BLOG

Gangnam Industrial Style: APT Campaign Targets Korean Industrial Companies

POSTED ON

December 17, 2019

AUTHOR

David Atch, Maayan Shaul, Gil Regev, Ori Perez, Phil Neray

SHARE

Section 52, CyberX's threat intelligence team, has uncovered an ongoing industrial cyberespionage campaign targeting hundreds of manufacturing and other industrial firms primarily located in South Korea.

The campaign steals passwords and documents which could be used in a number of ways, including stealing trade secrets and intellectual property, performing cyber reconnaissance for future attacks, and compromising industrial control networks for ransomware attacks.

For example, the attackers could be stealing proprietary information about industrial equipment designs so they can ed, credentials can provide attackers with remote RDP access to IoT/ICS networks, while plant schematics help adversaries understand plant layouts in order to facilitate attacks. Design information can also be used by cyberattackers to identify vulnerabilities in industrial control systems.

The campaign uses spear phishing emails with industrial-themed attachments including:

- **An RFQ for designing a power plant in the Czech Republic**, which appears to have been sent by an employee of a Siemens subsidiary that manufactures industrial machinery. This email includes a schematic of the power plant and a publicly-available technical white paper about the gasification of the plant, which is located in Vresova, Czech Republic.
- **An RFQ for designing a coal-fired power plant in Indonesia**, purporting to be from the engineering subsidiary of a major Japanese conglomerate. To increase its appearance of legitimacy, the email includes a publicly-available PDF of the company's corporate profile.
- **An email purporting to be from a buyer at a major European engineering company** that designs gas processing and production plants.

CyberX has identified more than 200 compromised systems from this campaign, including one belonging to a multi-billion dollar Korean conglomerate that manufactures critical infrastructure equipment such as heavy equipment for power transmission and distribution facilities, renewable energy, chemical plants, welding, and construction.

Examples of other South Korean victims include a:

- Steel manufacturer
- Chemical plant construction firm
- Pipe manufacturer
- Valve manufacturer

□ I consent to having this website store my submitted information so they can respond to my inquiry.

SUBMIT

The Section 52 team uses an automated threat extraction platform called Ganymede to identify malware and APT campaigns targeting industrial and critical infrastructure organizations.

Ganymede continuously ingests large amounts of data from a range of open and closed sources. It uses specialized machine learning algorithms to identify documents with IoT/ICS-specific content as well as any malicious attachments, and to monitor domains of industrial companies that might be targeted.

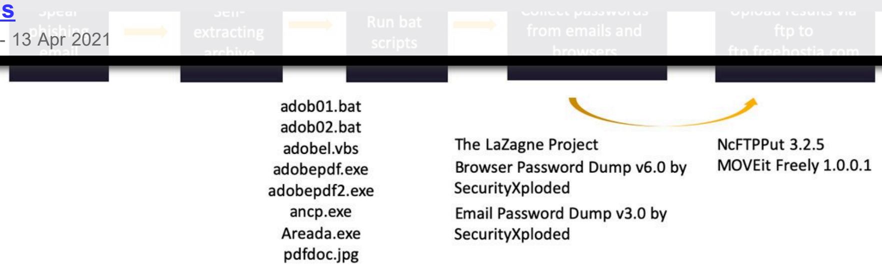
Section 52 is composed of world-class domain experts and data scientists who previously staffed a national military CERT defending against daily nation-state cyberattacks on critical infrastructure.

HOW THE MALWARE WORKS

The Gangnam Industrial Style campaign uses a new version of the Separ credential stealing malware, which was first identified by SonicWALL in 2013.

In this case, however, the malware is being used to specifically target industrial organizations.

Once installed, the malware steals browser and email credentials and searches for documents with a range of extensions, including Office documents and images. It exfiltrates all compromised information via FTP to a free web hosting service (freehostia.com).



The malware is hidden inside a zip file attached to the phishing emails. Once unzipped, the files often appear to be PDF files (with the PDF icon) but are actually malicious executables. The executables are a series of scripts that were compiled using the Quick Batch File Compiler.

