Threat Intelligence 2017 Predictions Report

NSFOCUS Threat Intelligence 2017 Predictions Report

Authors: *Stephen Gates - Chief Research Intelligence Analyst & Cody Mercer - Senior Threat Intelligence Research Analyst*

Table of Contents

1. Executive Summary

Looking back on 2016, there were a few key predictions that ended up becoming a reality. While many organizations have been reassuring themselves for years, saying: “Who would launch a DDoS attack against us?” - they ended up falling victim anyway, even without being openly attacked. Today, it no longer matters if you’re directly targeted or not; you could experience collateral damage from someone else under attack. In October 2016, the world witnessed the first DDoS attack exceeding 1 Tbps in size, impacting organizations all over North America that were not a direct target.

A second prediction came true as well. The 1 Tbps+ attack was not launched by compromised computers, servers, or smart phones, as some may have thought. Instead, the attack was comprised of IoT devices located all over the world; a threat which analysts have been predicting for years. With the public release of the Mirai malware, IoT-based botnets are poised to wreak havoc on a global scale like never before.

So, what does 2017 hold for the Internet? What attacks will be the most prevalent, and what defenses will begin to rise to maturity? What is certain is that 2017 will be one of the most interesting and tumultuous years yet, and it will likely rattle the Internet due to a host of factors.

Global financial instability, worldwide refugee migration, and the rise and fall of presidential regimes will be the catalyst. Every one of these global issues could increase cybercrime on a scale never before seen. As a result, the following predictions for 2017 are directly designed to help address the instability the Internet could experience in 2017 and beyond.

2. Evolution of Ransomware for Hire

Various thought leaders in the cyber-security community have identified ransomware to be the championed exploit in 2017. The ransomware infection technique often follows a repeated process where an unsuspecting victim unintentionally downloads an executable, or opens a questionable document through a spam or phishing campaign. Once the ransomware is downloaded to their computer, the victims hard-drive, memory, and data is ‘bricked’ or encrypted. The only way to decrypt the data is to receive the encryption key, once payment for that key has been made to the attacker.

However, recent reports have indicated that victims of ransomware campaigns now have the option to opt-in to the exploit process, once the attackers have been paid in full. According to Malwarebytes Labs (2016), “Tech support scams (TSS) have become incredibly advanced and dangerous over the last few years and most recently we have witnessed TSS deploying malware, and even extortionware. In 2017, TSS attackers will dive into this benefit headfirst and leverage the malware threat landscape more than ever before” (para. 10). Essentially, a victim will now have a chance at revenge, and can become the attacker; capable of receiving a percentage of the proceeds if they choose to be involved in the many attack vectors associated with various ransomware campaigns.

Additionally, as the rise in popularity of smart cars and vehicles, which now may fall into the classification of an IoT device with an IP address, it will not be unrealistic to imagine that ransomware can be deployed through means of firmware updates and network connectivity. As we witnessed with the Tesla Man-in-the-Middle (MitM) attack, cars that require firmware updates via satellite communications are susceptible to various vulnerabilities, to include ransomware and other exploits posed by other malware families.

3. Rise in DDoS-for-Hire Services

The year of 2016, and previous years for that matter, demonstrated the huge rise in DDoS attacks, along with increased complexity and ease of deployment through means of IoT devices. Various online outlets fell victim to these attacks to include but not limited to Krebs on Security, Dyn, Twitter, Reddit, and Spotify. According to a recent article published by DDoS Attacks (2016), they claim that, “The size of attacks has increased exponentially thanks to hackers and cyber criminals making use of the IoT. These devices – including the likes of webcams Digital Video Recorders, and even fridges, toasters and pressure cookers – are typically designed to be quick and cheap to produce, and inherently have very poor levels of security” (para. 4).

