HACKER'S ALMANAC

A FIELD GUIDE

to Understanding the Tactics, Techniques and Attack Vectors Used by Cybercriminals

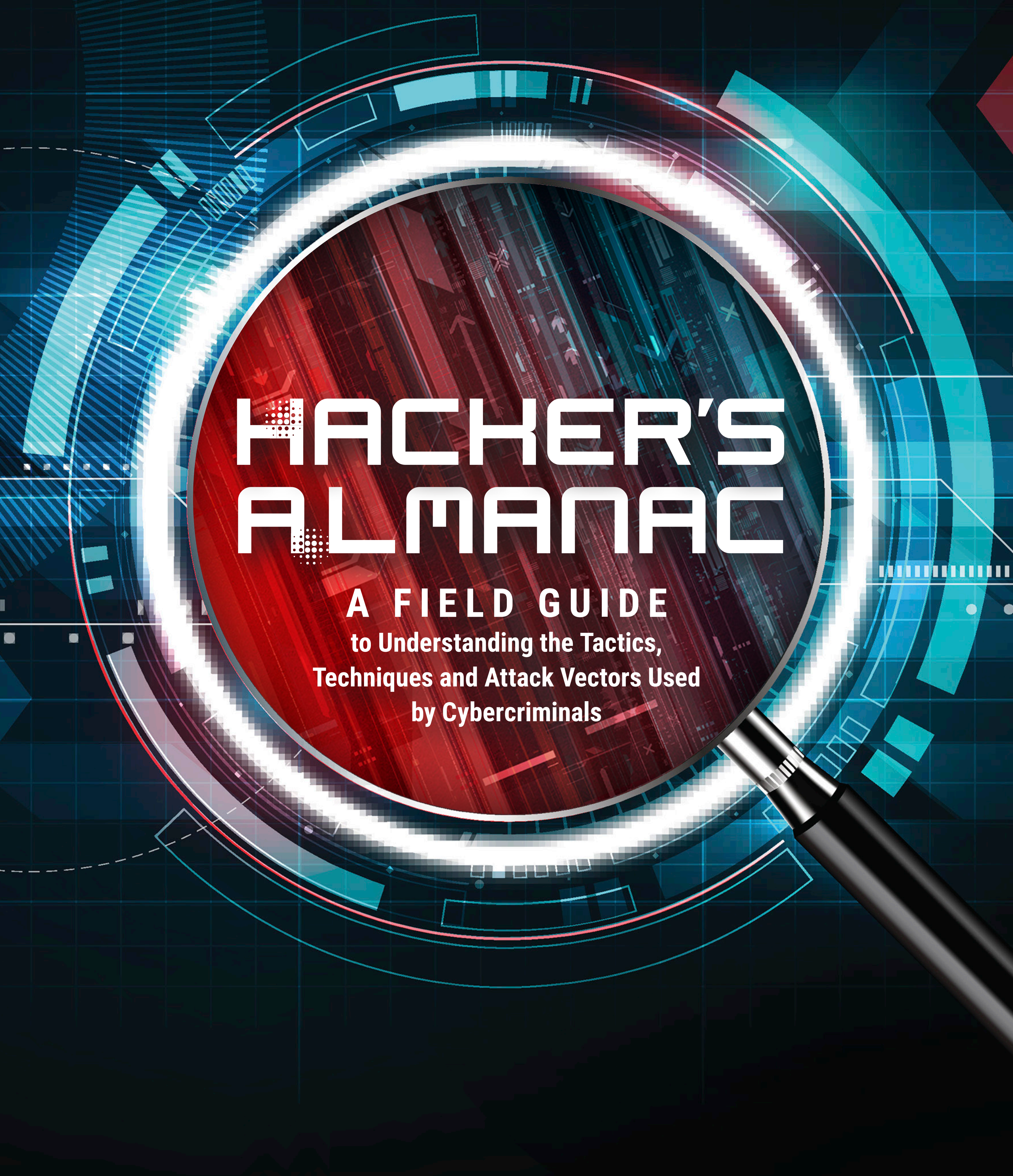


TABLE OF CONTENTS

INTRODUCTION:

THE EVOLVING THREAT LANDSCAPE

CHANGE IS ONE OF THE FEW CONSTANTS IN LIFE, AND CYBERSECURITY IS NO EXCEPTION TO THIS RULE.

The threat landscape is as diverse as it is sophisticated, thanks largely to the fact that the skills and tools behind launching cyberattacks have become commoditized. Dark web marketplaces, the increased availability of online attack tools, open-source botnets … they have all combined to provide cybercriminals with a plethora of user-friendly and highly scalable attack vectors and services. As a result, hackers and cybercriminals have reached a level of maturity and efficiency unsurpassed in the history of cyberwarfare, resulting in a dramatic increase in attack frequency, complexity and size.

Although these threats constitute a clear and present danger to organizations worldwide, knowledge is power. Radware's *Hacker's Almanac* assists security experts with understanding the threat landscape and generating awareness about current tactics, techniques and procedures used by today's cybercriminals. It is divided into three sections and covers common tools and tactics, threat actors and cybersecurity predictions.

Understanding these threats and techniques to mitigate them is the first step in preparing your security team and implementing the correct policies and systems. Before securing your network, be sure to conduct an audit of your organization's network and understand its vulnerabilities/weaknesses. Then leverage this almanac to study the threats posed against your organization.

1.1 CYBERTHREATS

BOTNETS

A BOTNET IS A COLLECTION OF COMPROMISED COMPUTERS, OFTEN REFERRED TO AS “ZOMBIES,” INFECTED WITH MALWARE THAT ALLOWS AN ATTACKER COMPLETE CONTROL. BOTNET OWNERS, OR “HERDERS,” CONTROL THE MACHINES BY MEANS OF A COVERT CHANNEL, SUCH AS AN INTERNET RELAY CHAT (IRC), ISSUING COMMANDS TO PERFORM MALICIOUS ACTIVITIES SUCH AS DDOS ATTACKS, SPAM MAIL AND DATA THEFT. ACTIVITY IN RECENT YEARS HAS SHOWN A SHIFT FROM TRADITIONAL PC-BASED BOTNETS TO IOT-BASED BOTNETS.

These groups aim to infect as many IoT devices as possible to build a massive botnet. With the expansion of IoT and the lack of regulation surrounding these devices, it’s expected that this problem will worsen. However, the victim is also the solution. Users who install IoT devices on their network should ensure that they are updated and patched and have all unnecessary ports closed. If you are a network operator, take steps to filter malicious traffic coming from IoT devices.

If you are a victim of a botnet attack, consult with a DDoS expert, as botnet attacks can last for days and flood networks at over 1Tbps. In most cases, victims will require a cloud-based mitigation solution for volumetric attack protection that scrubs network traffic and allows only legitimate user traffic to pass, so service is not interrupted.

NECURS

As one of the largest and longest-running spam botnets in history, Necurs was responsible for emailing massive amounts of ransomware, banking malware, dating spam, pump-and-dump stock scams, work-from-home schemes and cryptocurrency wallet phishing. The sinister botnet was active throughout 2016, 2017 and 2018. Necurs has been observed delivering banking Trojans such as Trickbot and Dridec, as well as ransomware like Locky.

Between August and November 2017, security researchers analyzed 32 distinct spam campaigns and found emails sent from almost 1.2 million distinct IP addresses in over 200 countries. Half of the IP addresses were concentrated in three countries: India, Vietnam and Iran. Through the 2017 holiday season, researchers stopped an average of 47 million Necurs emails distributing Locky and GlobeImposter ransomware per day. Necurs possesses a modular architecture enabling it to remain agile and adapt to the distribution type or collaborate with other malware distributors. There is speculation about a sophisticated kernel-mode rootkit feature that can disable firewalls and security solutions. Necurs also uses domain generation algorithms to switch meeting points between the bots and the C&C servers.

MIRAI

Mirai is a malware that turns network devices running Linux, such as IP cameras and DVRs, into remotely controlled "bots" that can be used as part of large-scale botnet network attacks. The Mirai botnet was first found in August 2016 and has since been used in some of the largest and most disruptive DDoS attacks, including a September 2016 attack against computer security journalist Brian Krebs's website, an attack on French web host OVH and the October 2016 Dyn cyberattack.

