Targeted Cyberattacks:

A Superset of Advanced Persistent Threats

Aditya K Sood and Richard J. Enbody | Michigan State University

Targeted cyberattacks play an increasingly significant role in disrupting the online social and economic model, not to mention the threat they pose to nation-states. A variety of components and techniques come together to bring about such attacks.

Unlike worms and viruses that usually attack broadly, targeted attacks involve intelligent planning with respect to the chosen target or class of targets. Also evident is a difference in attitude: the attacker wants to attack you and is willing to expend the extra effort to target you as an individual (or group). This type of attack has always been in the field, but its profile is growing as the world has become more interconnected and the value of online targets has increased.

The security industry has embraced the term *advanced persistent threat* (APT), with several definitions attempting to describe how it differs from other attacks.[1] There's some agreement that these attacks aren't necessarily more advanced than others, except in the sense that a high-value target might require a greater degree of sophistication. Persistence is a characteristic of targeted attacks because they persist in the face of adversity instead of moving on to weaker targets. Some like to apply "patient" to the P in APT because of the patience in the attacker's persistence.

Several incidents in the past few years illustrate the criticality of targeted attacks:

- GhostNet was a targeted attack discovered in the wild in 2009. Command and control (C&C) centers in China targeted more than a hundred nations. The attack occurred through a malicious email that included contextually relevant information; opening it resulted in execution of malware in the form of an attachment. Once installed, the malware downloaded the Ghost Remote Administration Toolkit for managing systems remotely. The C&C server in China could then send commands and store its victims' exfiltrated data.
- Operation Aurora, rumored to be from China, started in 2009 with the aim of stealing intellectual property and sensitive information from a wide variety of high-tech, security, and defense companies. Attackers exploited the "use after free" vulnerability in Internet Explorer, which resulted in HTML object memory corruption. (A use after free vulnerability lets attackers inject code in the memory area released by the object upon deletion without reallocating it further. In other words, the object is created, the object is deleted to release the memory, code is injected in the free memory without any reallocation by creating a new object, and the object executes the code to gain shell.) A drive-by download attack infected users' machines with malware by exploiting this vulnerability.
- In 2010, Chinese hackers targeted China's IP Telecom, the largest provider of broadband Internet connections in China, and exploited a problem in the Border Gateway Protocol (BGP) used by routers to determine paths for routing Internet traffic. The Chinese attackers sent erroneous traffic that updated the routing tables of several routers across the world. Because routers were the attack platform, the targeted attack had the side effect of impacting broader sectors of the Internet.

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/13/$31.00 © 2013 IEEE

- Also arriving in 2010, the targeted Stuxnet attack, attributed to the US and Israel, was designed to exploit the Siemens Programmable Logic Controllers in SCADA networks with the ultimate goal of destroying centrifuges used to process nuclear material. The Stuxnet framework exploited four 0-day vulnerabilities including Windows print spooler, LNK format, SMB server (kernel), and task scheduler. A variant of Stuxnet called Duqu was recently spotted in the wild.

Many of these types of attacks are labeled as APTs, but we consider APTs to be a general subset of targeted attacks. Regardless of what they're called, they seem to be increasing in frequency. This article's aim is to provide a complete model of targeted attacks and their different components.

The Targeted Attack Model

We can divide targeted attacks into three phases.

Intelligence Gathering

Reconnaissance is the starting point in a targeted attack. Without raw data, it's impossible to process the information, and without information, it's impossible to perform reconnaissance. In this phase, the attacker's primary aim is to gather the maximum amount of information to build diverse attack vectors against the target. Publicly available resources are a good place to start—a process sometimes called open source intelligence (OSINT) gathering, which is the process of collecting intelligence from public or openly available resources. Raw information collected using OSINT might not be totally accurate, but it can still provide useful information—for example, the employees in an organization. Some OSINT data can be time sensitive so it's important for attackers to check it regularly until the attack is completed. Because persistence and patience are part of targeted attacks, the information gathering might happen over a long period of time.

Attackers use different modes of information gathering such as passive, semipassive, and active to build a target profile. In passive mode, no actual interaction (traffic) takes place with the target—for example, attackers gather data from various resources on the Internet, some public and some not. In semipassive mode, attackers use generic information-gathering methods that generate normal traffic without suspicion, such as DNS queries or WHOIS lookups. Done correctly, passive and semipassive information gathering won't tip off the target. In active mode, attackers interact with the target to find resources such as open ports or running services to map the target network.

