WHITEPAPER

2018 Top Cybersecurity Threats

Table of Contents

Introduction

It's a cliché now to declare any year *the year of the* _____*-breach*. It's especially difficult to see around corners in the cybersecurity industry, but not impossible. To do so, it's necessary to closely watch and understand the latest technologies, socio-economic trends, legal/privacy trends and even political climates.

May 19th, 2018 will mark the 20th anniversary of the L0pht hacker group testifying at the US Senate[1]. It's a sobering reminder that, while the security industry has built amazing technologies and has advanced in some areas, it has made shockingly little progress in other areas, like software liability, data privacy and software quality.

For every enterprise and technology vendor that learns from its mistakes and 'grows up', we have new entrants making the 1990's era mistakes remarked by Mudge, Space Rogue, Weld Pond and the other members of L0pht in this 20-year-old video. It's a reminder that this industry is still young and building a lasting legacy is difficult when the software and technology we're tasked with securing changes so quickly.

In the early 2000's it was common to hear security practitioners discuss their luck after getting hit by a virus or worm. "Code Red only defaces websites and launches DDoS attacks, could you imagine if it deleted files?" In 2017, with WannaCry and NotPetya, we've finally seen malware that was both destructive and indiscriminate.

With the attacks against Saudi Aramco (2012) and Sony Pictures (2014), at least the wipers used in these campaigns were limited to the target companies. WannaCry happily spread across the Internet and NotPetya was able to spread through fully patched environments. Luckily, Marcus Hutchins found a kill switch for WannaCry early in the attack and NotPetya was restricted to the networks of organizations running a relatively

[1] kingpinempire. "Hackers Testifying at the United States Senate, May 19, 1998 (L0pht Heavy Industries)." YouTube, YouTube, 14 Mar. 2011. www.youtube.com/watch?v=VVJldn_MmMY.

obscure Ukrainian accounting software package. If not for these limiting factors, these events could have been orders of magnitude worse. Even with these limiting factors, these two events were some of the most damaging and costly ever seen. This year, NopSec predicts that the biggest cyber threats will be massive data breaches, ransomware, opportunistic crypto-mining attacks and IoT hacking.

2017 in Review

Like any other year, 2017 had its share of data breaches, malware campaigns and emerging threats leveraging new technology. Ransomware was still going strong, the data breaches reported included the largest ever (Yahoo), IoT threats are as worrying as ever and cryptocurrency mining emerged as an opportunity for both legitimate and illegitimate use. As interesting as what we did see is what was missing. Exploit kits remain scarce, as do PCbased botnets. After Mirai generated some of the largest DDoS attacks ever seen in late 2016, the following year was relatively quiet. Now, early in 2018, a vulnerability in memcached, an open-source distributed memory caching system, was taken advantage of to create DDoS amplification attacks. This was used to generate the largest DDoS attack ever recorded, a 1.35Tbps attack against GitHub in late February.

As technology changes and security improves, attackers shift strategies. The best pay for the least effort and risk changes from year to year. Increases in state-sponsored hacking activities have had a profound impact on the overall landscape as well. The vastly greater budget and capabilities of nation-state offensive cyber teams increase the difficulty of predictions. Nation-state involvement leads to one of the most troubling trends of 2017. Increasingly, malware attacks and breaches have been attributed to government-funded campaigns. Espionage is one thing, but WannaCry and NotPetya proved there are governments willing to create and release highly destructive malware that is indifferent to the owners or locations of the systems it destroys.

Most of the remainder of this piece will dive deeper into some of the key areas for cyber threats and vulnerabilities in 2018. Finally, the concept of ‘Black Swans’ will be introduced as a method for predicting future threats and vulnerabilities that often seem unpredictable.

