Targeted Cyber Attacks

By SearchSecurity and Syngress

Published: 2014-12-16 · Archived: 2026-04-05 12:36:14 UTC

The following is an excerpt from the book Targeted Cyber Attacks *by authors Aditya Sood and Richard Enbody and published by Syngress. This section from chapter three explains different attack models and vectors used to attack targets.*

Infecting the Target

In this chapter, we discuss about the most widely used mechanisms to initiate targeted attacks. This chapter not only discusses the attack model, but also details the different vectors used to attack the targets. In the last chapter, we covered the reconnaissance and information gathering tactics used by attackers to gain insight into the target environment and behavior. We continue from there and discuss how the attackers infect the targets directly or indirectly for compromise.

We classify the attacks used for infecting the target into two ways:

1. Direct attacks, in which target network is exploited using vulnerabilities to gain access to potential critical systems or to gain critical information that can be used to launch indirect attacks, for example, exploitation of web vulnerabilities.
2. Indirect attacks, in which attackers use a number of layered attacks to accomplish the process of intrusion, for example, spear phishing and waterholing attacks.

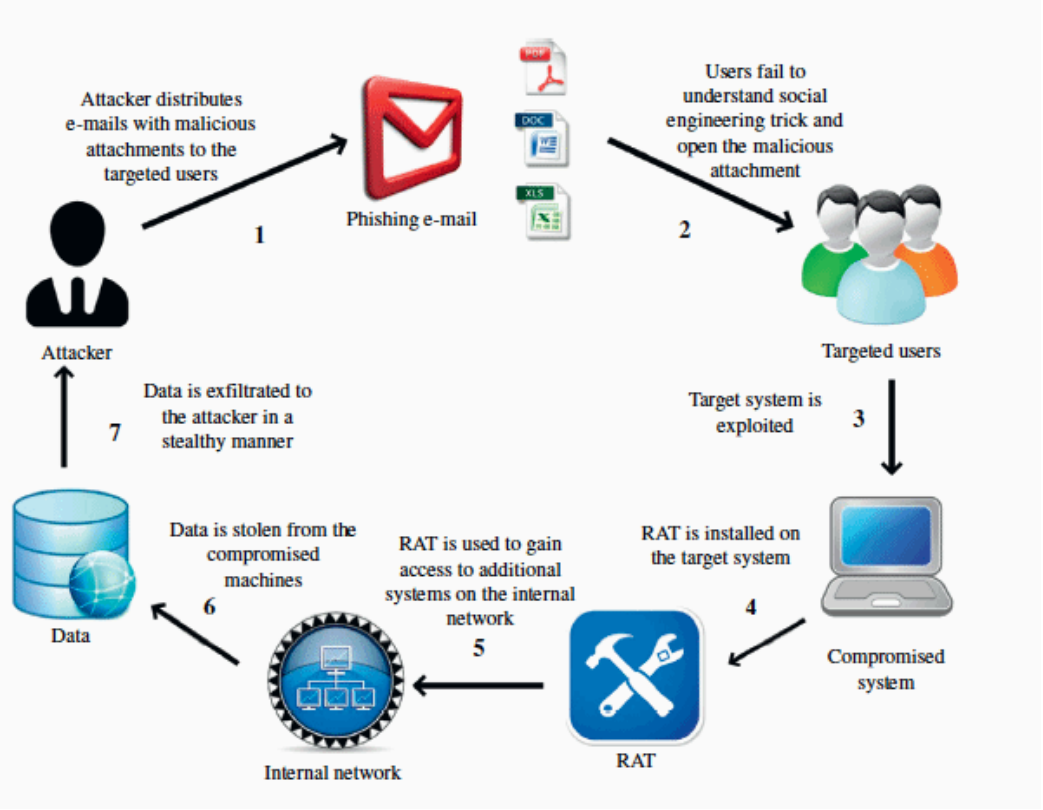
3.1 Elements used in incursion

It is important to understand the nature of the components that are used to conduct successful targeted attacks. The most widely used and effective components in targeted attacks are discussed below:

