WHAT’S ON THE HORIZON –
FOUR CYBER SECURITY PREDICTIONS FOR 2017

In many ways 2016 was a watershed year for cyber security. Internet of Things (IoT) botnets opened the 1Tbps attack floodgates, SSL-based attacks went mainstream, and cyber-ransom emerged as the easiest, and most lucrative, cyber-attack tool for hackers.

These trends had sweeping impacts on the industry, both in terms of the solutions used to defend organizations and the policies employed to build a sound security strategy. These impacts will combine with emerging technologies and old-school tactics to create new consequences for the industry in 2017.

What follows is four, very plausible cyber-attack scenarios for 2017. Read them for pleasure – and preparation.

Prediction 1: Rise of Permanent Denial of Service (PDoS) for Data Center and IoT Operations

Imagine a fast-moving bot attack designed not to collect data but rather to completely prevent a victim's technology from functioning. Sounds unlikely, but it's possible. Permanent denial-of-service (PDoS) attacks have been around for a long time; however, this type of attack shows itself spectacularly to the public only from time to time.

Also known loosely as "phlashing," PDoS is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of a system. It is a contrast to its well-known cousin, the DDoS attack, which overloads systems with requests meant to saturate resources through unintended usage.

One method PDoS leverages to accomplish its damage is via remote or physical administration on the management interface of the victim's hardware, such as routers, printers, or other networking hardware. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic software with a modified, corrupt, or defective firmware image—a process which when done legitimately, is known as flashing. This "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. Other attacks include overloading the battery or power systems.

Examples include:

- An article published by Help Net Security detailed a new USB exploit that, when inserted into a computer, can render the machine bricked. According to Help Net, the latest PDoS USB attack "when plugged into a computer … draws power from the device itself. With the help of a voltage converter, the device's capacitors are charged to 220V, and it releases a negative electric surge into the USB port."[1]
- An article in Dark Reading highlighted PhlashDance, a tool uncovered by HP Labs. PhlashDance finds vulnerabilities in often forgotten firmware and binaries that sit locally on computing devices. The risk occurs when a device hasn't been properly patched and upgraded. The article states that "remotely abusing firmware update mechanisms with a phlashing attack, for instance, is basically a one-shot attack. Phlashing attacks can achieve the goal of disrupting service without ongoing expense to the attacker; once the firmware has been corrupted, no further action is required for the DOS condition to continue."[2]
- Recent safety hazard incidents of the Samsung Note 7[3] is stoking concerns about devices that can be intentionally set on fire. There have been numerous test cases of malware and bots overheating devices, causing them to physically distort or worse. These attacks, bundled into a cyber-attack, could have devastating and lasting effects beyond what we commonly think about in the world of the "nuisance" DDoS attack.

Prediction 2: Telephony DoS (TDoS) Will Rise in Sophistication and Importance, Catching Many by Surprise

Cutting off communications during crisis periods would impede first responders' situational awareness, exacerbate suffering and pain, and potentially increase loss of life. A new era could consist of multiple components—including a physical attack with a corresponding cyber-attack targeting the communication systems that first responders use to contain and minimize damage.

Can the day be far away where a terrorist attack is magnified by an effective outage of first responders' communication platforms? If you doubt the feasibility, review this bulletin.[4] It was issued in 2013 by public safety organizations asking for assistance in cracking a TDoS attack against 911 systems.

[1] https://www.helpnetsecurity.com/2015/10/15/usb-killer-20-a-harmless-looking-usb-stick-that-destroys-computers/
[2] http://www.darkreading.com/permanent-denial-of-service-attack-sabotages-hardware/d/d-id/1129499?print=yes
[3] https://www.cnet.com/news/why-is-samsung-galaxy-note-7-exploding-overheating/
[4] http://psc.apcointl.org/2013/03/15/updated-bulletin-tdos-attacks/

Prediction 3: Ransom Attacks Become More Segmented, More Real and More Personal

Radware predicts that cyber-ransomers extend their reach beyond companies. In 2017, ransom attacks could get personal.

Hackers target personal implanted health devices. Imagine if your life depended on an implanted defibrillator or other medical device. Now imagine if such a device were hacked and held for ransom. The idea of hacking defibrillators is not science fiction. Cyber ransom is the fastest-growing motive and technique in cyber-attacks. Can a marriage between the two be far off? For those unfamiliar with these risks and U.S. Government-issued warnings in this category, please refer to the FDA's Advice to Medical Device Manufacturers, a summary of FBI & DHS alerts on Internet of things and these warnings on cyber ransom.

