radware

A Guide to State-Sponsored Cyberthreats

Who Are the Adversaries and How to Defend Against Them

A Guide To State-Sponsored Cyberthreats

Who Are the Adversaries and How to Defend Against Them

Contents

There is a global chess match between nation-states, businesses and the various digital assets contained within these organizations.

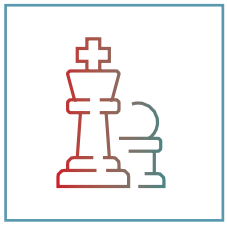
The result is that state-sponsored cyberattacks have emerged as one of the preeminent threats targeting companies today.

Backed by governments and funded with the biggest bankrolls, state-sponsored groups can apply seemingly limitless resources to achieve their malicious objectives in an age when security communities are strapped by tight budgets and a cybersecurity talent shortage.

The frequency and ferocity of these attacks continue to increase. Nation-state attacks increased from 12% to 23% in the past year, according to Verizon's 2019 Data Breach Investigations Report.[1]

In recent years, large-scale cyberattacks have been attributed to state-sponsored groups ranging from superpowers such as Russia and China to smaller countries such as Iran and North Korea. New battle lines have been drawn across the world, and organizations require the expertise and tools to fight state-sponsored cyberattacks.

This guide dissects the motivations that fuel these groups, their modi operandi, the largest state-sponsored groups that are currently active and steps that will mitigate the threats.



***State-sponsored cyberattacks** have emerged as one of the preeminent threats targeting companies today.*

[1]https://enterprise.verizon.com/resources/reports/dbir/?cmp=paid_search:google:ves:sem:awareness&gclid=EAIaIQobChMI84Ow9drE5QIViYVaBR2XIw8gEAAYASAAEgJW2_D_BwE

Motivations and Consequences

The motivations and resulting consequences of state-sponsored cyberattacks are as far ranging as the geographies from which they originate. Nation-state hackers target government agencies, critical infrastructure and any and all industries known to contain sensitive data or property. Typically, they strike via sophisticated techniques that interrupt business operations, leak confidential information and generate massive data and revenue loss.

Part of the onus falls on corporations. All too often, public and private organizations unwittingly leave sensitive, monetizable data, such as intellectual property (IP), unprotected, making cyberattacks a high-stakes, low-risk venture for nation-states.

Of all the primary impacts from state-sponsored attacks, one of the worst is the loss of IP. The compromise of IP can be one of the most crippling results of a state cyberattack for a business — with the results reverberating for decades. The IP Commission estimates that counterfeit goods, pirated software and stolen trade secrets cost the U.S. economy $600 billion annually.[2] For example, in recent years, Iran was charged with stealing $3.4 billion in scientific data from almost 8,000 professors at 320 universities.[3]

Download
Intellectual Property: The Ultimate Cost of a Cyberattack
Infographic

Watch the Video
Your Intellectual Property Is at Stake

Organizations unwittingly leave sensitive, monetizable data, such as IP, unprotected, *making cyberattacks a high-stakes, low-risk venture for nation-states.*

[2]http://ipcommission.org/press/IPC_press_release_030818.pdf
[3]http://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and

Notable Nation-State Attacks of 2019

DNS hijacking campaign

Iranian hackers are suspected of a wave of DNS hijacking attempts against domains belonging to government, telecom and internet infrastructure organizations.[4]

Operation Soft Cell

Hackers compromised the IT infrastructures of 10 telecom companies, setting up VPNs with administrator privileges to gain access to customer data, with specific interest in about 20 high-value targets.[5]

Operation ShadowHammer

Using the ASUS Live Update utility, hackers installed back doors on ASUS computers around the globe to target a pool of users identified by their network adapters' MAC addresses.[6]

[4]https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

[5]https://www.scmagazine.com/home/security-news/apts-cyberespionage/operation-soft-cell-campaign-targets-cellular-telecom-providers-points-to-chinas-apt10/

[6]https://securelist.com/operation-shadowhammer/89992/

Take the manufacturing industry for example. Remarkably, 94% of all cyberattacks currently aimed at the manufacturing industry are motivated by espionage, usually with the intent to steal trade secrets, according to the Swedish Security & Defense Industry Association (SOFF). According to the same research, 10 years ago, security researchers typically spent 90% of their time looking into criminal campaigns, such as botnets, Trojan horses, etc. Today, researchers spend the same amount of time investigating nation-state attacks aimed at stealing secrets and/or sabotage.[7]