Massive Data Breaches

Some of the largest and most unique data breaches ever were seen in 2017. In September, Equifax announced[2] that it lost data belonging to 143 million people — more than half the adults currently living in the United States. Between the time the attack began and when the announcements were made, almost 5 months passed — more than enough for the information to be misused before the public had an opportunity to respond. Unlike most other breaches, this wasn't just names, email addresses and credit card numbers. The credit reports kept on file by credit bureaus like Equifax contain much more information. In October, Equifax announced an additional 2.5 million records were exposed as well.

Also in October, Yahoo revealed[3] that the total number of accounts compromised in 2013 was 3 billion. This is easily the largest breach ever, but the worst news was that it occurred over four years ago. In June, a company named Deep Root Analytics exposed the voter records[4] of 198 million Americans for 12 days, due to misconfigured access controls on an Amazon Web Services (AWS) S3 bucket. S3 buckets are essentially cloud storage drives, typically used to store the data and content used by applications run in AWS. This was one of at least[5] twenty S3 bucket-related breaches in 2017. Others included Booz Allen Hamilton, the Dow Jones and NICE Systems — a third party vendor for Verizon.

Finally, there's the Uber breach reported on November 2017[6]. Uber hasn't had an easy time on any front lately and data privacy is no exception. The breach exposed the data of 600,000 drivers in the US in addition to 57 million drivers and riders worldwide.

[2] Kumar, Mohit. "Equifax Hack Exposes Personal Info of 143 Million US Consumers." The Hacker News, 7 Sept. 2017, https://thehackernews.com/2017/09/equifax-credit-report-hack.html.

[3] Khandelwal, Swati. "It's 3 Billion! Yes, Every Single Yahoo Account Was Hacked In 2013 Data Breach." The Hacker News, 4 Oct. 2017, https://thehackernews.com/2017/10/yahoo-email-hacked.html.

[4] Newman, Lily Hay. "The Scarily Common Screw-Up That Exposed 198 Million Voter Records." Wired, Conde Nast, 19 June 2017,www.wired.com/story/voter-records-exposed-database/.

[5] Houmann, Claus Cramon Houmann Cramon. "Publicly Accessible Amazon S3 Buckets - a List of Cloud Misconfiguration Breaches." Peerlyst, https://www.peerlyst.com/posts/Publicly-accessible-amazon-s3-buckets-a-list-of-cloud-misconfiguration-breaches-claus-Cramon.

[6] Khosrowshahi, Dara. "2016 Data Security Incident." Uber Newsroom, 22 Nov. 2017, https://www.uber.com/newsroom/2016-data-incident/.

Reportedly, two hackers gained access to an S3 bucket containing the data. The details aren't clear, but they were able to capture an Uber developer's credentials to gain this access. This was also a case where the truth of the breach wasn't learned until well after the incident occurred — over a year. The company reportedly paid $100,000 in exchange for the hackers agreeing to delete the data and keep quiet[7].

Ransomware

Ransomware dominated the news cycles in 2017 and we don't expect that to change in 2018. New trends, like Ransomware-as-a-Service (RaaS) will increase the volume and impact of ransomware.

Ransomware has progressively become more powerful and destructive over the past few years. This arms race peaked with the state-sponsored WannaCry[8] (attributed to North Korea) and NotPetya[9] (attributed to Russia), which weren't really ransomware at all. Any ransomware without a working method for decrypting files effectively becomes a 'wiper' — malware that simply aims to destroy data and make systems unusable.

Making things worse, both WannaCry and NotPetya introduced a worm component, allowing these wipers to spread automatically through networks. NotPetya included the additional trick of stealing passwords from an infected host and using these credentials to infect adjacent hosts. On a network where local administrator passwords are all the same (still a common occurrence), even fully patched systems weren't safe.

[7] Newcomer, Eric. "Uber Paid Hackers to Delete Stolen Data on 57 Million People." Bloomberg.com, Bloomberg, 21 Nov. 2017, www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.

