Title: Threat Intelligence Analysis

Group/Name: Aimé Fraser

Indicators and Technical Details

Datetime	Identifier (IP, Domain, URL, Hostname)	MITRE Technique ID	Analyst Comment
No date given	Henry.case@goodcorp.local receives an email from solevisible@gmail.com	T1566.002 Spearfishing link 1589.002 Gather the Victim's Email Address	The email contained personalized job ads. Case states he did not click anything in the email.
	GoogleUpdateschecker.vbs appears as a scheduled task.	T1059.005 Command and Scripting Interpreter: Visual Basic and T1053 Scheduled Task	
	Jake.armitage@goodcorp.local receives several emails from solevisible@gmail.com	T0865 Spear phishing attachment	
	Jake.armitage@goodcorp.local receives several emails from solevisible@gmail.com with .rtf attachments.	T1027 Obfuscated Files or Information	Armitage states he opened one attachment, and it contains nonsensical text.
	Armitage's computer is unpatched Windows 7 due to Excel legacy dependencies required for his work. The in-house developers have been unable to migrate him to a more secure system.	T1137.001 Office Template Macros and T1137 Office Application Startup	For the Outlook methods, blocking macros may be ineffective as the Visual Basic engine used for these features is separate from the macro scripting engine. Microsoft has released patches to try to address each issue. Ensure the following patches are applied to the systems. KB3191938 blocks Outlook Visual Basic and displays a malicious code warning, KB4011091 disables custom forms by default, and KB4011162 removes the legacy Home Page feature.
	Heavy network traffic from several PCs to unusual sites: ngaaksa.ddns.net and ngaaksa.sytes.net noted over the weekend.	T1041 Exfiltration Over C2 Channel	APT33 is based in Iran, where the work week is from Saturday through Wednesday or Thursday.
	Two unrelated PCs main partitions were wiped.	T1485 Data Destruction	This is characteristic of APT33's tool known as Shamoon, which
	Username artifact recovered on a pc: Xman_1365_x		This threat actor's handle has been found in other files suspected to be from APT33 and seen in Iranian online forums for software engineering. Mandiant links this threat actor to the Nasr Institute purported to be Iran's cyber army.

	Another host has many instances of certutil executed	T1105 Ingress Tool Transfer	certutil can be used to download files from a given URL.[
	The same host with certutil also has a zip file in the USER directory POWER_GEN_2012.zip	T1560 Archive Collected Data	APT 33 is known to use zip files to exfiltrate data.

Executive Summary

Last weekend, Good-Energy had a data breach. GoodCorp's Incident Response team performed an initial analysis and recovered some forensic artifacts.

The incident began with phishing emails to two employees that opened two different vectors of compromise. One was via an .hta file that executed upon opening the email, creating a scheduled task on the infected computer. The other email contained several malicious text files; the employee opened one.

While the exact sequence of events is not yet known, so far, the IR team has uncovered the following:

- Emails to two employees from the same Gmail account solevisible[@]gmail.com
- Scheduled task GoogleUpdatesscheduluer.vbs created on one of the PC with the .hta email
- Notably heavy network traffic over the weekend to ngaaksa.[ddns.]net and ngaaksa.[site.]net.
- Two other computers with their main hard disk partitions wiped
- Username artifact Xman_1365_x recovered on one PC
- On yet another PC, multiple instances of certutil.exe running, and a newly created file POWER_GEN.zip

These indicators of compromise add up to a textbook case of the attack originating from APT33.

This state-sponsored Iranian group is known for:

- Using spearphishing emails from solevisible[@]gmail.com based on job opportunities
- Attaching malicious Microsoft Office files to spearphishing emails
- Working on Saturdays and Sundays (Iran's "weekend" is Thursday and Friday
- Using ngaaksa.[ddns.]net and ngaaksa.[site.]net as C2 sites
- Having a member with the username Xman_1365_x
- Using certutil.exe and .zip files to exfiltrate data
- Targeting businesses in the energy sector for espionage to further Iran's military, political, and economic interests.

This breach is potentially as big and as severe as they come. The attacker is in the network and has already wiped two machines and exfiltrated data from at least one. Good-Energy's response needs to be aggressive and immediate.

This report provides a list of responses against the indicators of compromise the IR team has collected and includes additional mitigations to address all of APT33's known techniques. These include controls to

prevent the execution of code by unauthorized users, means of preventing the delivery of malicious files in emails, creating rules to identify and block traffic, patching and updating machines, and ongoing and engaging training for all employees against phishing. Since APT33 is a known actor, the cybersecurity community has collected much information Good-Energy can use immediately to strengthen its defenses.

Risk Summary

APT33 is a state-sponsored actor connected with Iran's cyber warfare group. It's been around since 2013, and its work supports Iran's political, military, and economic goals. It works to gather intel on Iran's rivals (primarily Saudi Arabia, the US, and South Korea, among many others) and to gather useful information to enhance Iran's economy in the petrochemical, aerospace, defense, energy, and healthcare sectors. Their work does not have a financial component. Instead, it seeks to cause chaos and destruction.

As a prominent company involved with the US government and the critical domestic energy sector, Good-Energy is a prime target for APT33. Its expertise and relationships would be valuable to Iran, from stealing intellectual property to providing information allowing them to access our partners.

Given their record of aggressive activity, the risk for Good-Energy is high. While we do not yet know the extent of the damage, we have already seen two machines wiped and at least one file exfiltrated. The threat actor is within the network and can severely damage the company's systems and reputation.