In addition to generating traffic volumes in excess of 1Tbps, the Mirai botnet features a selection of 10 predefined attack vectors, some effectively taking down service providers' and cloud scrubbers' infrastructure by attacking their DDoS mitigation systems. These attack vectors include highly sophisticated attacks such as GRE Floods, TCP STOMP and Water Torture attacks. Mirai also highlights the challenges organizations face when it comes to visibility into the legitimacy of GRE traffic or recursive DNS queries.

Devices were infected via Telnet Brute Force using a dictionary consisting of 61 default manufacturer CLI credentials. Record-breaking DDoS traffic volumes were generated during the attacks on Krebs and OVH in September 2016. In October 2016, a DNS Water Torture attack was leveraged during the Dyn attack. Later that month, the Mirai source code was made public, leading to numerous spinoffs being discovered.

The Mirai source code is now the basis for most botnets. Newer branches have adapted to scan and exploit more IoT vulnerabilities. Mirai exposed the IoT security problem and paved the road for new botnets that exclusively target IoT devices. It has given birth to vigilante botnets that try to protect vulnerable devices (Hajime) or purge the internet of them (BrickerBot).

BRICKERBOT

Imagine a quick-pace bot attack designed to render the victim's hardware from functioning. Coined as a permanent denial-of-service (PDoS) attack, this form of cyberattack became increasingly prevalent in 2017.

Authored by the hacker known as Janit0r, BrickerBot was the first autonomous PDoS botnet. BrickerBot's objective is to purge the internet of malicious IoT devices to prevent vulnerable IoT devices from becoming part of a botnet. BrickerBot attacks via remote execution using a destructive sequence — no malware is loaded onto the victim machine. It uses a network of detection sensors, including bots and sentinels, and only attacks infected devices. No scanning takes place, thereby not generating attention.

The Janit0r calls this project "Internet Chemotherapy." BrickerBot was first discovered in April 2017 by Radware. Janit0r announced his "retirement" in November 2017 and published some of his BrickerBot modules, including hundreds of vulnerabilities categorized by device, class and vendor. Janit0r wrote several white papers on his Internet Chemotherapy project, describing the deplorable state of the internet. During 2017, BrickerBot allegedly bricked millions of routers and affected multiple ISPs across different geographies.

WIREX

WireX was a botnet that targeted mobile devices such as cellphones and tablets and was uncovered in August 2017 when researchers observed its network traffic. The botnet was found to have infected over 100,000 Android smartphones via hundreds of malicious apps found in the Google Play™ store, many of which purported to be media/video players, ringtones or tools for storage managers. These apps infected with the WireX malware were leveraged to conduct massive DDoS attacks from those infected devices. Researchers estimated that the attacks originated from more than 70,000 distinct IPs across 100 countries, primarily performing Layer 7 HTTP GET request attacks.

MODUS OPERANDI: Default credentials and known device exploits are primary ways to compromise anything from a personal computer to an IoT device. Once compromised, the attacker profits by leveraging the botnet for denial-of-service (DoS) attacks, ad fraud or cryptomining.

PREFERRED TARGETS: Currently, the preferred targets for bot herders are insecure cloud servers, network switches and IoT devices.

CONSUMER TOOLS

OVER THE LAST FEW YEARS, TOOLS SUCH AS STRESSERS, REMOTE ADMINISTRATION TROJANS (RATS) AND RANSOMWARE HAVE BEEN PUBLISHED UNDER THE PRETENSE OF BEING STRICTLY EDUCATIONAL. THESE PROJECTS HAVE SET OFF AN INTERNATIONAL DEBATE IN THE SECURITY COMMUNITY, AND MANY WONDER IF THEY SHOULD BE PUBLICLY AVAILABLE.

Often the justification for these projects is the intention to highlight potential risks to prevent infections or reduce damage. With stressers, they claim that the services are used to improve and test security products and to understand the attack behavior targeting their networks.

As some of the most commonly available cyberattack tools, the risk of your organization being targeted by coin miners is high given the depth of these campaigns. If you are a victim of a DoS attack, you are also likely a victim of a botnet or a rented stresser service for which someone paid as little as $8 per month. In addition, criminals will use penetration-testing tools like Kali Linux to discover and exploit network vulnerabilities, so they can infect a system with RATs and other malicious software.

COIN MINER

Coin miner is a term used to refer to cryptocurrency mining software. Although certain uses of this software are legitimate, services such as CoinHive are used for malicious purposes. Typically, cryptocurrency mining happens when a connected device verifies a digital transaction and adds it to its respected ledger. Cryptojacking is the process of infecting an unauthorized device for cryptomining purposes. Over the last year, this trend has erupted and overthrown ransomware. Examples include ADB.miner, which targets Android devices, and Smominru, which spreads and infects devices with a Monero miner via the EternalBlue exploit.

DEFCON.PRO

Defcon.pro is a stresser service that also offers API access, so others can run their own stresser services. Packages range from $8 to $45 per month and offer unlimited attacks. They also offer a $3 trial version for a 200-second attack.

Defcon.pro gained media attention in 2017 when researcher Derrick Farmer discovered the leaked content of TrueStresser, and it was reported that TrueStresser had created a business out of Defcon.pro's API service. TrueStresser had 331 customers who all made upstream calls to Defcon.pro servers. At the time, Defcon.pro had 7,700 customers and had launched 117,000 DDoS attacks as of September 2017.

As of March 2018, Defcon.pro reported that it had 11,260 customers and had launched 2,107,817 attacks. The DDoS-as-a-service industry can be profitable for select services, especially for those that are first to market and offer a new attack vector. Defcon.pro states that it has the capability of launching 42 concurrent attacks from 17 servers and offers an 8–12Gbps DNS attack vector if the network load is below 50%.

RAT

A remote administration Trojan (RAT) is a malicious payload delivered via an exploit kit. Once infected with the RAT, an attacker can remotely connect to the device, control systems and spread the infection. The attackers can use the device to send spam or launch DoS attacks as well as install keyloggers to access personal information. RATs are often sold on forums and dark web marketplaces but are also found for free on websites like GitHub.

KALI LINUX

Kali Linux is a free and widely available operating system used by security professionals. As a result, Kali Linux is often downloaded and abused by hackers to infect systems. Kali Linux is preloaded with hundreds of tools classified by the following topics: information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, forensics tools, stress testing, sniffing and spoofing, password attacks, maintaining access, reverse engineering, hardware hacking and reporting tools. This operating system can run alone or on a live install, providing tools for users to “test” network vulnerabilities. A rogue user with Kali Linux is a serious threat because criminals can easily load Kali Linux onto a thumb drive to make the platform mobile. In recent years, Kali Linux has been the operating system of choice for many hackers.

1.3 CYBERTHREATS

DEFACEMENTS

A DEFACEMENT TYPICALLY REFERS TO A REMOTE CODE EXECUTION ATTACK OR SQL INJECTION THAT ALLOWS THE HACKER TO MANIPULATE THE VISUAL APPEARANCE OF THE WEBSITE BY BREAKING INTO A WEB SERVER AND REPLACING THE CURRENT WEBSITE CONTENT WITH THE HACKER'S OWN. DEFACEMENTS ARE CONSIDERED DIGITAL GRAFFITI AND TYPICALLY CONTAIN SOME TYPE OF POLITICAL OR RIVALRY STATEMENT FROM THE HACKER. HACKTIVIST GROUPS OFTEN LEVERAGE DEFACEMENTS.

These groups are typically unskilled, using basic software to automate their attacks. When major websites are defaced, it is typically due to network operator negligence. Web application firewalls are the best way to prevent these attacks, but updating content management systems or web services is also effective.

If you think that you are the target of a defacement campaign, update and patch your system immediately and alert network administrators to look for malicious activity, as a hacker will typically add a page to your domain. You can also monitor for such attacks retroactively via social media.

ERR0R SQUAD

Err0r SquaD is a group of Bangladeshi hackers that specializes in web application abuse. The group is known to target content management systems and carry out large-scale defacement campaigns to spread awareness of its messages. Attackers post YouTube videos on how to utilize attack methods against their victims so others will join.

