Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013

us-cert.cisa.gov/ncas/alerts/aa21-201a

Summary

This Advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

Note: CISA released technical information, including indicators of compromise (IOCs), provided in this advisory in 2012 to affected organizations and stakeholders.

This Joint Cybersecurity Advisory—coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI)—provides information on a spearphishing and intrusion campaign conducted by state-sponsored Chinese actors that occurred from December 2011 to 2013, targeting U.S. oil and natural gas (ONG) pipeline companies.

CISA and the FBI provided incident response and remediation support to a number of victims of this activity. Overall, the U.S. Government identified and tracked 23 U.S. natural gas pipeline operators targeted from 2011 to 2013 in this spearphishing and intrusion campaign. Of the known targeted entities, 13 were confirmed compromises, 3 were near misses, and 7 had an unknown depth of intrusion.

The U.S. Government has attributed this activity to Chinese state-sponsored actors. CISA and the FBI assess that these actors were specifically targeting U.S. pipeline infrastructure for the purpose of holding U.S. pipeline infrastructure at risk. Additionally, CISA and the FBI assess that this activity was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations.

This advisory provides information on this campaign, including tactics, techniques, and procedures (TTPs) and IOCs. The TTPs remain relevant to help network defenders protect against intrusions. The IOCs are provided for historical awareness.

CISA and the FBI urge owners and operators of Energy Sector and other critical infrastructure (CI) networks to adopt a heightened state of awareness and implement the recommendations listed in the Mitigations section of this advisory, which include implementing network segmentation between IT and industrial control system (ICS)/operational technology (OT) networks. These mitigations will improve a CI entity's defensive cyber posture and functional resilience by reducing the risk of compromise or severe operational degradation if the system is compromised by malicious cyber actors, including but not limited to actors associated with the campaign described in this advisory.

For more information on Chinese malicious cyber activity, see us-cert.cisa.gov/china.

Click here for a PDF version of this report.

Technical Details

In April 2012, CISA received reports about targeted attacks directed at multiple ONG pipeline sites; CISA (via a predecessor organization) and FBI provided incident response and remediation support to a number of victims from 2012 to 2013. CISA and FBI's analysis of the malware and threat actor techniques identified that this activity was related to a spearphishing campaign. The U.S. Government identified and tracked 23 U.S. natural gas pipeline operators targeted in this campaign. Of the 23 known targeted entities, 13 were confirmed compromises, 3 were near misses, and 7 had an unknown depth of intrusion.

Threat Actor Activity

The spearphishing activity appears to have started in late December 2011. From December 9, 2011, through at least February 29, 2012, ONG organizations received spearphishing emails [T1566.002] specifically targeting their employees. The emails were at constructed with a high level of sophistication to convince employees to view malicious files [T1204.002]. **Note:** see the appendix for a table of the MITRE ATT&CK tactics and techniques observed in this campaign.

In addition to spearphishing, CISA and the FBI were made aware of social engineering attempts by malicious actors believed to be associated with this campaign. The apparent goal was to gain sensitive information from asset owners [T1598]. One asset owner reported that individuals in their network engineering department, including managers, received multiple phone calls requesting information about their recent network security practices. Other employees in other departments were not targeted. The asset owner also reported that these calls began immediately after they had identified and removed the malicious intruder from their network and performed a system-wide credential reset. The caller identified himself as an employee of a large computer security firm performing a national survey about network cybersecurity practices. He inquired about the organization's policy and practices for firewall use and settings, types of software used to protect their network, and the use and type of intrusion detection and/or prevention systems. The caller was blocking his caller ID and when the targeted organization tried to return the call, they reached a number that was not in service.

During the investigation of these compromises, CISA and FBI personnel discovered that Chinese state-sponsored actors specifically collected [TA0009] and exfiltrated [TA0010] ICS-related information. The Chinese state-sponsored actors searched document repositories [T1213] for the following data types:

- Document searches: “SCAD*”
- Personnel lists
- Usernames/passwords
- Dial-up access information
- System manuals

Based on incident data, CISA and FBI assessed that Chinese state-sponsored actors also compromised various authorized remote access channels, including systems designed to transfer data and/or allow access between corporate and ICS networks. Though designed for legitimate business purposes, these systems have the potential to be manipulated by malicious cyber actors if unmitigated. With this access, the Chinese state-sponsored actors could have impersonated legitimate system operators to conduct unauthorized operations. According to the evidence obtained by CISA and FBI, the Chinese state-sponsored actors made no attempts to modify the pipeline operations of systems they accessed. **Note:** there was a significant number of cases where log data was not available, and the depth of intrusion and persistent impacts were unable to be determined; at least 8 of 23 cases (35 percent) identified in the campaign were assessed as having an unknown depth of intrusion due to the lack of log data.

