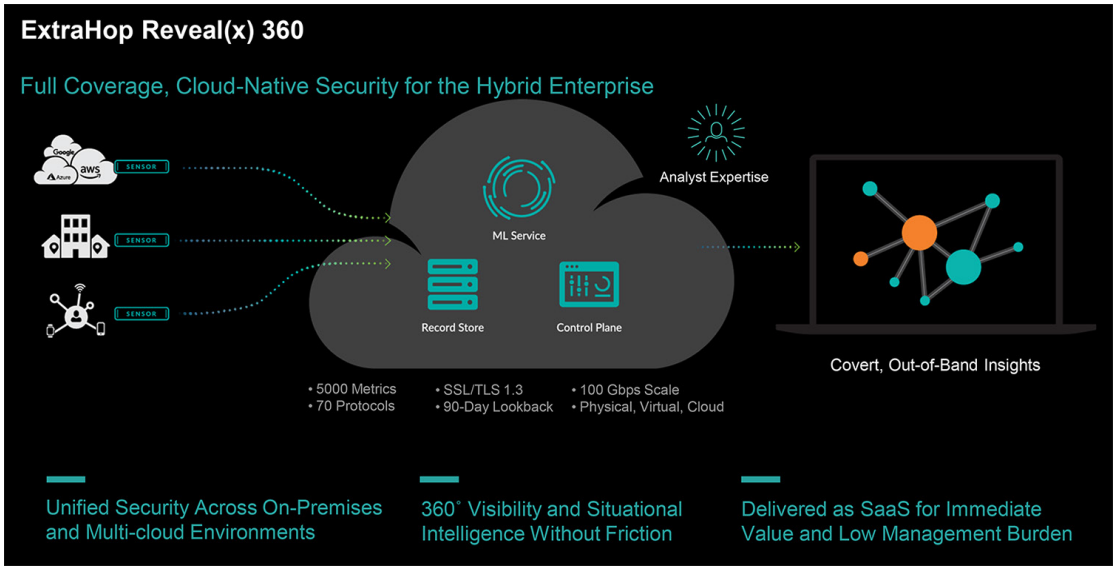
Proactively manage supplier risks

- Inventory all systems, including software and cloud apps.
- Vet suppliers. With multiple suppliers, prioritize which need to be reviewed first, assign responsibility, establish a standard questionnaire, track and follow up on responses, and include an annual assessment in contracts.
- Limit supplier access to systems.
- Ensure logging and monitoring is being done on all systems.
- Collaborate on supply chain security.
- Involve key suppliers in response planning.

ExtraHop identifies intruders using network detection and response.

When an attack occurs, organizations need to identify and respond to intruders as quickly as possible to reduce dwell time and limit damage. ExtraHop Reveal(x) 360 is a software-as-a-service (SaaS)-based NDR solution that allows incident responses to quickly identify intruders at the network level where it is difficult for attackers to hide.

Figure 3: ExtraHop Reveal(x) 360 provides full coverage, cloud-native security for the hybrid enterprise



> Network detection and response offers that high granularity that's difficult if not impossible to evade. There's no way to hide from a network; it monitors from a passive perspective.
>
> *Don Shin, Security Marketing Strategist, ExtraHop*

BIOGRAPHIES

Sherri Davidoff

CEO, LMG Security

Sherri Davidoff is the CEO of LMG Security and the author of the recently released book *Data Breaches*. As a recognized expert in cybersecurity and data breach response, Sherri has been called a "security badass" by *The New York Times*. She has conducted cybersecurity training for many distinguished organizations, including the Department of Defense, the American Bar Association, FFIEC/FDIC, and many more.

She is a faculty member at the Pacific Coast Banking School, and an instructor for Black Hat, where she teaches her "Data Breaches" course. She is also the co-author of *Network Forensics: Tracking Hackers Through Cyberspace* (Prentice Hall, 2012), a noted security text in the private sector and a college textbook for many cybersecurity courses. Sherri is a GIAC-certified forensic examiner (GCFA) and penetration tester (GPEN) and holds her degree in Computer Science and Electrical Engineering from MIT. She has also been featured as the protagonist in the book, *Breaking and Entering: The Extraordinary Story of a Hacker Called "Alien."*

Matt Durrin

Director of Response and Research, LMG Security

Matt Durrin is the Incident Response team lead at LMG Security. He is an instructor at the international Black Hat USA conference, where he teaches "Data Breaches." He regularly conducts cybersecurity webinars and seminars for hundreds of attendees in all sectors, including banking, retail, health care, government and more. A seasoned forensics professional, Matt specializes in incident response, ransomware cases, cryptojacking, and banking trojans. Matt holds a bachelor's degree in Computer Science from the University of Montana and previously worked as a "blue team" field technician/system administrator for over 10 years. His malware research was recently featured on NBC Nightly News.

Don Shin

Security Marketing Strategist, ExtraHop

Don Shin is a security marketing strategist who is passionate about simplifying the complex to solve real problems. He has extensive experience with application, database, and network security technologies, having served in various roles at Imperva, A10 Networks, AlienVault, Ixia, BreakingPoint, and others.