YOU HAVE BEEN BREACHED. WHAT'S YOUR MOVE?

Active Incident Response for Today's Advanced Threats

PERSPECTIVES FROM RSA
March 2016

"The winner of the game is the player who makes the next-to-last mistake."
Savielly Tartakower, Chess Grandmaster, author and journalist

- Organizations need to improve their ability to detect threats. They need the right tools and expertise to do this.
- RSA is uniquely able to help organizations defend themselves from cyber attacks in the growing digital world.
- Addressing cyber attacks requires an active strategy for incident response, like a game of chess with specific strategic dos and don'ts.

Chess is a complex game when played between two strategic opponents. There are many instructive parallels between chess and incident response when dealing with sophisticated adversaries. In chess, to be successful, you need to understand the rules (how can your opponent move?), typical defensive strategies and attack patterns. Beyond these basic tactics, to play at the highest level, you must also stay mindful of the bigger picture and plan your next moves in advance to ensure your opponent does not corner you into checkmate, where you lose the game.

In incident response, it is imperative to understand the attack surface that you must defend and the security controls in place that can prevent security incidents, but also understand how those controls can be circumvented and the typical tactics an adversary will use. Even more important is to ensure that you have proper advanced visibility of the enterprise to better detect attempts to compromise your most important digital assets. Where the analogy is strained is that there are a large but finite number of pieces and moves in chess, while in the cyber world there are orders of magnitude more potential vulnerabilities that can be exploited, unknown adversaries, and complexities that make it extremely difficult to prevent an incursion. As a result, planning your security incident response in advance is even more important.

In this whitepaper, we will examine why data breaches inevitably occur, provide examples of what to look for in order to detect potential compromises, and most importantly what to do and not to do when a likely breach is uncovered.

WHY DO BREACHES OCCUR?

The need for an effective incident response capability is driven by the inevitability of breaches, whether larger or small. Many organizations underestimate the need to plan and prepare for incident response and instead apply disproportionate effort to prevention, a failed strategy. Consider the following:

- The proliferation of mobile devices and the data in the cloud has accelerated the dissolution of the perimeter and massively increased the attack surface.
- Countermeasures for zero-day attacks – exploits of previously unknown vulnerabilities and associated tactics and procedures – cannot be predetermined.
- Cyber attacks are orchestrated and executed by humans. Networks and infrastructure are protected by humans, and humans are both infinitely inventive and fallible.
- Behavior of threat actors differ based on their objectives. Designing effective defensive strategies requires in-depth knowledge of a diverse and growing set of tactics, techniques, and procedures used by adversaries.

- The battlefield is asymmetric –attackers only have to succeed once and defenders have to be successful all the time.

- There is a consistent lack of investment in the resources – talent and technology – required to implement and sustain an effective information security program in many organizations. An internal lack of coordination among IT also increases vulnerability for an attack.

Accepting the inevitability of security infections and incidents doesn't mean accepting that they will result in major damage or loss to the organization. An effective incident response program can minimize the impact of a breach and keep it below the threshold of business materiality. It is thus essential for organizations to develop and improve their response capabilities. Detection, mitigation and remediation are the three pillars of incident response on which organizations need to focus.

INDICATORS OF COMPROMISE

Detection of a security anomaly should initiate the response process. Unfortunately, in many cases, organizations are notified about a data breach by a third party. With the appropriate visibility in place, an organization should be able to identify a potential data breach on its own. In either case, knowledge of attacker methodologies and what would be indicators of compromise is needed in order to determine if a compromise is opportunistic or targeted in nature.

Advanced threat actors, whose missions tend to be very targeted, patiently observe an organization, its people and technology, before launching an attack campaign. They blend in and wait to strike with precision. Their favored tactics, techniques and procedures (TTPs) are always evolving but often include custom malware, zero-day exploits, and credentials hijacked from an organization's employees or trusted third-parties via phishing or drive-by downloads, for example.

In many cases the warning signs of network intrusion can be so subtle that they are often overlooked. Other Indicators of Compromise (IOC) are more obvious. Knowing what to look for can help to stop an attack from impacting the business as well as provide starting points for the forensic investigation and response.

A few example IOCs include:

- Newly-created System Administrator accounts, accounts that are closed shortly after setup, and IT privilege escalation by non-IT users.

- Unusual activity by existing privileged accounts, including abnormally high usage and accessing multiple new servers.

- Consecutive IP "pinging" of internal systems from other internal systems.

- Sudden activity on dormant and seldom-used servers or systems.

- Data exfiltration or command and control communications over open ports.

- Unexpected spikes in Internet bandwidth usage.

- Movement of non-standard, large files or data streams internally or externally to unusual places.

- File transfers to previously unknown external servers, especially in geographies where an organization does not conduct business and are known to be cyber crime hot spots.

COMPROMISE CONFIRMED. NOW WHAT?

Unlike a chess match responders never have the opening move in an attack; they must react to intrusions. Incident response involves actions, but in the fog of cyber war when situational awareness may be incomplete, it is often measures not taken that heavily influence outcomes.

Determining when and how to respond to a likely intrusion requires restraint and judgment informed by expertise and experience. A rash response can prematurely alert hackers that they have been detected, enabling them to destroy forensic evidence to cover their tracks and return via other unknown channels or commandeered accounts. Valuable evidence that can reveal vulnerabilities and the attacker's tools and tactics that can help to prevent future attacks can be destroyed or obscured.

MITIGATION ACTION DOS AND DON'TS:

- **DO** fully assess the situation before taking action. Look for signs of lateral movement, exfiltration of data and files, and search for specific IOCs across all likely impacted hosts and network segments. The goal is to determine the nature, timing, and extent of the compromise.
- **DO** convene, brief and review the organization's incident response plan with all stakeholders on a regular basis. Leveraging intelligence from past experiences and from experts is critical to improving your incident response readiness. Collaborate accordingly with information sharing groups that are appropriate for your industry.
- **DO** log actions of the response team to track and distinguish between black hat activity and remediation and forensic activities.
- **DO** mitigate damage by isolating unaffected networks and systems.
- **DO** remediate gaps and vulnerabilities exploited by threat actors when the immediate threat has been neutralized and the eradication process has begun as part of an orchestrated response.
- **DO** share information from the forensic investigation with pertinent stakeholders. These may include involved partners and law enforcement.
- **DO** deploy network and endpoint monitoring systems to more efficiently detect and investigate current and future attacks.

- **DO NOT** panic or overreact. Cyber attacks are serious and stressful, but maintaining composure and a clear head is necessary for mitigating damage and remediating points of weakness.
- **DO NOT** respond disproportionally. Taking a "nuclear option" to countermand hackers can exacerbate the situation, cause significant business disruption and violate the laws of jurisdictions in which an enterprise operates.
- **DO NOT** Immediately change a password of an account in use by the attackers. If an intruder has been in the organization for any significant time, changing a password of a stolen account is a small hurdle to overcome that can have a counterproductive downstream impact on enterprise users.
- **DO NOT** block IP addresses and URLs. Hackers can quickly move from server to server. Trying to stop it is an exercise in futility that drains resources better spent on mitigation and remediation.
- **DO NOT** disable Internet access. This may be more disruptive and costly to the business than the actual attack.
- **DO NOT** shut down servers. They are only one type of entry point and doing so will be disruptive to the business, prematurely alert attackers, and increase the risk of losing vital data such as malicious code and encryption keys used in the attack.
- **DO NOT** take extraordinary, aggressive actions in unaffected systems. Unusual generation of reports, analytics or changes in preventive measures can make it difficult to discern between what the enterprise has done and what the attacker has done.

THERE IS NO SUBSTITUTE FOR EXPERIENCE

Like chess Grandmasters, the best cyber security professionals constantly work to improve their game. While the staggering frequency and sophistication of cyber attacks can be daunting, the challenge is not insurmountable. Identifying and analyzing the tactics and strategies of adversaries and determining counter moves should be an ongoing pursuit. World-class chess players scrutinize their own game, looking for areas of improvement and learning from past matches.

Cyber security professionals have ever-increasing access to information, tools and human resources to supplement internal capabilities. Hiring trained staff or contracting third-party expertise is essential to successfully protecting critical networks and data and diminishing the first mover advantage of cyber threat actors.

A BLUEPRINT FOR IMPROVING YOUR GAME

The inevitability of breaches makes a strong commitment to incident response essential. Better detection through enhanced visibility, coupled with proactive response planning that relies on tested best practices will help minimize the impact of breaches on the organization. A commitment to continuous improvement and leveraging trusted experts will improve resiliency to threats over time. Given today's threat landscape, there is no better time than the present to start developing or improving your incident response.

ABOUT RSA'S INCIDENT RESPONSE SERVICES

RSA's Incident Response (IR) Practice provides proactive and reactive services for enterprises. The services include Incident Discovery, Response, and Retainer services using advanced, enterprise-class, market-leading tools and methodologies. The specific tools used include those within the RSA product portfolio such as RSA's Security Analytics and Endpoint Solutions. In addition, IR consultants often use open source and commercial forensic and malware analysis tools, as well as leverage tools that are already available within a client's infrastructure. This allows organizations to obtain information that is critically necessary to provide real time awareness to the state of compromise. As a result of the analysis, the IR consultants are often able to identify compromised systems and fully understand the extent and scope of an incident that would otherwise remain undetected.

ABOUT RSA, THE SECURITY DIVISION OF EMC

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. RSA is driven by its uncompromising belief that organizations should not have to accept getting breached or hacked as an unavoidable consequence of operating in a digital world. In fact, RSA believes that organizations must become aggressive defenders of their right to operate securely and that no other company is in a better position to help them.

With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime.

RSA
www.RSA.com