CISA and FBI assess that during these intrusions, China was successful in accessing the supervisory control and data acquisition (SCADA) networks at several U.S. natural gas pipeline companies.

Chinese actors also gained information specific to dial-up access, including phone numbers, usernames, and passwords [T1120]. Dial-up modems continue to be prevalent in the Energy Sector, providing direct access into the ICS environment with little or no security and no monitoring, which makes them an optimal vector for hold-at-risk operations. The exfiltrated data provided the capabilities for the Chinese cyber actors to access ONG operational systems at a level where they could potentially conduct unauthorized operations.

Exfiltrated Information and Assessed Motives

The Chinese actors specifically targeted information that pertained to access of ICSs. Searches were made for terms involving “SCAD*,” and the actors exfiltrated documents, including personnel lists, usernames and passwords, dial-up access information, remote terminal unit (RTU) sites, and systems manuals. The Chinese actors also exfiltrated information pertaining to ICS permission groups and compromised jump points between corporate and ICS networks. The totality of this information would allow the actors to access ICS networks via multiple channels and would provide sufficient access to allow them to remotely perform unauthorized operations on the pipeline with physical consequences.

CISA and FBI assess that these intrusions were likely intended to gain strategic access to the ICS networks for future operations rather than for intellectual property theft. This assessment was based on the content of the data that was being exfiltrated and the TTPs used to gain that access. One victim organization set up a honeypot that contained decoy documents with content that appeared to be SCADA-related data and sensitive organizational information. According to this organization, the SCADA-related decoy content was exfiltrated within 15 minutes of the time it was made available in the honeypot. Other sensitive decoy information, including financial and business-related information, was ignored.

CISA and FBI assess that this activity was ultimately intended to help China develop cyberattack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations.

Indicators of Compromise

Table 1 lists indicators related to this spearphishing and intrusion campaign as of May 7, 2012, which are provided in this alert for historical completeness.

Table 1: IOCs from Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013

Type	Indicator	Filename
Malware	MD5:84873fae9cdecb84452fff9cca171004	ntshrui.dll
Malicious email content, including any attachments and/or message body	fpso.bigish[.]net	
Malware	MD5:e12ce62cf7de42581c2fe1d7f36d521c	ntshrui.dll

User agent string	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)	
User agent string	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	
Named pipe	ssnp	
Possible command and control (C2) domain	<xxx>.arrowservice[.]net Where xxx is the targeted company name abbreviation	
Malware	MD5:7361a1f33d48802d061605f34bf08fb0	spoolsvd.exe
Malware	5e6a033fa01739d9b517a468bd812162	AdobeUpdater.exe
Malware	e62afe2273986240746203f9d55496db	ins.exe
Malware	ed92d1242c0017668b93a72865b0876b	px.exe
Malware	6818a9aef22c0c2084293c82935e84fe	gh.exe
Malware	fcbbfadc992e265c351e54598a6f6dfb	fslist.exe
Malware	05476307f4beb3c0d9099270c504f055	u.exe
Malware	54db65a27472c9f3126df5bf91a773ea	slm.exe
Malware	a46a7045c0a3350c5a4c919fff2831a0	niu.exe
Malware	60456fe206a87f5422b214369af4260e	ccApp1.exe
Malware	d6eaadcbcf9ea9192db1bd5bb7462bf8	ntshrui.dll
Malware	52294de74a80beb1e579e5bca7c7248a	moonclient2.exe
Malware	e62afe2273986240746203f9d55496db	inn.exe
Malware	5e6a033fa01739d9b517a468bd812162	kkk.exe
Malware	4a8854363044e4d66bf34a0cd331d93d	inn.exe
Malware	124ad1778c65a83208dbefcec7706dc6	AcroRD32.exe
Malware	17199ddac616938f383a0339f416c890	iass.dll
Malicious email sender address	“(name of victim company official)@yahoo.com”	
Malicious email content, including any attachments and/or message body	“If not read this paper, pay attention.”	
Malicious email hyperlinked probable malware	The hyperlink indicated a “.zip” file and contained the words “quality specifications” in reference to a particular component or product unique to the victim U.S. corporation.	
Malicious email signature block	Contained the name, title, phone number, and corporate email address of an actual victim company official.	

