CYBER THREATS TO THE HEALTHCARE AND HEALTH INSURANCE INDUSTRY

THE HEALTHCARE AND PHARMACEUTICAL INDUSTRY FACES CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced Persistent Threat (APT)[1] groups aiming to steal intellectual property and proprietary information capable of benefitting domestic industries and assisting the government in achieving its strategic healthcare goals
- APT groups in pursuit of patients' personally identifiable information, potentially to facilitate further targeting and assist their sponsoring government in intelligence collection
- Enterprise-like cybercriminal groups working to turn personally identifiable information and financial data into profit
- Hacktivists seeking to disrupt access to websites and/or deface organization's webpages to publicize a political or ideological stance or protest an organization's activity.

CASE STUDY: APT GROUP COMPROMISES MEDICAL INSURANCE COMPANY

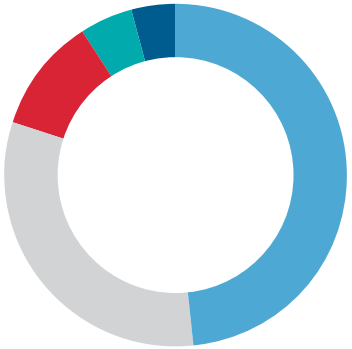
As part of an investigation at a health insurer, we witnessed threat actors use a combination of spear phishing directed against dozens of the insurer's users to gain access to systems within the organization's network. The messages offered disguised malicious links to the users, as is common with many phishing messages. The links downloaded malicious backdoors that allowed the actors to harvest passwords in order to move laterally across the insurer's network domain. Eventually, the threat actors accessed and retrieved the personally identifiable information (PII) of a large number of its insured subscribers.

WE HAVE OBSERVED AT LEAST 13 ADVANCED THREAT GROUPS COMPROMISE COMPANIES IN THESE SUBSECTORS

- Biopharmaceuticals & Biotherapeutics Manufacturing
- Electromedical, Electrotherapeutic & X-Ray Apparatus Manufacturing
- Healthcare Management Software
- Healthcare Product Manufacturing
- Hospitals
- Medical Equipment & Supplies Manufacturing
- Pharmaceutical Manufacturing
- Health Insurance

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 FAMILIES

- **49%** WITCHCOVEN
- **32%** XtremeRAT
- **11%** ChinaChopper
- **5%** Gh0stRAT
- **4%** Pingbed

TOP 5
CRIMEWARE FAMILIES

- **33%** Conficker
- **21%** POWESSERE
- **17%** Jenxcus (aka njw0rm)
- **15%** HOUDINI (aka H-Worm)
- **13%** Upatre

THREAT HORIZON & INDUSTRY OUTLOOK

The healthcare and pharmaceutical industry will likely continue to face cyber threats due to its potentially valuable access to research and manufacturing data and troves of personally identifiable information and other sensitive data. We anticipate that the following factors will also influence threat activity towards the sector:

- The move towards digitization of medical health records and the increasing connectivity of medical devices will likely increase organizations' attack surfaces, making the industry more vulnerable to threat actors.
- Technological and medical innovations will likely spur threat activity from APT groups seeking to obtain related intellectual property and proprietary information to benefit associated state-owned or indigenous companies.
- Countries' efforts to improve their own healthcare services and products to reduce health costs would likely lead to increased targeting from associated APT groups seeking to obtain intelligence that could assist in their efforts.
- Any perceived involvement in controversies, such as pertaining to medical care, drug-testing processes, perceived ethics violations, or other issues, may prompt targeting from hacktivists seeking to call attention to the issues and embarrass organizations that they view as responsible.

DATA STOLEN FROM HEALTHCARE AND PHARMACEUTICAL ENTITIES

- Patient Information
- Business & Strategic Plans & Goals
- Human Resources Documents
- Legal Documents
- Network Infrastructure Documents

TOP 5 MALWARE

FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the healthcare and health insurance industry:

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.
ChinaChopper	is a small webshell that provides threat actors unauthorized access to an information system using a simple password for authentication and is capable of executing Microsoft .NET code within HTTP POST commands.
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.
PingBed	is a Trojan capable of downloading and executing a file, killing processes, and executing command lines and return results, among other tasks. We observed some of the samples from this family to social engineer the user into opening zip or rar interface where file names and icons indicate readable files.

TOP 5 CRIMEWARE

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the healthcare and health insurance industry:

CONFICKER	is a worm that spreads by exploiting a vulnerability on removable drives and network shares. It is capable of disabling security settings, deleting backup files, and resetting system restore points.
Powessere	(aka Poweliks) is "file-less" malware that exists entirely within the Windows registry. Often arriving on a system via phishing emails with Canada Post or USPS themes and Microsoft Office exploits, Powessere does not create files on an infected system but rather exists entirely within the Windows registry. It executes in stages, starting with an encoded JavaScript stored in an auto-run key. Once fully installed, a memory-resident dynamic-link library collects basis system information and may download additional malware.
Jenxcus	(aka njw0rm, njworm) is an evolution of the popular tool njRAT that includes additional features such as the ability to spread across removable drives and credential theft. Often delivered via malicious links in email and drive-by downloads on compromised sites, Jenxcus provides the usual functionality of a RAT with additional features such as the ability to spread to new systems through removable drives, such as USB drives, and credential theft.
HOUDINI	(aka H-Worm) is a VBS-based RAT that uses HTTP to communicate information about the compromised system, such as operating system and host and user name. In some cases the VBS file is packed with multiple layers of obfuscation, including custom Base64 encodings. It supports several commands, such as command line execution, downloading and executing programs, and data theft.
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.

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

www.FireEye.com

FireEye