NRI

Iakyara vol.292

Cybersecurity's new borderless frontier

Masaki Nishitani

12.November.2018

Nomura Research Institute, Ltd.

Executive Summary

Cyberattacks have long been internationally borderless but various other boundaries besides national borders are now becoming blurred in cyberspace. Effective cybersecurity in a blurred-boundary environment requires the leadership of a full-fledged CISO.

Masaki Nishitani
Senior Security Engineer
NRI SecureTechnologies, Ltd.

At NRI SecureTechnologies (NRI Secure), we have been publishing a Cyber Security Trend Annual Review[1] (CSTAR), a compilation of analyses of data collected through our security services, since 2005. The following briefly highlights a few topics, all pertaining to boundaries, from the 2018 CSTAR, the series' 14th installment.

AOSSL coverage now exceeds 50%; cloud usage also growing

Data communications involving passwords and other sensitive information have hitherto been protected by HTTPS. Today, however, websites are increasingly using always-on SSL (AOSSL), which deploys HTTPS encryption to protect not only sensitive information but all communications between the website and its users. HTTPS sessions accounted for over 50% of our client companies' visits to external websites in fiscal 2017 for the first time ever. With the latest version of Chrome already warning users that their connection is not secure when they attempt to visit a non-HTTPS page, migration to AOSSL should continue.

Corporate use of cloud services also continues to grow. According to our survey on client companies' usage of leading cloud services, we found that 82.6% use Office 365[2] and 77.1% use DropBox[3].

While AOSSL's growing prevalence and cloud services' burgeoning use are two separate trends, they both complicate conventional boundary defense. The traditional approach to boundary defense is to separate internal networks from external networks and monitor and/or intercept cross-boundary communications with firewalls, proxy servers or other such filters. AOSSL increases in-line decryption costs for monitoring communications' content. Additionally, use of cloud services means moving what should be protected information beyond traditional boundaries (i.e., to the cloud).

NOTE

1) https://www.nri-secure.co.jp/report/2018/cstar2018.html

2) A suite of Microsoft Office applications offered as cloud-based SaaS.

3) A service offered by DropBox, Inc., that enables users to store data in the cloud and sync files between DropBox and local devices.

Proliferation of IoT devices

IoT devices such as home routers and webcams are often vulnerable to cyberattacks, as most vividly exemplified by the Mirai[4] malware attacks that wreaked large-scale havoc in 2016. Analysis of communications intercepted by NRI Secure-administered networks' firewalls revealed that access attempts suspected of being targeted at IoT devices decreased modestly in fiscal 2017 but still accounted for some 40% of total access attempts.

Meanwhile, we noticed a change in these access attempts' breakdown by destination port[5]. Specifically, attacks targeted at telnet ports decreased in fiscal 2017 from roughly 50% of all attacks in fiscal 2016 while the fiscal 2017 attacks were dispersed more widely among ports that target specific devices. Targets of attacks are thus becoming more diverse as IoT devices proliferate. Physically accessible devices that are commonplace in homes and offices throughout the world will be targeted for attacks or hijacked to launch attacks. IoT devices' proliferation increases risks that straddle the boundary between the online and real (physical) worlds and necessitates security measures in response to such risks.

Rapid growth in data traffic linked to cryptocurrency mining

Another recent development is scripts embedded in websites to enlist the processing power of website visitors' devices to mine cryptocurrency for the benefit of the party that planted the script. One such script is CoinHive, which first appeared in September 2017. CoinHive and similar crypto-mining scripts' access counts have since soared, increasing sevenfold between August and October 2017 alone. Some sites are infected with scripts planted without authorization by external third parties seeking to maliciously exploit vulnerabilities. In other cases, site administrators install the scripts themselves to monetize their sites through a means other than online advertising. UNICEF Australia has installed a crypto-mining script on its website, but the script executes only when visitors grant permission. It treats the cryptocurrency mined as donations from its website's visitors. On the flipside of the coin, a number of website administrators in Japan were arrested for surreptitiously installing CoinHive on their sites.

Unlike ransomware and theft of confidential information, such crypto-mining scripts are not directly detrimental to corporate activities. That said, they cannot be dismissed as innocuous, given that they consume companies' computing resources. CoinHive has proven to be reminder of the shades of gray involved in determining what to intercept as harmful and how much to tolerate something

4) A malware that targets networked IoT devices such as webcams. Bad actors use Mirai to remotely seize control of IoT devices and aggregate them into large-scale botnets (collections of malware-infected, remotely controlled devices) to stage DDoS (distributed denial-of-service) attacks (mass attacks that overload the resources of the victim website, thereby crashing it).

5) With the internet communication protocol TCP/IP, there is typically a predetermined port used to connect to every application. For example, port 23 is usually used to telnet (perform simple remote-control operations using unencrypted plain-text commands).

seemingly benign.

Increasingly blurred boundaries

The common takeaway from the developments discussed above is that boundaries are becoming more complex and increasingly blurred in various cybersecurity contexts. Many security professionals have been warning since the early 2000s that simple boundary defenses alone are inadequate. Our latest survey found that the environment is now clearly changing in ways that are proving these warnings correct. Although not directly substantiated by hard data, another observation in our latest CSTAR is that the growing prevalence of remote work, a high-profile element of Japan's so-called workstyle reforms, blurs the boundaries between the inside and outside of an office.

How should companies respond to such changes? While tools such as EDR[6] and CASB[7] will likely be a partial solution, there will obviously never be an all-encompassing "silver bullet" solution. To properly utilize various new technologies, it is important to first go back to basics by conducting a big-picture assessment to determine what to protect and what leave unprotected, formulating policies on a risk basis, setting guidelines in accord with those policies and incorporating processes into your organization for periodically reviewing and, as necessary, revising the policies. The chief information security officer (CISO) must be granted sufficient authority to set the guidelines, particularly risk-tolerance guidelines, for such core security measures' effective and continual implementation. According to another of our surveys (NRI Secure Insight 2018[8]), only 35% of Japanese companies have a CISO on their C-suite executive teams versus roughly 70% of overseas (US, UK, Australian and Singaporean) companies. Figuring out how to organizationally enable the CISO to play the requisite leadership role will be the key to effective cybersecurity in an increasingly borderless environment.

(Supervising editor: Satoshi Harada of NRI Secure's Cyber Security Services Development Department)

6) EDR (endpoint detection and response) is a tool that monitors and detects cyberattacks and other suspicious operations at network endpoints (e.g., PCs, smart devices), insulates the network from threats and preserves evidence.

7) A CASB (cloud access security broker) is a product or service for tracking users' cloud service usage, visualizing cloud usage, controlling access in compliance with the organization's policies and defending against cyberattacks and leaks of important information.

8) https://www.nri-secure.co.jp/report/2018/analysis_global2018.html

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.4 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit http://www.nri.com/global/

Inquiries to : Financial Market & Innovation Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index