Alert (TA17-293A)

Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: October 20, 2017 | Last revised: October 23, 2018

Print | Email | Share

Systems Affected

- Business Enterprises
- Energy Sector
- Industrial Control Systems

Overview

This alert has been superseded by newer information. The alert is provided below for historical reference only. For the newest version, please visit TA18-074A.

This joint Technical Alert (TA) is the result of activities between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides information on recent tactics, techniques, and procedures (TTPs) and indicators of compromise associated with actors targeting the energy and other critical infrastructure sectors. DHS and FBI are collaborating on this TA to provide cyber network defenders with information regarding the identified intrusions to enable them to take prompt actions to protect their networks against these TTPs and cyber threats, and to mitigate the cybersecurity risks associated with these and other similar cyber intrusions.

DHS assesses the activity as a cyber-espionage intrusion campaign by threat actors who have compromised multiple business enterprises and have identified, by intended or inadvertent, high value assets within the critical energy sector. Based on malware products and observed TTPs, DHS and FBI assess that the campaign is still ongoing, and that the actors have been successful in their efforts to compromise the critical energy sector. The intent of this product is to raise awareness of detected activity and enable network defenders to identify and remove compromises in their networks.

For a downloadable copy of IOC and signature and associated files, see:

- TA17-293A_stix.zip (zip)
- TA17-293A_IOC_MAR.txt (txt)
- WITH_KEYWORD_LIST_MAPPING.pdf
- WITH_KEYWORD_LIST_MAPPING.stix.zip
- WITH_KEYWORD_LIST_MAPPING.stix.txt
- WITH_KEYWORD_LIST_MAPPING.xlsx
- WITH_KEYWORD_LIST_MAPPING.xml
- WITH_KEYWORD_LIST_MAPPING.zip
- WITH_KEYWORD_LIST_MAPPING.txt
- WITH_KEYWORD_LIST_MAPPING.csv
- WITH_KEYWORD_LIST_MAPPING.stix.txt
- WITH_KEYWORD_LIST_MAPPING.stix.zip

For a machine-readable version of the indicators for ingest or intrusion and for mapped incident response resources or technical assistance.

Description

Since at least May 2017, threat actors have been conducting cyber intrusions targeting the energy, water, aviation, nuclear, critical manufacturing sectors, and to a lesser extent, commercial facilities. This campaign has been ongoing for at least two years, and the actors have been successful in their efforts to compromise the critical energy sector. DHS and FBI have observed the actors using a variety of TTPs, including spear phishing, watering hole attacks, and exploitation of known software vulnerabilities to compromise their victims' networks. The actors have also been observed using stolen credentials.

DHS and FBI have observed the compromised personnel has identified detection tools and defensive measures to the actors, IP spoofs, kick, the Sniper Espionage, Remote Control, and Netbus Trojan malware, and have attempted to delete log files, encrypt files, and wipe hard drives in an effort to hinder the discovery of their activity.

The campaign compromises two distinct categories of victims: staging and intended targets. The initial victims are unsophisticated organizations such as trusted third-party business enterprises with less robust cyber security practices. The actors use these initial victims to gain access to the intended targets' networks, which have more robust cyber security practices and malware equipped to detect and remove intruders. The adversary adjusts their cyber attack tactics to compromise organizations' networks based on the identity of the intended target.

Including the initial victims, the actors have compromised organizations in the following sectors:

- business enterprises providing services to energy, water, and aviation
- open-source reconnaissance,
- business enterprises providing manufactured hardware or accessories,
- engineering firms,
- nuclear energy and power generation,
- industrial control system (ICS) infrastructure targeting, and
- critical manufacturing sectors.