- *Social engineering*: Social engineering deals with the techniques of manipulating the user's psychology by exploiting trust. Social engineering often exploits a user's poor understanding of technology as users are unable to determine and fail to understand the attack patterns used in targeted attacks. Social engineering is one of the predominant components of targeted attacks because it helps to initiate the attack vector.
- *Phishing e-mails*: The term phishing was first used in the Internet literature in 1996 by the hacker group who stole America Online (AOL) accounts' credentials. Phishing is originated from Phreaking which is considered as the science of breaking into phone networks using social engineering. A phishing attack is also based on the concept of social engineering in which users are tricked to open malicious attachments or embedded links in the e-mails. These e-mails are designed and generated to look legitimate and potentially treated as baits or hooks to trap the targets (analogous to catch fishes in sea of Internet users). Phishing attacks are the most widely used attack vehicles in targeted attacks.
- *Vulnerabilities and exploits*: Vulnerabilities in web sites and software components, both known and unknown, can be exploited as part of an attack. The most virulent exploits are based on zero-day vulnerabilities for which details are not publicly available. They are often a component of effective targeted attacks.
- *Automated frameworks*: Automated frameworks are used in targeted attacks to ease the burden of exploitation from the attacker's side. The emergence of automated exploit kits has resulted in sophisticated and reliable exploitation of browsers. This is because a number of exploits are bundled together in one framework that fingerprints the browser for vulnerable component before serving the exploit. As a result, only vulnerable browsers are exploited and framework does not react to browsers that are patched. In targeted attacks, Remote Access Toolkits (RATs) are deployed on infected machines to ease data theft and command execution.
- *Advanced malware*: Based on the nature of targeted attacks, advanced malware plays a crucial role in successful campaigns. The idea behind designing advanced malware is to perform operations in a stealthy manner and to go undetected for a long period so that the attack persists. Stealthy rootkits are designed for these purposes as rootkits hide themselves under the radar where antivirus engines fail to detect them. However, less sophisticated malware has also been used in targeted attacks.
- *Persistent campaigns*: Attackers prefer to launch small campaigns in targeted attacks for a long duration of time. The motive is to persist and to monitor the target over a period of time to collect high quality and high volumes of data at the same time. After discussing the elements of targeted attacks, the following section talks about the different attack models used to conduct targeted attacks.

3.2 Model A: Spear phishing attack: Malicious attachments

Spear phishing attacks have been used for a long time. It is different from a generic phishing attack because spear phishing attack is targeted against a particular individual or organization. Traditional phishing attacks have been used to capture sensitive information from the end users by duping them with social engineering tactics or simply exploiting their naïve understanding of technology. Malware authors have used phishing attacks to spread malware broadly across the Internet. In targeted attacks, spear phishing plays a very effective role. Figure 3.1 shows a very generic model of spear phishing attack that is used in the wild.



Aditya K Sood and Richard Enbody

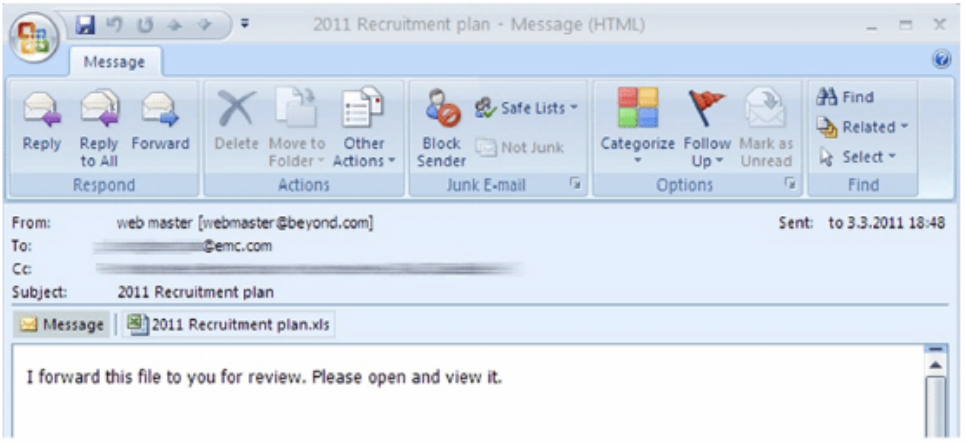
Figure 3.1: Spear phishing attack model use to launch targeted attacks.

The model can be explained as follows:

- The attacker conducts spear phishing attack in which devious e-mails carrying exploit codes in the form of attachments are sent to the targets.
- Target audiences believe those e-mails to be legitimate and open the attachment.
- The exploit code executes the hidden payload and exploits vulnerability in an application component to execute specific commands in the context of end-user system.
- Once the exploit is successfully executed, malware is downloaded on the end-user system to compromise and infect it.
- The malware further downloads a RAT to take complete control of the end-user system and to attack other systems on the internal network to steal potential data.
- Once the data is stolen, different channels or tunnels are used by malware to transmit the data to offshore servers managed by the attacker.

