Case Study: Data Breach in Singapore

Data of some 129,000 Singtel customers, including NRIC details, stolen in hack of third-party system

PUBLISHED FEB 17, 2021, 09:43 PM

SINGAPORE - The personal data of some 129,000 Singtel customers were extracted by hackers during the recent breach of a third-party file sharing system used by the telco.

Information such as names, addresses, phone numbers, identification numbers and dates of birth, in varying combinations, were stolen by attackers, said Singtel in a statement on Wednesday (Feb 17).

They also stole the bank account details of some 28 former Singtel employees, and the credit card details of 45 employees of a corporate customer, according to the statement.

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

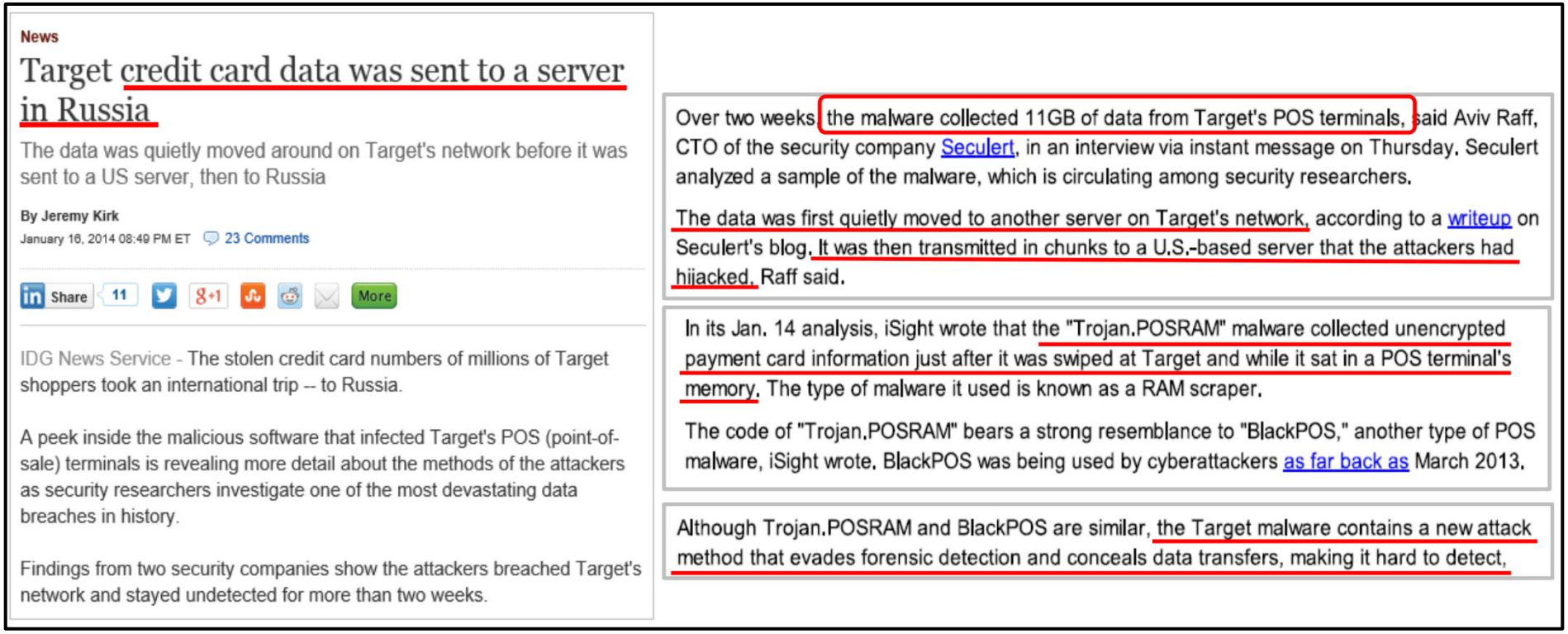
PUBLISHED JUL 20, 2018, 05:29 PM

SINGAPORE - In Singapore's worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.

The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

At a multi-ministry press conference on Friday (July 20), the authorities said PM Lee's information was "specifically and repeatedly targeted".