ELECTRONIC THUNDERBOLT TEAM

Electronic Thunderbolt Team is a group of hackers from the Middle East that specializes in defacement campaigns related to political events such as OpIsrael. Members will often target a number of small and unprotected sites to post a message related to their operation.

GIANT'S-PS

Giant's-PS is a group of hackers from an unknown location that currently targets Israeli businesses and websites with defacement campaigns on behalf of the Palestinians. Its messages often contain religious content and geopolitical events.

ANONPLUS

In 2011, AnonPlus was created with the purpose of becoming a social networking service developed for Anonymous members. Shortly after its creation, AnonPlus was hacked by rival groups and has since struggled to maintain a social presence and a secure IRC.

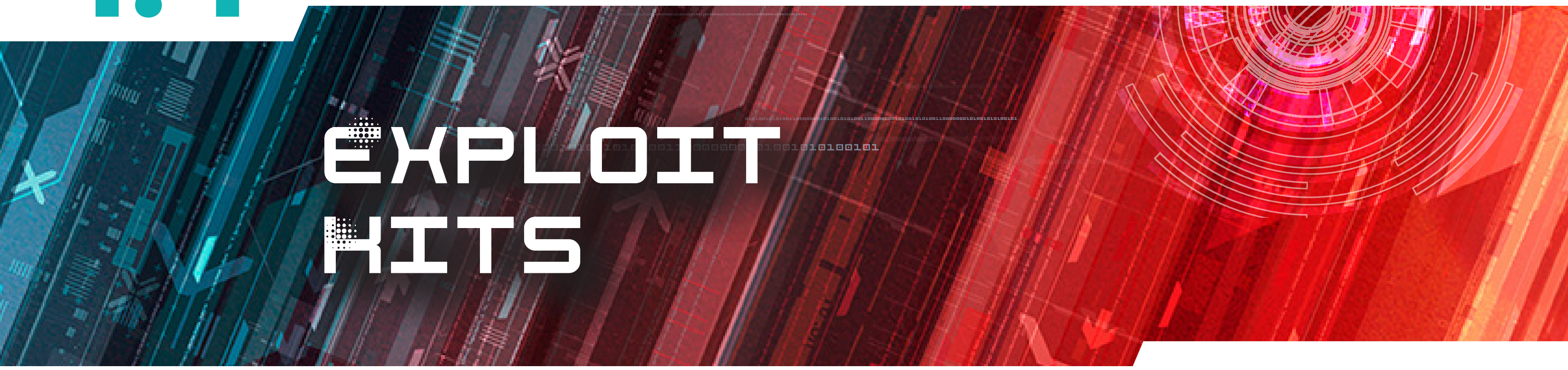
AnonPlus Italia is not affiliated with Anonymous Italia. This group has launched attacks against government-related websites in Italy and the United States as well as financial institutions. Since 2018, AnonPlus Italia has been involved in political hacktivism against the Italian government. It has also attacked the website of Milan and leaked personal data from the Florence Democratic Party. The leak provoked an internal debate within the Anonymous collective since it contained information of innocent citizens. After the data was posted on the AnonPlus IRC, the server was taken offline.

Following the leak, AnonPlus's main Twitter account, @AnonPlus_info, was suspended and the group decided to stop using social networks entirely. In March 2018, members created their own website. AnonPlus Italia announced its return with a new manifesto posted on its domains, Anonplus.tk and Anonplus.rf.gd. It uses these domains to host information about recent attacks. Its new IRC now resides at webchat.anonplus.cf.

Throughout April 2018, AnonPlus Italia claimed responsibility for defacing 21 websites, 20 of which use the content management system Drupal. Drupal's security team released a patch in March 2018 to prevent remote code executions, which allow attackers to execute arbitrary code on unpatched servers as a result of an issue affecting multiple subsystems with default or common module configurations. A remote attacker can construct a request with malicious content to exploit the vulnerability. A successful exploitation may lead to remote code injection on a Drupal server.

MODUS OPERANDI: Defacements primarily leverage unpatched website vulnerabilities, remote code execution attacks or SQL injections.

PREFERRED TARGETS: Nearly any website can be targeted by a hacktivist. Attackers will often use a defacement to spread a political message. They will often look for the most popular accessible website(s) to gain as much notoriety as possible.



EXPLOIT KITS

EXPLOIT KITS ARE PREPACKAGED TOOLKITS CONTAINING SPECIFIC EXPLOITS AND PAYLOADS USED TO DROP MALICIOUS PAYLOADS ONTO A VICTIM'S MACHINE. ONCE A POPULAR AVENUE FOR ATTACKS, IT IS NOW BARELY USED DUE TO THE POPULARITY OF OTHER ATTACK VECTORS, SUCH AS CRYPTOMINING. AUTHORS OF EXPLOIT KITS STOPPED UPDATING THEM FOLLOWING THE INCREASED POPULARITY OF CRYPTOMINING. EXPLOIT KITS ARE NOW OFTEN USED TO DEPLOY RANSOMWARE AND MINING MALWARE.

These tools can target nearly everyone. Organizations should consider themselves a daily target for possible exploit kits designed to deliver malicious payloads onto their network. To prevent this, update network devices and ensure that all employee devices are also updated. Often times, these attacks are browser based and exploit vulnerabilities once an employee visits the malicious landing page. Training and preparation start with user education. Humans are the weakest link, and authors of exploit kits target the masses in the hope that someone will fall for their landing pages.

MAGNITUDE EXPLOIT KIT

Magnitude is an exploit kit that contains a variety of exploits and payloads, gaining fame when it was used in the PHP.net, WordPress and Yahoo attacks. Once infected by the exploit kit, Magnitude allows remote access to the attacker to download payloads such as Zeus, Andromeda and Necurs. Today it is generally used to infect victims and download ransomware payloads, generating an estimated thousands of dollars per week for its authors. Magnitude uses a pay-per-campaign model and requires users to generate the traffic to the landing page containing the kit.

GRANDSOFT EXPLOIT KIT

This legacy exploit kit was thought to have disappeared in 2014 but resurfaced in 2017 when it began dropping ransomware and mining payloads. GrandSoft infects the victim's machine via Internet Explorer exploits, Flash exploits or an RCE vulnerability in the Windows VBScript engine.

TERROR EXPLOIT KIT

Terror, also known as Neptune, is used to install CCMiner and other cryptomining software, but it has also been involved with malvertising campaigns. Terror also uses HTTPS for its landing pages.

RIG EXPLOIT KIT

RIG is one of the most active exploits after the fall of Terror exploit kits. Known in the past for delivering ransomware payloads, it is leveraged today for infecting victims with coin miners or data-stealing malware. Similarly, users are redirected to a landing page containing an embedded JavaScript to locate security flaws in the user's browser. Once a vulnerability has been discovered in Internet Explorer, Java, Flash or Silverlight, it infects the victim and delivers its payload.

MODUS OPERANDI: An exploit kit is prepackaged malware that is found and traditionally distributed from a compromised website. Once infected, the attacker can capture credentials or malware like ransomware or a cryptominer.

PREFERRED TARGETS: The target for exploit kits is typically an end user's browser. More advanced spear-phishing pages can be used to target corporations.

1.5 CYBERTHREATS

RANSOMWARE

RANSOMWARE IS A TYPE OF MALWARE THAT RESTRICTS ACCESS TO USER DATA BY ENCRYPTING AN INFECTED COMPUTER'S FILES IN EXCHANGE FOR PAYMENT TO DECRYPT. THE ATTACKER OFTEN DISTRIBUTES A LARGE-SCALE PHISHING CAMPAIGN IN THE HOPE THAT SOMEONE WILL OPEN THE MALICIOUS ATTACHMENT OR LINK. ONCE INFECTED, THE DEVICE IS UNUSABLE AND THE VICTIM IS FACED WITH THE DECISION OF WHETHER OR NOT TO PAY THE EXTORTIONIST TO RECOVER THE DECRYPTION KEY.

Only in certain cases have keys been recovered. Over the years, Radware researchers have also followed the ransomware-as-a-service (RaaS) industry, which offers novice users the ability to launch their own campaigns for an established price or percentage of the profit. Ransomware has existed for over two decades but has only recently gained popularity among for-profit criminals. This trend has tapered off because ransomware campaigns generate a great deal of attention, notifying potential victims and thereby discouraging them from paying. Campaigns that attract less attention are typically more profitable.

