CYBER THREATS TO THE AEROSPACE AND DEFENSE INDUSTRIES

THE AEROSPACE AND DEFENSE SECTORS FACE CYBER THREATS FROM ADVANCED PERSISTENT THREAT (APT)[1] GROUPS WORKING IN ASSOCIATION WITH A NATION STATE TO PURSUE THE FOLLOWING OBJECTIVES:

- Steal intellectual property to advance domestic aerospace and defense capabilities, develop countermeasures, and produce technologies for sale on the global arms market
- Collect intelligence with which to monitor, and possibly infiltrate and subvert other nations' defense systems and capabilities

CASE STUDY: APT GROUPS COMPROMISE AEROSPACE AND DEFENSE COMPANIES

FireEye has performed threat assessments at many aerospace and defense firms. China-based threat groups likely targeted these companies to develop a competitive advantage for their indigenous defense and aerospace companies or to support the Chinese military's modernization.

A China-based threat group compromised at least seven systems in the environment of a defense manufacturer. The threat group stole documents on communications standards and initially gained access to the network through spear phishing emails. The employees' email addresses were included in public documents, and the threat actors likely used publicly-available sources to perform pre-attack reconnaissance.

Another China-based threat group compromised more than 300 systems at a aerospace company for several years. During the data breach, we found that the group was focused on acquiring sensitive data. The threat group performed targeted system reconnaissance in order to identify specific directories that were most likely to yield this information.

WE HAVE OBSERVED AT LEAST 24 ADVANCED THREAT GROUPS COMPROMISE ORGANIZATIONS IN THESE SUBSECTORS:

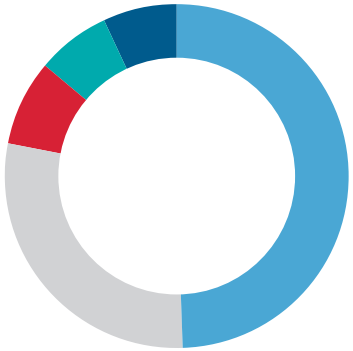
- Aerospace & Defense Parts Wholesalers
- Aerospace Products & Parts Manufacturing
- Aircraft Engine & Parts Manufacturing
- Guided Missile & Space Vehicle Manufacturing
- Industrial & Military Computer System Manufacturing

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

- **47%** Gh0stRAT
- **21%** PcClient
- **13%** ZXShell (aka Viper)
- **9%** NS01 (aka Mutter)
- **9%** WITCHCOVEN



TOP 5
CRIMEWARE FAMILIES

- **50%** Upatre
- **29%** Comame
- **8%** HOUDINI (aka H-Worm)
- **7%** Andromeda
- **7%** SERVSTART (aka Nitol)

THREAT HORIZON & INDUSTRY OUTLOOK

We expect that APT groups will continue targeting the aerospace and defense sectors in search of information that could provide their sponsoring governments with military and economic advantages. The following factors may influence future threat activity towards these sectors:

- New technologies such as unmanned aerial vehicles, directed energy, or hypersonic weapons, can lead to increased targeting as nation-states seek to keep pace with modern defense advancements.
- Threat actors may target defense technologies to counter an adversary's capabilities, or create disruptions on the battlefield; a relatively easy way to accomplish this is to identify critical technologies and seek out vulnerabilities in these platforms.
- The growth of the global arms and defense trade likely motivates nations to use cyber espionage to steal intellectual property to reduce their own research and development costs and produce and sell new products at lower prices, giving themselves a competitive advantage in this market space.
- Third party partners in the aerospace and defense supply chain could face increased targeting from threat actors seeking to target third parties and supply chain companies to use these victims as a vector to access other defense contractors' networks.

ABOUT FIREEYE THREAT INTELLIGENCE

FireEye Threat Intelligence draws on our proprietary access to intel data and analytics to equip security teams with the context required to help effectively identify, block and respond to advanced threat actors. FireEye has been curating intelligence on malware and advanced threat groups for over a decade, responding to attacker behavior across dozens of industries and sub-sectors – granting unparalleled institutional knowledge about the tactics used by advanced threat actors.

DATA STOLEN FROM AEROSPACE & DEFENSE ORGANIZATIONS

- Budget Information
- Business Communications
- Equipment Maintenance Records & Specifications
- Organizational Charts & Company Directories
- Personally Identifiable Information
- Product Designs/Blueprints
- Production Processes
- Proprietary Product or Service Information
- Research Reports
- Safety Procedures
- System Log Files
- Testing Results & Reports

TOP 5 MALWARE FAMILIES

FireEye most frequently detected threat actors using the following targeted malware families to compromise organizations in the aerospace and defense sector:

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.
PcClient	is a backdoor that provides an attacker the ability to execute commands via a command and control infrastructure and also gather sensitive data, including keystrokes, and log these to a local file. Typically, the backdoor is has an associated rootkit, making it harder to detect and remove, once compromised.
ZXSHHELL	(aka VIPER) is a backdoor that can be downloaded from the Internet, particularly Chinese hacker websites. The backdoor has features including launching port scans, running a keylogger, capturing screen shots, setting up an HTTP or SOCKS proxy, launching a reverse command shell, causing SYN floods, and transferring/deleting/running files. The publicly available version of the tool provides a graphical user interface that the attacker can use to interact with victim backdoors.
NS01	(aka Mutter) is a malware backdoor that may delivered via a malicious email attachment. It is proxy aware and may be capable of executing a shell command, uploading a file to the victim, and downloading files from the victim.
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.

TOP 5 CRIMEWARE FAMILIES

FireEye's sinkhole and dynamically shared threat data indicate that the following crimeware variants were the most commonly detected in the aerospace and defense sectors:

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 and has been observed distributing a wide variety of malware including, but not limited to, Zbot, Dyre, Rovnix, CryptoLocker, and Necurs.
Comame	is a Trojan capable of granting remote access to a computer. It also provides the capability to log keystrokes, download additional malware, capture system information and file listings, and manipulate the web browser for the purpose of click fraud. This Trojan may also establish persistence by modifying or creating a registry entry.
HOUDINI	(aka H-Worm) is a VBS-based RAT that communicates using HTTP. This communication typically includes information about the compromised system in the User-Agent field of the HTTP header, including but not limited to the system's host name, operating system, and user name. In some cases the VBS file is packed with multiple layers of obfuscation, including custom Base64 encodings. This backdoor supports several commands that provide it with traditional backdoor capabilities, such as command line execution, downloading and executing programs, and stealing data.
ANDROMEDA	(aka Gamarue) is a multipurpose Trojan that can be used as a keylogger, form grabber, or a dropper for other malicious software.
SERVSTART	(aka Nitol) is a Trojan that installs as either a binary executable or a dynamic link library and registers itself as a service. That service enables a remote user to connect to a remote server, download and run or install other malicious files, stop or restart the system, and perform distributed denial of service activities. The malware is capable of communication via TCP or UDP connections and it installs itself with a mutex to ensure a single copy of the software is installed. It is also capable of updating or uninstalling itself from a system.

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

www.FireEye.com

FireEye