Persistent threats and how to monitor and deter them


Colin Tankard

Colin Tankard, Digital Pathways

The UK Government has recently estimated that cybercrime costs the country some £27bn per year and, according to some estimates, the global cost is $1 trillion every year. This crime wave has been greatly facilitated by the rise of electronic communications, primarily those making use of the Internet. The purpose of electronic communications is to make it more efficient and easier to communicate – but they are also relatively easy to attack or intercept. No-one is immune – such attacks are aimed at individuals, small firms, multinationals and governments.

Just a decade ago, attackers targeting electronic networks and communications were largely motivated by gaining kudos among their peers. The main consequence of such attacks was the cost of downtime and cleaning up systems that had been compromised. Today, the primary reasons for such attacks are to steal proprietary information, to sabotage systems or for extortion. For individuals who have had their personal details stolen and used for identity theft, the consequences can be far-reaching. For commercial organisations or governments, the effects can be dire in terms of financial loss and tarnished reputations that can see customers taking their business elsewhere. It is vital that all organisations put controls in place for protecting critical assets such as intellectual property, including source code and trade secrets, and customer information such as cardholder data.

The new threat landscape

Over the past couple of years, a new class of threats has been seen – so-called Advanced Persistent Threats (APTs). The word 'advanced' refers to both the exploits used by hackers and the nature of the threats. Hackers using such threats are skilled and well-resourced criminals who employ a wide range of sophisticated reconnaissance and information-gathering tools, as well as attack tools and methods. The methods that they use to gain entry to networks are not, in the main, particularly advanced, using social engineering techniques or malware, but the attack methods used once entry is gained *are* advanced, always changing by recompiling malware code on the fly and using encryption for obfuscation. The term 'persistent' refers to the fact that the goal of an APT is to gain access to targeted information and to maintain a presence on the targeted system for long-term control and data collection. Many attacks go undetected for significant periods of time as hackers using APTs exploit a slow, stealthy approach to evade detection, but are constantly monitoring and interacting with the systems under attack. They rely on stealth tactics to avoid detection and aim to appear as close as possible to legitimate network traffic.

High-profile security breaches have been in the news for some years. However, the majority of those that have been publicised deployed attacks on front-end servers using methods such as SQL injection to look for financial information or sensitive customer data that could be used for fraud and theft. Once the attackers have found what they want, they generally move on. According to the Open Web Application Security Project (OWASP), such injection flaws are the top vulnerability affecting websites today, but are relatively easy to avoid using such techniques as: prepared rather than dynamic statements to prevent hackers changing the intent of the query; restricting access, especially for privileged accounts; and using whitelists to validate inputs and detect unauthorised inputs before they are passed to the SQL query.[1]

"Known as Operation Aurora, the attack was extremely wide-scale and is believed to have targeted 34 organisations"

APTs are much harder to defend against, owing to the use of multiple techniques in combination, such as undetectable zero-day exploits combined with social engineering techniques. The first widely reported APT was publicised by Google in January 2010, although it is believed to have begun some six months earlier. Known as Operation Aurora, the attack was extremely wide-scale and is believed to have targeted 34 organisations, including Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical, as well as Google itself.

Analysis of an attack

Analysis of the Operation Aurora attacks showed that they used extremely sophisticated tactics which, according to the security vendor McAfee, have never before been seen outside of the defence industry. The attacks started by using advanced social engineering

techniques and highly targeted emails to selected individuals that contained links to websites. These in turn hosted malicious JavaScript code that was used to exploit a zero-day vulnerability in the Internet Explorer browser. In total, it is believed that the attack used around a dozen pieces of malware to burrow deep into the network, and several layers of encryption to obfuscate the attack and avoid common detection methods.