A spear phishing attack was used against the RSA Corporation which is named as "RSA Secure ID Breach." The overall damage of this attack is not determined, but it is assumed that attackers stole Secure ID product information and number of token seeds used by several companies (organizations) such as Bank of America, Lockheed, JPMorgan Chase, Wells Fargo, and Citigroup. This indicates that RSA breach resulted in the compromise of Secure IDs (authentication tokens) of a large set of users. As a result of this, the majority of the companies had to restate the authentication tokens and RSA agreed to pay the managing cost related to customer service which was approximately 95 million dollars [1] as a whole. In RSA Attack, the attacker targeted two

different batches of employees over a period of 2 days with a well-crafted phishing e-mail. The e-mail carried an XLS file containing exploit code of a then unknown vulnerability. Figure 3.2 shows how the phishing e-mail targeting RSA looked like. There could be other variants, but this one was widely distributed. The attachment carried a "2011 Recruitment Plan.xls" file embedded with an exploit code. The attachment carried an exploit code of a zero-day for Adobe Flash Player vulnerability which was later identified as CVE-2011-0609. Once the exploit was successfully executed, the malware took control of internal servers. The attacker then used a RAT named as Poison Ivy [3] to take persistent control over the target servers. The stolen information was compressed and exfiltrated from the infected system using the FTP. The complete technical analysis of the exploit used in RSA breach shows how strongly the vulnerability was exploited in the embedded SWF (Adobe file format) component in the XLS file [4].



Syngress

Figure 3.2: Targeted e-mail used in RSA spar phishing e-mail. Source: Wired.com [2].

3.3 Model B: Spear phishing attack: Embedded malicious links

In the model discussed above, the attacker can alter the attack vector. Instead of sending malicious attachments, the attacker embeds malicious links in the spear phishing e-mails for distribution to the target audience. On clicking the link, user's browser is directed to the malicious domain running a Browser Exploit Pack (BEP) [5]. Next, the BEP fingerprints the browser details including different components such as plugins to detect any vulnerability, which can be exploited to download malware. This attack is known as a drive-by download attack in which target users are coerced to visit malicious domains through social engineering [6]. The attacker can create custom malicious domains, thus avoiding the exploitation of legitimate web sites to host malware. The custom malicious domains refer to the domains registered by attackers which are not well known and remain active for a short period of time to avoid detection. This design is mostly used for broadly distributed infections rather than targeted ones. However, modifications in the attack patterns used in drive-by download make the attack targeted in nature. The context of malware infection stays the same but the modus operandi varies.

Table 3.1 An Overview of Structure of E-mails Used in Targeted Attacks in Last Years