Case Study: Target Attack



News

Target credit card data was sent to a server in Russia

The data was quietly moved around on Target's network before it was sent to a US server, then to Russia

By Jeremy Kirk

January 16, 2014 08:49 PM ET 23 Comments

Share 11 8+1 More

IDG News Service - The stolen credit card numbers of millions of Target shoppers took an international trip -- to Russia.

A peek inside the malicious software that infected Target's POS (point-of-sale) terminals is revealing more detail about the methods of the attackers as security researchers investigate one of the most devastating data breaches in history.

Findings from two security companies show the attackers breached Target's network and stayed undetected for more than two weeks.

Over two weeks the malware collected 11GB of data from Target's POS terminals, said Aviv Raff, CTO of the security company Seculert, in an interview via instant message on Thursday. Seculert analyzed a sample of the malware, which is circulating among security researchers.

The data was first quietly moved to another server on Target's network, according to a writeup on Seculert's blog. It was then transmitted in chunks to a U.S.-based server that the attackers had hijacked, Raff said.

In its Jan. 14 analysis, iSight wrote that the "Trojan.POSRAM" malware collected unencrypted payment card information just after it was swiped at Target and while it sat in a POS terminal's memory. The type of malware it used is known as a RAM scraper.

The code of "Trojan.POSRAM" bears a strong resemblance to "BlackPOS," another type of POS malware, iSight wrote. BlackPOS was being used by cyberattackers as far back as March 2013.

Although Trojan.POSRAM and BlackPOS are similar, the Target malware contains a new attack method that evades forensic detection and conceals data transfers, making it hard to detect.

Case Study: WannaCry Ransomware

Significance of Computer Security

Critical to national security

- Cyber espionage: steal classified information from rival government or military systems, such as diplomatic strategies, defense plans, etc.
- Election interference: spread false information to influence public opinion, hack political campaigns, or manipulate voting systems.
- Cyber warfare: disrupt the military operations, or Distributed Denial of Service attacks against government services or infrastructure
- Supply chain attacks: target software or hardware suppliers to compromise the systems in government or defense agencies
- Cyber terrorism: launch attacks aimed at causing physical destruction or fear, such as targeting dams, chemical plants or hospitals

Case Study: Stuxnet Malware

Stuxnet 'hit' Iran nuclear plans

The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.

Olli Heinonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

Analysis carried out by security firm Symantec shows that a Stuxnet-infected controller in an industrial plant would make the devices it was connected to run at very high speeds almost indefinitely.

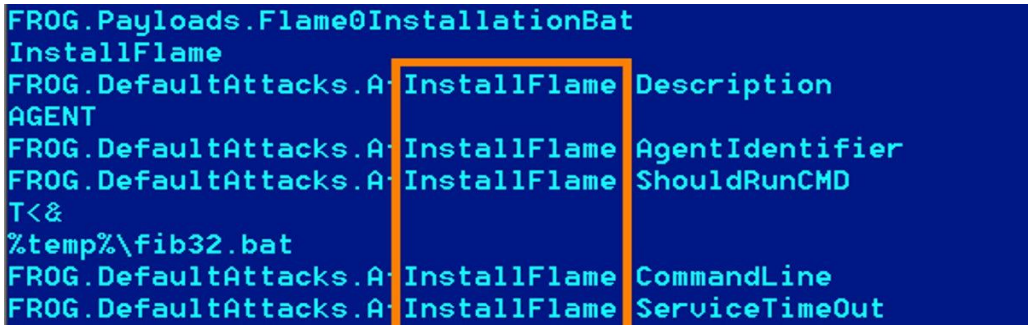
Symantec's research also suggests that Stuxnet was designed to hit motors controlling centrifuges and thus disrupt the creation of uranium fuel pellets.

Figures gathered by security firms show that 60% of all the infections caused by Stuxnet were on machines in Iran.

Case Study: Flame Spyware

Behind the 'Flame' malware spying on Mideast computers (FAQ)

With possible ties to malware targeting Iran, the Flame spying software is seen as the latest cyber espionage attempt from a nation state.



