WHITE PAPER

Raytheon | websense

Cyber Dwell Time and Lateral Movement

The New Cybersecurity Blueprint

By Joshua C. Douglas, CTO, Raytheon|Websense

Contents

1. Introduction 4

2. Shifting the Burden to the Attacker 4

3. A Trail in the Woods: Understanding Lateral Movement 5

4. Lifespan of an Attack: Containing Cyber Dwell Time 5

5. Five Practices to Shift the Burden 6

6. Conclusion 8

Introduction

In 1971, Ray Tomlinson, a young engineer at what is now Raytheon BBN Technologies, introduced the ubiquitous "@" symbol and changed communication, as we know it. The launch of email, the expansion of networking and data sharing, along with the introduction of the domain name system has created technological, innovative opportunities for individuals, businesses, and governments worldwide. However, these opportunities also presented themselves to threat actors – criminals hoping to take advantage of this newfound openness by exploiting protocols, applications, and operating systems.

In response, cyber defenders have found themselves in a never-ending cycle of attempting to fill security gaps with patches, overlays, and new technology. While admirable, these efforts fall short because, often, they are applied to what is fundamentally insecure technology infrastructure.

IT security professionals, and the executives at the helm of business, want nothing more than to keep attackers out of networks and systems, but this game plan has proven impossible. The headline stories are well known and the data is alarming: According to the 2015 Verizon Data Breach Investigations report, there were more than 79,790 security incidents in 2014[1].

In this context, the question remains: if preventing breaches is an impossibility, how should cybersecurity professionals focus their efforts in order to minimize the impact of an attack?

1 Source: http://www.verizonenterprise.com/DBIR/2015/

Shifting the Burden to the Attacker

The "moat and castle walls" approach to cybersecurity is clearly not enough; that point is abundantly clear. While organizations must work to fortify defenses, a pragmatic approach includes:

1. *Acknowledge today's reality* – cyber breaches will occur; do not deny the inevitable.

2. *Recognize the threat landscape* – attacks come from both the outside and the inside of an organization. When they originate from the outside, attackers will mimic your internal employees.

3. *Identify the attack paths* – the route attackers follow within a network – known as lateral movement – provides key insight into the intent and potential impact of a breach.

4. *Limit breach longevity* – take actions necessary to minimize the time an attacker is within your network – the cyber dwell time – limiting the potential impact by reducing exposure.

Points three and four will be the focus of this paper and introduce the concepts of **lateral movement** and **cyber dwell time.** Understanding these concepts, enable organizations to shift the threat burden to the attacker, making their assets and infrastructure a less desirable target.

According to the 2015 Verizon Data Breach Investigations Report, there were more than

79,790 security incidents in 2014[1].

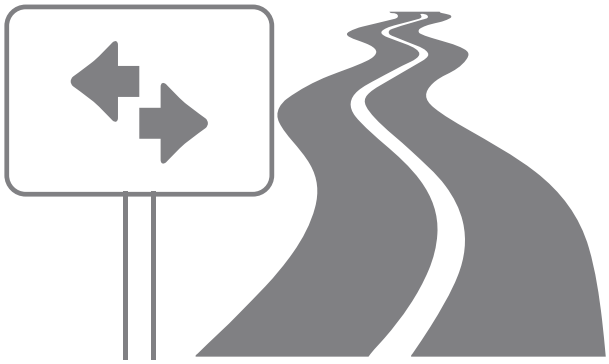
A Trail in the Woods: Understanding Lateral Movement

Advanced attacks occur with purpose; they are launched with clear intent. With that in mind, it is important that organizations not take a short-term view of attack analysis.

For example, when a machine is discovered to be compromised, there are a couple of fundamental questions that should always be asked: Where did the attacker traverse? How was the movement possible? What was the end target? What controls were executed to make the threat persistent?

When answering the questions posed, security defenders must understand that spear phishing, waterhole attacks, or any other malware delivery methodology are all means to an end. The infected systems, while important in their own right, are superfluous to advanced attackers. What they really care about is their ability to remain undetected while traversing the enterprise networks.