Targeted E-Mail Theme	Date	Subject	Filename	CVE
Job | Socio – Political ground	07/25/2012	• Application • Japanese manufacturing • A Japanese document • Human rights activists in China	• New Microsoft excel table.xls (password: 8861) • q{}(24.7.1).xls • 240727.xls • 8D823C0A3DADE8334B6C1974E2D6604F.xls • Seminiar.xls	2012-0158
Socio - Political ground	03/12/2012–06/12/2012	• TWA's speech in the meeting of United States Commission for human rights • German chancellor again comments on Lhasa protects • Tibetan environmental situations for the past 10 years • Public Talk by the Dalai Lama_Conference du Dalai Lama Ottawa, Saturday, 28th April 2012 • An Urgent Appeal Co-signed by Three Tibetans • Open Letter To President Hu	• The Speech.doc • German Chancellor Again Comments on Lhasa Protects.doc • Tibetan environmental statistics.xls • Public Talk by the Dalai Lama.doc • Appeal to Tibetans To Cease Self-Immolation.doc • Letter.doc	2010-0333
Socio - Political ground	01/06/2011	Three big risks to China's economy in 2011	Three big risks to China's economy in 2011.doc	2010-3333
Socio - Political ground	01/24/2011	Variety Liao taking – taking political atlas Liao	AT363777.7z | 44.doc	2010-3970
Economic situation	03/02/2012	Iran's oil and nuclear situation	Iran's oil and nuclear situation.xls	2012-0754
Nuclear operations	03/17/2011	Japan nuclear radiation leakage and vulnerability analysis	Nuclear Radiation Exposure and Vulnerability Matrix.xls	2011-0609
Nuclear weapon program	04/12/2011	Japan's nuclear reactor secret: not for energy but nuclear weapons	Japan Nuclear Weapons Program.doc	2011-0611
Anti-trust policy	04/08/2011	Disentangling Industrial Policy and Competition Policy in China	Disentangling Industrial Policy and Competition Policy in China.doc	2011-0611
Organization meeting details	06/20/2010	Meeting agenda	Agenda.pdf	2010-1297
Nuclear security summit and research posture	04/01/2010	Research paper on nuclear posture review 2010 and upcoming Nuclear security summit	Research paper on nuclear posture review 2010.pdf	2010-0188
Military balance in Asia	05/04/2010	Asian-pacific security stuff if you are interested	Assessing the Asian balance.pdf	2010-0188
Disaster relief	05/09/2010	ASEM cooperation relief on Capacity Building of disaster relief	Concept paper.pdf	2010-0188
US-Taiwan relationship	02/24/2009	US-Taiwan exchange program enhancement	A_Chronology_of_Milestone_events.xls US_Taiwan_Exchange_in-depth_Rev.pdf	2009-0328
National defense law mobilization	03/30/2010	China and foreign military modernization	WebMemo.pdf	2009-4324
Water contamination in Gulf	07/06/2010	EPA's water sampling report	Water_update_part1.pdf Water_update_part2.pdf	2010-1297
Rumours about currency reforms	03/24/2010	Rumours in N Korea March 2010	Rumours in N Korea March 2010.pdf	2010-0188
Chinese currency	03/23/2010	Talking points on Chinese currency	EAIBB No. 512.pdf	2009-4324
Trade policy	03/23/2010	2010 Trade Policy Agenda	The_full_Text_of_Trade_Policy_Agenda.pdf	2010-0188
Chinese annual plenary session	03/18/2010	Report on NPC 2010	NPC Report.pdf	2009-4324
Unmanned aircraft systems	01/03/2010	2009 DOD UAS ATC Procedures	DOD_UAS_Class_D_Procedures[signed].pdf	2008-0655
Human rights	02/26/2009	FW: Wolf letter to secretary Clinton regarding China human rights	2.23.09 Sec. of State Letter.pdf	2009-0658
NBC interview	09/08/2009	Asking for an interview from NBC journalist	Interview Topics.doc	Unknown
Chines defense	01/28/2010	Peer-Review: Assessing Chinese military transparency	Peer-Review - Assessing Chinese military transparency.pdf	2009-4324
Asian Terrorism report	10/13/2009	Terrorism in Asia	RL34149.pdf	Unknown
Country threats	01/07/2010	Top risks of 2010	Unknown	Unknown
Counter terrorism	05/06/2008	RSIS commentary 54/2009 ending the LTTE	RSIS.zip	Unknown
Anti-piracy mission	01/13/2010	The China's navy budding overseas presence	Wm_2752.pdf	Unknown
National security	01/20/2010	Road Map for Asian-Pacific Security	Road-map for Asian-Pacific Security.pdf	2009-4324
US president secrets	11/23/2009	The three undisclosed secret of president Obama Tour	ObamaandAsia.pdf	2009-1862

Syngress

Table 3.1 An Overview of Structure of E-mails Used in Targeted Attacks in Last Years

Table 3.1 shows the different types of spear phishing e-mails with attachments that have been used in the last few years to conduct targeted cyber attacks. The "Targeted E-mail Theme" shows the type of content used by attackers in the body of e-mail. The themes consist of various spheres of development including politics, social, economic, nuclear, etc. The model of waterholing attack discussed in the following section is a variant of drive-by download attack.

