DARKReading

Detecting, Analyzing, and Mitigating Targeted Attacks

Executive Summary presented by **Jason Clark**, Independent Security Researcher, and **Guy Raz**, Principal Sales Engineer, ExtraHop.

KEY TAKEAWAYS

- Protecting against targeted attacks is critical.
- Preventing targeted attacks starts with understanding how and why they occur.
- Multi-level tools provide optimal defense against targeted attacks.
- Cybersecurity in a “post-compromise” world requires focusing on the Midgame.
- Rethinking evidence collection can help support recovery efforts.

SPONSORED BY:

OVERVIEW

In today's cybersecurity landscape, targeted attacks are on the rise. Targeted attacks exploit the well-researched vulnerabilities of a specific organization and are carried out in a well-obfuscated and stealthy manner. Fortunately, there are tools and processes that organizations can put to use to recognize and mitigate targeted attacks before they do real damage to enterprise data.

In this post-compromise world, attackers gaining entrance is not a matter of "if," but "when."

CONTEXT

The presenters explained cybersecurity challenges associated with targeted threats and how to mitigate these threats.

DARKReading

KEY TAKEAWAY #1

Protecting against targeted attacks is critical.

Threat actors, including hackers, organized crime, "hacktivists," nation states, and even domestic intelligence services all have different means, opportunities, and motivations to launch cyberattacks. Threat actors often focus on compromising public-facing applications and carrying out phishing (including spear phishing) attacks. In addition, the proliferation of devices and IoT increases the attack surface available to threat actors.

Whether an attack is targeted or untargeted depends on an attacker's goals and objectives. An **untargeted (or general) attack** is conducted without a specific target. The attacker's goal is to cast a wide net that will catch as many victims as possible.

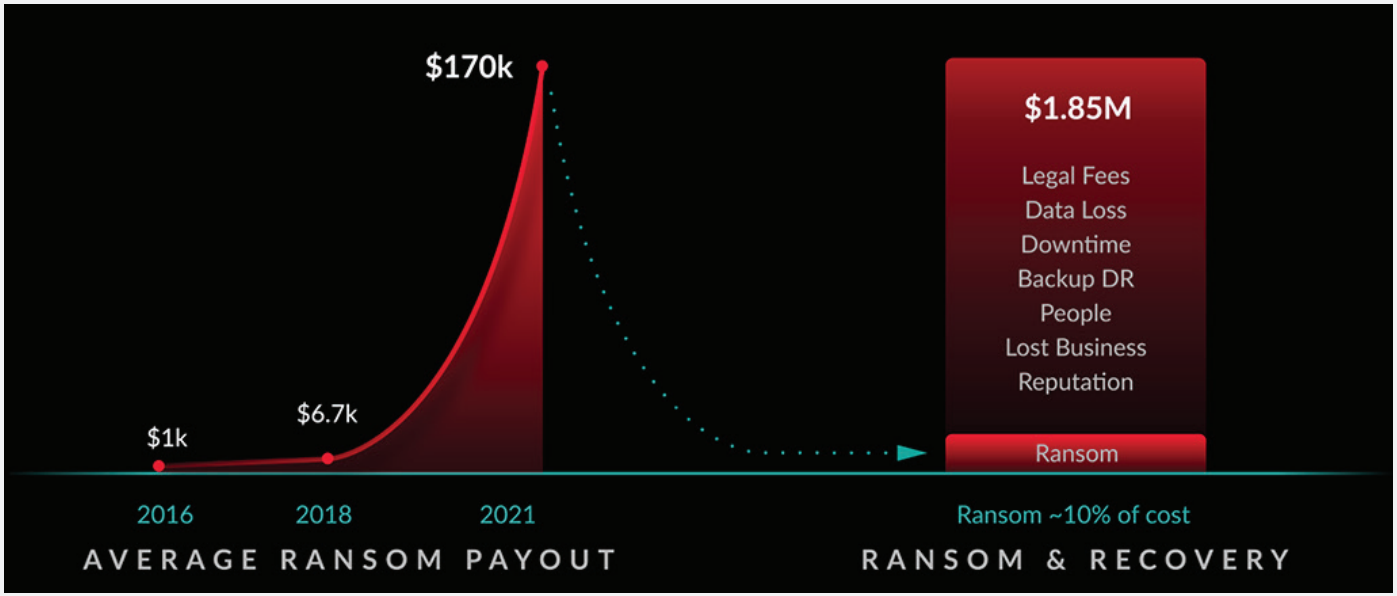
In contrast, a **targeted attack** refers to a threat where adversaries actively pursue and compromise a **specific predetermined target infrastructure**. Because targeted attacks are typically aimed at an enterprise, with a focus on a particular system or application, it is likely that attackers have performed reconnaissance and research before launching their attack; adversaries often rely on automation tools to find and exploit vulnerabilities in a target.

