FUNG GLOBAL RETAIL & TECHNOLOGY February 17, 2017

FLASH REPORT

Takeaways from RSA Conference 2017—Day 2

1) This week, the Fung Global Retail & Technology team is attending RSA Conference 2017 in San Francisco. The conference is focused on cryptography and information security.
2) There is an enormous amount of data available that can help companies detect employee theft of documents and information and other types of malfeasance. There are also software tools available that can sort through false alarms and generate urgent notifications when necessary.
3) The use of ransomware, and crypto-ransomware in particular, is becoming more prevalent, as it is fairly inexpensive for attackers to deploy and potentially lucrative.
4) The exploding consumer-related Internet of Things (IoT), in addition to the industrial IoT, offers new opportunities for hackers to find weaknesses to exploit.
5) In many cases, companies are running vulnerable software that they have not updated with long-available patches or using software libraries with known weaknesses. Focusing on system and network hygiene and setting policies regarding crisis situations, such as the payment of ransom, are essential.
6) The Fung Global Retail & Technology team will continue to report on key points and information presented during the rest of the conference.

The RSA Conference runs February 13–17. Our notes from selected keynote and other addresses and seminars on the second day of the event follow.

Copyright © 2017 The Fung Group. All rights reserved.

FLASH REPORT

Seminar: “War Stories: Corporate Cyberespionage Tales from the Trenches”
Much of the discussion in the first seminar we attended focused on the problem of employees who are about to leave a firm emailing sensitive files and business information to their personal account. Companies that are looking to prevent such behavior are able to set up systems that detect and act on sudden increases in email to a personal account.

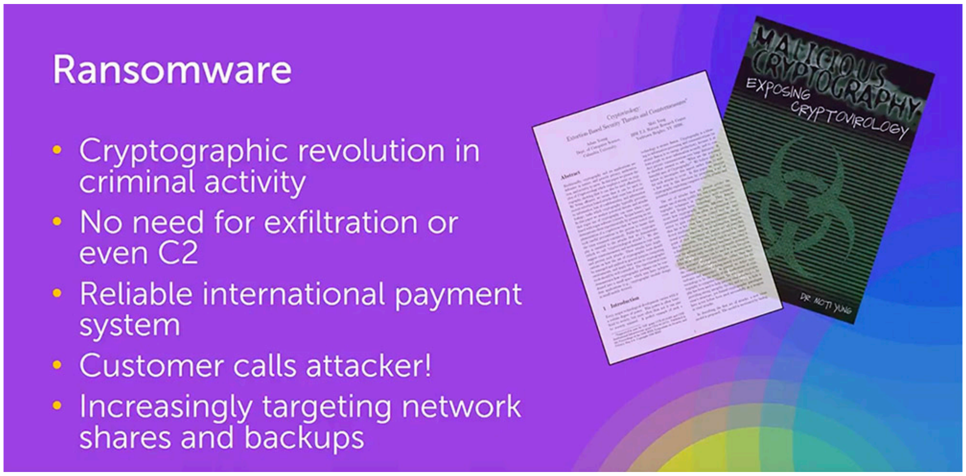
There is a large amount of security-related data available to companies, and IT managers need tools to determine which data are ordinary and which may suggest some kind of unwanted behavior.

Other types of infractions involve employees gaining inappropriate priviliges or granting them to others. One example cited was administrative assistants gaining or being given the ability to read the email of upper management.

In some cases, regular police-type work can catch cyberthieves and cybercriminals. In one example cited, an employee removed a large number of documents—both physically and electronically—shortly before resigning to work for a competitor. When confronted, the employee confessed that he and another former employee were using the documents to create their own software application.

In one final example that was discussed, an employee was taking photos of company information with his smartphone and uploading them to sites on the dark web. The employee was caught by enhancing one of the photos, which captured a reflection of his employee badge.

Keynote (Panel): “The Seven Most Dangerous New Attack Techniques, and What’s Coming Next”
The second panel we attended was led by three speakers, each of whom discussed a separate topic.



Ransomware

- Cryptographic revolution in criminal activity
- No need for exfiltration or even C2
- Reliable international payment system
- Customer calls attacker!
- Increasingly targeting network shares and backups

Source: Youtube

1. There has been an explosion of ransomware, particularly crypto-ransomware.
One survey tracker found 150 separate instances of crypto-ransomware deployment. With crypto-ransomware, the software encrypts the user’s hard drive, and the user has to pay the attacker a ransom (typically via an untraceable currency such as bitcoin)—meaning the victim actually has to ask the attacker for help.

Copyright © 2017 The Fung Group. All rights reserved.

The means to prevent and mitigate the use of ransomware include focusing on system and network hygiene and establishing in advance a company policy regarding the payment of ransom.

2. The explosion of the IoT offers new opportunities for hackers, especially in the industrial IoT.

Recent examples of industrial Internet hacking include several attempts to hack power generation facilities in Ukraine. Hackers are attempting to first disrupt, and then overwrite, the software of industrial machinery, often attempting to neutralize ("brick") the machinery. Accordingly, companies need to balance security with the benefits and cost reductions that come from automation.

3. There are still several insecure software components that are commonly used.

Many commonly used random-number generators, which are the basis for generating encryption keys, are not actually random, and can therefore be predicted. However, there are alternative generators available.

Hackers first attacked software libraries, but they are now turning their attention to cloud-based servers. And security of cloud-based assets is becoming more and more urgent, as more enterprises are moving data and services to the cloud. Authentication is important to ensure that companies connect to the correct servers.

Seminar: "Are Zero Days the Biggest Threat to ERP Systems?"

Zero days represent the time that elapses between when a security incursion is discovered and when it can be remedied.

Many companies use enterprise-resource planning (ERP) software, such as the solutions provided by SAP and Oracle, to manage operations, inventory and finances. However, one consultant discovered 36 organizations worldwide (including some multibillion-dollar global companies) that were being exploited through a vulnerability in SAP software. It turns out that this weakness was publicly disclosed in 2013, but these enterprises had not updated or patched their software.

In another survey, 65% of respondents said that their SAP systems had been breached in the last 24 months. The number of SAP security notes has increased dramatically since 2009, indicating that the system is becoming an increasingly attractive target for attackers.

Although it is complicated to shut down running systems to install patches, patch management for ERP systems is crucial.

Copyright © 2017 The Fung Group. All rights reserved.

FLASH REPORT

Deborah Weinswig, CPA
Managing Director
Fung Global Retail & Technology
New York: 917.655.6790
Hong Kong: 852.6119.1779
China: 86.186.1420.3016
deborahweinswig@fung1937.com

John Harmon, CFA
Senior Analyst

Hong Kong:
8th Floor, LiFung Tower
888 Cheung Sha Wan Road, Kowloon
Hong Kong
Tel: 852 2300 4406

London:
242–246 Marylebone Road
London, NW1 6JQ
United Kingdom
Tel: 44 (0)20 7616 8988

New York:
1359 Broadway, 9th Floor
New York, NY 10018
Tel: 646 839 7017

FungGlobalRetailTech.com

Copyright © 2017 The Fung Group. All rights reserved.