3.4 Model C: Waterholing attack

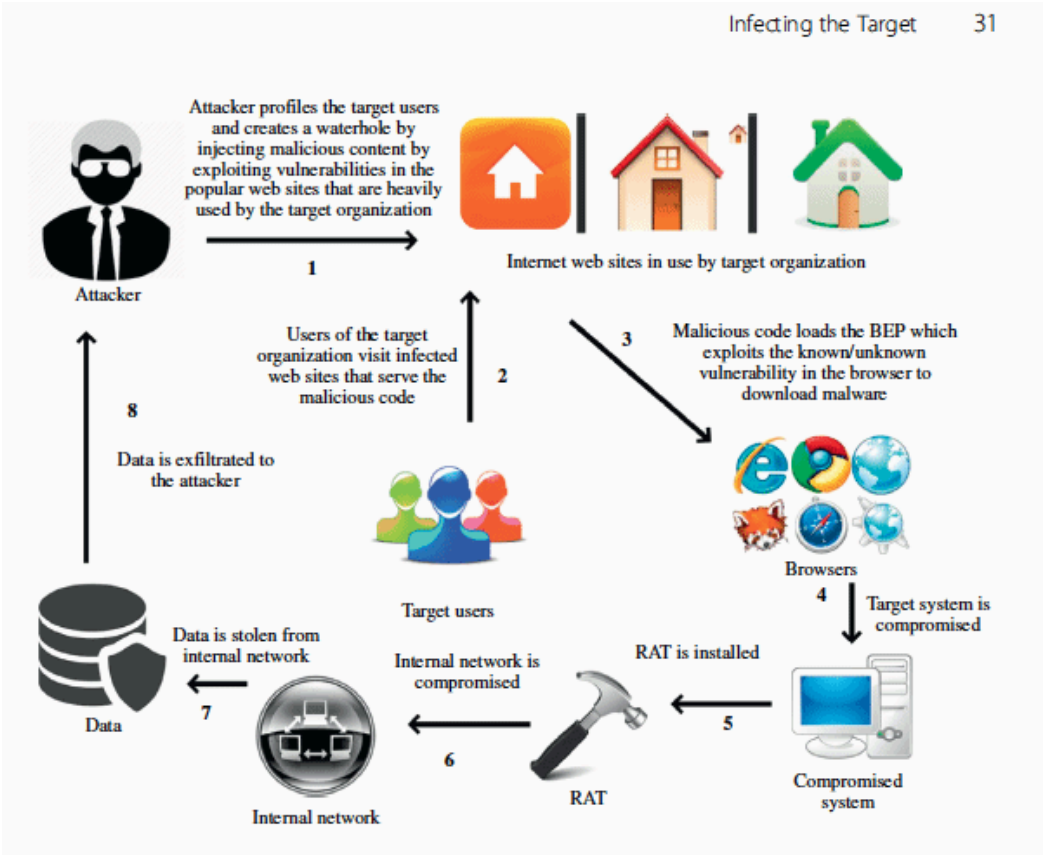
A waterholing attack [7] is a term coined by RSA researchers. In general terminology, waterholes are created to attract animals to hang out around a desired area so that hunting becomes easier. Waterholes are treated as traps

for hunting animals. The same concept applies to Internet users (targeted users) in which specific web sites are infected to create waterholes.

Waterholing is not a new attack vector, but a variant of a drive-by download attack in which browsers are exploited against a specific vulnerability to download malware on the end-user systems. The primary difference between the traditional drive-by download and waterholing attack is in the manner the attack is initiated. In waterholing, the attacker guesses or uses the stolen data (profiling users of the target organization) to determine the known set of web sites which are visited by the employees of target organization. In case of waterholing, spear phishing is not used as a mode of engaging users, instead the knowledge of their surfing habits is used to plant the attack. Users are not coerced through e-mails or attachments to perform a specific action rather the attacker waits for the user to visit legitimate web sites that are infected. Figure 3.3 presents a model of waterholing attack.

The model is explained as follows:

- The attacker profiles the target users based on the Open Source Intelligence (OSINT) methods or stolen information to determine the Internet surfing habits of the users to find a set of web sites that are frequently visited by them.
- Once the attacker profiles the users, the next step is to detect vulnerabilities in those web sites (likely a subset) and exploit them to inject malicious code. As a result, users visiting those web sites will get infected with malware.
- The attacker waits for the users to visit the infected web sites so that malware is installed onto their systems using the drive-by download technique.
- Once the browser is exploited and system is infected with malware, a RAT is downloaded onto the compromised system. The RAT allows the attacker to administer the system and to attack other systems on the internal network.
- Once compromised, data is stolen and exfiltrated to some attacker controlled system on the Internet.



Aditya K Sood and Richard Enbody

Figure 3.3: Waterholing attack model.

The waterholing attack has been broadly deployed and a number of cases have been noticed in the last few years. The Tibetan Alliance of Chicago [8] was hacked using waterholing to attack users visiting their web site. Malicious code was placed inside an iframe (an inline frame used to load HTML/JS content from third-party server) that redirected a user's browser to a malicious domain serving a backdoor. The US Department of Labor was compromised by a waterholing attack and was shut down for a long time [9]. VOHO [10] is yet another targeted attack based on the concept of waterholing. VOHO name is coined by RSA and considered as an attack campaign in which stolen FTP account credentials are used to implant malicious code on target web sites specifically present in Washington DC and Massachusetts. The infections were triggered across multiple organizations including defense, technology, educational, and government. The attackers installed Ghost RAT Trojan on the compromised machines for further maneuvering the operations happening on the system. This attack shows how stolen information is used in the targeted attacks to initiate infections which ultimately results in compromising the target systems.