[8] Cimpanu, Catalin. "Wana Decrypt0r Ransomware Using NSA Exploit Leaked by Shadow Brokers Is on a Rampage." BleepingComputer, BleepingComputer.com, 15 May 2017,www.bleepingcomputer.com/news/security/wana-decrypt0rransomware-using-nsa-exploit-leaked-by-shadow-brokers-is-on-a-rampage/

[9] Krebs, Brian. "'Petya' Ransomware Outbreak Goes Global." Krebs on Security, https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/

Huge damages were attributed to WannaCry and NotPetya with shipping giant Merck attributing hundreds of millions[10] in damages to it. Voice recognition software vendor Nuance Communications attached a $92 million bill[11] to NotPetya. Less well known was the fact that small businesses reportedly paid out $301 million[12] to ransomware in 2017.

Ransomware-as-a-Service is currently an evolving market with Satan[13], Philadelphia[14] and the less creatively-named MacRansom[15] spotted for sale. Like exploit kits, the idea is for more risk averse criminals to offset risk by selling ‘kits’ to those more willing to do the dirty work of running a ransomware campaign and having to launder or recover the illicit income from them.

For the remainder of 2018, try to imagine ransomware anywhere — everywhere that computers run code. As anti-ransomware defenses improve on personal computers and business systems, we’re likely to see attackers turn to other, less well-protected systems. We’ve seen AWS and Azure accounts held for ransom and we’ve seen researchers confirm that ransomware could hold a modern, Internet-connected car hostage from its owners. Also consider that ransomware doesn’t necessarily have to use encryption to hold something hostage.

[10] Forrest, Conner. “NotPetya Ransomware Outbreak Cost Merck More than $300M per Quarter.” TechRepublic, www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/.

[11] Ragan, Steve. “Nuance Says NotPetya Attack Led to $92 Million in Lost Revenue.” CSO Online, CSO, 28 Feb. 2018, www.csoonline.com/article/3258768/security/nuance-says-notpetya-attack-led-to-92-million-in-lost-revenue.html.

[12] Dark Reading Staff. “SMBs Paid $301 Million to Ransomware Attackers.” Dark Reading, 21 Sept. 2017,www.darkreading.com/threat-intelligence/smbs-paid-$301-million-to-ransomware-attackers/d/d-id/1329941.

[13] Osborne, Charlie. “Satan Ransomware-as-a-Service Starts Trading in the Dark Web.” ZDNet, ZDNet, 20 Jan. 2017, www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/.

[14] Abrams, Lawrence. “The Philadelphia Ransomware Offers a Mercy Button for Compassionate Criminals.” BleepingComputer, BleepingComputer.com, 9 Sept. 2016, www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/.

[15] Brook, Chris, et al. “Free Mac Ransomware-as-a-Service MacRansom Surfaces.” Threatpost | The First Stop for Security News, 12 June 2017, https://threatpost.com/free-mac-based-ransomware-as-a-service-macransom-surfaces/126204/.

Cryptocurrency Hacks - Cryptojacking

Cryptocurrency has been a game changer for the criminal world. The availability of anonymous currency with no geo-political ties has allowed criminals to cut down on the number of steps necessary to get paid and cuts down on risk. The concept of 'mining' to generate currency by using computing power opened new opportunities for criminals as well. Criminals have used Windows and Mac malware; AWS accounts; and even smartphones to mine coin.

While most mainstream cryptocurrency is well designed and secure on its own, the wallets, markets and exchanges used to buy, sell and manage these coins have not been as secure. We've seen a wealth of issues (literally) that often result in direct theft of funds from exchanges and individuals' wallets. Funds have been stolen from several initial coin offerings: $7.4 million from Coindash's ICO[16] , for example. A vulnerability in the Parity Multisig Wallet allowed $32 million to be stolen[17] from the ICOs of Edgeless, Casino, Swarm City and aeternity blockchain. The largest cryptocurrency coin heist in 2017 though, was $64 million worth of Bitcoin from NiceHash in December.
The next step in stealing computing cycles to mine coin is called 'cryptojacking' and leverages JavaScript to mine coin within a web browser. Coinhive[18] is a legitimate business that provides this JavaScript, with the idea of using cryptocurrency mining as an alternative to using advertisements to monetize websites. The creators of Coinhive say they didn't anticipate how popular their services would be with criminals[19].