As shown in the diagram above, the malware performs the following steps:

- Runs ipconfig to map all network adapters on the compromised system
- Disables Windows firewall
- Dumps browser passwords
- Dumps email passwords
- Collects files with specific extensions from user folders, mostly documents
- Uploads all the results to the ftp server ftp[.]freehostia[.]com

The malware incorporates the following tools, most of which are freely available on the internet:

- Browser Password Dump v6.0 by SecurityXploded
- Email Password Dump v3.0 by SecurityXploded
- NcFTPPut 3.2.5 – Free FTP client
- The LaZagne Project (password dumper from https://github.com/AlessandroZ/LaZagne)
- deltree (Folder delete from https://github.com/johnmbaughman/deltree)

HOW SEPAR MALWARE HAS EVOLVED

The Separ malware used in the Gangnam Industrial Style campaign has evolved from the Separ version described earlier this year in a Deep Instinct blog post.

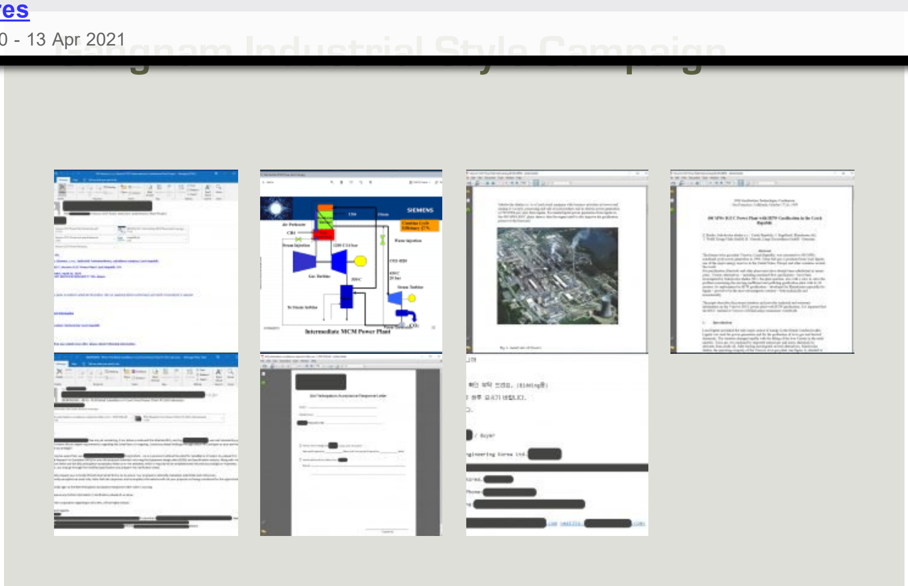
In particular, it collects files as well as passwords from compromised systems, whereas the previous version only collected passwords. In addition, the new version uses Autorun to persist after reboots.

The new version also uses certain components that were not used in the previous version including: The LaZagne Project , deltree, MOVEit Freely 1.0.0.1 – Secure FTP Client , and "Command Line Process Viewer/Killer/Suspender for Windows NT/2000/XP V2.03."

Distribution of Targets by Location and Industry

Our research indicates the Gangnam Industrial Style campaign is ongoing, because new stolen credentials are still being uploaded to the adversary's C2 server.

Over the past few months, Section 52 identified the following countries and industries as being targeted by the malware:



HOW TO PROTECT AGAINST THESE TYPES OF ATTACKS

Safeguarding your organization from these targeted industrial campaigns requires a multi-layered defense incorporating:

- Teaching employees to be wary of email attachments, especially zipped or compressed files purporting to contain details about “RFPs”.
- Email security to detect suspicious emails.
- Endpoint security to identify malware.
- Network segmentation to restrict the adversary’s ability to navigate from IT to OT networks.
- Secure remote access solutions with MFA to prevent unauthorized access using stolen credentials.
- IoT/ICS-specific network security monitoring to detect suspicious or unauthorized access to industrial control networks.
- Industrial threat intelligence to stay current about these types of attacks, while operationalizing this intelligence by integrating it with

SHARE THIS POST:

FROM THE BRIEFING ROOM

BLOG

A Leadership Perspective on Bridging the Gap Between IT & OT

BLOG

How to Translate “Safety” into “Security”

BLOG

How to Create Actionable IoT & ICS Security Dashboards for Management & Auditors

BLOG

BAD to the Bone — NIST, LOTL, and IoT/ICS Behavioral Anomaly Detection (BAD)

Privacy Policy Contact

Subscribe to the CyberX-Files for updates

SUBMIT