3.5 Model D: BYOD as infection carriers: USB

Universal Serial Bus (USB) devices such as thumb drives or portable hard disks are an excellent medium for carrying infections from one place to another when critical systems are not connected to the Internet. Targeted attacks against critical infrastructure such as Industrial Control Systems (ICSs) are on rise and those installations are sometimes not directly connected to the Internet. Targeted attack known as Stuxnet had the capability to

spread through an infected USB device which could be plugged into critical systems for performing certain operations. ICS Computer Emergency Response Team (CERT) released a report detailing a number of cases that have happened as a result of USB infection [11]. USB devices are infected to execute code in two different modes. First, an autorun.inf file calls the hidden malware present in the USB itself. Second, rogue link files (.lnk) are generated which are linked to the malicious code. When a user clicks the shortcut, malicious code is executed.

In an ICS environment, USB devices are used to backup configurations and provide updates to the computers running in a control network environment. Generally, to manage these control systems, an individual (third-party vendor or technician) is required, who manually performs operations on the critical systems. For that, a USB is used as a storage and backup device, but at the same time it acts as a carrier if infected with malware. This is a big problem with Bring Your Own Device (BYOD) arrangements which could result in compromise of the complete network when the device is plugged in and connected to the Internet. ICS-CERT reported an issue of the same kind where a third-party vendor used an infected USB to perform updates on the turbine control systems which got infected and failed to start for 3 weeks resulting in a considerable business loss. Similarly, one of a New Jersey company's critical systems [12] were infected to take control of heating vaults and air-conditioning systems. Carelessness in handling USB devices can result in serious security compromises.

3.6 Model E: Direct incursion: Network exploitation

Exploitation of vulnerabilities in the target network is a preferred mode of direct incursion. The information gained from this process can be used in conjunction with other indirect attacks. Attackers always look forward or keep an eye on target's network infrastructure and try to detect exploitable vulnerabilities. As a result of successful exploitation, advanced malware is planted on the server side to gain complete control of the critical servers. This automatically infects all the associated systems in the network.

In recent years, several firms have been hacked as a result of the targeted attacks which resulted in a substantial loss to the business of different organizations. One notorious targeted attack was launched against Bit9 [13,14]. Attackers exploited the Internet facing web server of Bit9 and conducted a successful SQL injection that provided access to the critical systems of Bit9. SQL injection is an attack technique in which unauthorized SQL statements are injected as input values to different parameters in the web applications to manipulate the backend database. In addition to data stealing, SQL injections are used to inject malicious iframes in the Internet facing vulnerable web applications. Due to insecure deployment of web applications (web server) in Bit9, SQL injection resulted in the exposure of Bit9 certificates which were stolen and used to sign malware, specifically the kernel mode drivers. Such certificates are particularly useful because newer version of Windows requires signing of the kernel mode drivers. The attackers planted advanced malware known as HiKit [15,16], a rootkit which is advanced and persistent in nature. The motive behind installation of HiKit was to infect other Bit9 systems in the network or Bit9 customers (organizations). Once the systems were infected with HiKit, attackers deployed their own self-signed certificates and installed them into local trust stores pretending to be a Root CA. In addition, attackers also turned off the kernel driver signing process by altering the registry entries. This case shows that the exploitation of Internet facing web infrastructure could result in launching targeted attacks.

A number of infection models used in targeted attacks have been discussed. Attacker can also tune some broad-based malware spreading mechanisms such as malvertisements and social network infections and use them in collaboration with targeted attacks. Malvertisements are heavily used to fool users in believing that the content

presented by the server is legitimate and they execute malicious code from the third-party domain. The attackers can also host malicious software such as fake Adobe Flash software on the infected domains to lure the victims to install malware. Social network infections result in chain infections which means, if one user in the network is infected, it can result in spreading subsequent infections to the complete network easily. Since user base is so large in social networks such as Facebook, attackers are exploiting this fact at a large scale. However, these infection mechanisms are noisy in nature which means these tactics can be easily detectable by existing defenses. In order to use these tactics in the context of targeted attacks, the attackers have to take additional efforts to build stealthy malware which can be spread under the radar without detection.

In this chapter, we have discussed about different strategies opted by attackers to engage target and initiate infections. Spear phishing and waterholing models are heavily used in targeted attacks, thereby resulting in successful infections. In majority of these models, social engineering plays a vital role in initiating the infection process. Overall, the infection models presented in this chapter provide a launchpad for the attackers to compromise the target systems.