After the recently released source code of the DDoS malware Mirai, both black and white-hat hackers worldwide now have access to the exploit code. Slight modifications of this code make it very difficult to initially recognize, and its simplicity allow even the novice user to employ. With this noted, a new trend has begun to emerge where DDoS Booters, also referred to as DDoS Stressors, allow users globally to participate in DDoS attacks. Netspoof, Dejabooter, Vexstresser, and Refinedstresser are a few of the well-known DDoS Stressors that have recently been taken out of circulation by Interpol, and other participating law enforcement agencies.

Government agencies, gaming industries, technology firms, education outlets, and financial moguls have suffered from the impact of DDoS Stressors; often causing significant financial losses. Moreover, children playing online games are now being coerced into participating in DDoS-for-Hire attacks, where their computer can be used to serve as a bot in a DDoS attack. Payment in the form of bitcoin is supplied to the children, if they choose to participate.

4. Enhanced Insider Threat Breaches

It is widely accepted throughout the cyber-security community that the greatest attack vector posed to any IT entity is an insider threat. However, it is important to understand that an insider threat is not always malicious and intentional. Statistically, security breaches are often attributed to poor IT administration practices, user inexperience, and/or improper employment and enforcement of a company's security policies and procedures. One can arguably declare that the "Edward Snowdens" pose the greatest risk to a network infrastructure; however, that is an exception rarely witnessed throughout history in the cyber-security arena. In the article, Insiders are today's biggest security threat, Durbin (2016), proclaims the following, "However, according to a worldwide survey of Information Security Forum (ISF) members, the vast majority of those network openings were created innocently through accidental or inadvertent behavior by insiders without any intention of harming their employer. In a number of cases, that vulnerability was, ironically, the result of a trusted employee doing a seemingly run-of-the-mill task like taking files home to work on in their own spare time" (para. 5).

Insider threats present themselves in multiple ways. As previously mentioned, not all insider threats are malicious, and the various categories of insider threats can be classified as malicious, negligent, and/or accidental. Often breaches occur through exploited vulnerabilities created by IT admins not following proper account lifecycle management, or security operations failing to adhere to standard practices such as update and patch policies. Not only does this create significant vulnerabilities for data centers and bare metal infrastructures, but as more industry standards migrate to a cloud-hosted-operation, the complexities of ensuring effective security measures increases exponentially. Societies' current state of mind focuses on the path of least resistance with an expectation for simplicity and efficiency. Therefore, the demand for consistent diligence in upholding strict adherence to a company's security policy and procedures, should remain of the utmost importance; assuming a company has such policies in place. Additionally, proper safeguarding of an entities copyrights, trademarks, source code, and intellectual property is often left in the hands of those unaware of its qualitative value; giving rise to easily accomplished nefarious breaches by those with low-level hacking skill-sets.

5. The Death of Anti-Virus

The pitfalls in current anti-virus applications are significant. The primary functionality behind a successful anti-virus application relies on the process of continuously querying a frequently updated database full of malware signatures. As per author, Covington (2016), the ComputerWorld article, *Is antivirus dead at last?,* declares the following, “Unfortunately, two major factors have greatly diminished the effectiveness of antivirus technology. First, malware can traverse the internet at a rate nobody ever imagined was possible. Today, a new virus can become widespread on the internet before the antivirus vendors even know it exists. Second, virus authors have learned to produce variants, which are version of their illicit programs that function the same way, but have deliberate changes in their signature to evade antivirus programs. Because much of our malware is now distributed in kit form, even a novice can produce a malware variant and get it out on the internet very quickly” (para. 6).

Malware of any type can be identified through means of a hash value such as an MD5 or checksum-like-value that uniquely identifies or fingerprints that specific malware. With this noted, slight modifications in the source code or malware application results in a different and unique hash value; making the current and/or previous signature value null and void. As previously released malware gets modified, it becomes increasingly difficult to pin-point specific hash values that anti-virus programs recognize and rely upon. Unfortunately, many pieces of malware source code are readily available from virus databanks and repositories that are open to the public; allowing anyone to modify the original code.

