CYBER THREATS TO THE FINANCIAL SERVICES AND INSURANCE INDUSTRIES

ORGANIZATIONS IN THE FINANCIAL SERVICES AND INSURANCE SECTORS FACE CYBER THREATS FROM THE FOLLOWING ACTORS:

- Enterprise – like cybercriminals seeking financial account data or other data they can monetize, and trying to make live fraudulent transfers
- Hacktivists engaging in disruptive activities and efforts to embarrass the victim as a means to protest a policy or action and gain publicity for their cause
- Advanced persistent threat (APT)[1] groups aiming to collect intelligence capable of providing their sponsoring government with insight into the targeted company's operations, or information on potentially - sensitive customers

CASE STUDY: CYBERCRIMINALS COMPROMISE BANK'S CARD MANAGEMENT SYSTEM

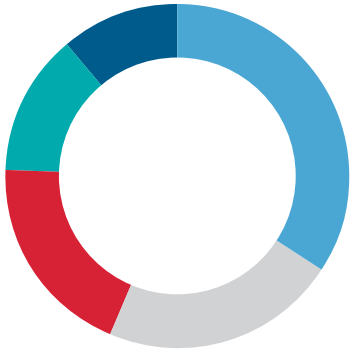
We investigated a compromise at a bank that had discovered threat actors using fraudulent debit cards to make unauthorized ATM withdrawals in Eastern Europe. The threat actors had compromised the bank's card management system and software, and then stole, or attempted to steal, $150,000 from customer accounts. They initially compromised the bank's network after an employee visited a web site hosting a browser-based exploit that installed a backdoor on the employee's system. Using the employee's legitimate credentials, the threat actors gained access to the card management system and increased the recorded balances and withdrawal limits for several customers' accounts. They then changed the accounts' PINs, which allowed them to take the maximum amount from these accounts using seemingly legitimate credentials.

WE HAVE OBSERVED AT LEAST 15 ADVANCED THREAT GROUPS COMPROMISE ORGANIZATIONS IN THESE SUBSECTORS:

- Asset Management
- Automated Teller Machine (ATM) Operators
- ATM & Other Self-Service Terminal Manufacturing
- Banks & Credit Unions
- Credit Reporting Services
- Electronic Payment Systems
- Financial Planners & Investment Advisers
- Financial Services, Legal & Government Software
- Financial Transaction Processing
- Institutional Securities Brokerages
- Insurance Agencies & Brokerages
- Investment Firms
- Mortgage Banks
- Property/Casualty Insurance Carriers
- Venture Capital

1 Advanced Persistent Threat (APT) actors are assessed to take direction from a nation state to steal information or conduct network attacks, tenaciously pursue their objectives, and are capable of using a range of tools and tactics.

FireEye



TOP 5
MALWARE DETECTIONS

- **34%** WITCHCOVEN
- **22%** XtremeRAT
- **19%** Gh0stRAT
- **13%** CANNONFODDER
- **11%** Hussarini

TOP 5
CRIMEWARE DETECTIONS

- **47%** Upatre
- **18%** Ruskill
- **14%** Zeus (aka Zbot)
- **10%** Jenxcus
- **10%** Fareit

THREAT HORIZON & INDUSTRY OUTLOOK

Companies in the financial services and insurance industries will almost certainly remain a high profile target for cybercriminals, hacktivists, and APT groups. The following factors may influence future targeting in these sectors:

- Consumer services and mobile applications that offer personal financial management are likely to be a target for credential theft, as cybercriminals may consider such third party apps a target of opportunity, especially if they have a large store of credentials and relatively lower defenses compared to major retail banks.
- Existing commodity infections such as bots can provide threat actors with a way to gain access to the networks of high value victims in the financial services sector. We've previously seen cybercriminals leverage Citadel infections to install custom malware, move laterally in the network, and steal financial data.
- Any perceived involvement in controversies may also result in increased threat activity from hacktivists seeking to call attention to the issues and embarrass organizations that they view as responsible. However, hacktivists may also target the sector to protest an unrelated issue, with the view that the sector is highly visible and therefore provides the best platform through which to gain attention for their actions.
- Increased tensions or conflict between countries may prompt associated APT groups to react by conducting disruptive or destructive attacks aimed at providing their government with leverage over its adversary.

DATA STOLEN FROM FINANCIAL SERVICES & INSURANCE CLIENTS

- Benefits Records
- Business & Strategic Plans & Goals
- Employee Handbook & Policies
- Employee Resumes
- Employee Training Materials
- Event Related Materials
- Finance Documents
- Invoices
- Organizational Charts
- Pricing Data
- Products Use Instructions & Training Materials
- Recurring Reports
- Software Descriptions & Configurations
- Statements of Work

TOP MALWARE DETECTIONS

WITCHCOVEN	is a profiling script design to learn information about the operating systems, browsers, and applications of site visitors. We suspect APT actors are using these scripts to engage in footprinting, an information gathering technique used to profile computer systems and the organizations to which they belong.
XtremeRAT	is a publicly available remote access tool (RAT) capable of uploading and downloading files, interacting with the Windows registry, manipulating processes and services, and capturing data such as audio and video.
Gh0stRAT	is a RAT derived from publicly available source code. It can perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.
CANNONFODDER	is a credential stealer that drops a malicious Microsoft Word file and steals credentials from Internet Explorer, Mozilla Firefox and Google Chrome. It also installs a key logger, and operates in interactive mode to allow the attacker to further investigate the target system, and exfiltrate data.
Hussarini	is a fully featured backdoor that is used by multiple suspected, China-based, APT groups

TOP CRIMEWARE DETECTIONS

Upatre	is a Trojan downloader that often arrives via a spam email, drive-by download or exploit, Upatre will download one or more additional types of malware onto an infected system. Upatre has been observed distributing a wide variety of malware including, but not limited to, Zbot, Dyre, Rovnix, CryptoLocker, and Necurs.
Ruskill	is a commercial crimeware kit sold on cyber crime forums and can be used to control compromised endpoints organized in a botnet to conduct distributed denial of service (DDoS) attacks.
Zeus	(aka Zbot) is a family of Trojans primarily designed to engage in banking credential theft. It is capable of a wide variety of functions, including the ability to remotely execute shell commands.
Jenxcus	(aka njw0rm, njworm) is an evolution of the popular tool njRAT that can spread across removable drives and steal credentials. It is often delivered via malicious links in email and drive-by downloads on compromised sites.
Fareit	is an information stealing Trojan that can also force infected systems to engage in DDoS attacks and download additional types of malware.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye