NOW YOU SEE THEM
NOW YOU DON'T

Hacker Tactics, Techniques and Procedures

PERSPECTIVE FROM RSA
DECEMBER 2015

Cyber security has become a leading issue for sovereign nations, businesses of all sizes, and individuals across the globe. The lack of a secure information technology (IT) infrastructure – the underpinning of modern life – puts in peril personal safety, innovation, and the global economy.

Failures of the Security Industry: Accountability and Action Plan[1] points out that "Despite heightened awareness, a panoply of new products and services, increasing investment, and concerted efforts from some of the smartest minds in business, government, and academia, the security industry struggles to keep pace."

One reason that hackers often remain ahead of government and industry is the wide and changing arsenal of tools at their disposal. An illicit market for malicious software of all kinds has emerged. Emboldened by burgeoning demand and facilitated by black market financial systems, a new operating model has emerged. Hackers no longer need to be coders. Finished applications are bought, sold, and exchanged. Free rootkits and software development kits (SDK) enable crowdsourced malware development. Viruses, bots, and worms are the Saturday Night Specials of the internet age; untraceable, disposable weapons.

The trickle-down knowledge of advanced attack techniques is a second contributing factor. "Advanced" attacks were once the exclusive purview of state sponsored cyber attackers. But successful executions of well-concealed compromises and sustained intrusions are no longer limited to expert teams of sovereign agents with deep resources: The Securities and Exchange Commission announced in September 2015 that two Ukranian hackers infiltrated networks in the United States and accessed confidential, embargoed financial performance information of public companies over a period of five years. One month prior, Impact Team, the cyber extortion ring behind the theft of personally identifiable information from extramarital-affair website Ashley Madison, admitted to stealing "complete source code repositories, financial records, documentation, and emails" over a period of years.

Organizational leadership and those directly responsible for protecting critical information systems must:

- **Recognize** that advanced attack techniques will be used by the majority of hackers, regardless of the type of information sought, or the size or industry of the target organization.
- **Understand** how these threat actors now operate.
- **Operationalize** response and adjust defense plans and strategies to account for the hostile tactics that the organization is likely to face.

Entities that fail to do so face certain cyber intrusion and attendant disruption and cost.

Effectively protecting information systems from cyber attack requires an understanding of tactics, techniques, and procedures (TTP) used by hackers – their modus operandi. Seminal research presented at the 6th Annual International Conference on Information Warfare and Security in 2011 by Lockheed Martin Corporation affirms the value and describes the goal of analyzing attack campaigns: "to determine the patterns and behaviors of the intruders, their tactics, techniques, and procedures (TTP), to detect *how* they operate rather than specifically *what* they do." This is an essential point. Though TTPs can vary among hackers and do evolve, they are less transitory than specific tools. While the goals of disparate actors – for example, nation states, organized crime syndicates, hacktivists and terrorists – differ, they exploit the same weaknesses and use the same entry points.

[1] *Failures of the Security Industry: Accountability and Action Plan,* Amit Yoran, president, RSA and William Robertson, assistant professor, College of Computer and Information Science, Northeastern University, February 2015.

Knowing how threat actors operate can enable cyber security professionals to better defend systems against attack by focusing efforts on detection and response.

Adversary Tactics, Techniques and Procedures

The RSA Incident Response team has cataloged multiple TTPs from active incident responses, subsequent forensic investigations, ongoing monitoring and research, and information sharing.

Most cyber attacks begin with reconnaissance. Threat actors acquire and leverage information on specific targets in several ways. Social media posts by potential targets revealing their organizational affiliation and area of responsibility are a rich source of data. Public sources such as news reports and business databases, for example, the SEC's EDGAR repository of filings, contain specific information about mergers & acquisitions, ownership and contact information. Enterprises supply chains are probed for weak links to exploit.

Once targets have been defined and potential entry points identified, attacks are carried out in three discrete phases:

Stage 1: Establishing a Foothold

Attackers first seek to gain an initial entry point into the organization's infrastructure. They may exploit software vulnerabilities in external-facing systems. They may obtain credentials from an individual user or compromise endpoint systems, often leveraging phishing and social engineering techniques. Once in, they establish reliable lines of communication back to the infrastructure from which they are carrying out the attack. Security awareness training and more advanced endpoint detection technologies have made this initial task harder for attackers over time. We see continued advancement of attacker TTPs in response.

Specific Stage 1 TTPs that the RSA Incident Response team has seen in use include:

- Combination of Waterhole Attacks with Zero Day Exploits
    - Targeting users who visit very specific websites
    - Downloaded and executed shellcode directly from memory, never hit disk
    - Dropped non-persistent RAT
- Hijacking legitimate user names/password combination, including privileged accounts, to gain network access without the risk of malware detection
- Signed APT Binaries
    - Signed Backdoors with bogus companies
    - Fraudulent Code Signing Certificates
    - Signed RAR Self Extracting Executables with PlugX scripted inside
    - DLL preloading vulnerabilities in common sandbox application to load malicious code
- Web App Framework Exploitation
    - Cold Fusion and other Content Management System software exploited to create initial staging area
- Use of custom Webshells. First stage (lightweight) second stage during operations (heavyweight)

Stage 2: Entrenching, Expanding, Exploring

Once initial access to the target organization is obtained, attackers move swiftly to accomplish their objectives. They establish more reliable access and seek to limit monitoring of their activity, downloading additional tools to aid their efforts. They work to expand control of more machines and accounts. Priority is placed on obtaining privileged or administrative access. The target's network is mapped to pinpoint high value targets such as domain controllers and email servers, copying directory listings, database schemas, and email. This activity is frequently referred to as "lateral movement." Spotting these tactics as they are being carried out is often the best chance that network defenders have to disrupt an attack in progress.