The initial onset of malware delivery typically is not to extract as much intellectual property as possible, but to establish a gateway into environments that the attackers do not control. That infiltrated system becomes a proxy to begin the process of lateral movement. There may be one lateral step or 100 steps to gain the targeted intellectual property or control of a system. In many cases, threat actors target an individual's credentials allowing them to move throughout the network under the guise of a legitimate user. Understanding where and how this occurs is critical, as it provides insight into both the intent and potential impact of an attack.



Lifespan of an Attack: Containing Cyber Dwell Time

As discussed, pragmatic organizations understand that breaches will occur and that prevention, although very necessary, cannot be their only security tactic. They must also focus on containment. Identifying and containing an attacker as quickly as possible is paramount.

Similar to vandals who have broken into a school during off hours, the goal of containing cyber dwell time is to ensure the vandals have as little time as possible to wreak havoc – and extricate important assets from the organization. Research shows that attackers spend an average of 200 days inside a network before being eradicated[2]. Imagine the damage an attacker could inflict over that period of time. If attackers can be contained in less time and subsequently have access to less enterprise surface area, they will burn through more resources to get what they want.

To reduce cyber dwell time, it is necessary to fully understand the concept. Cyber dwell time begins when an attacker enters your network and continues until you eject them or they leave (presumably after having completed the intended actions). The goal should be to reduce dwell time as much as possible, providing the attacker the least amount of opportunity to achieve lateral movement and remove critical data from your organization.

The next likely question is "how is cyber dwell time measured?" This can only be assessed by tracing the threat back to its origin. Determine when and where the compromise came from, in addition to tracing those lateral movements.

2 Source: INFOSEC Institute – The Seven Steps of a Successful Cyber Attack—July 11, 2015

Focus Areas To Reduce Dwell Time

- Fundamental security controls
- Granular visibility and correlated intelligence
- Continuous endpoint monitoring
- Actionable prediction of human behavior
- User awareness

Five Practices to Shift the Burden

As organizations move to reduce cyber dwell time, there are several fundamental concepts that should be considered. Listed below are five practices that serve to help organizations decrease dwell time by detecting, containing and controlling cyber threats.

1. **Fundamental Security Controls.** The first step, which is particularly relevant in the context of containing lateral movement, is ensuring your basic security controls are in place. By enacting fundamental security controls – such as regular patching, restrictive administrative access, two-factor authentication, and network segmentation where appropriate – the attacker is forced to invest greater resources in finding a way in. By forcing an attacker to increase their investment, they may elect to search for a more attractive target.

   In the process of implementing best practice security controls, a core step should be to identify high value targets – the systems and people vital to the success of your organization. These are the targets that adversaries most frequently want to exploit for financial or intellectual gain. Security monitoring should be elevated on these assets. Such an approach enables your cybersecurity teams to dedicate operational time to prioritize alerts while easing the process to apply focused controls on endpoints, network devices, or the high value targets themselves.

2. **Granular Visibility and Correlated Intelligence.** As previously stated, a breach will occur regardless of the fundamental security measures in place. However, enterprises can withstand breaches by ensuring both have granular visibility of their network and enterprise communications.

   Therefore, enterprises should implement network monitoring functionality such as Netflow and collect logs from any device that records indemnity usage. This enables organizations to create red flags related to identity theft, data loss, and abnormal activity on a day-to-day basis. While these alerts are important, a critical capability lies in correlating actions to every machine or user, whether on or off the network. Detailed information relating to all incoming emails, such as full headers and even content, will allow cybersecurity teams to cycle back to the origin of the incident.

   Forensic visibility is imperative when attackers breach the perimeter and internal security controls. With forensic data organizations have an increased ability to trace threats back to their origin and to calculate dwell time. Dwell time is a new metric for incident responders and incidentally is the only one Raytheon uses to measure its security posture. How effective is your response team in detecting, containing, and controlling advanced threats?