While untargeted attacks are far more common, as they are easier to execute, **targeted attacks are typically more destructive**, as attackers have the lethal combination of a desire to cause damage, and the knowledge to do so. Attackers have the ability to lay low and take their time to infect backups and exfiltrate legal documents, driving recovery costs magnitudes higher than ransom payouts.

Targeted attacks are not limited to a single industry or size company. Every enterprise is at risk and must understand how to detect targeted attacks.

> Determined and undetected attackers are going to continue until they have achieved their goals. With targeted attacks, they usually have a set of goals in mind. That's why they decided to target that particular organization in the first place.
>
> Jason Clark, Independent Security Researcher

Figure 1: Targeted attacks can have an exponential impact on recovery costs



KEY TAKEAWAY #2

Preventing targeted attacks starts with understanding how and why they occur.

Targeted attacks are often associated with ransomware. In general, malware is intrusive software designed to damage and destroy computers and associated systems. Forty-six percent of malware attacks use some form of SSL/TLS encryption, meaning that looking at encrypted envelopes is almost always not enough to detect advanced attacks.

Ransomware is a type of malware that prevents or limits users from accessing systems until a ransom is paid—usually via cryptocurrency. Targeted attacks are carried out through multiple methods. Common examples include:

- *Spear phishing*, a phishing campaign that targets a specific person or group. Higher-ranking leaders are often targeted because they possess valuable information about the business.
- *Living off the land (LOTL)*, a type of attack where threat actors use legitimate software and functions in a system to perform malicious acts on it. LOTL attacks leverage what is already available in the environment, rather than bringing along custom software and malware. As a result, these attacks are less likely to flag security controls.
- *Supply chain attacks*, which have increased in recent years. In these attacks, adversaries target equipment and software being delivered to an organization, exploiting vulnerabilities before the products reach the target victim's production environment.
- *Distributed Denial of Service (DDoS) attacks*, which focus on disrupting normal traffic within a target network, with the goal of overwhelming the victim by inundating the network. DDoS attacks are usually associated with a ransom.
- *Advanced persistent threat (APT)*, an attack campaign where an attacker establishes an illicit, long-term presence on a network to mine sensitive data. APTs are prolonged and targeted attacks with a goal of stealing data and causing damage.
- *Zero-day attacks*, which use security vulnerabilities to attack systems. In these cases, the vendor or developer only learns of a vulnerability upon attack, meaning there are zero days to fix it.

Much like in the chess game, targeted attacks have three primary stages:

Stage	Description
Opening	Attackers gain a foothold through a wide range of targeted attacks and techniques.
Midgame	The attacker begins conducting activities to harm the system, moving laterally through the network. Attackers will collect, hide, and protect valuable data within the environment, staging it in such a way to avoid detection before mass-exfiltration.
Endgame	The attacker launches their final assault, including expanding access and potentially establishing a persistent presence. Programs, folders, and other instruments used for data staging are deleted.

In the event of a targeted attack, it is important to understand **why the enterprise was targeted and what can be done to prevent future targeted attacks**. Most attacks are carried out for financial reasons, whether stealing money directly or through ransomware, or by stealing data and intellectual property and selling that information. Targeted attacks can also result in loss of reputation or public embarrassment, leading to loss of customers.

Figure 2: Concerns to consider when dealing with targeted attacks

A skilled adversary will try to cover their tracks once they've achieved their main objective. Typically, an attacker will do things like uninstall the programs used during the attack, delete any folders, try to get rid of any evidence . . . that was used during the data-staging aspect . . . and may delete audit logs that captured any of their nefarious activities.

Jason Clark, Independent Security Researcher

KEY TAKEAWAY #3

Multi-level tools provide optimal defense against targeted attacks.

