Trends in Global Security Threats

Yosuke Aragane, Kenji Ogura, Hitoshi Endoh, and Kenji Takahashi

Abstract

In this article, to illustrate the trends in global security threats, we examine two ingenious cyber-attacks that were recently reported, and we discuss the countermeasures to the attacks. We also introduce the Global Threat Intelligence Report, an NTT Group initiative related to global security threats. We believe that sharing this sort of information about security threats will help to raise awareness of cyber-security and lead to more secure systems.

Keywords: threat information, cyber-attack, global security

1. Introduction

In recent years, massive cyber-attacks have occurred that have inflicted damage on a scale that is difficult to assess. Examples include the JPMorgan Chase & Co. (a major American financial services firm) data breach targeting its customer information, the devastating cyber-attack on Sony Pictures that included the destruction of corporate systems and the publication of stolen corporate information, a large-scale data breach of government employee information from the United States Office of Personnel Management, and the leakage of information from Japan Pension Service. These cyber-attacks are often not reported in great detail from the viewpoint of ensuring security.

However, people can strengthen the security of their own systems by using cases such as these to understand the deceptive tactics used by attackers and the measures that can be used to defeat them. Consequently, sharing information about security threats will become increasingly important in the future.

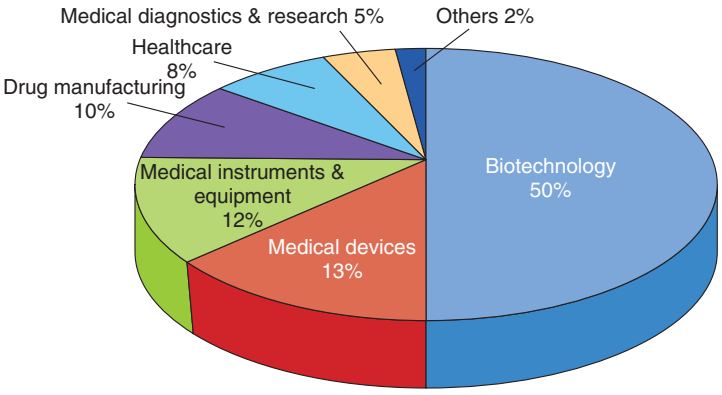
In this article, we report on some sophisticated cyber-attacks reported recently, and we explain the NTT Group's Global Threat Intelligence Report (GTIR) initiative that aims to accelerate the sharing of information.

2. FIN4: Secretly stealing confidential information

FireEye, Inc., a U.S. based network security company, analyzed certain incidents in its clients' networks as well as data it obtained separately through their products and detected a group that is focused on secretly stealing confidential company information that could affect the stock prices of publicly traded companies. FireEye named the group FIN4.

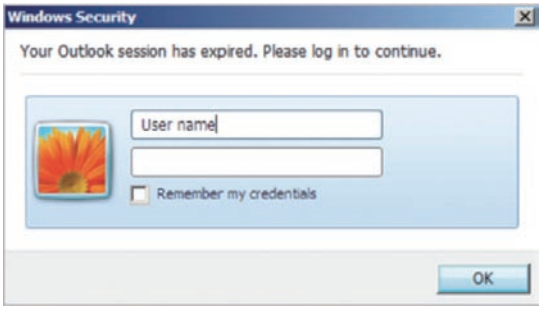
The members of this group have not been identified, so the purpose of their attacks is still unclear. However, FireEye believes that FIN4 is exploiting this insider information in order to profit on the stock market. It is very difficult to ascertain the actual damage because there have not been any apparent losses at the companies targeted in this type of cyber-attack.

FIN4's activities have been observed since mid-2013, and FireEye has discovered about 100 targets consisting of publicly traded healthcare and pharmaceutical companies (68%), firms advising public companies on matters concerning security, legal issues, and mergers & acquisitions (M&A) (20%), and other publicly traded companies (12%). For healthcare and pharmaceutical companies, information on the authorization of drugs or the development and clinical testing of new drugs can have a major impact on the share prices. Also, M&A consultants are privy to M&A information before it is made



Source: http://www2.fireeye.com/fin4.html

Fig. 1. Breakdown of the healthcare and pharmaceutical industry sectors targeted by FIN4.



Source: http://www2.fireeye.com/fin4.html

Fig. 2. Fake dialogue box used to steal login credentials.

public. A breakdown of the healthcare and pharmaceutical industry sectors targeted by FIN4 is shown in **Fig. 1**.