Ransomware campaigns follow a standard pattern of increased activity in the beginning before settling down. Ransomware, once incredibly popular, has fallen out of favor with attackers, who now prefer cryptojacking campaigns. Because of the amount of attention that ransomware campaigns generate, most groups target a wide range of industries, including manufacturing, retail and shipping, in the hope of finding some success.

If you think that your organization could be a target of a ransomware campaign, shoring up your network is critical. Ransomware can be delivered in various ways, most commonly via spam/phishing emails containing a malicious document. Other forms of infection include exploit kits, Trojans and the use of exploits to gain unauthorized access to an infected device.

WANNACRY

WannaCry was one of the more famous ransomware campaigns in recent years and was tracked back to North Korean programmer Park Jin Hyok, a member of the Lazarus Group. The campaign affected over 200,000 victims and infected over 300,000 computers across 150 countries with total damages approaching $1 billion. In terms of monetization, the campaign was considered a failure with a low profit margin for the operator. WannaCry leveraged the recently disclosed EternalBlue malware from the Shadow Brokers' NSA dump.

NOTPETYA

NotPetya was another famous ransomware campaign attributed to the Russian government. This attack originated from a malicious software update from MeDoc, a popular accounting and workflow software solution from Ukraine. The attack infected more than 200,000 computers and caused over $1 billion in damage. However, several issues did arise during the campaign. The email provider eventually shut down the extortionist account, making it impossible to communicate with the attacker. After further research, it was determined that NotPetya was not ransomware but rather a campaign designed to wipe infected computers.

SAMSAM

SamSam, one of the more profitable campaigns and groups in the ransomware arena, has earned the attackers over $1 million. Although most ransomware campaigns and groups are random and opportunistic with their attacks, the SamSam operators selectively targeted victims that were primarily in healthcare, education and government verticals because they were identified as probable payers.

LOCKY

Locky is a ransomware variant that appeared in 2016 as part of a phishing campaign containing a malicious Word document that would download the encryption Trojan. The Necurs botnet typically sent out these phishing emails. Over the years, the authors behind Locky have released several versions, with some of the latest including techniques to avoid detection.

MODUS OPERANDI: Ransomware typically spreads via phishing emails sent out from a spam botnet. Variants can also be spread via drive-by downloads.

PREFERRED TARGETS: There is no preferred target for ransomware. Ransomware is a "spray and pray" technique designed to send infected documents to as many people as possible.

TROJANS

A TROJAN HORSE IS A MALICIOUS COMPUTER PROGRAM MASQUERADING AS A USEFUL OR OTHERWISE NONMALICIOUS, LEGITIMATE PIECE OF SOFTWARE. GENERALLY SPREAD VIA SOCIAL ENGINEERING AND WEB ATTACKS, TROJAN HORSES OFTEN INSTALL A BACKDOOR FOR REMOTE ACCESS AND UNAUTHORIZED ACCESS OF THE INFECTED MACHINE.

An attacker can perform various criminal tasks, including, but not limited to, “zombifying” the machine within a botnet or DDoS attack, data theft, downloading or installing additional malware, file modification or deletion, keylogging, monitoring the user’s screen, crashing the computer and anonymous internet viewing.

If you think that you are a target of this attack vector, secure both your corporate network and user devices. Proper education and user hygiene help prevent an employee from infecting your network. Often an employee opens a malicious document via phishing or infects via a drive-by download, allowing the Trojan to download malicious payloads.

TINYLOADER

TinyLoader is an infamous backdoor malware used to deliver point-of-sale and banking Trojans. The malware's name originates from its size, which is typically only a few kilobytes. Once infected with TinyLoader, it downloads and installs other malicious programs, such as AbaddonPOS.

ZEUS

Zeus is a well-known Trojan horse that steals financial information from a user's browser using man-in-the-browser keylogging and form grabbing. Additionally, Zeus installs a backdoor on the infected machine to be used as part of a DDoS-purposed botnet.

Zeus was detected in 2007 when it was used to attack the U.S. Department of Transportation; however, its widespread use began in March 2009. Attacks involving Zeus occurred throughout 2010, including an October 2010 attack attempt by an organized crime ring to steal over $70 million from American individuals with Zeus-infected computers. The FBI made over 90 arrests of suspected members in the United States, and others were arrested in the United Kingdom and Ukraine in connection with this ring.

In May 2011, the source code for version 2 of Zeus was leaked, leading to various customized Zeus-based bots. Some of the more advanced custom bots based on the leaked code (such as Ice IX) attempted to fix the existing issues with Zeus, resulting in harder detection. However, security researchers have discovered that even the most well-known custom versions are similar to the original Zeus source code, and thus are not significantly more innovative or dangerous.

EMOTET

Emotet is a piece of malware that targets the banking industry. Once a system is infected, Emotet installs other banking malware for bank account information theft and modules for launching DoS attacks. Infections typically originate from users opening malicious documents containing infected download links and PDFs with embedded files. Emotet also includes a spreader to propagate throughout a network. Some of its more notable campaigns include Pinkslipbot and Dridex.

KOVTER

Kovter is malware designed to target network devices to commit ad fraud and is one of the most commonly updated malware families. This click-fraud Trojan spreads via spam attachments and malvertising campaigns, but once it delivered ransomware as well. These attachments, when opened, contain malicious documents such as infected office files. Kovter is known as "fileless" malware, meaning that it targets a victim's registry keys without storing itself on a victim's hard drive.

MODUS OPERANDI: Typically, Trojan malware is packed inside a legitimate software program and spread to the victim via social engineering attacks, such as phishing and drive-by downloads, for future use in DDoS, keylogging, data theft or exfiltration or for downloading other malware.

PREFERRED TARGETS: Like exploit kits, Trojans target the end user's devices. More advanced Trojans, such as Emotet and Trickbot, use spear-phishing emails with a financial lure to target the financial industry.

2.1 THREAT ACTORS

ADVANCED PERSISTENT THREAT

ADVANCED PERSISTENT THREAT (APT) IS A COMMONLY USED TERM TO DESCRIBE A CYBERTHREAT POSED BY THOSE WHOSE OBJECTIVES INCLUDE ESPIONAGE AND SUBVERSION FOR FINANCIAL OR POLITICAL MOTIVES.

These groups are often backed by governments possessing a variety of techniques and skills at their disposal with the ability to develop more advanced tools. Operators with specific objectives require a high degree of covertness to maintain a foothold in the network for long durations. Using various intelligence-gathering techniques and exploits, this troop can access and live-monitor sensitive data on a targeted network.

These groups do not attack indiscriminately, but when they do, they have specific purposes and generate a great deal of publicity. They are methodical and surgical. Government-backed operations are the most complex to attribute due to the resources in play. Although the government and financial and utility companies are among the most commonly targeted with APTs, all industries could be affected due to geopolitical events.

If you think that you are a target of an APT group, take every necessary measure to secure your network. Often the first step in preventing an attack like this is employee training. Your employees are the weakest link. Training them how to spot phishing and spear-phishing attempts can help prevent future attacks.

APT28 | RUSSIA

APT28, also known as Fancy Bear, Pawn Storm and Sofacy Group, is a cyber-espionage group associated with two Russian military intelligence agency units, Unit 26165 and Unit 74455. This nation-state group is known to have been in operation since 2008 and represents a constant threat to an array of organizations and government agencies allied with Western countries. This group is notorious for different exploits and spear-phishing attacks to deploy customized malware. Once inside a network, they compromise, disrupt and influence political agendas around the world. They target government elections, the media, sporting events and several global companies.

LAZARUS GROUP | NORTH KOREA

Lazarus Group, aka Hidden Cobra, is a cybercrime group associated with the North Korean government. This nation-state group has been in operation since 2019 and is responsible for various attacks over the past decade, including Ten Days of Rain, the Sony 2014 data breach, the WannaCry ransomware outbreak and the finance-targeted SWIFT attacks. This group typically relies on spear-phishing campaigns to deploy malicious malware designed to exfiltrate or encrypt user data.