Malicious attachment name		Project-seems-clear-for-takeoff.zip
Possible C2 domain	<xxx>.arrowservice[dot]net Where <xxx> may be the full name of the targeted company	
Possible C2 domain	<xxx>.federalres[.]org	
Possible C2 domain	<xxx>.businessconsults[.]net Where <xxx> may be the targeted company name abbreviation or full name	
Possible C2 domain	idahoanad[dot]org	
Possible C2 domain	energyreview.strangled[.]net	
Possible C2 domain	blackcake[.]net	
Possible C2 domain	infosupports[.]com	
Malware	7caf4dbf53ff1dcd5bd5be92462b2995	iTunesHelper.exe
Malware	99b58e416c5e8e0bcdcd39ba417a08ed	Solarworldsummary.exe
Malware	f0a00cfd891059b70af96b807e9f9ab8	smss.exe
Malware	ea1b46fab56e7f12c4c2e36cce63d593	AcroRD32.exe
Malicious email content, including any attachments and/or message body	3d28651bb2d16eeaa6a35099c886fbaa	Election_2012_Analysis.pdf
Possible C2 domain	balancefitstudio[.]com	
Possible C2 domain	res.federalres[.]org	
Possible C2 domain	18center[.]com	
Possible C2 domain	milk.crabdance[.]com	
Possible C2 domain	bargainblog[.com[.]au	
Possible C2 domain	etrace-it[.]com	
Possible C2 domain	picture.wintersline[.]com	
Possible C2 domain	wish.happyforever[.]com	
Possible C2 domain	mitchellsrus[.]com	
Possible C2 domain	un.linuxd[.]org	

Malicious email content, including any attachments and/or message body		How_Can_Steelmakers_Compete_for_Growth_in_the_Steel_Sector_in_2012.zip
Malicious email content, including any attachments and/or message body		(Company Name)_Summary.zip
Malicious email content, including any attachments and/or message body	f5369e59a1ddca9b97ede327e98d8ffe	Solarworldsummary.zip
Malicious email content, including any attachments and/or message body		(Company Name)_to_Sell_RNGMS_to_(Company Name).zip
Malicious email content, including any attachments and/or message body		Gift-Winter.zip
Malicious email content, including any attachments and/or message body		Happy_New_Year.zip
Malicious email content, including any attachments and/or message body		Debt_Crisis_Hits_US.zip

Malicious email content, including any attachments and/or message body	01-12-RATEALERT.zip
Malicious email content, including any attachments and/or message body	fni.itgamezone[.]net

Mitigations

CISA and the FBI urge Energy Sector and other CI owners and operators to apply the following mitigations to implement a layered, defense-in-depth cyber posture. By implementing a layered approach, administrators will enhance the defensive cyber posture of their OT/ICS networks, reducing the risk of compromise or severe operational degradation if their system is compromised by malicious cyber actors.

Harden the IT/corporate network to reduce the risk of initial compromise.

- **Update all software**, including operating systems, applications, and firmware, in a timely manner. Consider using a centralized patch management system.
- **Replace all end-of-life software and hardware** devices.
- **Restrict and manage remote access software**. Remote access tools are a common method for threat actors to gain initial access and persistence on target networks.
  - Manage and restrict users and groups who are permitted to access remote capabilities. Permissions should be limited to users that require the capability to complete their duties.
  - Require multi-factor authentication (MFA) for remote access.
  - Limit access to resources over networks, especially by restricting Remote Desktop Protocol (RDP). If RDP is operationally necessary, restrict the originating sources and require MFA.
- **Enable strong spam filters to prevent phishing emails** from reaching end users.
- **Implement unauthorized execution prevention by:**
  - Disabling macro scrips from Microsoft Office files transmitted via email.
  - Implementing application allowlisting, which only allows systems to execute programs known and permitted by security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular internet browsers.
- **Filter network traffic** to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL blocklists and/or allow lists.
- **Set antivirus/antimalware programs** to regularly scan IT network assets using up-to-date signatures.

