WHITEPAPER

The Top Cybersecurity Threats of 2017

NOPSEC

nopsec.com | info@nopsec.com

The Top Cybersecurity Threats of 2017

In the world of cybersecurity, the year 2016 will be remembered for some big moments: the largest known distributed denial of service (DDoS) attack; multiple successful breaches of the SWIFT banking system; a phishing attack on a United States presidential candidate's campaign; and ransomware attacks on major healthcare organizations, just to name a few. Financial services, healthcare, and government - sectors of the economy that underpin and are inextricably tied to nearly every aspect of modern life - saw the highest number of attacks.

Each year brings technology improvements at an exponentially higher rate, which only serves to bait cyber criminals to come up with new strategies and tools. As we look forward into 2017, it's necessary to think like a hacker in order to stay ahead of the security challenges to come. Based on current trends, this report outlines five of the biggest cyber threats that NopSec expects to see in 2017: nation-state cyber attacks; ransomware, DDoS attacks, the Internet of Things, and social engineering and human error. Read on for more information on what these trends could mean for your organization, and how you can mitigate them.

Nation-State Cyber Attacks

Nation-state cyber attacks refer to foreign government (or government-directed) organizations targeting other countries' government or commercial institutions or infrastructure. There are numerous possible motivations for these kinds of cyber attacks. Eroding rivals' economic and military competitiveness; influencing the political and diplomatic landscape; obtaining intelligence to advance weapons proliferation programs; and cyber warfare to create an advantage in armed conflict are just a few.

Media reports in 2016 brought nation-state-sponsored cyber attacks to the public consciousness to an unprecedented degree. The U.S. intelligence community assessed that senior Russian officials authorized data theft and disclosure in order to influence the 2016 U.S. election. Malware linked to the U.S. National Security Agency (NSA) was stolen, possibly by hackers with Russian ties, who attempted to auction the malware online. Yahoo reported that hackers who stole user data two years prior may have been state-sponsored.

In the spring of 2016, the U.S. Government Accountability Office (GAO) reported a 13-fold increase in cyber attacks on 24 federal agencies between 2006 and 2015, with nation-state-sponsored hacks remaining the biggest threat to high-impact government systems. Leading cybersecurity firm FireEye has kept a close watch on Russia's state-sponsored cyber activity. They predict that the aggressive actions seen in 2016 will continue this year given the country's capabilities, operational security, and ability to fund their objectives.

Given all that is at stake, nation-state attacks are only going to continue to grow in number and sophistication. As technology and security advance, countries will continue to devote resources toward cyber espionage and warfare.

1 Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States. Accessed January 9, 2017. http://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf

2 "Hacking group auctions 'cyber weapons' stolen from NSA." The Guardian. Accessed January 25, 2017. https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

3 "Yahoo 'state' hackers stole data from 500 million users." BBC. Accessed January 10, 2017. http://www.bbc.com/news/world-us-canada-37447016

4 Agencies Need to Improve Controls over Selected High-Impact Systems. U.S. GAO. Accessed January 9, 2017. http://www.gao.gov/assets/680/677293.pdf

5 "Questions and Answers: The 2017 Security Landscape." FireEye. Accessed January 19, 2017. https://www2.fireeye.com/WEB-RPT-2017-Cyber-Security-Predictions.html

Ransomware

Analysts' predictions for the degree to which ransomware attacks will grow this year vary - some say the growth will slow down, and others believe it will accelerate over what we saw in 2016. The U.S. Computer Emergency Readiness Team (US-CERT) reported 4,000 average daily ransomware attacks in 2016, or four times as many average daily attacks as in 2015. Some hope that increased awareness and law enforcement will stem this trend in the near future, but one thing is certain: ransomware attacks will continue.

In 2016 an average of 4,000 ransomware attacks were reported daily

Crypto-ransomware is the most effective form, using unbreakable encryption to lock users' files until a payment is received. Common office documents, like .docx, .xlsx, .pptx, photographs, and video files are usually targeted. Once the files have been encrypted, the ransomware will typically upload the private key to a remote server and delete the local copy. The victim will then see a demand for payment, usually using a cryptocurrency like Bitcoin, by a certain deadline in order to get the files back.