Given the depth and breadth of possibilities about how and where targeted attacks can occur, preventing breaches requires **addressing security at multiple levels**, using a variety of methods.

Implementing a security approach to counter targeted attacks requires evaluating and addressing vulnerabilities in terms of themes, tools, and strategies.

When considering general protection themes, there are four key areas in which organizations can focus on putting mitigation controls. These are:

Areas for mitigation controls	Description
Timely detection and response	Once security issues are identified, it is imperative to respond swiftly and appropriately.
Security awareness training	Providing the enterprise workforce with good security training to improve security hygiene is important, but it is critical that training is updated, interesting, and relevant.
Improved visibility	Without a good handle on visibility, enterprises leave holes in their security posture, which leaves them vulnerable to targeted attacks. Real-time visibility of all critical assets, services, and configurations is crucial.
Cybersecurity incident response	In event of an attack, it is important that enterprises can quickly respond, mobilize, and execute an appropriate level of response to limit the impact and reach of the attack.

Within those themes, there are **tools that address specific functionality**. This includes log-based, agent-based, network-based, and evidence-based solutions. When **used together**, these tools create a strong defense against cyberattacks. Tools must have the ability to scale their detection capabilities without requiring customers to redeploy, upgrade, or modify their tools. This means cloud scale computing backends for ML/AI threat detection.

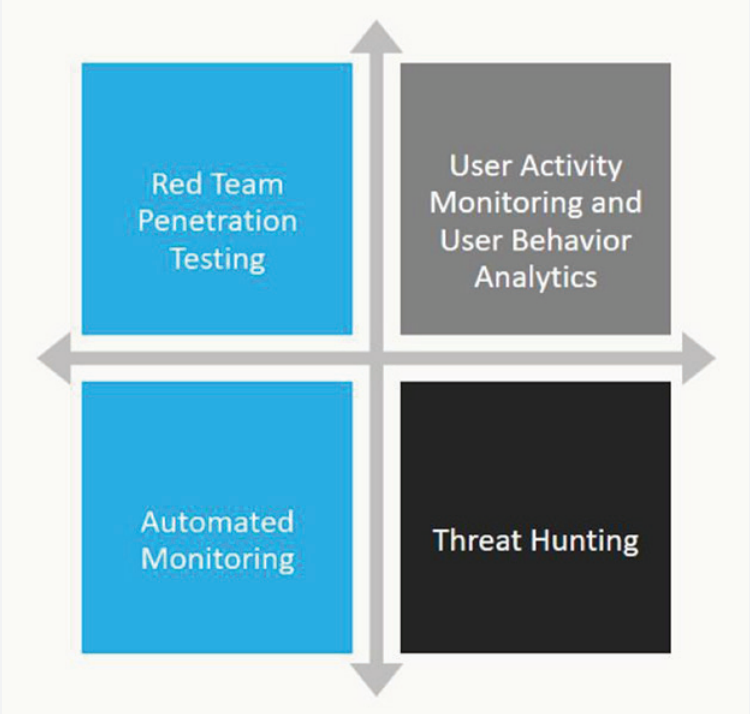
The **Defender's Dilemma** is based on understanding that ***defenders need to successfully defend 100% of the time*** to prevent a breach, while ***attackers only need one entry point*** to be successful. Therefore, breaches are inevitable.

Organizations will benefit from implementing **proactive security strategies**, such as threat hunting, red team penetration testing, user activity monitoring and user behavioral analytics, and more intelligent automated endpoint monitoring, for early detection and mitigation.

Leveraging multiple data and orchestration tool types (e.g. EDR, SIEM, NGFW, IDS, SOAR, and NDR) is the most efficient way to mature as a secure organization. But just as important for comprehensive and quick-to-consume information for security teams is that these tools communicate and enrich each other.