The public is currently split on mining coin in-browser. Some feel that it's an acceptable alternative to serving ads, whereas others believe it should never be used without an

[16] Osborne, Charlie. "Hacker Steals $7.4 Million in Ethereum during CoinDash ICO Launch." ZDNet, ZDNet, 18 July 2017, www.zdnet.com/article/hacker-steals-7-4m-in-ethereum-during-coindash-ico-launch/.

[17] "Hackers Seize $32 Million in Ethereum in Parity Wallet Breach." CCN, 20 July 2017, https://www.ccn.com/hackers-seize-32-million-in-parity-wallet-breach/.

[18] "Coinhive – Monero JavaScript Mining." Coinhive – Monero JavaScript Mining, coinhive.com/.

[19] Cox, Joseph. "Creators of In-Browser Cryptocurrency Miner 'Coinhive' Say Their Reputation Couldn't Be Much Worse." Motherboard, 13 Feb. 2018, https://www.vice.com/en_us/article/vbpbz4/creators-of-in-browser-cryptocurrency-miner-coinhive-say-their-reputation-couldnt-be-much-worse.

explicit opt-in. Salon Media Group has experimented with this, giving website visitors the option[20] — ads or coin mining. In fact, some go as far as referring to Coinhive as malware, which challenges the concept of what malware is and how we define it.

As interest in cryptocurrencies (and value) continues to increase, we will see its use in criminal campaigns continue to increase as well.

IOT

The technology market is in full swing[21] with IoT. Slick, Internet-connected devices hit the market daily, closely followed by less expensive (and often less secure) variants. While most experts, buyers and consumers agree that IoT devices must have security built-in[22] , not all do. Competition in the IoT market is fierce and since most devices can be updated remotely, manufacturers are more likely to prioritize beating a competitor to market over shipping the most secure device possible.

Even if all current IoT vendors were shipping secure devices right now, the industry still has content with the potential millions of insecure devices already in use. Many devices, like networked surveillance cameras have long lives as well. It could be a decade or more before they're swapped out for newer models. The Mirai botnet responsible for some of the largest DDoS attacks ever seen has left a legacy in its wake. The Satori[23] and Reaper[24] IoT botnets have competed fiercely for access to devices. They often attempted to steal directly from other botnets, then shutting down external access to prevent reprisals.

[20] Brodkin, Jon. "Salon to Ad Blockers: Can We Use Your Browser to Mine Cryptocurrency?" Ars Technica, 13 Feb. 2018, https://arstechnica.com/information-technology/2018/02/salon-to-ad-blockers-can-we-use-your-browser-to-mine-cryptocurrency/.

[21] Hung, Mark. "Leading the IoT -Gartner Insights on How to Lead in a Connected World." Gartner, Gartner, 2017, www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

[22] "Majority of Consumers Believe IoT Needs Security Built In." Dark Reading, 26 July 2017, https://www.darkreading.com/vulnerabilities---threats/majority-of-consumers-believe-iot-needs-security-built-in/d/d-id/1329459.

[23] Khandelwal, Swati. "Satori IoT Botnet Exploits Zero-Day to Zombify Huawei Routers." The Hacker News, 23 Dec. 2017, https://thehackernews.com/2017/12/satori-mirai-iot-botnet.html

[24] https://www.darkreading.com/mobile/reaper-iot-botnet-likely-a-ddos-for-hire-tool/d/d-id/1330235

While these IoT botnets have been largely comprised of enterprise level devices (IP cameras have been a popular target), future botnets could target consumer devices as well.

Smaller businesses[25] and medical devices[26] have been targets of IoT attacks as well. One of the biggest concerns with IoT is that device configurations tend to be homogeneous. These devices exist for convenience's sake in the first place, so complexity doesn't suit them and won't result in successful products. Consider one company that installs and maintains surveillance equipment. For simplicity's sake, they might configure all devices across all clients with the same password and configuration. Learning how to compromise one device could result in a compromise of all of them.