Thankfully, not all hope is lost. As new cyber-security capabilities emerge every day, next-generation firewalls (NG-FW) and next-generation intrusion prevention systems (NG-IPS) are incorporating new threat recognition capabilities that go beyond simple signature matching techniques. Many next-generation security technologies not only use signatures, but also utilize anomaly and behavior-based detection mechanisms that provide indicators of compromise (IOC) for threat detection and prevention.

6. The Growth of Crowdsourced, Actionable Threat Intelligence

Although Threat Intelligence (TI) is still in its infancy, it won't be for long - and that change will be very dramatic. Today's TI consists mainly of data feeds that contain known-bad IP addresses, dangerous domains and URLs, intelligence of command & control infrastructures, and masses of malware hashes. TI may also contain intel on threat-related tactics, techniques, and procedures, as well as information about threat actors and their campaigns. However, most of this is still quite primitive in nature, and it's only the stealthiest of organizations that can capture value from TI. But, that's about to change.

Soon, the industry, governments, and other influential institutions will heavily encourage all organizations to begin to crowdsource TI data. This effort will make TI more actionable and affordable for the masses. Soon, all cyber defenses will be fully capable of consuming TI in real-time, acting upon the intelligence gained, and delivering upstream crowdsource capabilities. All organizations, devices, applications, operating systems, and embedded systems will soon be fed TI, and in turn, will feed other organizations the TI they've gained from their own observations of the attacks they've experienced.

7. The Rise of the Automated, Machine Learning, and AI-Enabled Defenses

The attack predictions previously mentioned will force the Internet community, researchers, corporations, and governments to heavily fund automation, machine learning, and artificial intelligence-enabled (AI) technology research. These defenses will incorporate automated capabilities to allow for self-configuration on the fly. Others will have automated kill-chain capabilities designed to help stop the spread of contamination by immediately detecting infections, and shutting down systems before epidemics spread even further.

The next evolution of these defenses will possess machine-learning capabilities for complete awareness of their surroundings. They will be fully capable of detecting the slightest deviations from what is considered “good and normal”, and alert automated blocking engines to take immediate action, without human intervention.

The final characteristic of our soon-to-be-realized defenses is that they will soon maintain a rate of growth and become increasingly intelligent. These defenses will not only be able to detect anomalies in any type of traffic, user, or device, they will also be capable of inoculating systems on the fly; adapting their immunizations to whatever infection is presented to them. Human-feedback driven AI-enabled technologies are not too far in the future. Work on these concepts has already begun in universities, think-tanks, and research labs all over the globe.

8. Conclusion

The year of 2017 holds many new challenges and obstacles to maintain a proper cyber-security posture in all environments. New threat capabilities linked to previous threat exploits serve as reminder that the methods available to nefarious actors, foreign and domestic, continually grow exponentially in capability and complexity. Services for hire affiliated with DDoS and ransomware attacks that now permit and support victims becoming the attackers, has shed light on new approaches to accomplishing cybercrime.

Moreover, protection measures once employed to defend network infrastructures may prove to be inadequate in efficacy and protection. Present maneuvers utilized by white and black hackers alike, effortlessly allow for malware deception that renders anti-malware, signature-based devices as useless. However, the advances in AI and machine learning techniques continuously improves long-term. Considering this concept with the onboarding of free and open threat intelligence exchange, the opportunities in defense also identify new means of protection from a host of different perspectives.

9. References

Covington, R. (2016*). Is antivirus software dead at last*? Retrieved from: http://www.computerworld.com/article/3146996/malware-vulnerabilities/is-antivirus-software-dead-at-last.html

DDoS Attacks (2016). *The new age of DDoS – And we 'joked' that toasters would one day take down.* Retrieved from: https://www.ddosattacks.net/the-new-age-of-ddos-and-we-joked-that-toasters-would-one-day-take-down-our-banks/

Durbin, S. (2016). *Insiders are today's biggest security threat*. Retrieved from: http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin

Malwarebytes Labs (2016). Security in 2017: *Ransomware will remain king*. Retrieved from: https://blog.malwarebytes.com/threat-analysis/2016/12/security-in-2017-ransomware-will-remain-king/