Target profiling includes:

- querying publicly available repositories such as WHOIS and BGP looking glasses for domain and routing information;
- finding websites on the targeted network that have high-risk vulnerabilities, such as cross-site scripting (XSS) and SQL injections (SQLI); and
- fingerprinting organizational networks to check for opened ports, address ranges, network addresses, active machines, firewalls, IDS/IPS, running software, access points, virtual hosts, outdated systems, virtualized platforms, storage infrastructure, and so on, to decipher the network's layout.

Because social engineering is often part of a targeted attack, information on individuals can be invaluable. Human intelligence plays an important role in gathering data related to vendors, employees, and their daily operations in an organization. Useful information can also be culled from social networks such as Facebook or Twitter, phone directories, personal websites, and organizational webpages.

The main tasks in profiling are extracting valuable data from the large quantity of information gathered and building individual or group target profiles: Who are they? What are the details about their environments? The time spent on reconnaissance and profiling can make the difference between an attack's success or failure.

Threat Modeling

Once they collect information about the target, attackers move on to building a threat model. They analyze the gathered information to create a profile of the target and his or her environment—sometimes, they even construct a replica of the target system so that they can test various penetrations without revealing that an attack is imminent. Threat modeling includes:

- mapping the target environment (generating dependencies among objects in the environment to understand their relationships and how they can be used in attacks) and categorizing assets based on their importance and value into primary and secondary targets; and
- assessing risks and threats to determine which domains are most likely to reveal the attack and which domains might invite retaliation.

Threat modeling provides significant information about the weaknesses in an organization's network and employees that could be exploitable. It's a critical step in successfully executing targeted attacks.

Attacking and Exploiting Targets

The final phase is self-explanatory: attackers launch the attack, building on the information gathered and the

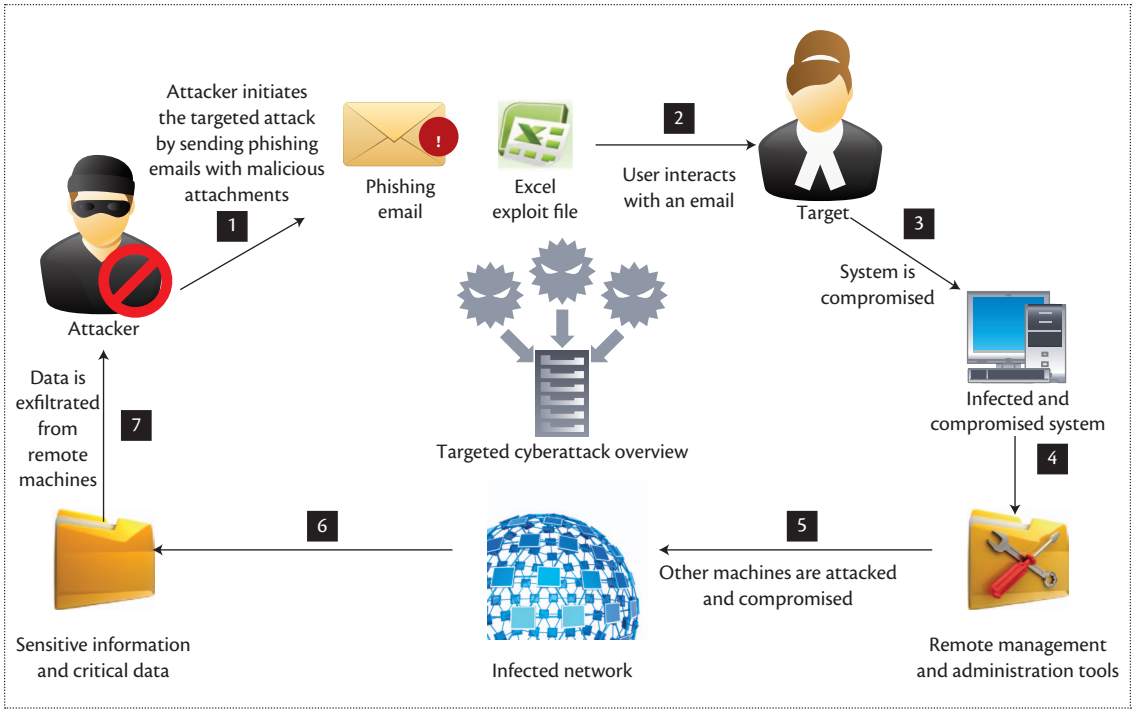

Figure 1. A targeted attack in action. A phishing email carries exploitation code as part of its attachments (DOC, PDF, XLS), similar to how a recent attack compromised the RSA organization.

profile developed. In general, the goal is to load malware onto a target's machine and use that platform to extract information. Targeted attacks can vary significantly in how they're executed, but they have some common patterns.