Black Swan Theory for Vulnerability Management

The black swan theory grew out of a metaphor that, at one point, referred to something that didn't exist. When it was discovered and proven that black swans actually did exist in nature, the term took on its current meaning, referring to big events that were unexpected prior to their occurrence.

In cybersecurity, these events aren't all that rare, however. We seem to be blind-sighted by black swans once every month or two. In 2017, we saw BlueBorne[27] — a group of vulnerabilities that affected nearly every Bluetooth implementation in use. On the same day (as far as we know, these announcements weren't coordinated), KRACK[28] was announced — a vulnerability that affected all modern Wi-Fi access point and client

[25] Kawamoto, Dawn. "10% Of Ransomware Attacks on SMBs Targeted IoT Devices." Dark Reading, 7 Sept. 2017, https://www.darkreading.com/application-security/10--of-ransomware-attacks-on-smbs-targeted-iot-devices-/d/d-id/1329817.

[26] Kawamoto, Dawn. "IoT Medical Devices a Major Security Worry in Healthcare, Survey Shows." Dark Reading, 15 Aug. 2017, https://www.darkreading.com/threat-intelligence/iot-medical-devices-a-major-security-worry-in-healthcare-survey-shows/d/did/1329631

[27] Khandelwal, Swati. "BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking." The Hacker News, 12 Sept. 2017, https://thehackernews.com/2017/09/blueborne-bluetooth-hacking.html.

[28] Hughes, Matthew. "The KRACK Wi-Fi Vulnerability, Explained Like You're Five." The Next Web, 17 Oct. 2017, https://thenextweb.com/security/2017/10/17/krack-explained-like-youre-five-years-old/.

implementations. Broadpwn[29] affected the baseband processors in nearly all mobile phones and finally, Meltdown and Spectre[30] affected the Intel processors in most modern laptops, desktops and servers in use, worldwide.

Why were all these vulnerabilities announced within six months of each other? As security researchers have exhausted some of the more popular sources of software bugs and vulnerabilities — operating systems, browsers, databases and server software, they've moved on to less explored territory — namely, hardware and protocols. Looking for vulnerabilities closer to the hardware often results in findings that are much more wide-ranging than the typical software bugs discovered day in and day out.

The Black Swan Theory for Vulnerability Management, developed by Michelangelo Sidagni, CTO of NopSec and Shawn Evans, Head of Security Research for NopSec, aims to describe a method for predicting these 'black swans' more reliably. By breaking down the aspects of what makes these vulnerabilities so serious, wide-ranging and damaging, it is possible to predict them with better accuracy.

Vulnerabilities, as a whole, can be effectively described with just a few characteristics:

- Criticality: The amount or significance of damage that can be caused, if exploited
  Popularity: The commonality of the component, hardware, software or protocol in question (Is it used by 50 businesses, 2 billion consumers or somewhere in-between?)
- Attack vector: One of the most often overlooked when the media tries to report on security vulnerabilities, attack vector is concerned with how the vulnerability is exploited. Meltdown and Spectre, for example, require the ability to run code on a computer to be leveraged. A piece of malware, for example, must first infect the

[29] Greenberg, Andy. "How a Bug in an Obscure Chip Exposed a Billion Smartphones to Hackers." Wired, Conde Nast, 27 July 2017, www.wired.com/story/broadpwn-wi-fi-vulnerability-ios-android/.

[30] "Meltdown And Spectre: What, When, Who, How.. What Is Managed Solution Doing To Support Our Clients?" Managed Solution, 17 Jan. 2018, www.managedsolution.com/meltdown-spectre-managed-solution-support-clilents/.

PC before Meltdown and Spectre could be used. This prevents these vulnerabilities from being used en masse. In another example, KRACK requires physical proximity to a wireless device or access point before an attack is possible. By comparison, a critical WordPress vulnerability will have a much more accessible attack vector and will often cause much larger and more immediate damage when compared to something like Meltdown and Spectre.