When FIN4 targets a particular company, it starts out by targeting other companies that do business with it. It then uses the email accounts of these other companies to send emails to the target company containing information on transactions that are currently in progress. These emails are addressed to people dealing with confidential information of the target company such as management executives, company attorneys, and researchers. They include attached Office[*1] documents that are exchanged in actual transactions but that have embedded macros that display a fake Outlook[*1] login prompt when the files are opened [1] (**Fig. 2**) and then send the login information to FIN4's server. For environments where macros are disabled, the email message includes a link to a fake Outlook Web App (OWA) login page from where the login information can be stolen. Using this stolen Outlook authentication information, FIN4 accesses the email accounts of people who work with the target company's insider information and obtains confidential information by intercepting and reading their email.

FIN4 also creates settings that automatically delete emails containing terms such as *hacking*, *phishing*, and *malware* from the target's Outlook account. As a result, the targeted individual is not able to see warning emails with messages such as "Is your company being targeted?" from external correspondents.

The U.S. Securities and Exchange Commission (SEC) was reported to have requested detailed reports on at least eight companies targeted by FIN4 [2], but as of the end of June 2015, they had not yet released

*1 Office and Outlook are registered trademarks of Microsoft Corporation in the United States and other countries.

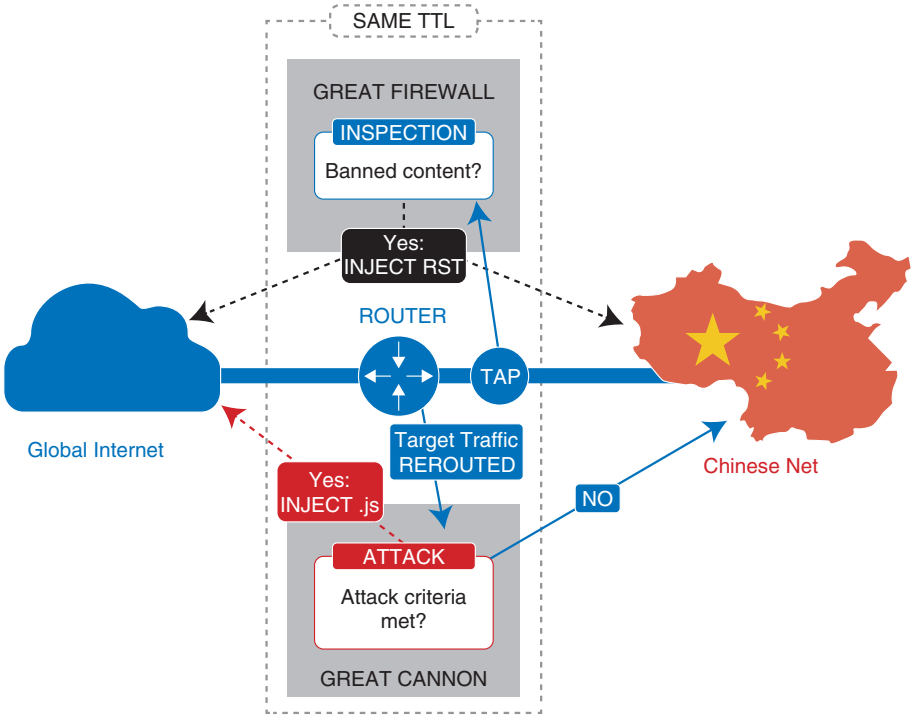


Fig. 3. Schematic model of GFW and GC.

a public statement on the issue.

Steps that can be taken to avoid becoming one of FIN4's victims include disabling macros in Microsoft Office and enabling two-factor authentication for OWA. Also, since FIN4 uses Tor[*2] to conceal the traffic that sends login information to its server, another effective measure is to monitor the internal network logs to check for communication with known Tor nodes.

3. The Great Cannon of China

A study by the Citizen Lab at the University of Toronto has shown that the Great Firewall (GFW)[*3] of China is now partnered with an attack system, which it calls the Great Cannon (GC). In March 2015, GreatFire.org and GitHub[*4] became the first observed victims of massive DDoS (distributed denial of service) attacks from GC. In the following, we describe the GC and GFW mechanisms on which they are based, as well as a GC attack.

3.1 GFW mechanism

The GFW is shown in the upper part of **Fig. 3** [3]. All Internet traffic in and out of China passes through the GFW. The traffic is intercepted at the element labeled TAP, and content that is subject to restrictions or blockades is identified at the element labeled INSPECTION. When such content has been identified, the INJECT RST part transmits RST (reset) packets, which are used when blocking communication or denying access, to the source and destination servers. A load-balancing mechanism is used in the GFW so that it can process multiple communication streams in parallel. In this way, the GFW continuously monitors network traffic in order to block access to content that the Chinese authorities regard as undesirable.

*2 Tor: Software that anonymizes the paths of network connections without encrypting the content of the traffic carried by them.

*3 GFW: A large-scale censorship system used by Chinese authorities to restrict and cut off Internet connections into and out of China.