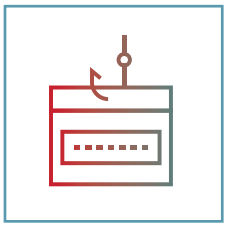
Recent state-sponsored threats also leverage cyberattacks to influence elections worldwide. While manipulating elections is not new, using cyberattacks to alter them is, and the collateral damage resulting from a breach and the subsequent release of sensitive information can have a far-reaching impact. These operations are typically complex, lengthy campaigns designed to influence voter behavior by releasing sensitive information at crucial times. For example, in July 2018, a United States federal grand jury filed indictments against Russian military intelligence officers for their alleged role in interfering with the 2016 U.S. presidential election.[8] These indictments include gaining unauthorized access to the computers of U.S. entities involved in the 2016 elections and staging the release of the ensuing stolen documents to influence the election.

Lastly, military/national defense goals are also impacted. In particular, smaller nation-states seeking to gain military parity with larger countries will rely on cyberattacks to level the playing field. In addition to launching cyberattacks to steal sensitive defense information, they will orchestrate for-profit cyberattacks to fund defense budgets. In September 2018, the Department of Justice announced criminal charges against Park Jin Hyok, an alleged member of a North Korean government-backed hacking team known as Lazarus.[9] This group is known for the creation of the malware used in the 2017 WannaCry ransomware attack, the theft of $81 million from Bangladesh Bank and several other attacks on the financial services industry, all with the goal of funding North Korea's defense programs.

[7]https://soff.se/wp-content/uploads/2018/03/Cybersecurity_statsunderst%C3%B6dda-akt%C3%B6rer.pdf
[8]https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
[9]https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Modus Operandi

Generally speaking, state-sponsored threats are cyberthreats posed by those whose primary objectives include espionage and subversion. These groups are often backed by governments and possess a variety of techniques and skills at their disposal with the ability to develop more advanced attack vectors. Unlike hackers, state-sponsored groups often create and leverage custom attack vectors by incorporating previously undiscovered software vulnerabilities, called zero-day attacks. These advanced attacks are why state-sponsored cyberthreats are often referred to as advanced persistent threats (APTs).



The State-Sponsored Threat

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.

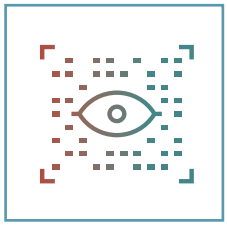
Preferred Targets

Nation-state actors typically target the public sector, the defense industry/government agencies, financial institutions and critical infrastructure. They look for any data that will benefit their country's economy and strengthen both key business and military strategies.

In recent years, the cybersecurity community has found itself vexed by a handful of attacks that could not be easily pinned on a single group. This is mainly due to an overlap in tactics, techniques and procedures (TTPs). This uptick in unidentifiable incidents suggests that state-sponsored hacking groups have enhanced their ability to deceive researchers as to which group is responsible for an attack.

Covertness is key, which makes attributing government-backed attacks difficult and complex. State-sponsored actors rarely make a lot of "noise" or cause sufficient disruption to warrant suspicion or trigger detection. This allows these cybercriminals to maintain a foothold in a target's network for longer durations, as their objective is to remain persistent to retain oversight of communications or access sensitive data. For example, they will often plant persistence mechanisms (hidden malware) throughout a victim's network, which may go untouched or dormant for years.

These groups do not attack indiscriminately, but when they do, each of them attacks with a specific purpose. They are methodical and surgical. Using various intelligence-gathering techniques and exploits, they will often access and live-monitor sensitive data on a targeted network. The aerospace/defense, government and financial sectors and utility/energy companies are the most common targets, but all industries can fall into the crosshairs of a state-sponsored group due to specific types of sensitive data/IP that they possess and/or geopolitical events.



Nation-state attacks increased from 12% to 23% in the past year, according to ***Verizon's 2019 Data Breach Investigations Report.***

The Threat Landscape

There are approximately two dozen countries around the world currently suspected of state-sponsored programs for governmental cyberattacks.[10] World governments are actively investing in building and operating cyber-espionage teams to both protect their national interests and collect IP for their domestic industries. Their goals are to acquire expertise, malicious botnets and cyberattack tools to further advance their craft. If an organization competes based on its IP in a global marketplace, then it may be a mark for governmental cyberattacks.

Certain nations are more direct and public about the domestic industries that they are interested in expanding/growing and even go as far as detailing the types of IP that they are interested in acquiring from foreign corporations.

Take China for example. It's position paper, *Made in China 2025*, describes specific industries in which it has a strategic interest in building domestic expertise.[11] The plan lays out a very aggressive goal of producing 70% of the content in the following industries with Chinese enterprises: IT, robotics, green energy and electric vehicles, aerospace, ocean engineering, railroads, power, materials, medicine, and medicine tech and agriculture engineering. These plans require domestic industries in developing countries to acquire massive amounts of new IP to meet this 70% local content threshold.