EQUATION GROUP | UNITED STATES

The Equation Group is a cyberwarfare and intelligence-gathering unit associated with the Tailored Access Operations (TAO) of the National Security Agency (NSA). This nation-state group has been in operation since 1998, monitoring and infiltrating enemies of the United States, both foreign and domestic. As one of the largest components of the NSA's signal intelligence program, this group has the ability to compromise commonly used hardware such as routers, switches and firewalls. In 2016, the hacking group The Shadow Brokers announced that they had compromised Equation Group's tool set containing undisclosed exploits and posted them to GitHub. Exploits contained in the publication included EternalBlue, which served as the basis of the WannaCry attack by the Lazarus Group.

APT1 | CHINA

APT1, also known as Unit 61398 and The Comment Group, is a cyberwarfare organization associated with the Chinese People's Liberation Army. This nation-state group has been known to be operating since 2006 and has been attributed to a number of attacks, including the indictment of five members for stealing intellectual property and information from U.S. corporations. This government-backed group focuses on stealing trade secrets and confidential information from corporations across every vertical, with emphasis on manufacturing, engineering and electronics. They accomplish this with spear-phishing attacks, malware and password dumping to gain future access and exfiltrate targeted data.

MODUS OPERANDI: Nation-state operators often rely heavily on spear-phishing attacks to compromise a specific user and capture credentials. Once a user is compromised, attackers look to escalate privileges and deploy malware designed to compromise more users on the network and exfiltrate data.

PREFERRED TARGETS: Nation-state actors typically target the public sector, utilities and critical infrastructure. They look for any data that will benefit their country's economy and strengthen both key business and military strategies.

2.2 THREAT ACTORS

DENIAL-OF-SERVICE GROUPS

DOS ATTACKS ARE CYBERATTACKS DESIGNED TO RENDER A COMPUTER OR NETWORK SERVICE UNAVAILABLE TO ITS USERS. A STANDARD DOS ATTACK IS WHEN AN ATTACKER UTILIZES A SINGLE MACHINE TO LAUNCH AN ATTACK TO EXHAUST THE RESOURCES OF ANOTHER MACHINE. A DDOS ATTACK USES MULTIPLE MACHINES TO EXHAUST THE RESOURCES OF A SINGLE MACHINE.

DoS attacks have been around for some time, but only recently has there been an emergence of denial-of-service groups that have constructed large botnets to target massive organizations for profit or fame. These groups often utilize their own stresser services and amplification methods to launch massive volumetric attacks, but they have also been known to make botnets available for rent via the darknet.

If a denial-of-service group is targeting your organization, ensure that your network is prepared to face an array of attack vectors ranging from saturation floods to Burst attacks designed to overwhelm mitigation devices. Hybrid DDoS mitigation capabilities that combine on-premise and cloud-based volumetric protection for real-time DDoS mitigation are recommended. This requires the ability to efficiently identify and block anomalies that strike your network while not adversely affecting legitimate traffic. An emergency response plan is also required.

LULZSEC

LulzSec was a computer hacking group responsible for numerous high-profile attacks, which occurred during the peak of its existence. This group infiltrated the computer networks of government agencies, corporations and individuals, publishing private and personal information as well as launching DoS attacks.

LIZARD SQUAD

Lizard Squad was active from 2014 to 2016 and gained notoriety for attacks against gaming networks such as PlayStation and Xbox Live on Christmas Day 2014. In 2016, several copycat RDoS groups attempted to impersonate Lizard Squad and sent out ransom emails demanding payment. Lizard Squad never conducted extortion campaigns because it ran successful stresser services that made a substantial profit, such as Lizard Stresser and Shenron. Members often used these stressers to launch attacks to advertise their services. AppleJ4ck, a Lizard Squad member, made close to $1.2 million selling DDoS attacks before his arrest.

GHOST SQUAD HACKERS

Ghost Squad Hackers launches attacks in support of anti-government and anti-hate speech. It has been active since 2016 with notable attacks against the U.S. military, Israeli Defense Forces, the Ku Klux Klan and ISIS. This group collaborated with hacktivist groups such as Anonymous on OpIcarus, a prolonged campaign against financial institutions in response to alleged corruption within the industry. In addition to DDoS attacks, this group has also been observed gaining access to sensitive information and publishing this data.

MCA DDOS TEAM

Magdalo Cyber Arm is a politically motivated hacktivist group from the Philippines that has been active since 2012. The group engaged in hacktivist activity against the Philippine, Israeli and Gabon governments.

MODUS OPERANDI: Threat actors typically leverage botnets and attack scripts. The preferred attack vector is one that allows spoofing or amplification. Spoofing will allow for any additional layers of security, while amplification will produce more bandwidth and mask the origin of the attack. Recently, combing volumetric, botnet-based attacks in combination with bursting or pulsing waves of bandwidth proved successful.

PREFERRED TARGETS: Those that conduct DDoS attacks outside of extortion tend to be activists. Their targets include governments, corporations and anyone else with an opposing political or moral view. A DDoS attack is used to silence or embarrass their targets.

2.3 THREAT ACTORS

HACKTIVISTS

HACKTIVISTS ARE POLITICALLY DRIVEN GROUPS THAT USE CYBER CAPABILITIES TO STAGE DIGITAL PROTESTS OR MALICIOUS ACTS AGAINST POLITICAL OPPONENTS DUE TO A CONFLICTING OPINION OR ACTION. MOST ATTACKS CONSIST OF NETWORK AND APPLICATION ATTACKS LIKE DDOS, SQLI OR XSS ATTACKS. THESE ATTACKERS ARE NOT FINANCIALLY MOTIVATED AND OFTEN WILLING TO DOX/POST SENSITIVE INFORMATION FREE OF CHARGE. AT THE CORE OF THESE ATTACKS IS A POLITICAL AND IDEOLOGICAL DIFFERENCE.

These groups attack anyone who they think is directly involved in the protested event. They believe inaction is action against their cause. Those that do not join the cause are also considered enemies. These hackers also target the innocent to make a political point and mainly utilize basic GUI-based tools or those found within typical penetration testing systems. These attackers may download basic Python code to automate basic DDoS attack vectors, but they are largely unable to conduct attacks solely and instead rely on renting stressers and paying others to launch their own attacks.

If your organization thinks that it is the target of a hacktivist, prepare your network accordingly based on the aforementioned attributes. Most attacks are annual and announced publicly days before the operation. Make sure that all networks are updated and patched. Inform employees of possible increases in malicious emails seeking to compromise your network. Secure social media accounts and enforce two-factor authentication where applicable. In addition, monitor social media for specific hashtags related to the event to provide advanced notification.

MILW0RM

Little is known about milw0rm, which often conceals members' identities to avoid prosecution. This international hacking team is best known for penetrating the computers of India's primary nuclear research facility, Bhabha Atomic Research Centre (BARC) in Neyveli, on June 3, 1998. The group conducted hacks for political reasons, including the largest mass hack at that time, and inserted anti-nuclear weapons and peace messages on its websites. The group's logo featured the slogan "Putting the power back in the hands of the people."

WIKILEAKS

WikiLeaks is an international nonprofit organization that publishes secret information, news leaks and classified media provided by anonymous sources. Its website, initiated in 2006 in Iceland by the organization Sunshine Press, claims a database of 10 million documents in the first 10 years since its launch. Julian Assange, an Australian internet activist, is generally considered its founder, editor-in-chief and director and has been hiding in the Embassy of Ecuador in London since 2012.

CHAOS COMPUTER CLUB (CCC)

The Chaos Computer Club (CCC) is Europe's largest association of hackers with 7,700 registered members. It is incorporated as an *eingetragener Verein* (registered association) in Germany, with local chapters (called *Erfa-Kreise*) in various cities in Germany and other German-speaking countries. Some chapters in Switzerland are organized in the independent sister association Chaos Computer Club Schweiz.

The CCC describes itself as "a galactic community of life forms, independent of age, sex, race or societal orientation, which strives across borders for freedom of information." In general, the CCC advocates for more transparency in government, freedom of information and the human right to communicate. Supporting the principles of the hacker ethic, the club also fights for free universal access to computers, technological infrastructure and the use of open-source software.