*4 GitHub: A web service provided by GitHub, Inc. as a platform for sharing software development projects. Its basic functionality is available for free, and extended features can be used for a fee.

3.2 GC mechanism

In the GC, the Target Traffic REROUTED component in Fig. 3 reroutes the corresponding traffic, and the ATTACK component identifies whether or not it is to be used in an attack. If so, an attack code is sent to the access source; otherwise it connects to the requested destination server. On receiving an attack code, the access source becomes a temporary agent that supports a GC attack. Just as with the GFW, all Internet traffic in and out of China passes through the GC, so it is possible to launch a large-scale attack even when only a tiny fraction of traffic is used by the GC. The GC takes over this traffic, which makes it capable of launching man-in-the-middle (MITM) attacks. The GC is compatible with high-bandwidth communications, so it collects only IP addresses of the access sources. It also has a mechanism for caching previous traffic so that it can eliminate unnecessary work when the same process is performed repeatedly on the same traffic. Citizen Lab's test results suggest that up to 16,000 access source IP addresses can be stored in this way.

According to Citizen Lab, the results of sending traffic configured to respectively operate the GC and GFW, and the results of analyzing the responses to this traffic suggest that the GC and GFW do not share attack facilities but have their own systems. However, there are similarities in the way they rewrite data packets, so they appear to share parts of the same program code and are thought to be very closely related. The GC and GFW have similar load balancer functions and are thought to distribute traffic based on the IP addresses of access sources.

A Citizen Lab survey of communication paths set up to activate the GFW and GC indicated that both are on the same destination network, so it seems that the GC and GFW are installed right next to each other [3]. In one test environment, the destination network was China Telecom, and in another test environment the destination network was China Unicom. The research done by security blogger Robert Graham suggests that the GC exists in the infrastructure of China Unicom.

3.3 Attacks on GreatFire.org and GitHub

From March 14 to March 25, 2015, a large-scale DDoS attack was carried out against GreatFire.org, which was hit with 2.6 billion requests per hour (2500 times the usual rate). GreatFile.org provides functions that use the Amazon CloudFront CDN (content delivery network) service to bypass the GFW and allow blocked sites to be viewed. Note that the Cyberspace Administration of China has already identified GreatFire.org as a foreign anti-Chinese organization.

From March 25 to April 7, 2015, GitHub was also hit by a large-scale DDoS attack, causing the site's response times to increase several times over [4]. GreatFire.org has two GitHub repositories that provide technology to users wishing to circumvent Chinese censorship. The attack on GitHub appears to have been carried out with the aim of forcing the removal of these repositories from GitHub.

The GC attacked GreatFire.org and GitHub by intercepting and redirecting traffic destined for Baidu Analytics and Baidu Advertising, which are parts of the Baidu common platform. However, not all the traffic to these sites was used in the attack. According to Citizen Lab's observations, the majority of traffic (about 98.25%) passed through to Baidu unaffected, while the remainder (about 1.75%) was used in the attack [3]. The web requests used in the attack included page views of sites containing advertising from Baidu, so the visitors to these sites were unwittingly taking part in the attacks on GreatFire.org and GitHub.

3.4 Who built the GC?

Citizen Lab considers that the GC could not have been built or used without the approval of the Chinese government, since its attacks are too overt to have been conducted without government permission. It also stated that although it is not clear why the GC was built, it may have resulted from the conflict between the activities of GreatFire.org and the Chinese Communist Party's ideology [3]. These destructive acts may be designed not only to block access to content that the party finds undesirable but also to set an example for other organizations engaged in similar activities.

3.5 Predictions

Since the GC is evidently capable of launching attacks based on the source of Internet traffic, it is assumed to have latent capabilities for other forms of cyber-attack besides DDoS, even though they have not yet been observed. For example, it could be easily reconfigured to send malware to specific individuals that access servers in China without using encryption. Also, since the GC is a complete MITM, it could even replace attachments of an unencrypted email with malware.

It is very difficult for organizations and individual users to defend themselves against attacks by the GC. However, due to the way in which the GC works,

these attacks only work on unencrypted traffic, and will not work on traffic encrypted using the protocol HTTPS (Hypertext Transfer Protocol Secure) or the like. The GC can therefore be rendered less effective by promoting the encryption of traffic and content by many organizations and users.

4. GTIR

The 2015 edition of GTIR [5] was produced by NTT Innovation Institute, Inc. (NTT I^3) with the cooperation of NTT Group companies (NTT Com Security, Dimension Data, Solutionary, NTT Secure Platform Laboratories, and NTT DATA). It contains detailed descriptions of the following important trends based on the analysis of about 6 billion attack events observed by the NTT Group during 2014.