About the authors:

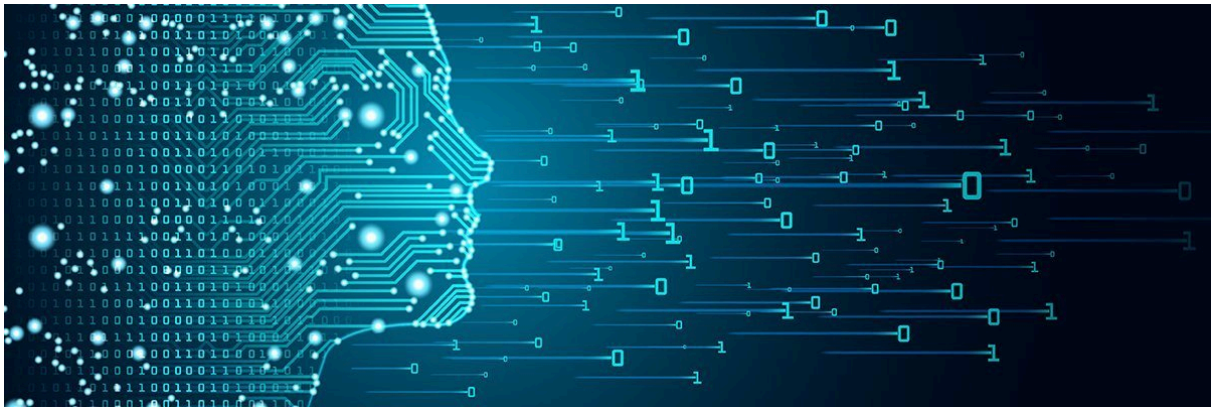
Aditya K Sood (Ph.D) is a senior security researcher and consultant. Dr. Sood has research interests in malware automation and analysis, application security, secure software design and cybercrime. He has worked on a number of projects pertaining to penetration testing specializing in product/appliance security, networks, mobile and web applications while serving Fortune 500 clients for IOActive, KPMG and others. He is also a founder of SecNiche Security Labs, an independent web portal for sharing research with security community. He has authored several papers for various magazines and journals including IEEE, Elsevier, CrossTalk, ISACA, Virus Bulletin, Usenix and others. His work has been featured in several media outlets including Associated Press, Fox News, Guardian, Business Insider, CBC and others. He has been an active speaker at industry conferences and presented at DEFCON, HackInTheBox, BlackHat Arsenal, RSA, Virus Bulletin, OWASP and many others. Dr. Sood obtained his Ph.D from Michigan State University in Computer Sciences.

Dr. Richard Enbody is an Associate Professor in the Department of Computer Science and Engineering. He joined the faculty in 1987 after earning his Ph.D. in Computer Science from the University of Minnesota. Richard received his B.A. in Mathematics from Carleton College in Northfield, Minnesota in 1976, and spent six years teaching high school mathematics in Vermont and New Hampshire. Richard has published research in a variety of areas, but mostly in computer security and computer architecture. He holds two nanotechnology patents from his collaboration with Physicists. Together with Bill Punch he published a textbook using Python in CS1: The Practice of Computing Using Python (Addison-Wesley, 2010), now in its second edition. When not teaching, Richard plays hockey, squash, canoes, as well as a host of family activities.

