The Year of the defender

Cybersecurity Predictions for 2018



Our Speakers





Sam Curry Cybereason | CSO

Lital Asher-Dotan Cybereason | Sr. Director



Setting The Stage

» A lookback at 2017 » Our predictions for 2018 » Recommended action steps

2017 Security Look Back





2018 PREDICTIONS

2018 Predictions

1.

- Supply Chain Attacks increase
- 2. Destructive Attacks do not let up
- 3. The line blurs between APT Actors and Cyberecriminals
- 4. Fileless malware attacks become ubiquitous
- 5. The Year of the Defender!



1. CHAIN, CHAIN – SUPPLY CHAIN ATTACKS INCREASE, AND REMAIN UNDER-REPORTED

Intro: Supply Chain Attacks

- » Attacks in which the victim is not the ultimate target of the attack, but rather a stepping stone to other networks.
- » Usually targeting the less secure elements in the supply network.
- » In 2017 most supply chain attacks (other than M.E.Doc) targeted software used by IT and developers.



Why are they growing

- » Increased security defenses make attackers look for the weakest link
- » Decreasing price of leaked data -> attackers looking for better efficiencies in their hacking operations
- Supply chain attacks can be scaled up, allowing many organizations to be compromised at the same time
 Robust spread mechanism with high persistence

Mitigating the Risk of Supply Chain Attacks

- » Monitor vendor access to internal data and networks
- » Establish boundaries and adhere to these boundaries strictly
- » Log and monitor any external vendor access,
- » Be knowledgeable of third-party providers' incident response and disaster recovery plans
- Decrease your attack surface by limiting users' ability to install third party software on machines, primarily freeware.
- » Create Resilience IT infrastructure: Redundancy in supply chain, Good Recovery and Backup system



2. HIGHWAY TO THE DESTRUCTIVE ZONE



Destructive Attacks – A Growing Trend

SONY - 2014 SIBERIAN PIPELINE - 1982 STONEDRILL - 2016 Data theft and subsequent Iranian hackers leverage US planted falsified disclosure, perpetrated by drive wiping tools to attack information in designs the DPRK also involved Saudi Arabian targets in stolen by Russian agents SAUDI ARAMCO - 2012 substantial damage to SPE's government, private sector, that resulted in one of the IT infrastructure telecommunication, and world's largest non-nuclear transportation. explosions Iranian actors wipe over GERMAN STEEL - 2014 BRICKERBOT - 2017 GEORGIA - 2008 35k drives in an attack on Saudi Arabia's state owned oil company Russian forces conduct ioint Unknown attackers infected the A simple piece of malware that arms campaign against ICS of a German Steel Mill attacks insecure IoT devices Georgia-website defacement, causing an unscheduled shutdown and formats their internal DDoS. and potentially of a blast furnace that memory rendering the device pipeline explosion resulted in significant damage useless. 1982---2013------ 2015 ----NOW 2008 ---BLACK ENERGY - 2015 NOTPETYA – 2017 DARK SEOUL - 2013 KOSOVO - 1998 Russian attackers, using a Self propagating malware that primarily opensource toolkit wiped approx. 15k hard drives The US military used cyber DPRK hackers attacked three managed to attack Ukrainian upon rebooting. Most victims South Korean television capabilities to reduce the distribution companies in the Ukraine, but damage stations and an bank. The effectiveness of Serbian interrupting the power to spread from Russia to Spain. malware used wiped drives air defense systems approximately 225,000 and overwrote data **STUXNET - 2010** customers **CRASH OVERRIDE - 2016** CIH - 1998 **TV5MONDE - 2015** US and Israeli cyber forces attack Iranian nuclear program in the Also known as Chernobyl or Russian actors used malware This malware, used against attempt to slow down the Spacefiller was a virus the Ukrainian power grid, was to destroy the hardware that country's ability to that overwrote critical controlled the TV stations specifically designed to enrich uranium system data resulting in attack ICS systems associated operations over \$250 million in with power grids. Not only damages does it have the capability

to delete data and disrupt IT systems but it also has the capability to physically damage ICS systems.

Why Are Destructive Attacks Growing?

- » Lack of consequences
- » A variety of basic tools can cause severe damage
- » Very effective in causing disruption and driving attention
- » Cheap, dirty and effective is all any actor needs to play in this arena, a realization that many are having.

For the private sector this means an increased risk of being hit by unsophisticated, yet destructive attacks.



Minimizing the Risk of Destructive Attacks

» Create an effective data backup system
 » Develop an effective patch management process
 » Maintain a zero-trust environments and network segmentation

3. APT-ACTORS: GOING FROM FINE DINING TO FAST FOOD



Cybersecurity Data Analytics Platform

The Reasons Behind the Development

- » The commoditization of advanced toolset
 » Public disclosure of attack techniques by leaks and security research
- » Talent migration
- » Availability of hacking tools



The Result

» A Breaking Point for Attack Attribution» Everyone is a target

e.g. corporate espionage, data theft, financial motivetion



How to Minimize the Risk

» Don't ignore low-level threats >> Work from Risk and Threat Vector analysis » Develop hunting capabilities » Assume a breach » Look for SPF » Get above the system level (Endpoint myopia)



4. FILELESS ATTACKS ARE THE NEW NORMAL

What are Fileless Malware Attacks?

- » AKA memory-based or living-off-the-land attacks
- » Leverage built-in mechanisms in the OS such as WMI and PowerShell
- » Initially used by nation-state actors
- » Currently used by common cybercriminals thanks to the availability of attack toolkits

Why are Fileless Attacks Common?

- » Plethora of free tools and free scripts that can be abused to create malicious payloads
- » Very few security tools are able to detect fileless attacks
- » Scripting languages are notoriously flexible, making them easy to obfuscate
- » Since PowerShell is as ubiquitous as Windows OS, these tactics are very effective, especially as malware droppers.



Minimizing the Risk of Fileless Malware

- »Upgrade to PowerShell 5, require PowerShell signing, and explore the option of activating new Windows features to mitigate PowerShell downgrade attacks.
- »Implement and stick with a patch management process.
- »Restrict unnecessary scripting languages, limit user access to WMI
- »Implement endpoint security solutions with active monitoring and granular control and authorization (as available)





5. THE YEAR OF THE DEFENDER!

Why We Believe this Trend is Real?

- Organizations have made small, yet meaningful strides:
 No. of days to detect a breach is down from 201 (2016) to 191 (2017)
 No. of days to contain a breach is down from 70 (2016) to 61 (2017)
- » Fileless malware attacks finally get the attention of defenders and security vendors
- » GDPR makes Cybersecurity everyone's problem
- If security wasn't already a board-level topic of discussion in 2016, damaging attacks like NotPetya undoubtedly made it one in 2017. During earnings calls, C-suite executives from global corporations discussed how NotPetya impacted quarterly and yearly revenue.



HOW TO MAKE IT THE YEAR OF THE DEFENDER?



Questions?

Sam.Curry@cybereason.com Lital.Asher@cybereason.com