Specific Stage 2 TTPs that the RSA Incident Response team has seen in use include:

- Replacing proxies
    - Proxy does not proxy its own traffic
    - Firewall cannot log successful traffic
- SSL Webshells placed laterally after initial compromise
    - Placed on customer Outlook Web Access servers
    - SSL encrypted communications of the malicious backdoor
- Custom attack support tools with Windows Management Instrumentation capabilities
- Using Windows Sticky Keys feature to create backdoors in conjunction with lateral Remote Desktop Protocol access

Stage 3: Exfiltrating and Maintaining

If attackers are not detected and their activity disrupted, they will eventually gain access to confidential organizational intelligence such as financial data, personal data, and intellectual property. Their actions will turn to removing this data from the network without being detected. The data will often be aggregated and staged on a compromised asset prior to removal. It will almost always be obfuscated in some way, most commonly compressed and encrypted to resist automated detection by content monitoring tools such as data loss prevention (DLP) software. Attackers will take advantage of a multiplicity of exfiltration options, from simple file transfer protocol (FTP) and email, to http and https on compromised web servers. Once attackers have accomplished their initial objective, they will return periodically to access and exfiltrate updated target data, as well as update toolsets to help maintain persistent access to the victim organization.

Specific Stage 3 TTPs that the RSA Incident Response team has seen in use include:

- Email exfiltration through compromised messaging application programming interface (MAPI)
- Exploiting cloud proxy services

Chasing Phantoms

Even the most elusive threat actor will leave indications of their presence and movements. Knowing what to look for and where may be the difference between preventing and mitigating the damage of a cyber attack or suffering potentially catastrophic loss.

Vigilance, unrelenting persistence and continuous learning are essential. This situational awareness must be operationalized by tools that provide visibility and forensic data. A detailed view of the entire potential attack surface is critical to discovering and disrupting intrusions. Many organizations who may face advanced adversaries have put in place solutions for log collection, monitoring and analysis. But these systems provide incomplete visibility into potential points of compromise, or lack the data or ability perform certain types of analysis that will lead to more rapid and more effective detection of attacker activity. As a result, other technologies are becoming must-haves to improve defenders' existing visibility. These include:

- **Packet Capture (PCAP)**: The ability to capture and analyze network activity can help spot multiple TTPs described above that other telemetry cannot. It is particularly effective to spot command and control (C2) traffic between compromised systems and attacker infrastructure, and can provide granular visibility into specific actions being taken by attackers inside the target's infrastructure. It is also the only way, in the event of successful data exfiltration, to understand exactly what was taken. This information helps quantify the breach impact on the victim organization, as well as provide insight into attackers' motivation, which can aid in attribution, which in turn can lead to further assumptions regarding other likely active TTPs.
- **Endpoint Detection & Response (EDR)**: The ability to capture detailed state information from endpoints is another essential tool for detection. These tools can validate the integrity of a given system and files, and leverage this data to identify hidden processes, modifications, and tampering that are indicative of compromise. Armed with this information, these tools can instantly find similarly infected endpoints, allowing handlers to quickly expand their visibility into the full scope of a compromise. Many of these tools also offer quarantine or blocking functionality, which can be used to disrupt malware-driven TTPs, and limit attacker lateral movement.

- **Behavioral Analytics**: Multiple attacker TTPs described above either aim to gain or depend on use of compromised user credentials. The reason why such tactics are so widely used is their effectiveness. Legitimate credentials allow attackers broad access that blends in alongside normal user activity. However, while the credentials may be valid, the actions themselves are often not consistent with the user's normal behavior. Behavioral analytics seek to spot this anomalous activity by building a baseline view of a given users activity, and highlighting deviations from the norm, especially when considered within business context. For example, a user may start accessing a set of systems that they have never accessed in the past, or start transmitting much greater data volumes than normal to external IP addresses. Effective behavioral analytics can highlight this inconsistent activity for investigation. It is particularly important to apply these analytics to high-privilege, high-value user accounts targeted by attackers.

Knowledge is (Still) Power

The velocity, volume, and ephemeral nature of cyber weapons makes it daunting to keep current. However, the cyber security community has a heritage of collaboration and information sharing. Cyber security professionals and other enterprise stakeholders can access intelligence from many resources:

- **Government Agencies**. The United States Computer Emergency Readiness Team (US-CERT) provides timely information about current security issues, vulnerabilities, and exploits. Anyone can register to have technical alerts sent via email or RSS.

- **Vendors and Security Researchers** provide in-depth security news and investigation, often free of charge.

- **Industry Analysts**. Though most firms charge for access to syndicated content, analysts often share insight and perspective through publicly accessible blogs.

- **Media**. News coverage and analysis by specialized media points.

Enterprises should act on emerging information from credible sources. Specific action steps should be pre-defined in the organization's incident response plan.

We also recommend establishing a relationship with security consulting and professional services provider in advance of an immediate need, that is, during a breach.

About RSA

Everyday, and for over 30 years, RSA's singular mission has been to help our more than 30,000 customers around the world protect their most valuable digital assets. 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.

RSA helps organizations aggressively defend their right to operate securely in a digital world. Through visibility and analytics, RSA solutions give customers the ability to effectively detect, investigate and respond to advanced threats; confirm and manage identities; harness risk; and ultimately, prevent IP theft, fraud, and cybercrime.