- The financial industry continues to represent the number one targeted sector, accounting for 18% of all detected attacks. Attacks against business and professional services increased from 9% to 15%.
- Basic controls are still not implemented in all cases; 74% of organizations do not have formal incident response plans.
- Incident responses involving malware threats increased 9% compared to 2013, from 43% to 52%.
- During 2014, 76% of identified vulnerabilities throughout all systems in the enterprise were more than 2 years old, and almost 9% of them were over 10 years old.
- Over 80% of vulnerabilities in 2014 exploit kits were published in 2013 and 2014.
- There was an increase in Adobe Flash*5 exploit usage in exploit kits from 2012 to 2014.
- Of the attacks on NTT's customers worldwide, 56% originated from IP addresses in the US. The attackers are not necessarily in the US but are taking advantage of the rich cloud services available there.
- DDoS amplification attacks using User Datagram Protocol accounted for 63% of all DDoS attacks observed by NTT Group.

5. Future prospects

The NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) at NTT Secure Platform Laboratories is working to improve security throughout the NTT Group and the information network society. NTT-CERT provides consultation services on information security and also delivers security-related information.

We will continue with our ongoing incident response support for NTT Group companies. We also plan to continue providing security information with the aim of expanding the global scale of our activities.

References

[1] FireEye, "Hacking the Street? FIN4 Likely Playing the Market." https://www2.fireeye.com/fin4.html
[2] REUTERS, "Exclusive: SEC Hunts Hackers Who Stole Corporate Emails to Trade Stocks," Jun. 23, 2015. http://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623
[3] B. Marczak et al., "China's Great Cannon," Apr. 10, 2015. https://citizenlab.org/2015/04/chinas-great-cannon/
[4] XDNet, "Google says Chinese Great Cannon shows need to encrypt web," Apr. 27, 2015. http://www.zdnet.com/article/google-says-chinese-great-cannon-shows-need-to-encrypt-web/
[5] Website of NTT I^3 GTIR, http://www.nttgroupsecurity.com

*5 Adobe and Flash are registered trademarks or trademarks of Adobe Systems Incorporated in the United States and other countries.

Yosuke Aragane
Senior Research Engineer, Supervisor, NTT-CERT, Security Risk Management Project, NTT Secure Platform Laboratories.

He received his M.S. and Ph.D. from Tokyo Institute of Technology in 1997 and 2005. He joined NTT Multimedia Network Laboratories in 1997, where he worked on intelligent transportation systems. Since 2003, he has been with NTT Information Sharing Platform Laboratories and NTT Secure Platform Laboratories focusing on cybersecurity research. His current research interests include security operation optimization, security intelligence sharing, and human factor influences on the information security. He is a member of the Institute of Electrical and Electronic Engineers (IEEE), the Association for Computing Machinery (ACM), the Information Processing Society of Japan (IPSJ), and the Institute of Electronics, Information and Communication Engineers (IEICE).

Kenji Ogura
Senior Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in electrical engineering from Keio University, Kanagawa, in 1988 and 1990. He joined NTT LSI Laboratories in 1990, where he researched and developed CAD (computer aided design) systems for LSI (large-scale integrated circuit) design. Since joining NTT Secure Platform Laboratories in 2014, he has been working on security information analysis at NTT-CERT. He is a member of IPSJ.

Hitoshi Endoh
Research Engineer, Security Risk Management Project, NTT Secure Platform Laboratories.

He received an M.A. in arts and sciences from the University of Tokyo in 1997. He joined NTT Cyber Space Laboratories (now, NTT Media Intelligence Laboratories) in 1997. During 2000-2012, he was a member of the Cyber Security Department at NTT EAST Corporation, where he developed information system security guidelines and a security vision with medium and long term action plans. Since joining NTT Secure Platform Laboratories in 2012, he has been working on computer security incident response team (CSIRT) activities at NTT-CERT. He is currently working on information sharing projects with other CSIRT teams and cyber threat analysis.

Kenji Takahashi
VP, Product Management, Security, NTT Innovation Institute, Inc.

He received his B.S., M.S., and Ph.D. in computer science from Tokyo Institute of Technology. He has over 28 years of international experience in the information and communication industry. He has led many projects at NTT R&D in Japan, including those related to cloud computing, software engineering, digital identity management, collaboration environments, and ubiquitous computing. He was previously President and CEO of NTT Multimedia Communication Laboratories, Inc. (NTT MCL) in Silicon Valley, where he successfully launched and led open source, open standard based cloud, and software-defined networking projects. He was a visiting scientist at the College of Computing at Georgia Institute of Technology and a member of the Discovery Park Advisory Council at Purdue University. He received the Kiyasu Special Industrial Achievement Award from IPSJ for his pioneering work on federated identity management. He is a member of IEICE, IPSJ, IEEE Computer Society, and ACM.