U.S. intelligence agencies have stated that Chinese recruitment of foreign scientists, its theft of U.S. intellectual property via cyber espionage, and targeted acquisitions of U.S. firms constitute an ***"unprecedented threat" to the U.S. industrial base.***

[10]https://www.cfr.org/interactive/cyber-operations
[11]https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

The Major Players

Here is a breakdown of the five-largest state-sponsored groups that are currently active.

APT28 | Russia

APT28, also known as Fancy Bear, Pawn Storm and Sofacy, 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, the malware compromises, disrupts and influences political agendas around the world. The group targets government elections, the media, sporting events and several global companies.

Most recently, a group identifying itself as Fancy Bear has claimed responsibility for a global ransom denial-of-service (RDoS) campaign targeting financial service institutions. This RDoS campaign included extortion letters, which requested two bitcoins, with the ransom increasing by one bitcoin every day without payment.

Lazarus Group | North Korea

Lazarus Group, also known as Hidden Cobra, is a cybercrime group associated with the North Korean government. This nation-state group has been in operation since 2009 and is responsible for various attacks over the past decade, including Ten Days of Rain, the 2014 Sony data breach, the WannaCry[12] 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 signals intelligence (SIGINT) program, this group has the ability to compromise commonly used hardware such as routers, switches and firewalls. In 2016, the Shadow Brokers hacking group announced that it had compromised Equation Group's toolset 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 Crew, is a cyberwarfare organization associated with the Chinese People's Liberation Army. This nation-state group has been known since 2006 and has been attributed for a number of attacks, including stealing intellectual property and information from U.S. corporations resulting in indictments against five members. 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.

APT33 | Iran

APT33, also known as Elfin, is a suspected Iranian-backed cyber-espionage unit that targets government agencies, research firms, financial institutions and engineering companies in the U.S. and Saudi Arabia. The group has been in operation since 2013 attributed for a number of high-profile attacks,[13] including the recent exploitation of the known vulnerability CVE-2017-11774 against U.S. government agencies.[14] Elfin uses a combination of publicly available attack tools and custom malware to target its victims. Like many other nation-state groups, its first stage of attack comes in the form of a phishing email. After the initial compromise, the group downloads additional payloads to further compromise the network and exfiltrate targeted data.

[12]https://security.radware.com/ddos-threats-attacks/wannacry-ransomware/
[13]https://www.fireeye.com/blog/threat-research/2018/12/overruled-containing-a-potentially-destructive-adversary.html
[14]https://www.bleepingcomputer.com/news/security/outlook-flaw-exploited-by-iranian-apt33-us-cybercom-issues-alert/

Attack Techniques and Trends

When it comes to TTPs, attacks can be as complicated and far ranging as the geographies from which they originate. For gaining initial access into an organization's network, spear-phishing attacks continue to loom as one of the primary attack vectors. These attacks serve as a beachhead, allowing threat actors to establish persistence access within a targeted device, so they can escalate their privileges and move across the network before "breaking out" to exfiltrate or encrypt sensitive data and IP.

Spear-phishing emails typically contain a malicious attachment, link or service. This is also known as malspam or malicious spam. Other common vectors for initial access include supply chain compromise and exploitation of public-facing applications. During the initial compromise, a payload will be executed that is designed to gain access to the targeted machine and perform specific tasks for further exploitation.

Breakout time — the speed at which adversaries accomplish lateral movement in the victim's environment after their initial compromise — is important because it represents the time limit for defenders to respond to and contain or remediate an intrusion before it spreads widely in their environment and leads to a major breach. Within the industry, Russian-backed actors have shown their ability to break out in less than 20 seconds. Speed is essential in cybersecurity — for both offense and defense.

Lastly, in an alarming trend, hackers acting on behalf of nation-states and APT groups are also increasingly carrying out zero-day attacks. Cybersecurity Ventures research[15] predicts there will be one zero-day attack per day by 2021. The ability to quickly identify and mitigate these attacks is critical. A zero-day attack is the first instance of a vulnerability being exploited, so if adequate defenses aren't in place, organizations are left vulnerable.

