FROM POSSIBLE TO PLAUSIBLE: PETYA AS PORTENT, WANNACRY AS WARNING, NOTPETYA AS GATHERING STORM

Article by Luke Tenery, Ted Theisen & Bill Bray

During a 2013 speech at George Washington University, former National Security Agency director Michael Hayden delivered an alarming assessment of the 2010 Stuxnet attack on Iran's nuclear weapons program. Hayden stated, "This has a whiff of August 1945. Someone, probably a nation-state, just used a cyberweapon in a time of peace to destroy what another nation could only describe as their critical infrastructure."[1] In Hayden's telling, Stuxnet's disruption of a top-secret military program heralds an age in which global conflict is defined by a dangerous and unprecedented weapon in much the same way Little Boy heralded the start of the Cold War when it exploded over Hiroshima in the waning days of World War II. Hayden's message was clear: cybersecurity henceforth must be a paramount concern to geopolitical actors.

Hayden's analysis is proving painfully prescient. In May 2017, a massive global cyberattack invaded 230,000 computers in more than 150 countries.[2] Also in May 2017, the WannaCry ransomware attempted to extract money from entities as diverse as corporations, banks, and the governmental infrastructure of nation-states and healthcare services. On the heels of these attacks, a similar intrusion occurred in June, causing network interruptions around the world, disrupting even the electronic programs monitoring Chernobyl.[3] One short month later yet another ransomware hybrid surfaced during an attack in Ukraine that was eventually named NotPetya, which combined code from older ransomware attack Petya and its ancestor WannaCry. Although it is still unclear who perpetrated the attacks (a leaked NSA memorandum points at North Korea for the WannaCry outbreak),[4] the lesson from this event is clear: businesses and nations must immediately make cybersecurity an integral and paramount aspect of their internal infrastructure. Hayden's warning from 2013 is by now several technological light years in the past, but it is still relevant.

A STRATEGIC RESPONSE TO RANSOMWARE

The world continues to recover from and gain insight into these most recent hybrid malware outbreaks composed of worms and ransomware. The worm component of the malware is responsible for propagating the infection to multiple hosts, whereas the ransomware component encrypts and/or deletes the files on an infected host. Combining these elements into the latest hybrid variants has created significant destructive power that spreads like wildfire. All individuals and organizations must consider the potential impact of ransomware threats as well as the broader ways in which security safeguards are evolving to battle modern cyberthreats. Much has been said about the rise of ransomware, but a preset incident response strategy is not the security panacea of viruses past. Typical preset incident response strategies include an overdependence on patch management and virus signatures — both of which are important, but they do not create a cure-all by any means. In today's technological landscape, one size does not fit all. Knowing how your system could be impacted — or strengthened — is critical.

WEAK IMMUNITY SYSTEMS – YOUR OWN EVOLUTION MAKES YOU VULNERABLE

As we noted in **our March article regarding the WikiLeaks CIA arsenal exposures**, technology leaders now have new vulnerabilities to consider. The May and June attacks are yet another wake-up call in support of a more resilient technology enterprise. It is increasingly clear that many organizations still operate using antiquated security sanitation and prevention systems. Traditional anti-virus software updates and system patching cycles are incapable of protecting your technology endpoints from malware without signatures, namely ransomware. Malware signatures are unique binary patterns, such as hash values that identify known variants. Present-day security systems are focused on the challenge of preventing malware attacks and generally work only against known malware software and associated signatures. There is a lag between the deployment of increasingly sophisticated security threats and the deployment of the defenses designed to counter them. Another issue that should be considered is publicly exposed machines running unnecessary services on the internet. In the cases of WannaCry and NotPetya, the ransomware/worm propagated to other machines via a vulnerable Windows service. Minimizing the exposure of the vulnerable windows service, which can often be accomplished by simply disabling this service, would have certainly reduced the propagation rate of the malware outbreak.

As the dust settles from the latest examples of the new global cyberthreat normal, WannaCry, Petya, and NotPetya have highlighted the fact that global organizations have evolved into IT enterprises that no longer operate within four walls. Large populations of employees are working remotely, in numbers that are often nearly as large as those of their in-house counterparts at their places of employment.[5] Also, many employees telecommute across the globe, seldom linking their computer security to their corporations at which they are perceived to be bastions of safety. This perception of security is largely related to corporate security solutions, such as anti-virus programs that these employees rely on. But traditional anti-virus software can no longer adapt, protect, or provide immunity quickly enough to counter rapidly changing cyberbugs for scenarios in which users are no longer required to reside exclusively within their physical office place. Businesses can gain a significant strategic advantage against hostile parties by implementing security protocols that factor in company culture regarding remote working styles and telecommuting.