Once installed on the network, the malware used backdoors to communicate with remote Command and Control (C&C) centres via TCP port 443, which is usually associated with encrypted traffic and which is therefore difficult to inspect. Now with direct access to the network, the hackers were able to use pivoting, which is a method by which hackers exploit the systems they have compromised to attack other systems on the same network and avoid restrictions such as those set by firewalls. This allowed the hackers to explore protected intranets in order to search for intellectual property and other vulnerabilities, and then exfiltrate the information obtained to the C&C servers. Even after the C&C centres were taken down, it is known that the attacks continued for some time.

"Attacks such as these will cost the organisation dearly in financial terms, leave it in danger of further fines for non-compliance with regulations, as well as damaging its reputation"

Since this first highly publicised attack, the number of APTs reported in the media has increased substantially, including attacks against organisations such as Sony, Barracuda Networks, Citigroup, Epsilon and RSA Security. In the case of Sony, the attacks were carried out over a period of several months and exploited a number of vulnerabilities, including those in outdated software. At least 10 separate breaches have been seen to date, leading to some 100 million customer records being compromised and affecting the company's web operations in several countries. Attacks such as these will cost the organisation dearly in financial terms, leave it in danger of further fines for non-compliance with regulations, as well as damaging its reputation – potentially for the long term.

The RSA APT is an example of an attack using a Remote Access Toolkit (RAT) to allow connection to a remote C&C centre. RATs have the ability to perform a number of functions, including capturing screenshots and images from cameras and other network equipment; search for and manage files on the system; control shell functions; power computers on or off; and query, add, delete and modify registry entries. Once the information had been found, the data was moved to staging servers and aggregation points in compressed and password-protected RAR files, which were exfiltrated out of the organisation.

Characteristics of APT attack methods

What makes these attacks so much more insidious than those seen in previous years is their sophistication and the use of multiple attack techniques, including social engineering and automated tools. According to Cutler, in 'Anatomy of an Advanced Persistent Threat', the following constitutes the typical APT strategy:[2]

- Attacker gains a foothold on the system via social engineering and malware.
- Attacker then opens a shell prompt on victim system to discover if the system is mapped to a network drive.
- Victim system is connected to the network drive, prompting the attacker to initiate a port scan from victim system.
- Attacker will thereby identify available ports, running services on other systems, and identify network segments.
- Now that attacker has the network map in hand they move to targeting VIP victims with high-value assets at their disposal.

Advanced social engineering techniques

Phishing is one social engineering technique that is used to trick users into giving away sensitive information such as user name and password combinations, bank account numbers or credit card details. In many cases, emails or other forms of electronic communication are sent to users that purport to come from trusted sources, such as their bank or company IT administrator. These messages will often contain a link to a website that has actually been spoofed and is riddled with malware designed to harvest sensitive information from the user. According to the Anti-Phishing Working Group (APWG) in a report issued in 2011, 37% of respondents to its survey reported that they had had phishing or spoofed sites planted on their web server two or more times in the previous year, which the APWG states points to the increasing persistence of hackers.[3]

"Organisations should look to raise awareness among their network users of security issues and the problems that their actions can cause, such as by clicking on malicious links"

A particular trend being seen by the APWG is the use of spear-phishing – and this is something that has been widely used in the APT attacks seen over the past 18 months. Such attacks are much more technically competent and efficient than phishing attacks launched *en masse*. Spear-phishing attacks target specific individuals in organisations – and especially those, such as key executives or their assistants, that have privileged access to sensitive information. Attackers looking to launch APTs spend a considerable amount of effort on reconnaissance and information-gathering from the Internet and other sources, including from social networking sites such as Facebook and LinkedIn that provide a wealth of valuable personal information on users. They will then use the information gathered for highly targeted communications to specific individuals that appear to come from trusted friends or colleagues who would normally be privy to such information. The targeted individual is therefore

much more likely to click on a link in the communication, taking them to a compromised website or causing them to install information-harvesting malware on their devices.