Drive-by downloads and spear phishing. The attacker uses drive-by download attacks to get the target to download malware from the Internet.[2] To do this, the user is coerced to visit a compromised website, which hosts a hidden Iframe that redirects the user's browser to yet another malicious domain running a Browser Exploit Pack (BEP) that exploits vulnerabilities in the user's browser or plugins to download malware directly into the system.[3] Spear phishing is the primary means of directing a targeted user to a drive-by download site. It's simply targeted phishing—personal and business information in an email convince a user to visit a compromised website, typically via an embedded link in the message. Customized spear-phishing attacks can involve obfuscation to assist in bypassing automated defenses. If spear phishing targets a big fish, such as an executive, it's sometimes called "whaling." Botnets provide a handy mechanism for launching phishing anonymously, especially when targeting a group of users. However, the built-in anonymity of botnets can also be useful when targeting individuals. Figure 1 details a common strategy for conducting targeted attacks by combining spear phishing with drive-by downloads.

The process works as follows. Attackers begin by collecting email addresses to initiate the spear phishing. These addresses might be publicly available, but high-value targets can have private email addresses that will be more susceptible to phishing. An abundance of online outlets offers them for a price. If an attacker has time and resources, the data mining of raw, bulk email dumps can yield useful addresses that might not have shown up through other approaches. The attacker can also search online resources and websites to find targeted user email addresses. Once the desired email addresses are collected, the attacker initiates an automated process of sending email with malicious attachments.

The technique of sending malicious email attachments persists as an effective attack vector. High-value organizations have software to verify email attachments, but file formats such as PDF, XLS, or DOC can get through with embedded malicious code.

One advantage of using email is that it usually slips past peripheral security devices such as firewalls and intrusion detection systems. Security depends on later attachment checking. Once the user inside the organization opens the email, many levels of security have already been bypassed. The malicious code now attacks vulnerable software in the system to expand the exploitation—it can even download more malicious content

from remote parties. The idea is to slip something small and seemingly innocuous through the defenses and then upload more virulent code.

In targeted attacks, the exploit code is usually designed to download a Remote Administration Toolkit that allows the attacker to manage the exploited system remotely. These toolkits are sophisticated software with a variety of built-in tools to manage systems across an intranet. A single compromised host can infect other machines on the network, as internal defenses are often weaker than external ones. The attacker is now inside the fortress.

An excellent example of this type of attack was performed against RSA: attackers used a malicious XLS file embedded with an Adobe Flash exploit (a 0-day vulnerability later drafted as CVE-2011-0609).[4]

Exploiting Web infrastructure. Web application security flaws play an important role in targeted attacks. Two techniques, XSS and SQLI, have been used to conduct mass online attacks in which attackers exploit a specific vulnerability in a large number of servers across the Internet. Specifically, attackers exploit SQLI vulnerabilities to extract database details and use the resulting information to conduct additional attacks. Some attackers combine XSS and SQLI in a hybrid attack known as SQLXSSI, which updates a database of vulnerable websites with malicious Iframes via SQLI. When a user visits a vulnerable website, the content is retrieved from the database, which consists of Iframes pointing to a malicious domain serving malware. In another scenario, a SQL injection attack can reveal a domain's password, allowing malware to be installed directly.