Even if ransomware defenses are improving, the revenue that hackers can get from it - by some accounts, $1 billion or more last year - means they won't be scared off easily. Not only that, but just like the technology evolves with new ransomware variants and families popping up, the business model for ransomware is changing, too. Ransomware as a service (RaaS) is now being sold on the dark web, opening up an opportunity for more criminals who lack technical sophistication to execute this form of cyber attack.

Typically, the RaaS user can download the malware for little or no cost, and splits any proceeds earned with the originator. RaaS malware Cerber reportedly makes millions in revenue each year despite a small percentage of victims choosing to pay the ransom. Ransomworms, which are ransomware that replicates itself to rapidly spread to multiple computers, have also been reported, and will likely proliferate. (For more information on preventing damage from ransomware, see our white paper.

6 "Ransomware took in $1 billion in 2016--improved defenses may not be enough to stem the tide." CIO.com. Accessed January 10, 2017

7 http://www.cio.com/article/3154988/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html

Distributed Denial of Service (DDoS) Attacks

The fall of 2016 saw what was at that time believed to be the world's largest distributed denial of service (DDoS) attack on French cloud computing company OVH. Then a month later, it was surpassed when internet performance management firm Dyn was hit by an attack that may have approached a volume of 1.2 terabits per second, taking down multiple popular sites like Amazon, CNN, Visa, and Twitter.

Most DDoS attacks fall into one of three categories, each measured differently and targeting different components of the IT infrastructure. Volume-based attacks, measured in bits per second (BPS), saturate a site's bandwidth to block other visitors. Protocol attacks, measured in packets per second, attack servers and intermediate communication equipment in order to tie up enough of these resources to lead to denial of service. The third major category is application layer attacks, which are measured in requests per second. These attacks attempt to crash web servers through a flood of requests that appear legitimate.

These attacks have the ability to take down multiple major websites like Amazon, CNN, Visa, and Twitter

Victims of a DDoS attack may or may not know the reason they were targeted. Hackers may have political motivations, desire to take out business competition, use it as a means of extorting money, or execute an attack to distract victims while performing another malicious action.

Based on 2016's trends, we expect in 2017 to see more frequent and severe DDoS incidents. Both Dyn and OVH can thank the Mirai botnet for the disruption. Mirai's targeting of Internet of Things (IoT) devices allowed it to reach the massive scale that it did in these high-profile attacks. This brings us to our next top cyber threat for the year: IoT.

The Internet of Things (IoT)

The constantly expanding world of the Internet of Things (IoT) has already given hackers plenty of opportunity. The largest known DDoS attacks described above were made possible by a botnet that targeted IoT devices, whose rapidly growing number also means the proliferation of unpatched security vulnerabilities. Gartner estimates that by 2020, consumers and businesses will be using more than 20 billion IoT devices (compare to just under 5 billion in 2015). We can only expect to see more attacks in 2017 on smart devices that are often insufficiently monitored or secured.

IoT security easily falls under the radar for many users. But imagine the leverage that a malicious actor could have over a large healthcare organization if the attacker were to gain access to the amount of electronic protected health information stored on the organization's network of medical devices. Vulnerable networked video cameras and camera-enabled smart devices provide criminals access to sensitive recorded audio and visual information behind closed doors at target organizations. And recall Ukraine in late 2015 and again late last year, when hackers proved that they could target IoT to take down massive swaths of a country's power grid, leaving residents in the dark in the middle of winter.