> Different phases of attack have different risks and different rewards for these attackers, so something like a multi-tiered defense strategy is really the way to go.
>
> Guy Raz, Principal Sales Engineer, ExtraHop

Figure 3: Strategies for detecting targeted attacks



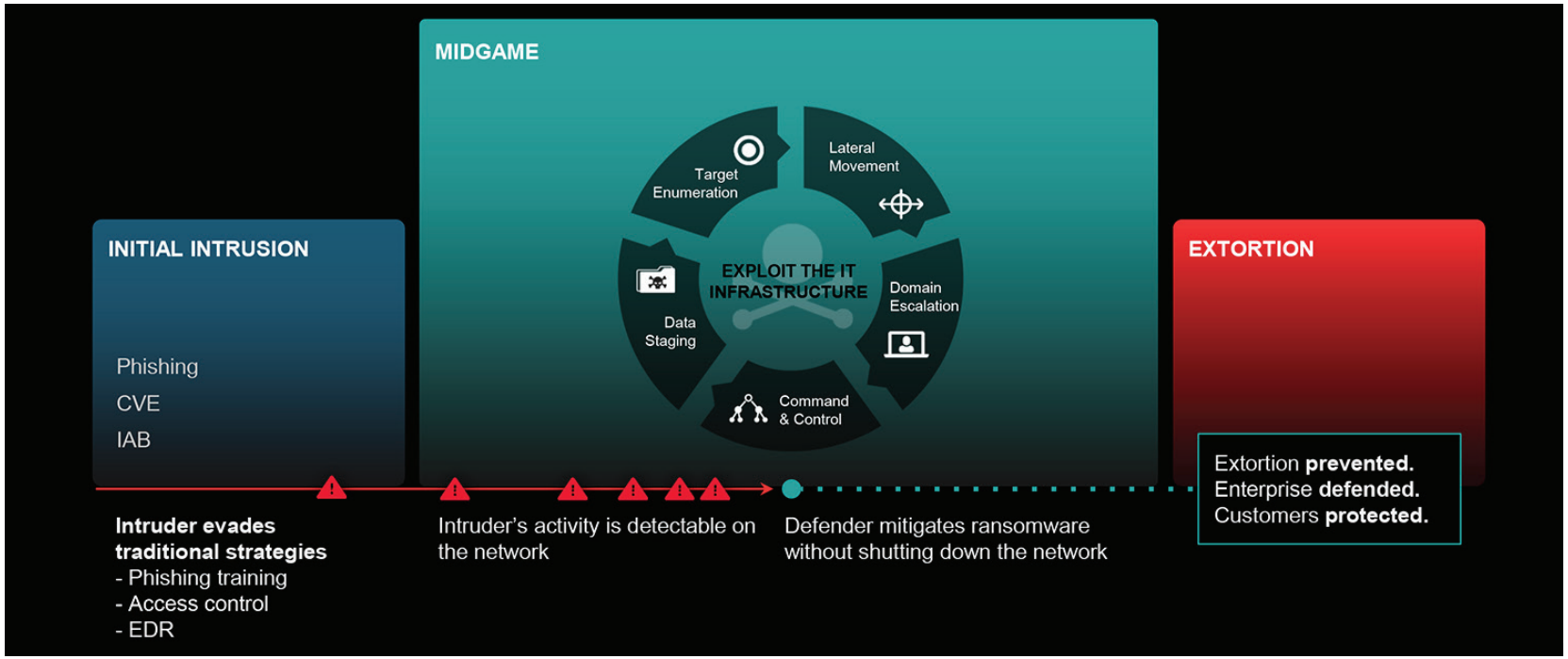
KEY TAKEAWAY #4

Cybersecurity in a "post-compromise" world requires focusing on the Midgame.

ExtraHop is helping enterprises flip the script, by turning the Defender's Dilemma into the **Attacker's Dilemma**. Implementing security controls with the right data collection tools empowers the defenders, forcing attackers to have to avoid detection in an environment they no longer control.

- On average, enterprises spend ***75% of cybersecurity budgets on the Opening*** to prevent intrusion.
- This results in a ***scarcity of tools and technologies to respond to an attack*** when it happens, which prevents the attacker from getting to the Endgame stage.

Figure 4: Deploying security around and within networks addresses post-compromise challenges



> Perimeter and education defense are crucial strategies. So are cybersecurity, insurance, and backups. But those can't be the end-all-be-all of a modern defensive strategy, especially when we start seeing more targeted attacks hitting our organizations.
>
> Guy Raz, Principal Sales Engineer, ExtraHop

However, the likelihood of a breach in the modern cybersecurity landscape is almost guaranteed, driving the need for a **new approach to cybersecurity** that focuses investment and security on the **"post-compromise" stage**. To address the new challenges of the post-compromise world, security teams must both build a perimeter around networks *and* deploy security measures within them.