Using Cyber Kill Chain TTPs, the actors have:

DHS Investigators Cyber Kill Chain models to analyze, discern and disclosure cyber activity. Phases of the model include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. This section will provide an overview of activity within the following phases:

Stage 1: Reconnaissance

The threat actors appear to have deliberately chosen the organizations they targeted, rather than pursuing them at targets of opportunity. Targeting targets held promising information on business partnerships, business processes, and information technology and industrial control system (ICS) vendors. Once the actors compromised their victims, DHS and FBI have observed the actors conducting open-source reconnaissance against victim enterprises to identify potential targets of interest and intended targets. "Trusted partners" refers to organizations that DHS observed the threat actors are leveraging as an ear interest, to learn about the compromised business partnerships, business processes, and information technology and industrial control system (ICS) vendors. The actors have also used open-source reconnaissance against victim enterprises.

Stage 2: Weaponization

Stage 3: Delivery

The threat actors are gaining a foothold, threat actors could attract business to storage logistics information Microsoft Office to access to remote a document from a remote server. Upon opening the document, the document requests the download of a template from a remote server. The PDF/RTF exploit was not observed and did not contain any active code. The document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

In a previous campaign, DHS and FBI identified the common theme used in these spear phishing emails, all emails referred to current events or personal content pertaining to the victim company, such as employment, publications, publications, publications, and business partnerships. Some of the emails contained a Microsoft Word attachment with a malicious macro. The emails were targeted to individuals that would have an interest in the topic and were crafted to appear as if they were sent from a known associate of the victim. The emails did not contain any malicious attachments or links.

Stage 4: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 5: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 6: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 7: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 8: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 9: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 10: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 11: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 12: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 13: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 14: Exploitation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Stage 15: Installation

Threat actors gained access and accessed TTPs to a successful intrusion to the phishing campaign should an engaging targets. Emails contained a Microsoft Office, demonstrating that the actors have an Intel, DHS, and FBI believe, with a moderate level of confidence that actors use Netbus Trojan and Netbus Trojan malware to gain access to victim networks. Once the victim has opened the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server. Upon opening the document, the document requests the download of a template from a remote server.

Impact

The impacts of this campaign may be affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors.

Solution

We recommend the campaign network and cyber defenders implement the following detection and prevention guidance to help defend against the actors.

Network and Host-Level Mitigation/Defense

- Implement a cyber security management information system (SIEM) of software, known names, file hashes, and TARG and Event Signature provided and the IPs. Use the network and host-level detection and defense measures provided in the attached files. Implement a cyber security management information system (SIEM) of software, known names, file hashes, and TARG and Event Signature provided and the IPs. Network defenders and system analysts should use the TARG and Event Signature provided in the associated TARG and Set to Implement Network Defenses.

Detections and Prevention Measures

- Users and administrators are alert to phishing attempts, watering holes, and drive, and remote access tools by comparing IP addresses and domain names listed in the provided IOCs with those in network logs.
- Implement a cyber security management information system (SIEM) of software, known names, file hashes, and TARG and Event Signature provided and the IPs.
  - anti-virus logs,
  - intrusion detection/prevention messages,
  - system and network IPS messages,
  - firewall logs,
  - workstation internal browsing history logs,
  - Microsoft Windows Event Logs, Sysmon, Open-based intrusion prevention system (HIPS) logs,
  - data loss prevention logs,
  - exchange server logs,
  - proxy server logs,
  - mail server logs,
  - domain controller logs,
  - AV logs,
  - DNS logs,
  - Windows Scheduler Service logs, and
  - Windows Task Manager logs.
- To detect the presence of tools used by actors, on external facing servers, computer IP addresses, filenames, and file hashes listed in the IOC packages with the following:
  - application logs,
  - system logs,
  - file systems,
  - Windows Management Instrument Prevention system logs,
  - Proxy logs,
  - Sysmon logs, and
  - Windows Scheduler Service logs.
- Implement a cyber security management information system (SIEM) of software, known names, file hashes, and TARG and Event Signature provided and the IPs.
- Network administrators should be on the lookout for and block, if possible, the following ports: 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376,