A recent example is the Lizamoon mass SQLI attack, in which an attacker targeted Microsoft servers running ASP.NET and exploited SQL injections using search engines to inject malicious code (Iframes pointing to malware) in the websites. Visiting users to those infected websites were served with malware.[11] Goal.com, MySQL.com, and content delivery networks such as DoubleClick have all been exploited recently to serve malware.[12]

Exploiting communication protocols. Attackers tend to exploit several communication protocols over the Internet to circumvent the normal flow of operations during an attack. They can compromise SMTP servers configured as open relays and use them to spread spear-phishing emails. Insecure FTP and HTTP servers can be used as storage repositories to host malicious programs. Attackers can exploit the DNS protocol to redirect legitimate traffic to a malicious site by manipulating DNS entries. Malware on a system can tweak DNS entries in the host configuration file or perform DLL injection to redirect a browser to different domains. Attackers have executed DNS cache-poisoning attacks, in which a server-side cache is filled with rogue DNS entries that can redirect the user's browser. Of course, some of these activities can impact many more people than the targeted individual or group, which can increase the probability of detection.

Online social network exploitation. The growth of online social networks has provided a bountiful source of personal information as well as opportunities for social engineering. In social networks, users connect to each other and share information. From the perspective of targeted attacks, they provide attackers with an opportunity to exploit trust among friends—a suggested link from a friend is more likely to be opened. Broad-based attacks on social networks indicate the potential with respect to targeted attacks.

Exploiting co-location services. Several different services can exist in a single location. Their numbers are growing, so they're being exploited more frequently and can be useful in targeted attacks.

Virtual hosting is beneficial from a business perspective, but if an attacker compromises one vulnerable website, there's a real possibility that he or she can take control of the entire hosting server. Owning such a server provides multiple places to host malware. Attackers can use two approaches to exploit target servers by using virtual hosting to gain access to them. One compromises a vulnerable website and installs a remote administration shell such as C-99 that allows the host to be compromised. Alternatively, an attacker can write scripts to inject malicious Iframes to infect all hosts on the server.

The cloud provides another platform for hosting malware. If infected, targeted users could compromise the cloud services of thousands of customers. IsecLab's security analysis of Amazon's cloud, Amazon Web Services (AWS), showed exactly this, by highlighting the state of AWS insecurity with respect to security vulnerabilities and exploitation.[5]

Rogue Wi-Fi services and open or weak wireless networks provide yet another attack surface. Weaknesses here allow for information gathering or hosting of malware for drive-by downloads. For example, the soft AP/virtual Wi-Fi functionality in Windows 7 can be turned into a rogue Wi-Fi access point, which is an unauthorized network capable of communicating with the hosts in a network without explicit permission from the administrator. These soft APs are usually hidden because of the Windows Port Address Translation feature, which allows several networks to run behind a single IP address. Consequently, stealthy infections can be initiated using peer-to-peer (P2P) protocols.

Bluetooth services can be subverted or exploited to

gather information or allow access for hosting malware. In 2004, Cabir was the first proof of concept that demonstrated the practicality of Bluetooth malware.[6]

Finally, instant messaging and online chatting are other mediums for spreading malware. As with social networks, this approach exploits the trust of friends and colleagues to increase the chance of users clicking malicious links.

Physical attacks. Hardware provides yet another attack surface. USB sticks are ubiquitous and often shared among individuals—yet another easily crossed trust boundary. Malware can copy itself onto USB sticks that spread malware whenever the stick is used in another system. This technique is especially useful for infecting machines that aren't connected to the Internet (for example, Stuxnet or other government stations). Shared memory devices such as CDs, DVDs, and memory cards can be carriers as well. Recently, teensy human-interface devices were used to conduct physical attacks by user-assisted attackers to execute arbitrary programs using a USB on target machines, including smartphones.[13] By design, a teensy device can emulate itself as a keyboard or a mouse. Once connected with the CPU, it can capture keystroke information and execute payloads. Other types of devices include pineapple Wi-Fi and Pwn Plug, which attackers can use for wireless hacking.

Recent research has focused on hardware preloaded with backdoors.[14] A backdoor provides a window for installing malware. An obvious advantage of preloaded hardware is that it bypasses all Internet security because it's embedded in the hardware and moves into an environment as an inherent component of the machine. Hardware-based backdoors (malicious firmware) have the capability to access the kernel and use a Direct Memory Access (DMA) engine.

Elements of Targeted Attacks

Several elements are used frequently in targeted attacks.

Malware Infection Frameworks

Malware infection frameworks (MIFs) are used extensively for spreading malware, but they're also useful for targeted attacks that aim to control machines remotely. MIFs have evolved over time. First-generation MIFs typically used the Internet Relay Chat (IRC) protocol, the second generation used P2P protocols, and the current third generation uses Hypertext Transfer Protocol (HTTP) for running C&C services. Not surprisingly, hybrid MIFs are also deployed that use a mix of various capabilities of different generations (first, second, and third) botnets. MIF attacks use the C&C server to send commands to infected machines, instructing them to perform nefarious operations. Because of their sophisticated design, MIFs have proven useful in controlling target machines.