When an attacker is working to gain entry, they have the advantage. They can choose when, how, and where they attack, essentially ensuring some success in the Opening stage.

However, once inside the target's network, the Midgame stage begins. Attackers no longer control the environment, and targets can begin to **gain back the advantage**. This is because attackers are noisy—scanning, moving laterally through the environment, looking for domain credentials. For example, the ExtraHop NDR solution detected lateral movement events occurring in a client's network, alerting the security team and destroying the VDI profile that the attacker had created. This occurred before any data was encrypted or any execution of data left the environment.

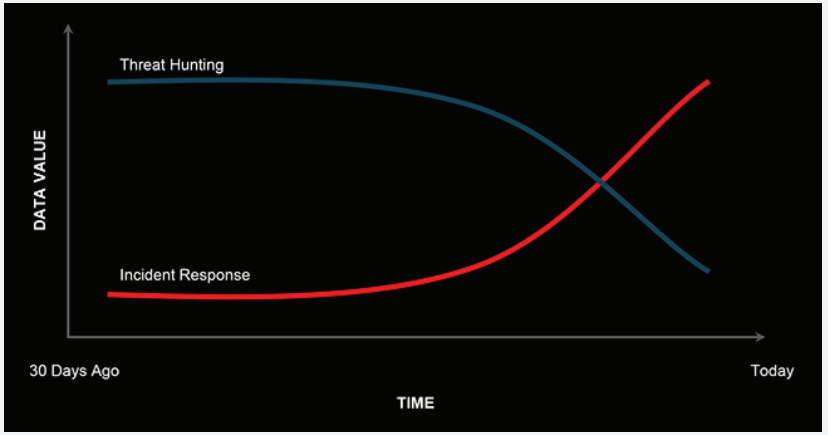
KEY TAKEAWAY #5

Rethinking evidence collection can help support recovery efforts.

Before recovery can begin, organizations must completely contain a malicious actor and prevent any further damage from occurring. Determining that the threat is no longer in the system requires the right data.

The value of operational data depends on specific use cases. For example, threat hunters value historical data over real-time data, while IR teams are heavily dependent on real-time data. The time value of data will drive operational strategy around tool efficiencies, tool consolidations, and data collection. **ExtraHop rethinks evidence collection** based on the optimal intersection of real-time needs versus historical data storage to solve as many use cases as possible, including supporting recovery efforts.

Figure 5: Data value changes over time for different use cases



BIOGRAPHIES

Jason Clark
Independent Security Researcher

Dr. Jason Clark is a subject matter expert in cybersecurity with nearly 20 years of real-world experience within the intelligence community, academia, and industry. He has served in important leadership, development, analyst, and research roles in fields such as network security, cloud computing, and insider threat.

Currently, Dr. Clark is researching ways to mitigate various cloud computing security challenges in the modern (multi-cloud and hybrid IT) world. He has recently performed assessments and evaluations for Fortune 500 companies that are interested in modernizing and moving their applications to the cloud in the most secure manner possible.

In addition to his academic achievements, Dr. Clark also holds a CISSP and is a member of both IEEE and ACM. He has served on a number of program committees, delivered numerous virtual webinars, and has presented his published work at a variety of conferences around the world.

Guy Raz
Principal Systems Engineer
ExtraHop

Guy Raz is a principal systems engineer at ExtraHop with previous experience as a network engineer and solution architect. As a systems engineer, Guy is one of the SMEs leading the unique ExtraHop approach to cloud-native NDR for the hybrid multi-cloud enterprise. Before joining the Systems Engineer team, Guy was one of the ExtraHop solution architects, responsible for conducting deep technical and business discovery sessions, assisting in troubleshooting and problem resolution during war-room and security/network investigations, and developing strategies for acquiring high-value data from the wire; requiring in-depth technical understanding of L2-L7 networking principles. Before ExtraHop, Guy was a network engineer at Cox Communications, where he helped architect the next generation DOCSIS infrastructure to provide gig-speed internet to customers through automation in provisioning and quality assurance of end user experience.

Additional Information

To learn more about ExtraHop, visit www.extrahop.com.