Seven Cyber Security Predictions

Cyber-attacks have become commonplace. In many ways, the only "news" is that they continue to grow in frequency and variety. When dealing with the day-to-day, it can be difficult to tally the mounting toll associated with this awful state of affairs—and even more challenging to predict what surprises lie ahead. Based on industry trends, legal framework changes, expert insights and technological evolution, Radware makes seven cyber security predictions.

Prediction #1:

APDoS as SOP

Advanced persistent DoS (APDoS) will become hacktivists' preferred technique—and the cause of a significant portion of business outages. APDoS attacks involve massive DDoS attacks, from assaults on the network layer to focused application layer floods. Those attacks are followed by repeated SQLI and XSS attacks, which occur at varying intervals. Because APDoS is essentially a potpourri of attack types, they require diverse technology that protects both the network and application level to effectively mitigate.

Perpetrators of APDoS attacks will simultaneously use two to five attack vectors, involving up to several tens of millions of requests per second. All the while, large SYN floods attack not only the direct target but also the service provider as it implements managed DDoS mitigation. APDoS attacks can persist for weeks at a time—challenging the resources of even the most sophisticated security infrastructures.

APDoS attacks have become standard operating procedure for many hacktivist groups. Attackers in this scenario often switch tactically between several targets to create a diversion to evade defensive DDoS countermeasures while eventually directing the main thrust of the attack on a single victim.

Prediction #2:

Continued Rise of RDoS

Ransomware and RansomDoS (RDoS) schemes will affect everything from traditional enterprises to cloud companies. It is reminiscent of the old joke: Why do robbers burglarize banks? Because that is where the money is! Cloud companies, beware; Radware predicts ISPs will experience significant RDoS attacks.

Cloud companies, beware!

We predict you will experience significant RansomDoS (RDoS).

Prediction #3:

Privacy as a Right (Not Just a Regulation)

Around the world, privacy's legal comeuppance is upon us. Some countries already recognize privacy as a human right and provide for constitutional covenants to protect its citizens. It's no longer a matter of whether or not data can be secured in pursuit of privacy, but rather if privacy is endemic to the human condition. If privacy is a human right, what must we do to protect it?

In the meantime, security professionals and businesses entrusted with data will bear the cost and responsibility of safeguarding it. Around the world, early adopters will lead the way, with this trend picking up.

Prediction #4:

More Laws Governing Sensitive Data

Many countries took notice when the US Government's PRISM program was revealed to the public. Contention exists regarding the handling and use of data and this has given rise throughout the world to special laws governing use, processing and domiciling of certain data. Some examples include the Canadian government's decree on processing sensitive Canadian data within Canada following U.S. passage of the Patriot Act. Other examples can be found in Brazil, Japan and China—and more will follow, further complicating the privacy and security officer's responsibility to technically secure data.

Prediction #5:

Arrival of Permanent Denial-of-Service (PDoS) Attacks, Albeit Very Slowly

PDoS, also known loosely as phlashing, is an attack that damages a system so badly that replacement or reinstallation of hardware is required. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of the 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.

PDoS can accomplish its damage via remote or physical administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. The attacker uses vulnerabilities to replace a device's basic software with a modified, corrupt or defective firmware image—a process that, when done legitimately, is known as flashing. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced.

Prediction #6:

Growing Encryption to and from Cloud Applications

A few years ago, effective technology to secure communication to and from cloud providers and user communities of companies simply did not exist. Now there is a great capability to encrypt this data en masse. It's a trend that's necessary but also wrought with folly and will ultimately prove a short-term solution to a larger problem.

Prediction #7:

The Internet of Zombies

Security on Internet of Things (IoT) devices is abysmal—data will be breached at a higher rate than any other technical regime. Technical adoption is the paramount concern while security is an afterthought. These devices represent a cottage industry for privacy violators and the risks to this rich data source will be highlighted, transforming the Internet of Things into a dangerous Internet of Zombies.

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.

© 2016 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.