Botnets such as SpyEye and Zeus have used MIFs in targeted attacks against online banks.[7] For example, SpyEye has a built-in plug-in that attacks Bank of America websites. If attackers know that their target banks online at Bank of America, these existing tools are perfect.

Browser Exploit Packs and Glype Proxies

BEPs such as BlackHole and Phoenix are composed of browser-based exploits bundled together into one framework.[3] Browsers send identifying information in a user-agent HTTP header with every server request. Based on the information in the user-agent header, the attacker can fingerprint the victim's machine to determine the OS, browser version, installed plug-ins, and so on. With this information, the BEP can automatically serve the appropriate exploit.

An attacker can install a BEP in a domain that a target commonly visits, infect legitimate websites and inject an Iframe that points toward the malicious domain running the BEP, or direct victims to infected sites via phishing. Several browser design flaws such as spoofing, URL obfuscation, and so on contribute in spreading of malware.[8] In drive-by downloads, BEPs load malware onto the victim's machine.

Web-based Glype proxies are used to surf the World Wide Web anonymously. They're an efficient way to gather and find information about targets, letting attackers anonymously search for vulnerable targets on the Internet. These vulnerable targets become part of targeted attacks' initialization phase because they can be used as a launching pad for targeted infections.

RATs and Rootkits

Remote Administration Toolkits/Remote Access Toolkits (RATs) and rootkits play a crucial role in targeted attacks once a machine has been compromised. RATs such as Poison Ivy are installed on infected computers to facilitate remote management. In the GhostNet attack, Chinese attackers installed their own Ghost RAT on infected computers. Rootkits are stealthy programs that reside in an infected computer's OS and hide the infections. Once a rootkit is installed, it downloads a RAT to communicate with C&C servers. ZeroAccess and TDL rootkits have been used recently in targeted attacks. These rootkits are sophisticated and have the capability to hook critical functions in the processes used to manage the communication flow. Once this is done, these rootkits gain control over the infected machine and download other malware into the system.[15]

Morphing and Obfuscation Toolkits

To avoid detection by antivirus solutions, malware is

usually morphed or obfuscated to hide its identity. Morphing is done primarily on HTML code, JavaScripts, Flash, executables (EXEs) and dynamic-link libraries (DLLs), and Iframes used in malware propagation and distribution. Several classes of toolkits allow morphing and obfuscation:

- *Packers* compress the malware, reducing the malicious executable's size and easing infiltration.
- *Crypters* encrypt malware to bypass signature-based antivirus protection.
- *Code protectors* embed anti-debugging and anti–virtual machine (VM) code in the malware to help prevent it from being debugged and executed in a controlled VM environment. These techniques increase the difficulty of detecting the malware.
- *Packagers* masquerade the malware as, or repackages it in, legitimate software. They might pack multiple malware instances together.

These services, readily available in the underground market, are used extensively to make malware difficult to detect.

Interface with an Underground Market

An underground market exists for malware and personal information, both of which are needed for targeted attacks. This underground market serves hackers from around the world, and malicious tools are exchanged regularly. As a result, the most sophisticated techniques are available—for a price.

Users' information including credit card numbers, personal information, and account passwords are available for very low prices. This information is primarily extracted from botnets. Infection services are also available; access to compromised domains is sold for few dollars, so attackers can use them without investing time in finding vulnerable domains. Attackers might place BEPs at these domains.

Software obfuscation services are available, so malicious programs can slip past host and network-based protection mechanisms. If money is the goal of an attack, the attacker can hire mules (agents) to launder online finances into cash.

MIFs, BEPs, rootkits, and 0-day exploits are also available underground; the most sophisticated ones can be very expensive.

Preventive and Precautionary Measures

Detecting targeted attacks can be difficult. A robust traffic-monitoring and network-analysis system as part of a strong perimeter defense is helpful but not sufficient. Behavioral analysis can also be useful.