The ability to quickly identify and mitigate zero-day attacks is critical. *A zero-day attack is the first instance of a vulnerability being exploited, so if adequate defenses aren't in place, organizations are left vulnerable.*

[15]https://cybersecurityventures.com/zero-day-vulnerabilities-attacks-exploits-report-2017/

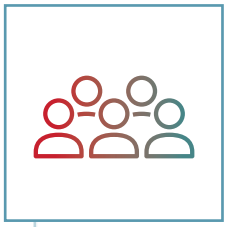
Mitigating the State-Sponsored Threat

Simply put, most enterprises don't have the in-house expertise to battle government-backed cyber operations. It is neither advisable nor practical for businesses to go at it alone when facing APT groups. Most organization don't have the budget or expertise to battle APT groups in real time.

There is, however, protection in numbers. While nation-states continually fine-tune and expand their respective APT groups, security communities counter this by pooling the expertise and knowledge of security experts. Organizations such as MITRE ATT&CK™ seek to stay abreast of the growing threat landscape.[16] These knowledge bases are designed for organizations to develop specific threat models and strategies for defense based on real-world attacks and observations. These real-world observations include initial access, execution, persistence, escalation, evasion, access, discovery, movement, collection, command and control, exfiltration and impact.

The security industry is witnessing new innovations as well, such as the United Kingdom's Cyber Skills Immediate Impact Fund.[17] This fund promotes neurodiversity to help close the security skills gap. This new initiative taps into groups of people that are able to improve cybersecurity through their different and valuable coding abilities such as those on the autism spectrum for their puzzle-solving prowess. However, initiatives like this alone will take years to provide the additional security talent required today.

Ultimately, managed security solutions are the near-term answer. Cloud and service security providers represent the cornerstone for protecting businesses. Enterprises can never invest enough resources to stay ahead of the rapidly evolving threat landscape; however, cloud DDoS and service providers have both the scale and power of crowdsourcing (see Cybersecurity Intelligence Agency, below) to supplement an organization's in-house expertise to protect it from the most nefarious state-sponsored actor. It is the security experts and SOC engineers at leading DDoS mitigation



Cloud DDoS and service providers have both the scale and power of crowdsourcing *to supplement an organization's in-house expertise to protect it from the most nefarious state-sponsored actor.*

[16]https://attack.mitre.org/
[17]https://www.gov.uk/government/publications/cyber-security-skills-immediate-impact-fund

vendors who are best positioned to protect the IP of enterprises worldwide, not the hundreds of disparate IT managers who comprise the IT department of a Fortune 500 company.

Here are four key strategies that any and every organization should consider before mitigating the state-sponsored threat:

Train Your Employees

The first step in preventing these attacks is employee training. Your employees are the weakest link. Training them how to spot phishing and spear-phishing attempts can help prevent future attacks, as these techniques can thwart even the most informed, well prepared defenses. Still, CISOs can lower risks by regularly training and testing employees about proper cyber hygiene and awareness.

In addition, insider threats may be the biggest vulnerability to any enterprise. These threats are typically caused by opportunistic or disgruntled employees whose primary objectives are profit, company shaming or espionage.

If you believe that 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 and network hardware that can be plugged into other devices.

Coordinate With Law Enforcement and Other Businesses

The sharing of cyberthreat information among businesses and governmental organizations can help mitigate attacks from nation-states and enhances situational awareness as well. Monitor the threat landscape, and collaborate with industry bodies, law enforcement and government agencies to stay on top of attack patterns and trends.

A Cybersecurity Intelligence Agency

Data is the key. The future of automated security is evolving into an ecosystem of virtual intelligence that learns from big data, informs network perimeter defenses and then collects data from both perimeter and endpoint security as well as the network's traffic flow — in real time and over long trend lines.

The sheer volume and expansive nature of the cybersecurity threat landscape combined with the difficulties associated with information overload denote that organizations need assistance. Enter your DDoS mitigation vendor, which should serve as an "intelligence agency," providing unique, real-time intel on emerging nation-state threats for preemptive protection. This data should come from your vendor's global network of DDoS scrubbing centers, its team of security experts who assist its customers and its ability to leverage a global community of millions of users from which to collect live intelligence and analyze it via machine learning algorithms. Ultimately, knowledge is power.

Automation and Machine Learning

Given the aforementioned breakout times that state-sponsored threats can now achieve, human diagnosis and mitigation are no longer enough. Mitigating these highly advanced state-sponsored attacks requires DDoS protection solutions that combine machine learning capabilities with negative and positive security protection models.

Traditional DDoS solutions use rate limiting and manual signature creation to mitigate attacks. Automation and, more specifically, machine learning overcome the drawbacks of those approaches by automatically creating signatures and adapting protections to changing attack vectors. Machine learning leverages advanced mathematical models and algorithms to look at baseline network parameters, assess network behavior, automatically create attack signatures and adapt security configurations and/or policies to mitigate attacks.