Flame is a sophisticated attack toolkit that leaves a backdoor, or Trojan, on computers and can propagate itself through a local network, like a computer worm does. Kaspersky Lab suspects it may use a critical Windows vulnerability, but that has not been confirmed, according to a Kaspersky blog post. Flame can sniff network traffic, take screenshots, record audio conversations, log keystrokes and gather information about discoverable Bluetooth devices nearby and turn the infected computer into a discoverable Bluetooth device. The attackers can upload additional modules for further functionality. There are about 20 modules that have been discovered and researchers are looking into what they all do. The package of modules comprises nearly 20 megabytes, over 3,000 lines of code, and includes libraries for compression, database manipulation, multiple methods of encryption, and batch scripting.

System Complexity Leads to Insecurity

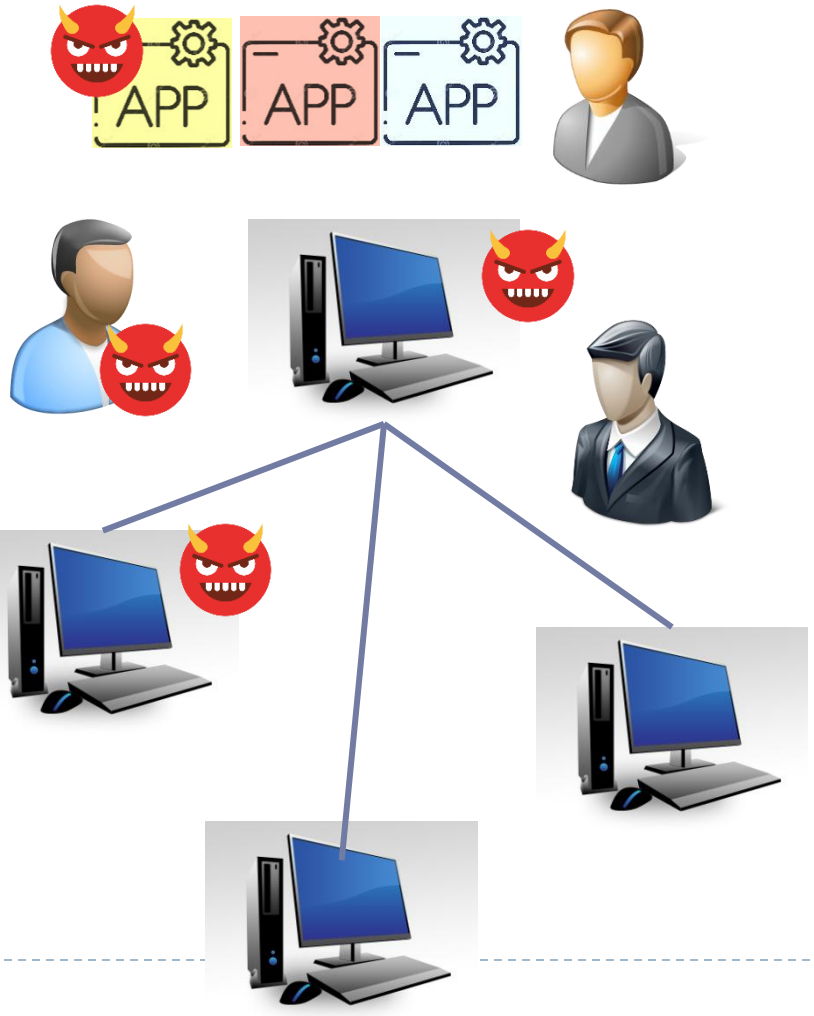
Provide a protected environment for data and their processing

Standalone computer single user monoprogram

- Physical security

Standalone computer single user multiprogram

- Physical security
- Process protection



Standalone computer multiple user

- Physical security
- Process protection
- Data protection
- User authentication

Networked computer

- Physical security
- Process protection
- Data protection
- User authentication
- Communication protection

Human Factors Lead to Insecurity

System Users

- Security features are not used correctly, e.g., misconfiguration.
- Users like convenience and may try to disable some security configurations that are not inconvenient

System Developers

- Security features are not designed correctly; security components are not implemented correctly
- Developers are humans, and humans can make mistakes.

External Parties

- Individual's trust can be manipulated for profit, e.g., social engineering