GROUP ANONYMOUS

Anonymous started in 2003 as a collection of amateurs striking websites for fun, but their activities have taken a far larger, more sinister turn during the past decade. It is known as an anti-establishment group of which targets have ranged from big businesses and governments to websites that host questionable/unethical content. Anonymous swamps websites, tricks targets into revealing details with “phishing” emails and uses computers to crack passwords. This group vowed to destroy the online recruitment service of ISIS. It has already taken down more than 1,000 terrorist websites in retaliation for the “jihadis’ war on free speech.” Members come from all over the world, discussing operations in secret online chatrooms.

MODUS OPERANDI: Hacktivists typically engage in crowdsourced operations or team efforts. Normal operations include doxing, defacements and denial-of-service attacks directed at their targets and anyone directly or indirectly associated with them.

PREFERRED TARGETS: Hacktivists’ targets include corporations or individuals associated with a political opinion or lifestyle with which the hacktivists disagree.

2.4 THREAT ACTORS

INSIDERS

INSIDER THREATS ARE ONE OF THE MOST DAMAGING THREATS THAT AN ORGANIZATION CAN FACE. THESE THREATS ARE TYPICALLY OPPORTUNISTIC OR DISGRUNTLED EMPLOYEES WHOSE PRIMARY OBJECTIVE IS PROFIT, COMPANY SHAMING OR ESPIONAGE.

These types of employees might represent the most critical threat to your business due to the level of trust between employee and employer. Ensuring employee happiness and motivation helps ensure them as one of your best defenses against cyberattacks and data theft. If you believe your organization is a target of an insider threat, contact the authorities immediately. If an employee is compromising your organization, move to limit insider knowledge and access and remove the employee from the property. Look for unauthorized hardware that may have been placed in your facilities. Items can include USB drives, rogue access points or network hardware that can be plugged into other devices.

In addition to malicious actors, innocent employees also present a threat. Sometimes employees accidently or maliciously leak data on social media.

OPPORTUNISTS

Opportunist insiders are generally law-abiding citizens who do not possess advanced knowledge about network security or how to hack their employers. They only act when the moment arises and steal digital goods for profit. They typically abuse their privileges or steal coworkers' access to do so.

DISGRUNTLED EMPLOYEES

Disgruntled employees can often be a huge cybersecurity risk for an organization. When employees perceive that their company has wronged them, it can serve as motivation to damage the company or its superiors. Often these employees sit at their position for years collecting the information needed to expose the company. The best way to deal with this threat is to prepare an emergency plan to isolate any resulting black swan event.

CASH OUT

In a growing trend, some employees are not who they seem to be. They deliberately gain access to positions in a corporation that allow them to aid the process of fraud against the organization's customers. These attackers often look to compromise or incentivize employees in the financial industry who can assist in committing fraud.

ESPIONAGE

Corporate espionage, a premeditated theft attack and often one of the hardest to spot, involves an employee who is employed by a specific company for the sole purpose of stealing data and intellectual property.

MODUS OPERANDI: Insiders typically depart the organization with sensitive data. Other methods include data or credential theft via phishing emails or USB/mobile devices left behind by an insider as a lure/trap. Insiders can also deploy rogue access points to inspect corporate network traffic.

PREFERRED TARGETS: Employers, coworkers and direct supervisors are the main targets of an insider threat.

ORGANIZED CYBERCRIME

ORGANIZED CYBERCRIME IS AN UMBRELLA TERM THAT DESCRIBES “DIGITAL GANGS” THAT USE COMPUTERS TO CONDUCT MALICIOUS ACTIVITY MOTIVATED BY FINANCIAL PROFIT. ORGANIZED CYBERCRIMINALS LEVERAGE A VARIETY OF ATTACKS FROM DIRECT TO OPPORTUNISTIC, INCLUDING EXTORTION-BASED ATTACK VECTORS SUCH AS RANSOMWARE, DENIAL OF SERVICE FOR RANSOM, CRYPTOMINING AND FRAUD.

These groups strike individuals or organizations that they believe they can financially exploit. They will often spam their target(s) in short time spans and typically target organizations with large numbers of customers because any resulting outages typically garner attention. In addition, any stolen data is usually valuable. Besides companies with large customer bases, financial institutions are also at risk for ransom demands, which result in the organizations often paying. High-profile targets include the executive class for extortion, as well as physical targets such as point-of-sale systems and ATMs.

If your organization is the target of a cybercriminal gang, ensure the security of your data and devices; cybercriminals prey on the weak. Your organization is more susceptible if you do not keep your system updated, patched and utilizing two-factor authentication wherever possible. Because attacks are often unannounced and difficult to prepare for, corporations should have a response plan in place for extortion attempts. In addition, retailers should be particularly wary of criminals targeting machines in stores with skimmers or networks via point-of-sales systems with financial malware designed to harvest and steal credentials.

RTM

RTM is an organized cybercrime group, apparently active since 2015, which is known for its own Trojan malware, RTM. The group targets user data on remote banking systems in Russia and neighboring countries. The RTM Trojan is used to spy on victims, log user credentials and target accounting software.

DARK HOTEL

Dark Hotel is a group popular for its spear-phishing campaigns, delivering malware to targets staying at luxury hotels and business centers in Asia and the United States. Active since the early 2000s, the group is known to compromise a hotel's WiFi, redirecting users to its phishing page for collecting personal information/data.

CARBANAK

Carbanak, also known as Carbon Spider, is an organized cybercrime group notorious for its eponymously named malware, Carbanak. The group targets financial institutions and is responsible for stealing 1 billion euros from over 100 financial institutions globally. Carbanak's tactics, techniques and procedures support the shift in criminals targeting banking systems over end users and their personal data.

FIN7

Fin7 is a financially motivated, organized cybercrime group, which is known for attacks against retail and hospitality verticals. This group leverages point-of-sale malware to target its victims and has been witnessed leveraging Carbanak malware for data exfiltration and providing remote access to network systems.

MORPHO/WILD NEUTRON GROUP

Wild Neutron Group is an organized cybercrime group that also goes by the name Jripbot or Morpho. This group focuses on corporate espionage around the world, with particular effort in the United States and Europe. Over the last decade, this group has conducted a number of operations that leveraged attack vectors such as Water Hole attacks and exploit chaining using multiplatform malware. In recent attacks, the group utilized stolen code signing certificates and gained attention when it infected companies such as Apple, Microsoft and Twitter.

MODUS OPERANDI: Organized cybercriminals will use nearly any attack vector, from basic legacy to advanced assaults. Most commonly, they deploy malware via phishing emails or compromised websites. Some of the more advanced groups will deploy physical or digital skimmers on popular e-commerce websites to capture credit card data without the victim's knowledge.

PREFERRED TARGETS: Cybercriminals follow the money. They will target anyone from individual users to large organizations. Similar to a mafia organization, cybercriminals extort small and medium-sized businesses that are most vulnerable and due to their propensity to pay.

2.6 THREAT ACTORS

PATRIOTIC HACKERS

PATRIOTIC HACKERS ARE POLITICALLY MOTIVATED CYBERATTACKERS WHO GENERALLY FOLLOW SOME FORM OF POLITICAL EVENT. THE TERM "PATRIOTIC HACKERS" IS USED TO DESCRIBE NONGOVERNMENT ACTIONS BY INDIVIDUALS WHO ARE HACKING GOVERNMENT NETWORKS CONSIDERED TO BE ENEMIES OF THE STATE.

These attacks are typically in response to foreign aggression and can be retaliatory attacks by citizens or attacks launched by freelance hackers operating for a government. As a result, these attacks can create problems for victims because they have to determine if the threat is from a nation-state or rogue hackers. These groups will respond quickly and furiously to a political event, and resulting attacks can cause geopolitical turmoil because these actions could be considered an act of war.

If you think that you are a target of patriotic hackers, you should be concerned with advanced persistent threat groups as well. Patriotic groups are not typically backed by governments but possess government-type cyberattack capabilities. Protecting your network and employees should be the highest priority. These attackers typically target low-hanging fruit (i.e., organizations with vulnerable networks), which can cause maximum damage.