Hackers proved that they could target IoT to take down massive swaths of a country's power

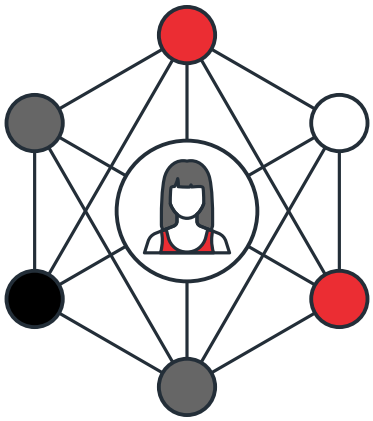
Those are just a few examples among many. Recognizing the threat to consumer health, safety, and privacy by vulnerable mobile medical devices, in December of 2016, the U.S. Food and Drug Administration (FDA) released their final guidance report, "Postmarket Management of Cybersecurity in Medical Devices." The report provides only guidance, not new enforceable responsibilities for medical IoT manufacturers - but it does point to the fact that "FDA-approved" does not necessarily mean "secure" in the cyber world. (Manufacturers must notify the FDA if a patient is seriously harmed as a result of a security vulnerability in a device, but not if a vulnerability is identified before anyone is harmed nor every time a patch is installed.)

The IoT brings an unprecedented level of connectivity and convenience to our modern lives. Unfortunately, with the myriad of benefits and efficiencies that are created by IoT technology comes additional risk that manufacturers and users need to remain vigilant about throughout the product life cycle. Regulators will struggle to keep up with the evolving threats. The possibilities are nearly endless for creative and motivated hackers to use IoT to steal, damage, destroy, or simply mess with people's heads.

8 "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015." Gartner press release. Accessed January 11, 2017.
http://www.gartner.com/newsroom/id/3165317

Social Engineering and Human Error

Security experts can hardly say it enough: humans are your biggest cybersecurity vulnerability. The breaches can be intentional or unintentional. They can be the result of a single employee's carelessness, a disgruntled employee seeking revenge, or the victimization of an employee by a sophisticated hacker.



Humans will continue to be the biggest cybersecurity threat in 2017

"Social engineering" is a fancy way of saying "tricking" a user into providing sensitive information. Most email-savvy employees probably assume they can identify a spam email meant to scam the recipient out of money. What they often don't realize is that these kinds of attacks are becoming much more sophisticated. Tactics that rely on social engineering, like spear phishing, succeed because the attacker has an intimate understanding of an employee's motivations and role within an organization so that these can be precisely exploited. They know enough about the personal and professional lives of their victims to effectively impersonate someone the victim trusts or craft an email or pop-up window that looks legitimate to someone without sufficient training.

Then there are good old-fashioned human errors that leave networks open to opportunistic cyber criminals. Remembering strong passwords for multiple devices is a struggle for most consumers and employees, leading to poor password hygiene. Busy high-volume businesses like healthcare organizations may have difficulty managing privileged users effectively, leading to inappropriate access.

Human beings increasingly rely on technology to make their lives easier and achieve aims that they could not reach using people power alone. But there has yet to be technology developed to make humans infallible, and they will continue to be the biggest cybersecurity threat in 2017 and beyond.

What Can Be Done?

The challenge of keeping risk to an acceptable minimum is big, but it is by no means insurmountable. There are ways to mitigate these threats.

It's crucial that you have an ongoing security strategy. Invest in a security program, comprehensive policies, and training, not just a compliance checklist. If you have not already done so, we recommend starting with a thorough security assessment and gap analysis to identify areas of risk and opportunity to build on your existing security measures.

Conduct regular penetration testing and vulnerability assessments, and take advantage of threat intelligence in order to determine who is targeting your industry, what approaches they employ, and whether you are likely to be targeted. You should also have a remediation strategy that will allow you to resolve any vulnerability or compromise with a minimum of disruption to your business and customers. [http://info.nopsec.com/2016-Remediation-101-A-White-Paper.html]

As we gain a better understanding of how things like ransomware and social engineering work, mitigation strategies are simultaneously emerging. On the human level, this involves training employees to identify potential attack vectors, and making them aware of the risks to their organization and the role they have to play in protecting it.

2017 will see major advancements in technology. With these advancements, we must monitor the technology we use to make sure we're protected from ever-evolving cyber threats. Remember that your security program cannot be successful through a top-down approach that merely involves management, nor just the IT team. Every employee has a role to play in protecting the business and must have the training and awareness to do their part.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email info@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.