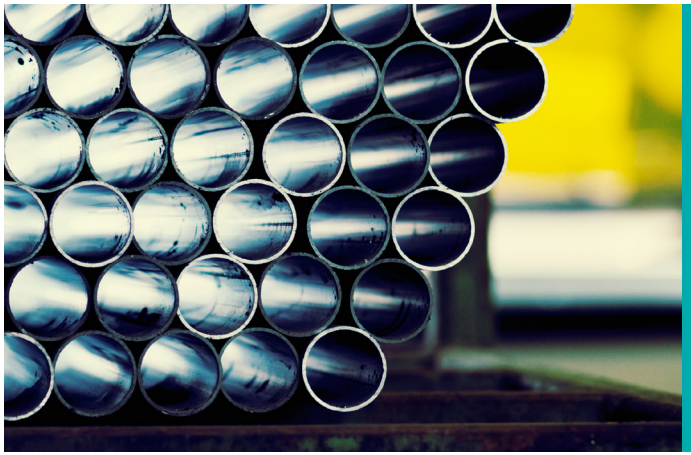

CYBER THREATS TO THE CONSTRUCTION AND ENGINEERING INDUSTRIES

ORGANIZATIONS IN THE CONSTRUCTION AND ENGINEERING INDUSTRIES FACE CYBER THREATS FROM ADVANCED PERSISTENT THREAT (APT)[1] GROUPS PURSUING THE FOLLOWING OBJECTIVES:

- Attempting to steal intellectual property pertaining to technical innovations, expertise, and processes, which help develop both state-owned firms and their indigenous construction and engineering industry.
- Accessing data on foreign firms engaged in high profile projects such as government, infrastructure, or large-scale urbanization developments to provide their sponsoring government with insight it might use to facilitate its own domestic projects.
- Seeking to monitor foreign competition to either allow associated state-owned firms to outbid, and potentially outperform their competition, and permit a sponsoring state considering working with a foreign company to have an advantage in negotiations and secure the best possible price.

CASE STUDY: THREAT ACTORS STEAL DATA FROM COMPANY MANUFACTURING INDUSTRIAL ENERGY EQUIPMENT

We previously investigated a compromise at a company that developed industrial infrastructure for the energy sector, and found that threat actors had compromised an Internet-facing webserver that was configured with default credentials. The threat actors installed webshells that provided them with remote access to the company's system. After harvesting domain account credentials and network information, the threat actors

WE HAVE OBSERVED AT LEAST 25 ADVANCED THREAT GROUPS COMPROMISE ORGANIZATIONS IN THESE SUBSECTORS:

- Architectural & Engineering Services
- Architectural & Structural Metals Manufacturing
- Commercial Equipment Repair & Maintenance
- Commercial & Heavy Construction Contractors
- Construction Machinery Manufacturing
- Electronic Equipment Repair Services
- Electronic Inspection & Monitoring Instruments Manufacturing
- Engineering, Scientific & CAD/CAM Software
- Engineering Services
- Erosion Control Services
- Fabricated Metal Product Manufacturing
- Industrial Control Products Manufacturing
- Machinery Manufacturing
- Metal Valve & Pipe Fitting Manufacturing
- Steel Production
- Turbine 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 DETECTIONS

- **52%** LEOUNCIA
- **20%** LV (aka NJRAT)
- **13%** Gh0stRAT
- **11%** 9002 (aka HOMEUNIX)
- **4%** SpyNet

TOP 5
CRIMEWARE DETECTIONS

- **40%** POWESSERE
- **24%** Kovter
- **16%** Fareit
- **12%** Perlbot
- **8%** CryptoWall

moved laterally to the corporate environment, where they began to generate encrypted RAR files, which they then began to remove from the network. The threat actors continued to access and remove data from the environment the company remediated two months later.

THREAT HORIZON & INDUSTRY OUTLOOK

The construction and engineering industry's contributions across multiple industries, such as manufacturing, energy, transportation, aerospace, and defense, will likely continue to make the sector a high profile target for state-sponsored threat actors engaged in cyber espionage. We expect that increasing urbanization and infrastructure investment in the developing world will also contribute to greater targeting towards these industries, as sponsoring governments seek to obtain information that would facilitate their efforts and assist in cutting costs. We frequently observe state-sponsored threat actors steal victim companies' intellectual property and business intelligence that could provide their indigenous companies with a future competitive advantage, such as using or marketing breakthrough materials to build more efficiently.

DATA STOLEN FROM CONSTRUCTION & ENGINEERING FIRMS

- Business & financial documents
- Government briefings, reports, & records
- Human resources documents
- Internal communications
- Legal documents
- Network infrastructure documents
- Product designs, blueprints, instructions, & training materials
- Testing results & reports

TOP MALWARE DETECTIONS

FireEye most frequently detected threat actors using the following targeted malware families to compromise construction and engineering organizations:

LEOUNCIA	is a backdoor that is capable of uploading and downloading files, launching executables, running arbitrary shell commands, listing and killing processes, obtaining directory listings, and communicating with a command and control (C2) server using HTTP requests.
LV	(aka NJRAT) is a publicly available remote access tool (RAT) capable of keystroke logging, credential harvesting, reverse shell access, file uploads and downloads, and file and registry modifications. It also offers threat actors a "builder" feature to create new variants.
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.
9002	(aka HOMEUNIX) is primarily a generic launcher for downloaded plug-ins that are stored in a memory buffer, before the backdoor manually loads and links them. The plug- ins therefore never have to touch disk. This backdoor may also store and save plug-ins, which will then run after the system is rebooted without the threat actors having to send them again to the victim system.
SpyNet	is a publicly available RAT that allows threat actors to interact with a compromised system via a remote shell, upload and download files, interact with the registry, and start and stop processes and services. It can capture images of the desktop, record from webcam and audio inputs, extract saved passwords, and turn a compromised system into a proxy server. There is also keylogging functionality, as well as anti-debugging/virtual machine defensive mechanisms.

TOP CRIMEWARE DETECTIONS

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

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 (DLL) collects basis system information and may download additional malware.
Kovter	is a form of ransomware. Upon taking control of an infected system, it checks the user's browser history against a list of known pornographic websites and if a match is found it displays the result in a dialog box threatening that the computer has been seized by a law enforcement agency due to suspicion of illegal activity. Kovter demands a payment to unlock the system.
Fareit	(aka Pony Loader, InfoStealer) is an information stealing Trojan that can also force infected systems to engage in distributed denial of service (DDoS) attacks and download additional types of malware.
Perlbot	is malware, written in Perl, targeting web servers which might run vulnerable Content Management Systems or components like PHP. If it finds a vulnerable system, it will try and run arbitrary code via command line options within the HTTP query string, providing the bot with the ability to download and execute further code. Typically, these compromises are associated with Bitcoin mining, but can potentially also expose servers to remote control as well as exfiltration of sensitive files.
Cyptowall	(aka Crowti) is ransomware that encrypts files on victim's endpoint and uses the onion router (TOR) for C2 communication.

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

www.FireEye.com

FireEye