Spear-phishing attacks take a great deal more work on the part of the attacker to pull off than random phishing attacks and have been used in many high-profile APT attacks, including Operation Aurora, and those against the International Monetary Fund, Oak Ridge National Laboratory in the US and the French foreign ministry. In all these cases, spear-phishing was used to fool users into installing malware or revealing account information. In the case of Operation Aurora, the malware used was previously unknown, enabling it to avoid detection by signature-based anti-virus technology, and the initial piece of code used was shell encrypted three times to protect it from detection.

Since so many APTs utilise social engineering techniques, organisations should look to raise awareness among their network users of security issues and the problems that their actions can cause, such as by clicking on malicious links. They should also look to manage the information that ends up being placed on social networks through education and policies, which need to be effectively enforced through monitoring.

Defending against APTs

According to a recent study by researchers IDC, 50% of European manufacturers are unaware of the number and nature of security threats that they face.[4] Their top security priorities are firewalls and anti-virus technologies, but less focus is given to data loss prevention, with employees often given excessive access rights. Organisations often put in place security controls once they have suffered a security incident, but fail to keep policies and procedures up to date or to proactively defend against new threats being seen. This is a problem, as APTs are specifically designed to defeat controls such as firewalls, anti-virus and intrusion-detection systems, and especially those that rely on signatures and can therefore guard only against known threats. Although such tools are useful, they should be supplemented with more-advanced controls such as whitelisting technologies that allow only known good traffic through, and can therefore block unknown, zero-day threats.

To defeat APTs, organisations should look to understand as much as possible about their network traffic and the services provided. For defence in depth, multiple network monitoring measures are required – such as log analysis, file integrity checking, registry monitoring and rootkit detection – and will provide an indication of any break-ins. Proper log configuration and analysis of logs, including those from firewalls, network intrusion detection systems, web servers and databases is essential as without this, attempts at monitoring will not be successful. Organisations should establish baselines for security and compare log data against these. Many vendors offer log-management technologies, many of which are combined in Security Incident and Event Management (SIEM) technologies that automate the detection, alerting and visualisation of log records. Log reviews should be performed often and regularly and all alerts should be followed up in a timely manner.

"With all these controls in place, organisations will be better positioned to proactively monitor for APTs that look to burrow deep into their networks and to prevent data from being lost"

Network intrusion and detection systems are also useful tools that have matured in recent years and now use a combination of signature, protocol and anomaly-based analysis. Now with more granular and flexible capabilities, the number of false positives that they throw up has been reduced – a factor that was preventing many organisations from switching on their intrusion prevention capabilities owing to the amount of legitimate traffic that they previously stopped.

Vulnerability assessments and analysis are useful tools for determining which vulnerabilities can be exploited by hackers. However, vulnerability testing is not performed often enough – as shown by the fact that 80% of security incidents are detected by third parties, according to the APWG. This is because too few organisations use real-time network-monitoring tools or adequately manage and analyse log records for suspicious activities. Vulnerability assessments should also be performed in combination with penetration testing, which aims to use the same tools as hackers to test whether vulnerabilities can be exploited under real-world conditions.

Latest fixes

It is also essential to keep all operating systems, web servers and applications patched with the latest fixes and ensure that security configurations are kept in an optimal state. Organisations should look to establish a baseline configuration for each application or system, which should be locked down. A cryptographic hash should be used to ensure its integrity for future use.

For detecting APTs, it is especially important to analyse outbound traffic as the aim of the attacks is to exfiltrate information from the network. This can be achieved through a combination of the use of rule sets to analyse phishing campaigns, recognise and block malicious traffic and search for malicious registry entries, statistical and correlation methods to monitor traffic for possible compromise and data exfiltration, manual approaches for anomalies such as large SQL statements that can indicate an injection attack, and automated blocking of data exfiltration. To prevent hackers from exfiltrating data via TCP port 443 – as was seen in Operation Aurora – organisations should configure the port so that only traffic from its own proxy is allowed to exit via this port and should use access-control lists to permit or deny traffic according to the permissions set.