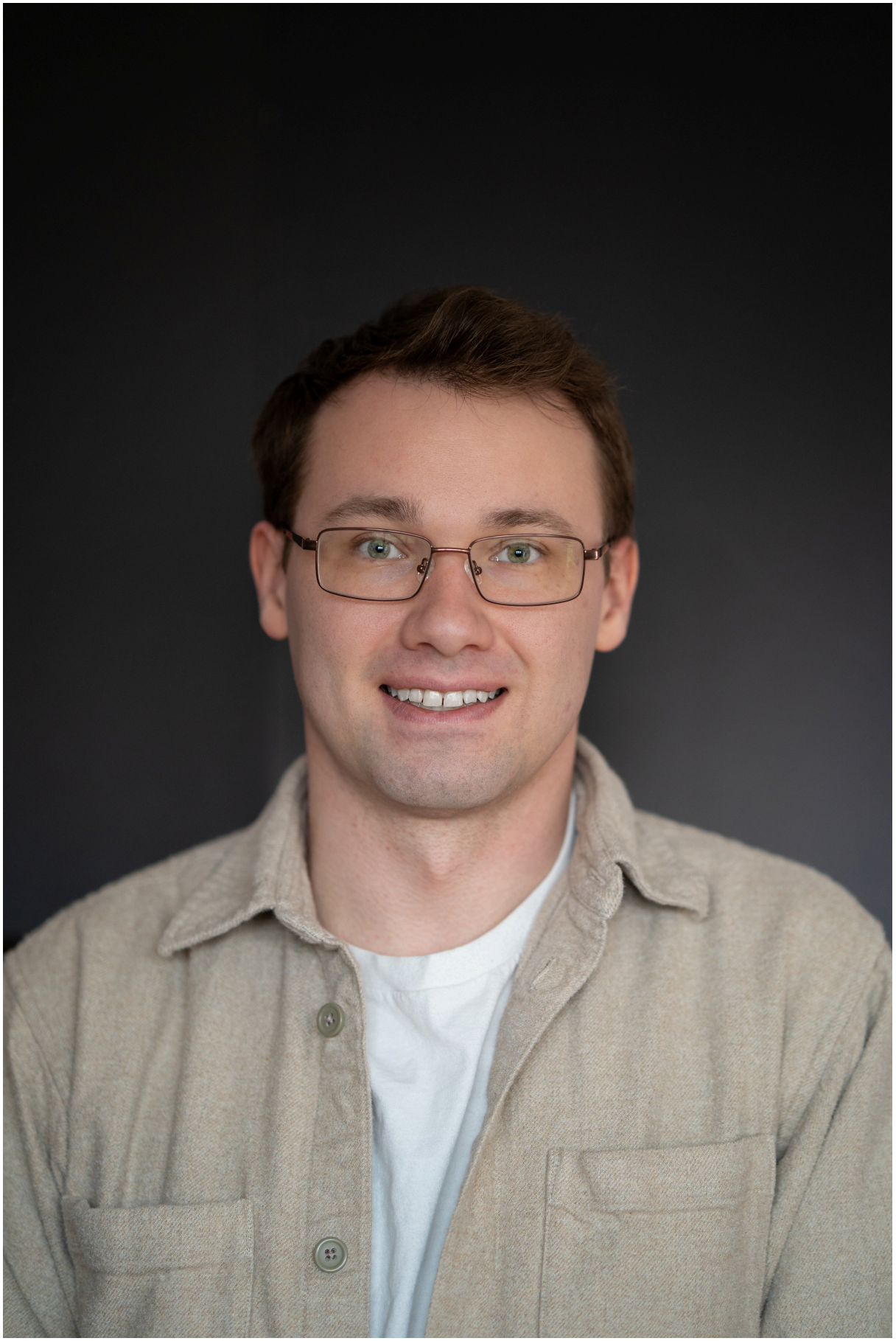
Next Steps

Gain insight into preventing phishing attacks, defending against watering hole attacks and ensuring USB security.

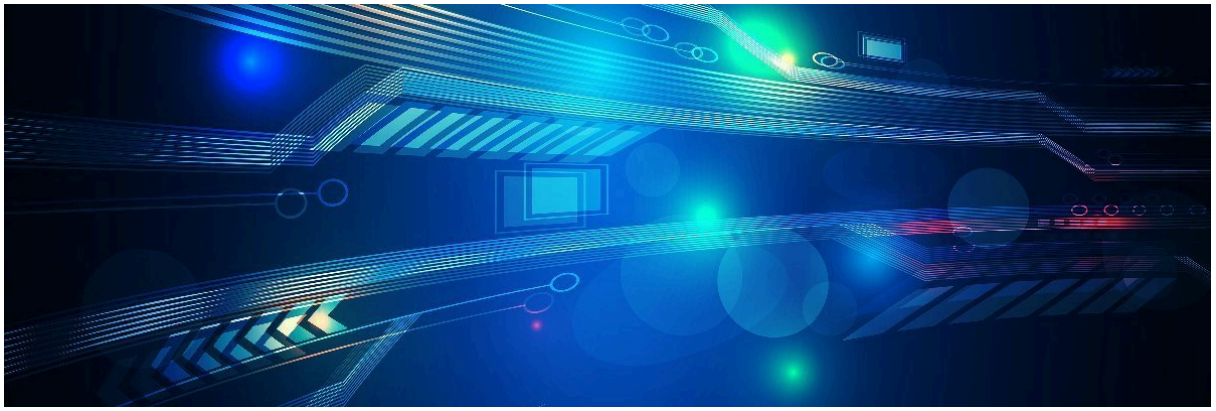
Dig Deeper on Threats and vulnerabilities

- 

What is the WannaCry ransomware attack?



By: Alexander Gillis

- 

What is a watering hole attack?

By: Mary Shacklett

- 

Pegasus malware

By: Andrew Zola

- 

blended threat

By: Kinza Yasar