System defenses should be equipped to detect malicious traffic by dissecting C&C protocols using DNS intelligence, communication patterns, domain and netblock reputation, geolocation, and data origin. After successful detection, the system should raise alerts and block the traffic. Traditional intrusion detection and prevention techniques are useful but insufficient because targeted attacks use the latest attack methods and exploits that can easily bypass these network perimeter security solutions.

The monitoring system should also dissect attachments such as PDF, DOC, and XLS and perform deep inspection to trace the exploit payloads in the file. However, deep packet inspection can be costly. Ideally,

Motives behind Targeted Attacks

Every attack has a motive behind it—often more than one. Frequently, the primary one is money, but national and industrial espionage also play a major role:

- Targeted attacks are used extensively for espionage,[1] in which a country compromises the target country's critical infrastructure to spy on its internal operations.
- Attacks often target IP, an extremely valuable commodity that can benefit a country by improving its military or its industry. Inconsistent and nonexistent international IP and patent laws mean that stolen IP can be used openly in many countries.
- Stuxnet demonstrates that targeted attacks can sabotage critical infrastructure,[2] which can achieve both military and commercial objectives.
- Attacks on social networks can reveal a wealth of information about people—especially public figures—and their habits.

A recent report by the US Government Accountability Office suggests yet another motivation for a targeted attack: tampering with military-grade electronic parts.[3] Dishonest vendors have used legitimate numbers from authentic parts to sell substandard products. Consider the scenario of a targeted attack in which an attacker compromises a vendor's website and tampers with its information to allow degraded electronic parts to be sold to the military. We haven't yet seen this scenario in the wild, but it's still a grave risk to national security.

References

1. G.O. Hara, "Cyber-Espionage: A Growing Threat to the American Economy," 2011; http://commlaw.cua.edu/res/docs/articles/v19/19-1/11-v19-1-O-Hara-Final.pdf.
2. A. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-Based Load Altering Attacks against Smart Power Grids," 2011; www.webpages.ttu.edu/amohseni/MRLGjTSG11.pdf.
3. *Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms*, GAO-12-375, US Government Accountability Office, Feb. 2012; www.gao.gov/assets/590/588736.pdf.

suspicious code should be trial-executed in a virtual environment before being accepted, but this isn't generally feasible. Monitoring systems should also be updated regularly and be set up to detect the anomalies in both outbound and inbound traffic to prevent data exfiltration.

To reduce the impact of targeted attacks, we can take several proactive steps:

- Security configurations such as firewalls and host-based antivirus solutions should be kept up to date. In particular, firewalls should be checked regularly to ensure that they're working effectively. Websites should be audited regularly.
- Browsers are the primary window to the Internet. Like any other piece of software, they should have the latest patches and updates. If possible, users should have browser-based protection such as NoScript (Firefox) to filter illegitimate scripts and reduce that attack vector. For other browsers such as Internet Explorer and Google Chrome, the default client-side XSS filters should be activated to prevent the execution of malicious scripts.
- Always think twice before clicking a link, especially ones embedded in emails or other communication such as instant messaging or Twitter. Attackers use social engineering techniques to convince users to click. Users should keep their OS and software up to date with the latest patches and updates and avoid downloading pirated software because attackers use these platforms to circulate malware.
- Organizations should practice good physical security. Allowing malicious people into facilities can make the attacker's job easier.
- User education is essential. Regular sessions on applied security should be conducted to spread information about cybersecurity and steps to make online use secure. Users shouldn't send any sensitive information such as account numbers, PINs, or credit card numbers in emails. They should be educated enough to distinguish between legitimate email and a phishing scam and should use strong passwords with required complexity. Use of personal USB devices should be restricted, and an appropriate security policy should be defined with respect to hardware.

These protection measures aren't the complete solution against targeted attacks. However, practicing these principles can significantly reduce the impact of targeted attacks. To build a strong defense, we need a war-fighting system that integrates architectural and assessment components and achieves survivability by implementing a polymorphic system that can sustain itself in the attack environment.[9] In addition, we need laws such as the Protecting Cyberspace as a National Asset Act that allows the highest authority to deactivate some parts of Internet during emergency situations.[10]

Targeted attacks go after individuals, groups of individuals, and businesses. They're usually perpetrated for financial gain (see the related sidebar), but they've also helped attackers steal national secrets and critical IP. In some cases, these attacks appear to be government sponsored or condoned. But in all cases, international law lags behind technical reality, so prosecuting perpetrators is difficult if not impossible. Understanding these attacks is the first step in responding to them. ■

