CYFIRMA

REPORT

CYBERTHREAT LANDSCAPE:

FINANCIAL SERVICES

BY KUMAR RITESH
Chairman and CEO, **CYFIRMA**

TO IMPROVE THEIR CUSTOMER EXPERIENCE, FINANCIAL INSTITUTIONS ARE EMBRACING INNOVATIVE TECHNOLOGIES — AND CREATING A NEW ATTACK SURFACE.

Overview

Over the past two years, digitilization in financial services has contributed to the growth of high-profile cyberattacks.

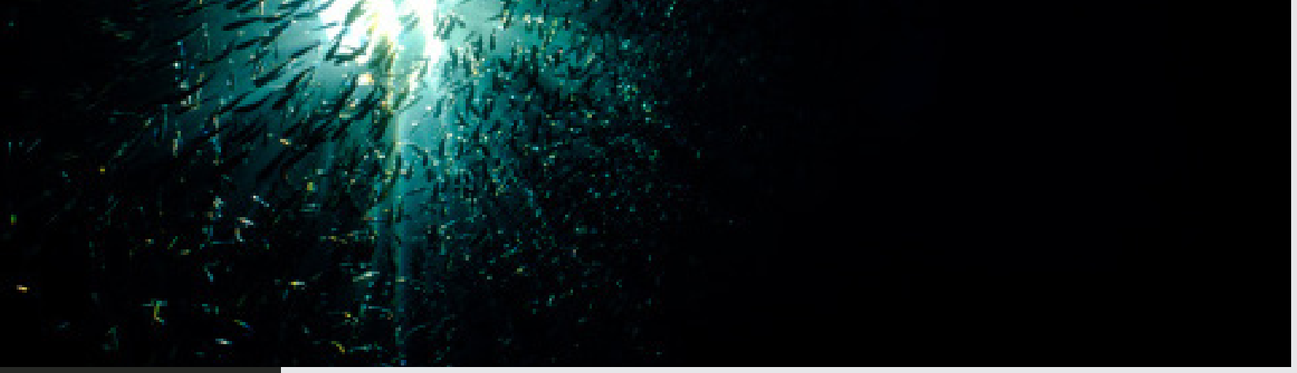
The rapid proliferation of cyberattacks is fueled by the rise of the dark web, a safe enclave where threat actors exchange ideas, trade or teach each other new hacking techniques or mechanisms. It is also a marketplace for stolen financial and personally identifiable information, that can be used to spearhead further attacks, including identity theft and tailored social engineering campaigns, such as spear-phishing emails to specific targets.

The evolution of ransomware, escalating attacks on virtual currency and new attack techniques in 2017 are sobering reminders of how aggressively cybercriminals work together to reinvent attack mechanisms and dramatically change tactics. We do not expect ransomware and attacks on virtual currency to fall out of favor; in fact, we think they will diversify further, and digital extortion will become even more prevalent. With ransomware-as-a-service actively offered in hacker forums, combined with the handsome profits generated by ransomware campaigns and the meteoric rise in bitcoin value, threat actors targeting virtual currency are more enticed by this “profitable business model” than ever.

In Jan. 2018, a cyberattack on the Japan-based Coincheck exchange saw hackers ***steal $530 million worth of XEM cryptocurrency****.*

Since 2015, approximately half of all financial institutions in Japan have experienced a cyberattack. In a 2017 survey of banks, credit associations and other financial organizations conducted by Bank of Japan 1.2% noted that they suffered catastrophic damages from a cyberattack, while 9.7% said they suffered minor consequences. Fear of subsequent media and investor fallout led major banks in Japan to invest heavily in cybersecurity measures, and threat actors are aware of this.

In 2018, we expect threat actors to focus attention on small and midsized financial institutions, whose senior management might not fully appreciate the potential severity of a cyberattack.