Rather than accept the traditional limitations of antiquated security measures that do not adapt to an increasingly mobile workforce, organizations must now strategize about how to handle modern threats such as WannaCry which is just one of the persistent onslaught of evolving cyberattacks. Decisions about how to protect a company's cybersecurity tools and the implementation of those decisions must constantly move as quickly and widely as that same company's employees and contractors are moving.

Organizations must take the steps necessary to prepare for threats by improving security protocols, advancing threat-related controls, and introducing the most modern layered security safeguards. These are the most effective means available to compensate for an evolving and amorphous enterprise.

Advanced malware controls — such as endpoint threat monitoring or technologies that constantly run analyses of systems, looking for intrusions or data extraction[6] — can give early visibility into emergent security threats and are not reliant on exclusively looking for malware signatures; rather, they are focused on detecting threats based upon many other technical factors that are present on the endpoints. Endpoint threat monitoring is much more comprehensive than archaic anti-malware solutions. These solutions are deployed as a software as a service (a cloud computing service that automatically updates the latest security upgrades[7]) and can ensure protection that is more agile and more thoroughly updated than traditional anti-virus solutions are.

RESILIENCY AND PREPAREDNESS

Due to the limited supply of experts and strategic misalignment, organizations are often not nimble enough to apply sufficient analytical resources to fully maximize their existing security. These issues are made worse by required updates to generational security controls that professionals without deep experience in this type of cybersecurity training are not able to implement swiftly.

The constant need to adapt injects increased complexity and yields a broader attack surface; more systems operating in one's cyberinfrastructure means more targets for outside parties to attack. This necessitates further adequate protections. One cannot reduce all risk to zero against constantly changing threats. At some point, even the best-prepared infrastructure is going to experience a successful attack. Resiliency to cyber incidents is therefore just as important as prevention. It is critical to integrate the expectation of future attacks when designing the optimal cybersecurity option for your institution.

If principles of resiliency had been applied in advance of any variant of ransomware, damage would not have been eliminated, but its severity would have been greatly reduced. With the near-inevitable chance of attacks, prudence remains a key component in implementing effective cybersecurity strategies.

It is imperative for businesses and governments to stay abreast of the frequent advances threatening technology and to prepare to withstand future threats. Information is valuable but incredibly difficult to contain. This makes the challenge of managing data more difficult. The most recent ransomware outbreak serves as a bellwether for smarter action in defending against tomorrow's computer attacks. For the shrewd professional, unfortunate events such as the WannaCry and Petya incidents may serve as a forge through which smarter, more effective, and robust cybersecurity solutions may be crafted.

The authors thank Paul Wilson and Karl Kahn for providing research, writing, and editing assistance on this article.

[1] **https://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima**
[2] **http://www.bbc.com/news/world-europe-39907965**
[3] **http://www.bbc.com/news/world-europe-39907965**
[4] **https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north- korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?hpid=hp_hp-more-top-stories_northkoreacyber744pm%3Ahomepage%2Fstory&utm_**

[5] https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html

[6] https://digitalguardian.com/blog/what-threat-monitoring

[7] http://www.pcmag.com/encyclopedia/term/56112/saas

View a PDF version of this article.

FOR MORE INFORMATION ABOUT ANKURA CONSULTING'S CYBERSECURITY GROUP, PLEASE CONTACT:

Luke Tenery | luke.tenery@ankuraconsulting.com
Ted Theisen | theodore.theisen@ankuraconsulting.com

FOR MORE INFORMATION ABOUT ANKURA CONSULTING'S GEOPOLITICAL ADVISORY GROUP, PLEASE CONTACT:

Michelle DiGruttolo | michelle.digruttolo@ankuraconsulting.com
Bill Bray | william.bray@ankuraconsulting.com

BACK TO NEWSROOM

ANKURA LOCATIONS

Ankura Consulting is headquartered in Washington, DC. Our firm has offices across the nation to better serve our clients.

Legal