Implement and ensure robust network segmentation between IT and ICS networks to limit the ability of cyber threat actors to move laterally to ICS networks if the IT network is compromised.

- **Implement a network topology for ICS that has multiple layers**, with the most critical communications occurring in the most secure and reliable layer. For more information refer to National Institute of Standard and Technology (NIST) Special Publication 800-82: Guide to ICS Security.
- **Use one-way communication diodes to prevent external access**, whenever possible.
- **Set up demilitarized zones (DMZs)** to create a physical and logical subnetwork that acts as an intermediary for connected security devices to avoid exposure.
- **Employ reliable network security protocols and services** where feasible.
- **Consider using virtual local area networks (VLANs)** for additional network segmentation, for example, by placing all printers in separate, dedicated VLANs and restricting users' direct printer access.

Implement perimeter security between network segments to limit the ability of cyber threat actors to move laterally.

- **Control traffic between network segments** by using firewalls, intrusion detection systems (IDSs), and filter routers and switches.
- **Implement network monitoring** at key chokepoints—including egress points to the internet, between network segments, core switch locations—and at key assets or services (e.g., remote access services).
- **Configure an IDS** to create alarms for any ICS traffic outside normal operations (after establishing a baseline of normal operations and network traffic).
- **Configure security incident and event monitoring (SIEM)** to monitor, analyze, and correlate event logs from across the ICS network to identify intrusion attempts.

Implement the following additional ICS environment best practices:

- **Update all software**. Use a risk-based assessment strategy to determine which ICS network and assets and zones should participate in the patch management program.
  Test all patches in off-line text environments before implementation.
- I**mplement application allowlisting on human machine interfaces.**
- **Harden field devices**, including tablets and smartphones.
- **Replace all end-of-life software and hardware devices.**
- **Disable unused ports and services on ICS devices** (after testing to ensure this will not affect ICS operation).
- **Restrict and manage remote access software**. Require MFA for remote access to ICS networks.
- **Configure encryption and security for ICS protocols.**
- **Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.**
- **Do not allow vendors to connect their devices to the ICS network**. Use of a compromised device could introduce malware.
- **Maintain an ICS asset inventory** of all hardware, software, and supporting infrastructure technologies.
- **Ensure robust physical security is in place** to prevent unauthorized personal from accessing controlled spaces that house ICS equipment.
- **Regularly test manual controls** so that critical functions can be kept running if ICS/OT networks need to be taken offline.
- **Manage the supply chain** by adjusting the ICS procurement process to weigh cybersecurity heavily as part of the scoring and evaluation methodology. Additionally, establish contractual agreements for all outsourced services that ensure proper incident handling and reporting, security of interconnections, and remote access specifications and processes.

Implement the following additional best practices:

- **Implement IP geo-blocking**, as appropriate.
- **Implement regular, frequent data backup procedures** on both the IT and ICS networks. Data backup procedures should address the following best practices:
  - Ensure backups are regularly tested.
  - Store backups separately, i.e., backups should be isolated from network connections that could enable spread of malware or lateral movement.
  - Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt.
  - Retain backup hardware to rebuild systems in the even rebuilding the primary system is not preferred.
- **Implement a user training program** to train employees to recognize spearphishing attempts, discourage users from visiting malicious websites or opening malicious attachments, and re-enforce appropriate user response to spearphishing emails.

APPENDIX: Tactics and Techniques

Table 2 provides a summary of the MITRE ATT&CK tactics and techniques observed in this campaign.

Table 2: Observed MITRE ATT&CK tactics and techniques

Tactic	Technique
Reconnaissance [TA0043]	Phishing for Information [T1598]
Initial Access [TA0001]	Phishing: Spearphishing Link [T1566.002]
Execution [TA0002]	User Execution: Malicious File [T1204.002]
Discovery [TA0007]	Peripheral Device Discovery [T1120]
Collection [TA0009]	Information from Document Repositories [T1213]
Exfiltration [TA0010]	

Revisions

Initial Version: July 20, 2021

July 20, 2021: Corrected "unknown depth of intrusion" in Technical Details from 8 to 7.

July 20, 2021: Removed "Office Viewer" recommendation since it's deprecated.

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.