CYBER THREATS TO THE HIGH TECH AND IT INDUSTRY

ORGANIZATIONS IN THE HIGH TECH AND INFORMATION TECHNOLOGY (IT) INDUSTRY FACE CYBER THREATS FROM THE FOLLOWING ACTORS:

- Advanced persistent threat (APT)[1] groups seeking to steal economic and technical information to support the development of domestic companies through reducing research and development costs, or otherwise providing a competitive edge.
- Hacktivists and other threat actors with disruptive motivations may target Internet service providers to gain attention for their cause.
- Enterprise-like cybercriminals aiming to steal customers' account and financial data (e.g. credentials, payment information) or personal identifiable information that they can use for monetary gain.

CASE STUDY: TWO APT GROUPS COMPROMISE HIGH TECH COMPANY

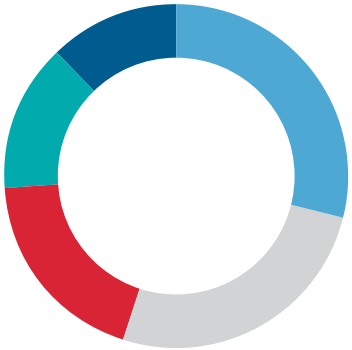
We investigated a case in which two China-based APT groups compromised a high-tech producer of consumer and military grade technology. The groups were active in the company's environment more than three years. One or both groups worked on a nearly daily basis, performing reconnaissance and stealing data; stole proprietary files related to a consumer product that at the time was non-public R&D but has since has been on sale to consumers; and also may have specifically searched for information on a certain military-grade product that the company produces. The groups maneuvered throughout the network to important users and systems, deployed multiple tools that were capable of stealing information, recorded the screen and keystrokes, and stole emails. In total, the two groups stole over 100GB of data.

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.

WE HAVE OBSERVED AT LEAST 20 ADVANCED THREAT GROUPS COMPROMISE COMPANIES IN THESE SUBSECTORS:

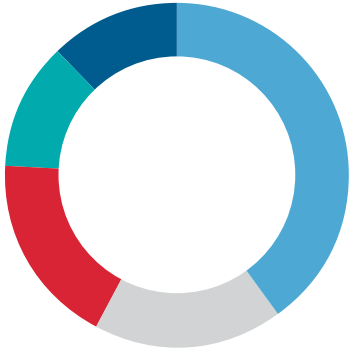
- Computer Software
- Information Technology Services
- Control, Electromedical, Measuring & Navigational Instruments Manufacturing
- Consumer Electronics & Personal Computer Manufacturing
- Electronics Component Manufacturing & Wholesalers
- Logic Device Manufacturing
- Network Access & Communications Device Manufacturing
- Networking & Connectivity Software
- Routing & Switching Equipment Manufacturing
- Search, Detection, Navigation & Guidance System Manufacturing
- Security Software
- Semiconductor Equipment Manufacturing
- Storage & Systems Management Software

FireEye



TOP 5
MALWARE DETECTIONS

- **29%** Gh0stRAT
- **26%** TAIDOOR
- **19%** PoisonIvy
- **14%** SUNBLADE
- **12%** SOGU (aka Kaba)



TOP 5
CRIMEWARE DETECTIONS

- **40%** Conficker
- **18%** Sality
- **18%** Upatre
- **12%** Obitel
- **12%** Andromeda

THREAT HORIZON & INDUSTRY OUTLOOK

The high tech and IT sector's relevance to economic, intelligence, and security concerns likely make it a target for a variety of threat actors. We expect that the following factors may contribute to threat activity facing the sector:

- The development of new technologies will likely spur threat activity against the industry as threat groups will most likely target related intellectual property and proprietary information capable of providing companies in their own domestic industry with a rapid competitive advantage.
- Partnerships with government or military entities would likely also place companies at risk, as foreign state-sponsored threat actors would probably target such companies to gather intelligence on network security to enable future data theft, gain access to research and development, better understand military technology programs, or seek to disrupt an adversary's capabilities in the event of conflict.
- Access to customers' account and payment information or financial data, or other sensitive data such as personally identifiable information could also lead to increased threat activity towards the sector as financially motivated cybercriminals seek to obtain information that they can monetize for their own profit.
- Any perceived involvement in controversies, such as labor, environmental, surveillance, or other issues, may also result in increased threat activity from hacktivists seeking to call attention to the issues and embarrass organizations that they view as responsible.

DATA STOLEN FROM HIGH TECH AND IT SECTOR CLIENTS

- Blueprints
- Proprietary Product & Service Information
- Testing Results & Reports
- Production Processes
- Hardware & Software Descriptions & Configurations
- Security & Risk Management Documents
- Diagrams and Instruction Manuals
- Marketing Strategies & Plans

TOP MALWARE DETECTIONS

FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the high tech and IT industry:

Gh0stRAT	is a remote access tool (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.
TAIDOOR	is a backdoor capable of file transfers and command execution. It communicates over HTTP, and its communications are RC4 encrypted using the victim system's MAC address string as the key.
PoisonIvy	is a publicly available RAT that provides comprehensive remote access capabilities on a compromised system. Its variants are configured, built, and controlled using a graphical management interface available online. It can be configured to produce shellcode, which can be packaged into an executable or combined with an existing executable to hide its presence. It is typically configured to inject multiple shellcode stubs into the explorer.exe process.
SUNBLADE	is a backdoor capable of remote code execution and credential stealing. There are two variants; one variant has anti-sandboxing and anti-virtualization capabilities. This backdoor is primarily delivered in a self-extracting RAR or ZIP file, which may also include a decoy document.
SOGU	(aka Kaba, PlugX), a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the command and control (C2) server with graphical access to the desktop.

TOP CRIMEWARE DETECTIONS

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the high tech and IT 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.
Sality	is a file-infecting trojan that can prevent anti-virus software from functioning, send spam, download additional malicious software, and engage in information 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.
Obitel	is a Trojan downloader that communicates with a hard-coded list of command and control domains in order to receive instructions and download additional malicious executables.
Andromeda	(aka Gamarue) is a multipurpose Trojan that can be used as a keylogger, form grabber, or a dropper for other malicious software.

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

www.FireEye.com

FireEye