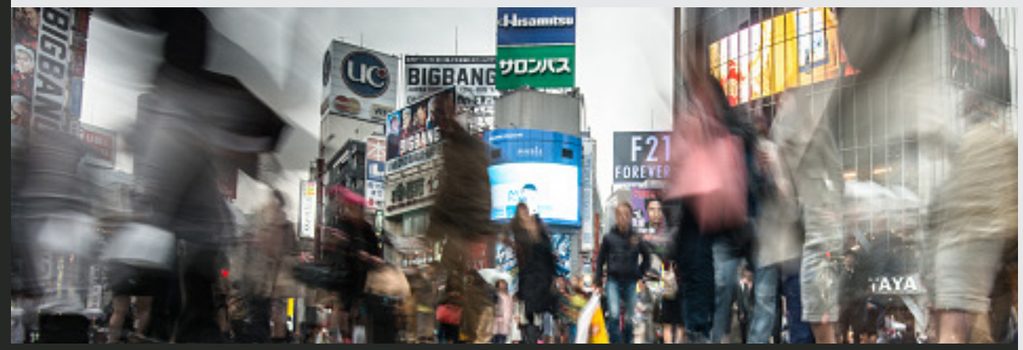
LOOKING AHEAD

HOW THREAT ACTORS ARE TARGETING JAPAN

We are witnessing a growing number of state-sponsored hackers from China, North Korea and Russia and turbulent nations targeting global financial institutions. We also see a rise in threat actors from emerging economies.

Historically, the language barrier made it very difficult for foreign threat actors to conduct cyberattacks on Japanese organizations or citizens; as a result, threat actors could only attack the English websites of Japanese entities successfully.

Recently, however, we have observed a growing number phishing emails written in grammatically fluent Japanese focused on the public or middle- and small-sized organizations. Threat actors, be they domestic or foreign, are developing a strong grasp of the Japanese language and the underlying cultural nuances.



Emerging Trends

Our observations in various deep/dark web and hacker forums reveal that more advanced and sophisticated attacks are planned for 2018. Trends include increases in attacks on or via:

PHISHING: In 2017, unknown threat actors made multiple phishing attempts on Japanese consumers and businesses, and large-scale campaigns impersonating Apple, Amazon, Microsoft and more were perpetrated on unsuspecting consumers. The extent of financial or data exfiltration from these attacks remain undisclosed.

We believe that this trend will continue in 2018, as evidenced by several viral campaigns launched in January, one of which targeted retail customers of Mitsubishi UFJ Financial Group (MUFG). In this viral campaign, consumers received phishing emails leading to an impersonated registration screen on a camouflaged web site, where credit card and personal information were stolen. Perhaps the most alarming aspect of the hack was the use of honorific business Japanese in the emails..

ATMS: Cash or genkin is still the main form of monetary exchange in Japan, despite measures to move away from hard currency. Because ATMs in Japan are highly sophisticated, money can be easily transferred between accounts, making it difficult to track ATM fraud. Common fraud tactics include social engineering techniques where threat actors contact victims by phone, ply them with a fake scenario or story and pressure them to transfer money to a specific account. Given the high level of trust in Japanese society, this has been an effective way to trick victims. We expect threat actors to develop new methods to exploit cash-rich Japanese consumers throughout the year.

THIRD PARTIES: In 2017, security breaches via compromised third parties was a growing problem affecting multinational companies across industries. We believe that vendor security will become even more critical in 2018, because many cyber-readiness evaluation standards for vendors are not significantly robust. Cybersecurity must become a critical criterion for vendor selection, rather than an afterthought.

INTERNET OF THINGS (IOT): IoT is now riding the FinTech wave in Japan, and many banks consider it as a competitive advantage to offer a seamless banking experience for customers via connected devices. However, IoT devices are highly vulnerable to cyberattack, and we anticipate the continued use of IoT devices to launch DDoS attacks, DNS-changing malware or cryptocurrency mining malware.

In 2016, the notorious Mirai botnet attack led to one of the biggest DDoS attacks in history; in 2017, an attack led to the recall of 500,000 pacemakers over concerns that threat actors could manipulate these devices. Also in 2017, we saw Satori, the successor to Mirai, infect 280,000 IP addresses in 12 hours. In January 2018, threat actors posted the source code of the Satori botnet on Pastebin, a public sharing website, and we expect to see new iterations of Satori throughout 2018.

CRYPTOCURRENCY: The recent rise of cryptocurrency, especially Bitcoins, and the growing willingness of financial institutions to explore this technology has gained hackers' attention. They are covertly installing mining malware on target machines and have executed multiple attempts to attack cryptocurrency wallets. In 2018, a cyberattack on the Japan-based Coincheck exchange saw threat actors steal US $530 million worth of XEM cryptocurrency.