SYRIAN ELECTRIC ARMY

The Syrian Electronic Army (SEA) is a group of computer hackers that first surfaced online in 2011 to support the government of Syrian President Bashar al-Assad. Using spamming, website defacement, malware, phishing and DoS attacks, it has targeted political opposition groups, Western news organizations, human rights groups and websites that are seemingly neutral to the Syrian conflict. It has also hacked government websites in the Middle East and Europe, as well as U.S. defense contractors. The SEA has been linked to a string of attacks focused mostly on news organizations and technology companies. In addition to hacking the Associated Press Twitter account, the group has been linked to attacks on ITV, *The Onion*, Outbrain, *The New York Times*, the United States Marine Corp's recruiting portal, Microsoft, eBay, Facebook, *Forbes*, *The Sun*, *The Sunday Times*, *The Independent*, *Time Out*, NBC, *The Daily Mail* and *Le Monde*.

TARH ANDISHAN

Tarh Andishan (a Farsi translation meaning "innovators") was created while Iran was still recovering from the Stuxnet worm attack (created by the United States and Israel). With an estimated 20 members, many based in Tehran, Iran (along with multiple fringe members located globally), Tarh Andishan demonstrates what a sophisticated hacker group is capable of. By using automated wormlike propagation systems, backdoors and SQL injections, along with other advanced tactics, this group has launched a large number of attacks on prominent agencies, government and military systems, and private companies globally under what has been termed "Operation Cleaver."

GUCCIFER 2.0

Guccifer 2.0 is the "lone hacker" who took credit for providing WikiLeaks with stolen emails from the Democratic National Committee in 2016. Varying reports exist of Guccifer's nationality; however, apparently, the common belief is that he is an officer of Russia's Main Intelligence Directorate.

THE JESTER/TH3J35T3R

The Jester is an unidentified computer vigilante who describes himself as a “grey hat” hacktivist. He claims to be responsible for attacks on WikiLeaks, 4chan, Iranian President Mahmoud Ahmadinejad and Islamist websites. He claims to be acting out of American patriotism. The Jester uses a DoS tool known as “XerXeS,” which he claims to have developed. One of The Jester’s traits is to tweet “TANGO DOWN” on Twitter whenever he purports to have successfully taken down a website. In recent years, The Jester focuses on political issues within the United States.

MODUS OPERANDI: The primary methods of these groups range greatly from hacktivist abilities to those posed by nation-state operators. In some cases, these actors could just be considered political hacktivists, such as The Jester, who engage in DDoS attacks and defacements, whereas actors such as Guccifer 2.0 and SEA use more advanced techniques, such as worming malware, credential theft and data exfiltration.

PREFERRED TARGETS: Political hackers typically target government agencies but are known to attack key figures and corporations associated with opposing political parties.

2.7 THREAT ACTORS

RANSOM DENIAL OF SERVICE

RANSOM DENIAL OF SERVICE (RDOS) IS A TYPE OF DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK MOTIVATED BY MONETARY GAIN. IN AN RDOS ATTACK, THE PERPETRATORS SEND A LETTER THREATENING TO ATTACK AN ORGANIZATION BY RENDERING ITS OPERATIONS OR CAPABILITIES UNAVAILABLE UNLESS A RANSOM IS PAID BY A SPECIFIED DEADLINE.

In some cases, attackers will launch a small-scale attack on the victim's network as evidence that the threat is real.

These attacks have increased since 2010 and typically take the form of volumetric DDoS attacks. However, it is increasingly in vogue to find more piercing and efficient techniques without generating large volumes. The most advanced attacks combine both volume and nonvolumetric cyberattack techniques. Additionally, over the last several years, a number of copycat groups has emerged to profit off the names of others. Groups such as Fancy Bear and Lizard Squad have allegedly sent out RDoS ransom notes; however, neither is known to launch ransom campaigns, and both have been deemed to be fake groups.

These criminals have an array of targets. Actual RDoS criminals typically target only a handful of victims in a single vertical. However, as stated earlier, there are also fake RDoS groups that target hundreds of companies across multiple verticals in a single day, leveraging the same bitcoin address and expiration time. In reality, there is no way a single group could follow through and attack such a large number of companies simultaneously.

Although it is almost impossible to determine if a ransom note comes from a competent hacking group or an amateur unit, there are several indicators to distinguish between the two:

- Fake RDoS groups often request a different amount of money than the original
- "Real" groups prove their competence; "fake" groups exclude the "demo" attack
- "Fake" groups do not have official websites or target lists
- When hackers launch real RDoS attacks, they normally target less than a dozen companies, all within the same industry
- Look for other suspicious indicators: Is the group known for DDoS attacks?

DD4BC

DD4BC was the pioneer of the DDoS extortion tactics and inspired a wave of other extortionists. Emerging in 2014 and rapidly gaining notoriety in late 2015, this group executed over 100 confirmed attacks before members' arrests.

ARMADA COLLECTIVE

The original Armada Collective surfaced in 2015, after the rise of DD4BC, with a series of attacks focused on banks, e-commerce sites and hosting services in Russia, Thailand and Switzerland. This group followed the same mission pattern as DD4BC by sending a ransom note to select companies in a single industry, followed by a sample DDoS attack. If the ransom was not paid in the allotted time, the group launched a persistent multivector DDoS attack campaign.

XMR

RDoS group XMR_Squad emerged in 2017. Its attacks targeted companies in Germany and the United States, but were notably different from others. XMR_Squad has an official Twitter account and a website, likely set up during its original campaign to garner recognition. The group also changes currencies as its campaigns continue. The group began with euros, followed by bitcoins, and now uses XMR. This group has also engaged victims by sending out threats via Twitter.

PHANTOM SQUAD

Another group of extortionists emerged in 2017 and leveraged the same name of the original, notorious Phantom Squad from 2015. This new group began spamming ransom demands in September 2017 to companies throughout Europe, Asia and the United States. The threat was deemed fake because the group did not follow through with an attack.

MODUS OPERANDI: Typically, RDoS actors will send an extortion demand to their victim and follow it with a sample attack to prove their competence. If the ransom is not paid, the attackers will launch a denial-of-service attack.

PREFERRED TARGETS: Like organized cybercriminals, RDoS extortionists tend to target small and medium-sized businesses that lack advanced DDoS detection and mitigation and are therefore easier to extort.

3.0

CYBERSECURITY FORECAST

ACCURATELY FORECASTING CYBERATTACKS IS AKIN TO FINDING A NEEDLE IN A HAYSTACK … IN THE DARK. ATTACKS ARE GENERALLY THE RESULT OF OPPORTUNISTIC SITUATIONS THAT CAN ARISE IN THE MATTER OF DAYS OR HOURS. PREDICTING THESE TYPES OF ASSAULTS IS NEARLY IMPOSSIBLE.

However, a large percentage of other attacks are carefully coordinated and planned responses to events that organizations should be aware of in advance. By understanding cybercriminal tactics, techniques and procedures, you can eliminate the fear of the unknown so prevalent in cybersecurity.

DDOS

Denial-of-service campaigns vary in size and duration, but they often occur in parallel with specific events. For example, network operators in the gaming industry can expect attacks and degradation of services during gaming tournaments or product releases. Nations and regions can now expect to face cyberattacks associated with political, economical, or social events that are opposed for ideological reasons. For example, Israel faces a yearly campaign, OpIsrael, that is executed annually April 7–14.

Organizations involved directly and indirectly with the hunting and shipping of sea life (whales and dolphins) can expect to be targeted by OpKillingBay, an annual Anonymous operation, at the start of the hunting season. Organizations associated with large sporting events will draw unwanted cyber attention and should develop a pattern of auditing their systems ahead of events to prevent large-scale service outages.

MALICIOUS BOTS

There are “good” bots, and there are “bad” bots. While most good bots are active daily, crawling the internet for new content or gathering prices for consumers, bad bots typically follow a more predictable pattern. If observed, this can assist network operators with preparing for malicious activity. Scrapers that target the e-commerce industry typically increase activity between June and August as bot herders become more competitive during the slower shopping months. Holidays such as Black Friday, Cyber Monday and Valentine’s Day typically witness spikes in bot activity related to denial of inventory, carding and ad fraud. The travel industry is no exception either. It typically witnesses spikes in web scraping activity during September, but can also suffer from inventory exhaustion, carding and ad fraud, in addition to rating and review spamming.