References

1. F. Li, A. Lai, and D. Ddl, "Evidence of Advanced Persistent Threat: A Case Study of Malware for Political Espionage," *6th Int'l Conf. Malicious and Unwanted Software* (Malware 11), IEEE, 2011, pp. 102–109.
2. M. Cova, C. Kruegel, and G. Vigna, "Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code," *Proc. 19th Int'l Conf. World Wide Web*, ACM, 2012; http://doi.acm.org/10.1145/1772690.1772720.
3. A.K Sood and R.J. Enbody, "Browser Exploit Packs—Death by Bundled Exploits," *Proc. 21st Virus Bulletin Conf.*, 2011; http://secniche.blogspot.com/2011/10/virus-bulletin-2011-conference-browser.html.
4. R. Branco, "Into the Darkness: Dissecting Targeted Attacks," Qualys Blog, Nov. 2011; https://community.qualys.com/blogs/securitylabs/2011/11/30/dissecting-targeted-attacks.
5. M. Balduzzi et al., "A Security Analysis of Amazon's Elastic Compute Cloud Service," *Proc. 27th Ann. ACM Symp. Applied Computing*, ACM, 2012; http://doi.acm.org/10.1145/2245276.2232005.
6. P. Ferrie and P. Szor, "Cabirn Fever," *Virus Bulletin Magazine*, Aug. 2004; http://vallejo.cc/proyectos/cabir/cabir.pdf.
7. H. Binsallee et al., "On the Analysis of the Zeus Botnet Crimeware Toolkit," *IEEE 8th Ann. Conf. Privacy, Security and Trust* (PST), IEEE, 2010; http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5593240&isnumber=5593224.
8. A.K Sood and R.J. Enbody, "Browser User Interface Design Flaws," *Crosstalk*, May 2011; www.crosstalkonline.org/storage/issue-archives/2011/201105/201105-Sood.pdf.
9. H. Okhravi, J.W. Haines, and K. Ingols, "Achieving Cyber Survivability in a Contested Environment Using a Cyber Moving Target," *High Frontier: The Journal for Space and Cyberspace Professionals*, May 2011; http://web.mit.edu/ha22286/www/papers/journal/Achieving_Cyber_Survivability_in_a_Contested_Environment_Using_a_Cyber_Moving_Target.pdf.

10. N. Christin, "On Critical Infrastructure Protection and International Agreements," School of Public Policy, Univ. of Maryland, Mar. 2011; www.cissm.umd.edu/papers/files/on_critical_infrastructure_protection_and_international_agreements__033111__final.pdf.
11. W. Huang, C. Hsiao, and N. Lin, "Mass Meshing Injection: Sidename.js (now cssminibar.js) Ongoing," Armorize Malware Blog, 15 June 2011; http://blog.armorize.com/2011/06/mass-meshing-injection-sidenamejs.html.
12. W. Huang, C. Hsiao, and N. Lin, "Malvertising on Google Doubleclick Ongoing," Armorize Malware Blog, 25 Aug. 2011; http://blog.armorize.com/2011/08/malvertising-on-google-doubleclick.html.
13. A. Stavrou and Z. Wang, "Exploiting Smart-Phone USB Connectivity for Fun and Profit," BlackHat DC Conf., 2011; https://media.blackhat.com/bh-dc-11/Stavrou-Wang/BlackHat_DC_2011_Stavrou_Zhaohui_USB_exploits-wp.pdf.
14. J. Rutkowska, "Thoughts about Trusted Computing," EuSecWest Conf., 2009; http://invisiblethingslab.com/resources/misc09/trusted_computing_thoughts.pdf.
15. "McAfee Threats Report: First Quarter 2012," McAfee, 2012; www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2012.pdf.

Aditya K Sood is a senior security researcher/consultant and PhD candidate at Michigan State University. His research interests include Web security, malware analysis, mobile security, and penetration testing. Sood has an MS in cyber law and information security from the Indian Institute of Information Technology, India. Contact him at soodadit@cse.msu.edu.

Richard J. Enbody is an associate professor in the Department of Computer Science and Engineering at Michigan State University. His research interests include computer security, computer architecture, Web-based distance education, and parallel processing. Enbody has a PhD in computer science from the University of Minnesota. Contact him at enbody@cse.msu.edu.