For improving data security, organisations should use a combination of encryption for databases, files, backup and storage systems, as well as end-points. This will help prevent the hackers from actually reading data unless they can gain access to passwords or encryption keys. Therefore, efficient key and certificate management practices are essential. Strong access controls should be used to lock-down access to data according to need and role in the organisation, backed up by strong authentication techniques such as security tokens with one-time passwords. Host integrity technologies should be used for all files and databases, which is important for detecting unauthorised changes to systems, files and databases, and misconfigurations which, according to much industry research, is responsible for 60-65% of network downtime and which are also commonly exploited by hackers.

Conclusions

With all these controls in place, organisations will be better positioned to proactively monitor for APTs that look to burrow deep into their networks, and to prevent data from being lost. However, owing to the persistent nature of the threats, this should be an ongoing process with controls continuously monitored for their effectiveness with real-time reporting capabilities, including alerts for any anomalies found. This will provide the audit trail that organisations need to show where controls need to be improved and to prove the effectiveness of those controls for internal governance and compliance efforts, as well as for shielding themselves as much as possible from the sophisticated and complex threats facing networks today.

About the author

Colin Tankard is managing director of data security company Digital Pathways, which specialises in the design, implementation and management of systems that ensure the security of all data, whether at rest within the network, mobile device, in storage or data in transit across public or private networks.

References:

1. Open Web Application Security Project. Accessed Jun 2011. <http://www.owasp.org>.
2. Cutler, Terry. 'The Anatomy of an Advanced Persistent Threat'. Security Week, 6 Dec 2010. Accessed Jun 2011. <http://www.securityweek.com/anatomy-advanced-persistent-threat>.
3. LaCour, John; McRee, Russ; Capps, Robert; Rasmussen, Rod; Ceesay, Ebrima; Holt, Thomas; Warner, Gary. 'APWG Web Vulnerabilities Survey'. Anti-Phishing Working Group, 3 Jun 2011. Accessed Jul 2011. <http://www.anti-phishing.org/apwg_web_vulnerabilities_survey_june2011.pdf>.
4. Veronesi, Lorenzo; Mananti, Pierfranco; Lee, William; Li, Wendy; Doorly, Jane. 'Know Your Enemies: IDC's EMEA Manufacturing Survey Results'. IDC Manufacturing Insights, May 2011. <http://www.idc-mi.com>.

...News Continued from page 2

Microsoft used Black Hat to launched the BlueHat Prize, with $200,000 on offer the person who comes up with "a novel runtime mitigation technology designed to prevent the exploitation of memory safety vulnerabilities". There's a second prize of $50,000 and the deadline is 1 April 2012. More information at: <http://www.microsoft.com/security/bluehatprize/>. This is the first time that Microsoft has offered a prize to the general programming community: unlike Google, Mozilla and Facebook, it still doesn't pay bounties to bug-finders.

A keynote speech gave Peiter Zatko, programme manager at DARPA, the opportunity to launch the **Cyber Fast Track**, a way of building bridges between the hacker/programmer community and the intelligence community. It aims to simplify the process of initiating, and getting funding for, new projects and is also designed to better exploit the pool of talent available for improving national cybersecurity. Zatko anticipates 20-100 projects a year.

The **Cloud Security Alliance** unveiled its Security, Trust and Assurance Registry (STAR), part of its self-regulatory model for security in cloud environments. Planned to be fully operational by the end of 2011, it allows cloud service providers to document how they comply with CSA best practices. It will also provide a registry of technologies that are compatible with these best practices. More information at: <http://www.cloudsecurityalliance.org/star>.

At DefCon:

A panel session concluded that the likes of **Anonymous**, **LulzSec** and their imitators need to become more focused and organised. Speakers such as Josh Corman of 451 Group and security blogger Krypt3ia suggested that the current wave of hacks are producing leaks of low value and a chaotic situation with little long-term benefit.

Continued on the back page...