SOCIAL EVENTS

The threat of bots is not limited to just online marketplaces. Malicious activity can also be forecasted based on social events. The crowds and target-rich environments created by high-profile events can bring an elevated risk for sponsors and vendors. The Super Bowl, Olympics and World Cup present a risk to organizers, partners, sponsors, suppliers, service providers and attendees. Bot herders are aware of these events and the profit that can be generated by targeting them.

These bad actors also have been known to target social events, such as political elections. Typically, these events are easy to forecast but difficult to pinpoint a starting point. Attacks typically include DDoS assaults and web defacement aimed at censoring or distorting information. Social bots can be used to manipulate voters. To maintain the integrity of an election, network operators and governments need to recognize patterns so they prepare for spikes in cyber activity as an election draws near.

4.0

PROACTIVE MEASURES

SAFEGUARDING YOUR ORGANIZATION MEANS NOT ONLY KNOWING YOUR ENEMY BUT ALSO UNDERSTANDING YOUR ORGANIZATION'S NETWORK.

Cybersecurity is a proactive, not a retroactive, industry. Today's evolving threat landscape omits the luxury of a hurry-up-and-wait strategy. To prepare for future threats, organizations must work to get ahead of modern cybercriminals. Information security requires a proactive team, which is constantly researching the latest threats before criminals have an opportunity to leverage the latest tactics, techniques and procedures against its networks.

Before researching the enemy and potential attack vectors, understand your organization's weaknesses. Ensuring regularly updated hardware and consistently patched software is the first step in the right direction. Second, conduct major audits of your networks in advance of potential conflicts. Some threats are impossible to predict, but most have a motive. If you can prepare for an event that may trigger an attack ahead of time, your organization will be better positioned to defend itself if/when an attack is launched.

Third, get in front of the problem by knowing cybercriminals, the way they operate and how they launch attacks. By understanding your network, its limitations and how hackers launch attacks, your organization can prepare for attack vectors commonly leveraged by different threat groups.

Last, understanding your network and IT infrastructure allows you to select the optimal DDoS solution for your organization. DDoS protection is not a one-size-fits-all menu, but rather it is an a la carte menu with many choices. Cybersecurity solutions come in various deployment options and with different capabilities, requiring each company to select the optimal solution that best fits its needs, threats and budget.

To know more about today's attack vectors, understand the business impact of cyberattacks or learn more about emerging attack types and tools, visit DDoSWarriors.com.

5.0

GLOSSARY

Amplification Attack — An amplification attack is a sophisticated denial-of-service attack that takes advantage of different server protocols to amplify the attack traffic. To launch an amplification attack, an attacker must locate an exposed server with a vulnerable protocol capable of facilitating an amplification attack. The attacker will generate a list of vulnerable servers known as an amplification list and then automate the process of sending spoofed requests to every device on the amplification list, resulting in the servers responding to the spoofed IP address with bandwidth-amplified attacks.

Cross-Site Scripting — In this attack, malicious scripts are injected into websites through a web application flaw where there is no validation of user input used by the application. The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine or spoof content to fool the user.

Data Theft — Sensitive data is compromised while the data is at rest or in transit through stealing encryption keys or hashed passwords or clearing text data off the server — and even from a user's browser.

Defacement — The attacker modifies the visual appearance of the website by hacking a web server and replacing the current website content with the attacker's own. This attack is most commonly associated with SQL.

Distributed Denial of Service (DDoS) — A distributed denial-of-service attack occurs when an attacker or a group of attackers simultaneously employ multiple machines to carry out a DDoS attack, thereby increasing its effectiveness and strength. The infected machines carrying out the attacks are often innocent, infected IoT devices controlled by the attacker via a C&C server.

DNS — A DNS amplification attack is an attack that sends an "ANY" DNS name lookup request to a list of open DNS servers with the source IP address spoofed to be its victim's IP address. The DNS server responds by sending all known information about the DNS zone to the victim's IP address, resulting in an amplified attack.

HTTP/S Flood — An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP Floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources and therefore can result in a denial of service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS Flood attacks are two of the most advanced threats facing web servers today because it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

Internet Control Message Protocol (ICMP) — Internet Control Message Protocol is a connectionless protocol used for IP operations, diagnostics and errors. An ICMP Flood — sending an abnormally large number of ICMP packets of any type (especially network latency-testing "ping" packets) — can overwhelm a target server that attempts to process every incoming ICMP request until a denial-of-service condition is achieved for the target server.

Local File Inclusion (LFI) — Although similar to RFI, with this vulnerability, the attacker has to upload the malicious script to the target server to be executed locally.

Memcached — A Memcached amplification attack is a UDP volumetric denial-of-service attack in which the attacker performs two malicious tasks similar to that of a DNS attack. First, the attacker builds an amplification list of vulnerable Memcached servers with UDP port 11211 exposed. In the second step, the attacker will send a spoofed GET request to the vulnerable Memcached servers on the amplification list. As a result, the Memcached servers will reply to the GET request and forward an amplified response to the spoofed IP address, the victim. The Memcached bandwidth amplification factor can range between 10,000x and 51,000x.

NTP — An NTP amplification assault sends spoofed NTP packets containing monlist — a command requesting a list of the last 600 hosts that connected to the addressed NTP server — to a list of vulnerable NTP servers. As a result, the NTP servers send the large, amplified reply to the spoofed IP address — the victim — thus flooding its network.

Phishing — A digital attempt to obtain sensitive information by using a malicious email or website. The attacker solicits personal information by posing as a trustworthy organization or the company itself. These attempts are either sent to everyone in the company or designed to target key associates. Once an associate falls victim to these, the hacker will then have the sensitive information required to gain access to certain systems.

Remote Code Execution — A remote attacker can construct a request with malicious content to exploit the vulnerability. A successful exploitation may lead to remote code injection of a Drupal server, which may lead to the server being completely compromised. Remote code execution attacks are an attacker's ability to execute malicious code or command on a target's machine to extract sensitive information and/or abuse the system functionality and can result in taking full control of the server.

Remote File Inclusion (RFI) — This type of vulnerability is most often found on PHP running websites. It allows an attacker to include a remotely hosted file, usually via a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can be as minimal as outputting the contents of the file, but depending on the severity, it could lead to arbitrary code execution.

Social Engineering — A process of psychological manipulation, more commonly known as human hacking. The goal is to have the targeted victim divulge confidential information or give unauthorized access because the hacker has played off the victim's natural human emotion of wanting to help or support. Most of the time, the attacker's motives are to gather information for future cyberattacks, commit fraud or gain system access for malicious activity.

SQL Injection — This technique takes advantage of poor application coding. When the application inputs are not sanitized, they become vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database and more.

SSDP — An SSDP amplification attack sends spoofed packets containing the victim's IP address to a list of active universal plug-and-play (UPnP) devices. The spoofed packet with an ssdp:rootdevice or ssd:all sent to each UPnP device on the list replies back with an amplified answer to the victim's machine that contains all the services on the device.

SYN — A SYN Flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and to subsequently wait for an ACK packet that never arrives. A server under a SYN Flood attack will continue to wait for a SYN-ACK packet for each connection request because the delay could be normal and related to network congestion. However, since a SYN-ACK packet never arrives for any of the connection requests, the massive number of half-open connections quickly fills up the server's TCB table before it can time out any of the connections. This process continues for as long as the flood attack continues.

TCP Flood — One of the oldest, yet very popular denial-of-service attacks, TCP Flood involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP, so the reply (SYN-ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives, and they store this state in tables that have limited size. As big as this table may be, it is easy to send a sufficient amount of SYN packets that will fill the table. Once this happens, the server starts to drop new requests, including legitimate ones. Similar effects can happen on a firewall that also has to process each SYN packet. Unlike other TCP or application-level attacks, the attacker does not have to use a real IP — which is perhaps the biggest strength of the attack.

UDP Flood — In a UDP Flood, the attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP Flood is to saturate the internet pipe. In most cases, the attackers spoof the SRC (source) IP.

radware

www.radware.com