Public transportation held hostage. In many ways, cyber ransoming a public transportation system is the ultimate hack—empowering attackers to hold a community hostage for financial or criminal gain. If you live in France, the United States or many other countries, you may have grown accustomed to railway or airline workers striking and wreaking havoc on the communities around them.

From trains and planes to buses and automobiles, our entire system of transportation is becoming more automated. This automation is meant to provide us with increased safety, improved reliability and higher efficiencies. But is it really providing those things? If you have been following cyber-security threats to public transportation, you likely know there have already been numerous attacks—some of which have distinguished themselves as harbingers of future attack categories.

Just as other forms of transportation face increased threats, so does the aviation industry. Like water, aviation terror threats tend to take the path of least resistance. Via external analyses and documented evidence, we now know that the aviation sector is vulnerable to cyber-attacks. How long will it be until terror strikes evolve in the aviation industry—as they have around the world—to the cyber front? If you have responsibility for any aspect of these areas, please don't be a bystander. Be proactive about onboarding controls and saving lives.

If transportation systems are vulnerable, could ransoming of these systems be far behind? If so, what would politicians pay for a return to operations and safety for their constituencies? Does "pay-for-play" government behavior reward the pursuit of future combinations of terrorism and crime?

Military devices ransomed. Military branches have long been heavy technology users. They have also had a technology procurement model based on an outdated approach and xenophobic buying behavior. In a world of commercial-off-the-shelf (COTS) products, goods are procured fairly at will. Will these COTS packages—frequently made with large amounts of foreign components—be the small pebbles that undermine the operational capabilities of the world's largest military forces? Seemingly innocuous cameras, sensors and other IoT devices pervade the military—but are just as rife with security issues as any on the planet. Once demonstrable vulnerabilities are validated, how much would a government pay to regain control of weapons or other crucial resources?

Prediction 4: The Darknet Goes Mainstream

Many people live two or more lives: One life in flesh and blood; and the other life or lives are various online avatars, which are essential for highly functioning citizenry. These avatars span health, finances, education, love interests, and more. Today the Darknet offers easy, affordable access to terrorize or otherwise alter someone's personal avatar for financial or other benefits. What, exactly, do we mean? Here are a few examples of what 2017 could bring:

- Compromised surveillance systems available for rent, enabling someone to see through another person's cameras
- Access to FBI files and lawsuit information
- Access to emails and computer systems of people going through a divorce, as well as teachers' personal communications or lawyers' strategic documents and communications
- Personal medical records or previous criminal activity or misdemeanors

In the face of these frightening prospects, who is the definitive source of who we are, and how do we reconcile file/record issues? Before you answer, picture yourself in a job interview. You provide one set of information about your educational history; a report from your school serves up conflicting data. Who rules the day?

This analogy can be extended to numerous scenarios. The common thread: that your online avatar now represents and requires high security and fidelity in order for you to function properly in society. In light of that, one of the single most personalized acts of terror that can occur is a wide-scale loss, alteration or deletion of records—with no reconstitution capability. This should strike fear in us all.

Is the Best Behind Us?

The conclusion we draw from all of these predictions: If growth of attack surface, techniques and means continues into 2017, then the best years of security of our systems may be behind us. As we move forward into 2017, Radware views these as key questions to explore:

- With physical terror playing such a major role in global strife, how could cyber-security sabotage NOT be far behind?

- Given the threat landscape, what controls/testing can be performed to ensure that the public risk is abated through proactive measures—and that private scenarios are regulated so that we can trust our Internet avatar system as we trust our financial system?

Given the evolution of threats and the importance of the sanctity and trustworthiness of online systems, government needs to step in and provide something akin to a Federal Bureau of Cyber Security with a separate and distinct charter. This agency's role would be equivalent to the physical Secret Service in numerous ways. However, its operating space and domain would be one with the ghostly characteristics of computer warfare. In defending the citizenry, this agency would need to cover freedoms of press and speech overall.

No matter when or how the government responds, each organization has a responsibility to be aware and prepared. Radware urges you to contemplate how our 2017 predictions could affect your organization and the people you serve—then work to devise appropriate strategies and controls for mitigating the risks.

Download the 2016-2017 Global Application & Network Security Report to learn more.

www.radware.com/ert-report-2016

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.