Web mining is a cryptocurrency mining technique used directly in a browser via a special script installed on a web page. We believe that web mining will lead to new ways of website monetization. We also expect an increase in the number of phishing and hacking attacks targeting initial coin offerings, smart contracts or crypto wallets.

DIGITAL IDENTITIES: In the face of growing use of tokenization and biometric security measures, threat actors are now shifting focus to account takeover attacks —a hacker exploits a customer's personal information, stored with a merchant, to take control of an account or establish a new one. Since most consumers use the same credentials for multiple online sites, hackers have been able to use brute force to take over online banking accounts. Industry estimates suggest fraud of this type will run into the billions of dollars in 2018.

RANSOMWARE: Traditional ransomware campaigns via phishing emails will become less attractive to threat actors as the Japanese financial services industry educates consumers/employees and uses other strategies to mitigate phishing. We anticipate that attackers will repurpose ransomware via new attack vectors or compromised third-party vendors to conduct cyber sabotage and disruption (For example, a U.S. hospital paid thousands of dollars to unlock their systems after hackers launched a ransomware attack using a third-party vendor's credentials.). These activities could be driven by the lucrative ransomware-as-a service business in the deep/dark web, as competitors hire threat actors to wreak reputational and financial damage and disruption on peers.

PERVASIVE THREAT ACTORS

Several threat actors have continually shown interest in Japanese financial institutions, including:

CHINA

Elderwood Group

A highly sophisticated group that is well-funded Chinse hacking group, Elderwood has been linked to numerous attacks in the financial services, shipping, aeronautics, energy, manufacturing, engineering, electronics and software industries. This group specializes in “waterhole” attacks, in which they seek to compromise legitimate websites used frequently by employees in a target company much like lions stake out their prey at a watering hole. In these attacks, unsuspecting users download malware to their machine when they click any links in the website; this custom malware performs an automated search in the infected network for sensitive files or data to exfiltrate.

Nectar

A Chinese hacking group affiliated with Chinese governments, Necter has historically expressed active interest in attacking a spectrum of industries, including financial services, engineering, commodities, energy, telecommunications, retail, food and beverage, and manufacturing. This highly sophisticated group maintains its focus on compromised systems for months or even years; during this period, Necter exfiltrates enormous amounts of data and laterally propagates malware to infect new systems.

NORTH KOREA

Gemoun

A suspected splinter of the Lazarus Group (below), Gemoun targets construction, manufacturing, technology services, financial institutions, financial trade software development companies and cryptocurrency organizations. Gemoun specializes in cyber espionage, sabotage and data exfiltration. Our researchers have found multiple attacks worldwide attributed to this threat group, and we have high confidence that close links exist between Gemoun and the North Korean government.

Lazarus Group

This highly sophisticated cybercriminal group affiliated with the North Korean government rapidly develops, mutates or evolves existing exploits/ malware via its internal malware factory. The group is notorious for multiple attacks on the manufacturing, construction and engineering industries in the last decade. It is believed that the group was also involved in the notorious 2017 WannaCry attack, leveraging a National Security Agency (NSA) exploit known as EternalBlue released publicly by “Shadow Brokers,” another hacker group, a few months previously. Lazarus is believed to be directly responsible for the Bangladesh bank heist in 2016 and the Sony breach in 2014.