- Ease of Exploitation: This characteristic describes the difficulty of performing the exploit, including the effort and skill necessary to create it, find it and execute it. For example, if reliable exploit code already exists and is publicly available, exploitation is very easy.

Combining these characteristics provides the ability to perform a sort of ‘backward search’ to find these black swans. By searching through known software, hardware, devices and protocols using these criteria, it is possible to predict where serious vulnerabilities may be waiting to be discovered. This is the same logic researchers, criminals and government-funded hackers will use to find new and novel targets as well.

Using this criteria, the following are some of NopSec’s predictions for 2018:

- Remote command execution (criticality) vulnerabilities in JavaScript frameworks, like JQuery, Angular and Node: these frameworks are widely used (popularity), web-based (ease of exploitation) and are accessible via the Internet (attack vector).
- SQL injection and command execution vulnerabilities in popular open source content management systems (CMSs), like Wordpress, Drupal and Joomla.
- Enterprise platforms exposed to the Internet or internal corporate networks, like ManageEngine (IT management software), lesser-known (and thus probably not well-examined) web-based enterprise resource planning (ERP) and asset inventory platforms.

- Web application servers based on open source technologies, like Apache Struts 2, famously responsible for the initial foothold used in the Equifax breach. Other likely targets include Apache Spark, Flask, Django and Spring/Hybernate.
- Extremely common libraries and interpreted languages, like openssl, libc, golang, ruby and python.

General threat intelligence can also help to create likely risk scenarios by studying and analyzing past attacks and breaches. Industry reports like Verizon's Data Breach Report[31], FireEye's M-Trends report[32] and Microsoft's Security Intelligence Report (SIR)[33] contain intelligence and recommendations based on actual attacks, breaches and incidents.

Conclusion

Technology is advancing quickly and it's not all about robotics, space exploration and whatever else graces the cover of Popular Mechanics magazine these days. Advancements in payment technology, augmented reality and authentication (like the upcoming WebAuthN[34] standard) should be watched closely. As these new technologies emerge, use them and understand them. Then think about ways to abuse them. This thought process makes it possible to mitigate a portion of threats before they become threats.

For example, mitigation strategies have emerged for ransomware through an understanding of how this particular type of malware works. These can be implemented on the 'front end' of the attack, like better awareness of how ransomware infects victims (phishing… phishing always works…). They could be implemented on the back end, like ensuring backups are constant, reliable and that staff can quickly and reliably recover

[31] "Verizon Enterprise Solutions." Verizon. https://enterprise.verizon.com/resources/

[32] "M-Trends 2018 Cyber Security Trends." FireEye, https://www.fireeye.com/current-

[33] "Webcast: Get the Latest on Top Cyberthreats and Events." Microsoft Security - US (English), 2017, www.microsoft.com/enus/security/intelligence-report.

[34] "Web Authentication: An API for Accessing Public Key Credentials Level 1." W3C, https://www.w3.org/TR/webauthn/.

systems crippled by ransomware. Speaking of backups, remediation strategies are also important. Ultimately, attacks will get through, requiring a business to resolve compromises with minimal disruption for customers and business. This should not be just a top down approach, however. It should not merely involve management and C-suite level staff. Every employee has a role to play in protecting the business. Every employee should have the security training that would allow them to do their part.

Accurately predicting the next attack is a lot like playing chess — consider what's possible, try to think like your opponent, consider worst-case scenarios and try to plan several moves ahead. Considering most vulnerabilities are exploited before public awareness or immediately after, it is important to include prediction exercises when planning and developing security strategy.

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 hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec provides automated IT security control measurement and risk remediation solutions to help businesses protect their IT environments from security breaches. The company's flagship SaaS product, Unified VRM, utilizes passive analysis, active exploitation and contextual enrichment that enables security teams to visually forecast threat risk, and dramatically reduce the time to remediation of critical security vulnerabilities across infrastructure and applications.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com