3. **Continuous Endpoint Monitoring.** With continuous endpoint monitoring, organizations are able to cultivate a keen perception of people, processes, and machines – translating user activity on the endpoint to policies and vice versa in near real-time. Why does this matter? When done right, the resulting contextual awareness allows security teams to stitch together the framework of an incident, and correlate seemingly unrelated events. This means faster response times and less time spent doing traditional forensic work trying to understand attacker movements and intentions.

"...Contextual awareness allows security teams to stitch together the framework of an incident, and correlate seemingly unrelated events."

As previously mentioned, the majority of attacks start with the host or employee, so continuous endpoint monitoring is a major evolution in security posture, and critical for expedited incident response. This heightened insight into the endpoint allows for quicker detection of malware and abnormal behaviors of users. By not only looking for malware and paying attention to odd user activity, organizations will be able to reduce dwell time. This reduction in dwell time and forensics evidence will provide the ability to apply context and protect more than single systems.

4. **Actionable Prediction of Human Behavior.** Predicting attack profiles based upon an adversary's likely plan, a science within the broader topic of incident response, allows organizations to anticipate movements an attacker might take to access high value targets. More specifically, by understanding the previous path of an attacker – where he/she previously traveled – security professionals can start to predict his/her future path.

   Why does this matter? The ability to predict future movement is critical to containing lateral movement and reducing dwell time. The cybersecurity team is better able to anticipate the next steps of an attack and isolate it. This is much like the game of chess, in that the adversary has multiple pieces on the board and has taken multiple moves. The attacker also has many more planned moves to create a checkmate scenario. Security professionals can determine steps they should take, such as taking certain resources off-line or notifying users to be on the lookout for odd behavior, to ensure that checkmate does not happen.

   For this effort to be effective, cybersecurity teams must accept that external attackers are no different from an insider. They know as much about internal systems as IT administrators do. Their activities blend in as normal behaviors on the network, and thanks to custom malware, exploited users provide an overall ability to behave as an insider. Organizations should assume that all high profile employees (people known outside of the company due to external media exposure or executive level visibility) are entry points into the enterprise and a path to a final destination. As an attacker, they have access to certain resources and those resources have access to other resources. This can yield actionable predictions of both normal and abnormal human behavior to create a framework for creating zones, reducing privileges, and enabling the security team the ability to combat attackers once inside the enterprise.

5. **User Awareness.** It is imperative that organizations educate employees not only on corporate policies and government mandates, but also on the growing risk that advanced threats pose to the organization. By launching formal educational programs, security professionals gain greater buy-in from end users, increasing the likelihood of changing risky behavior. Additionally, the security team must also be able to educate employees in one-off situations such as when users become targets of threat actors.

   When an attack is identified, successful or not, it is important to provide the targeted users with information about the attack so they can be aware of what future attacks may look like. If an attack is successful, security professionals should not punish the users, but realize that mistakes are going to occur. This is an opportunity to steer future actions in the right direction. In effect, users become human "Intrusion Detection Systems" and provide information that might otherwise be missed within the cybersecurity framework. No product on the market is going to find all malware or all bad user behaviors. With that said, if you combine good technology and processes with great people, enterprises amplify the ability to combat advanced threats, reduce dwell time, and detect lateral movements.

"If you combine good technology and processes with great people, enterprises amplify the ability to combat advanced threats, reduce dwell time, and detect lateral movements."

Conclusion

The longer attackers remain in the enterprise (longer dwell time), the more damage they can cause, and the more intellectual property they can steal. Today's organizations should not focus solely on keeping attackers out, but on ensuring that the attacker stays in the network for as little time as possible — constantly striving to further reduce dwell time. Attackers may come back, but they will realize that their efforts are too costly and have little return on investment. When attackers experience an enterprise attuned to dwell time, they quickly realize that even if they found an open door the enterprise would immediately detect them, and boot them out. They will then go somewhere else, in search of a less-protected enterprise.

For further information contact:

Raytheon|Websense
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheoncyber.com

Raytheon | websense