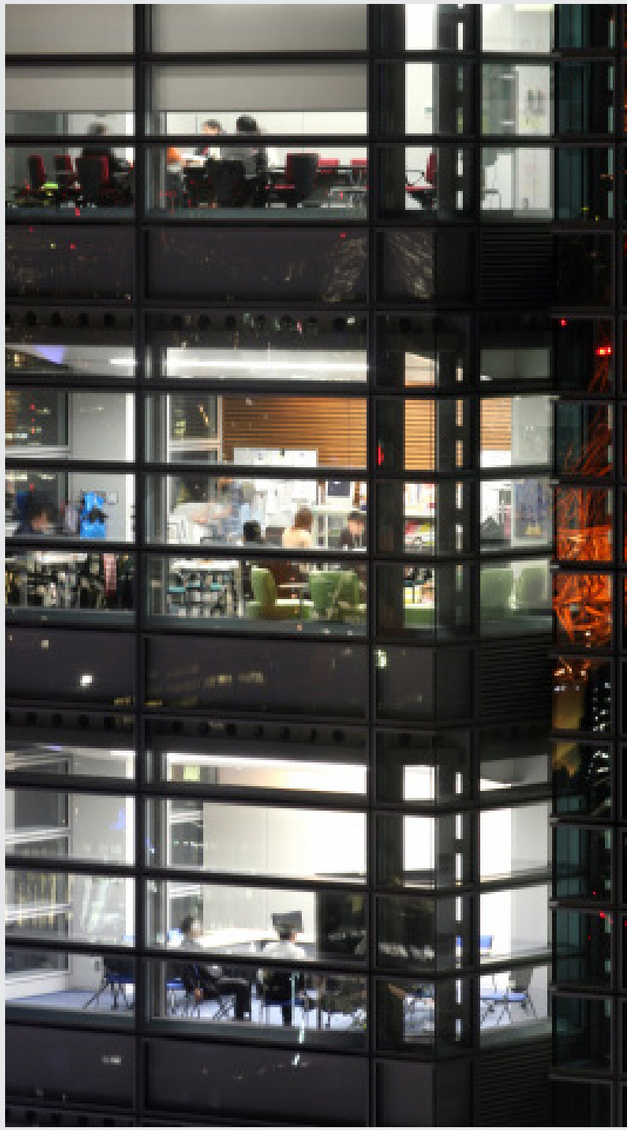
RUSSIA

Carbanak a.k.a Anunak

This group’s modus operandi typically involves sending spear phishing emails with malicious CPL of Word documents containing shellcodes that open a back door in the victim’s machine. This back door, designed for cyberespionage and data exfiltration, allows hackers to control the compromised machine. Up to 100 attacks on financial institutions globally have been attributed to this group; the losses suffered by each bank range from $2.5 million to $10 million. It is estimated that Carbanak has stolen.

Fancy Bear a.k.a. APT28, Pawn Storm, Sofacy Group

A Russian state-sponsored hacking group closely af¬filiated with Russian intelligence services, Fancy Bear is suspected of serving the interests of the Russian government, leading researchers to believe that it interfered in elections in certain countries to help candidates favored by Russia. Fancy Bear, which typically applies zero-day vulnerabilities via spear phishing emails disguised as news sources in attacks



to compromise targets, is interested in exfiltrating sensitive data from victims. Previous victims in the financial services industry include United Bank for Africa, Bank of America, TD Bank and UAE Bank.

OUR PERSPECTIVE

CYFIRMA

The financial industry can expect to face a broad range of threats in 2018, including new exploits, ransomware, social engineering and targeted attacks and, most importantly, attacks on emerging technologies.

Financial institutions are subjected to strict regulations and compliance requirements, which explains their risk aversion and conservative attitude towards addressing cyber risks proactively. Cybersecurity is often viewed as a deterrent rather than a business enabler — a lack of understanding that contributes to its downgraded prioritization.

At the same time, threat actors are highly skilled, coordinated and sophisticated, armed with the latest exploits and constantly devising new methods of attacking the financial services industry. To actively detect and prevent new attacks, organizations must adopt a proactive, integrated approach.

The ever-changing threat landscape and rapidly evolving attack mechanisms render traditional methods of defense futile; the only way to address the elastic attack surface is with a detailed cyberstrategy, and complete assessment of the entire attack surface, possible attack scenarios, integrated monitoring controls, emerging technology threat modeling, and potential risks and mitigating controls.

CYFIRMA's intelligence-driven solutions enable CISOs to make better-informed decisions regarding how to maintain their cyber posture in response to emerging threats, attack mechanisms and motives — an approach that has proven highly effective for clients in Japan, who evaded compromise by WannaCry, Petya, Bad Rabbit and other significant cyberbreaches in 2017.

Powered by AI and machine learning, CYFIRMA's flagship platform automatically aggregates, correlates and analyzes security information and events from thousands of data sources daily, including the deep/dark Web and hacker forums.

As a result, CYFIRMA delivers unrivaled threat visibility and intelligence, applying predictive insights to an organization's strategies, policies, processes, people and technologies to prevent cyberattacks.