Immediate action is required to close the breach, shut down ongoing activities, and harden defenses against further attacks by this aggressive and sophisticated actor.

Attack Narrative

Like most APT33 attacks, this one began with spearphishing emails. Two employees reported reading job opportunity emails from solevisible[@]gmail.com. Henry.case[@]goodcorp.local reports his email had links he did not click. However, merely opening the email downloaded a file upon opening, which is the likely cause of a new scheduled task on his machine called GoogleUpdateschecker.vbs.

Jake.armitage[@]goodcorp.local says his email contained attached .rtf files, one of which he clicked. It opened a file with unreadable text. Though further analysis is required, Armitage's attachment likely contained an Office macro that compromised his machine. He runs an older Windows 7 computer that the IT team cannot update because of the legacy Excel dependencies his job requires. This setup is a known vulnerability for these kinds of macro attacks.

Other machines on our network have been affected, as shown by network traffic and indicators of compromise on additional PCs. We are still determining if that infection vector came from a worm within the network, direct email contact with solevisible, or if they were reached directly by the threat actor through lateral movement within the network.

The network traffic was notably heavy over the weekend to ngaaksa.[ddns.]net and ngaaksa.[site.]net. The unusual domain names of these sites suggest a connection to Northrup Grumman Aviation Arabia, which previously owned the site ngaaksa[.]com.

These two sites (among many others) are known command-and-control centers APT33. While we don't know the details, we can formulate a hypothesis of the following events based on others' experiences with the threat actor.

APT33 typically forces the download of custom dropper software in their phishing attacks. The dropper then installs a backdoor that can be used to enumerate the network topology, upload and download files, take screenshots, create reverse shells, and wipe the hard drives entirely or selectively.

Some of this activity seems to have taken place on Good-Energy's network already. Two PCs (neither used by Case nor Armitage) have had their hard drives' main partitions wiped. On another PC, a recovered artifact revealed the username of Xman_1365_x, an Iranian developer connected to APT33. Yet another PC had many instances of cerutil.exe running. Certutil.exe is a legitimate Microsoft process sometimes abused to exfiltrate data. This machine also had a zip file in the user directory named POWER_GEN_2012.zip, suggesting exfiltration occurred.

Tactics, Techniques, and Protocols

As noted, ATP33 works to further Iran's military, industrial, economic, and intelligence efforts worldwide. Their focus has evolved as Iran's geopolitical issues change.

They have been active since 2013 and in 2016 began to focus on the aerospace and petrochemical industries. Their primary vector was phishing emails related to job opportunities. At this time, they also focused on Saudi Arabian government organizations, again using spearphishing, this time with malicious Microsoft Office documents.

They next started leveraging stolen credentials often obtained from third-party breaches, scams, or brute force password attacks targeting the cloud infrastructure of various industries, including industrial control system vendors and service providers.

They have attacked US government computers using many different attack vectors and were able to install their custom tools. They also attacked US and Middle Eastern financial institutions using malicious Microsoft Office macros and commodity malware.

APT 33 attacks usually begin with spearphishing. The emails show some knowledge of the victim, typically spoofing job opportunities or an organization of professional interest. The emails can contain links to malicious sites to force the download of malicious files or attachments (typically Microsoft Office documents) to compromise the machine directly.

The domains to which the links lead change frequently with Dynamic DNS providers. The names of the sites usually differ only slightly from legitimate sites and businesses with which the victims would be familiar.

As expected of an established state actor, APT33 has created powerful custom tools.

- DROP SHOT can drop and launch additional tools
- TURNEDUP backdoor down- and uploads files, enumerates the victim system and can create a reverse shell.

- SHAPESHIFT (aka STONEDRILL) downloads files and contains a wiper that deletes the master boot record.
- Powerton is PowerShell-based, creates multiple persistence mechanisms, uses an encrypted C2, and can dump password hashes.
- SHAMOON wiper deletes and then overwrites the file with random data or images. It can also encrypt files and master boot record. Some versions contain a spreader that runs the tool on a list of targeted computers gathered by the attackers.

APT33 also uses commodity software, including:

- Nanocore
- Network
- PoshC2
- Remcos
- DarkComet
- Quasar RAT
- Puppy RAT
- Mimikatz
- Procdump
- Ruler
- Microsoft SysInternals

References

APT33, Mitre |ATT&K, Accessed January 10, 2023.

Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware, Mandiant, Accessed January 10, 2023.

Additional Insights into Iranian Cyber Espionage | APT33, ShadowDragon, Accessed January 10, 2023.

APT33 Hunt Report, Mike McPhearson and Matthew Pennington, Booz|Allen|Hamilton, Accessed January 10, 2023.

APT33: The Lesser Known Adversary with Ties to Advanced Espionage Threats, Cyware, Accessed January 10, 2023. Accessed January 10, 2023.

Iranian APT33 Targets US Firms with Destructive Malware, Threatpost, Accessed January 10, 2023.

Magnallium Threat Group Operations, Dragos, Accessed January 10, 2023.

Shamoon Attackers Employ New Tool Kit to Wipe Infected Systems, McAfee, Accessed January 10, 2023

Shamoon Returns to Wipe Systems in Middle East, Europe, McAfee, Accessed January 10, 2023

New Group of Iranian Hackers Linked to Destructive Malware, Wired, Accessed January 10, 2023.

From Shamoon to Stonedrill; Wipers Attacking Saudi Organizations and Beyond, Version 1.05, Kaspersky Lab, Accessed January 10, 2023.

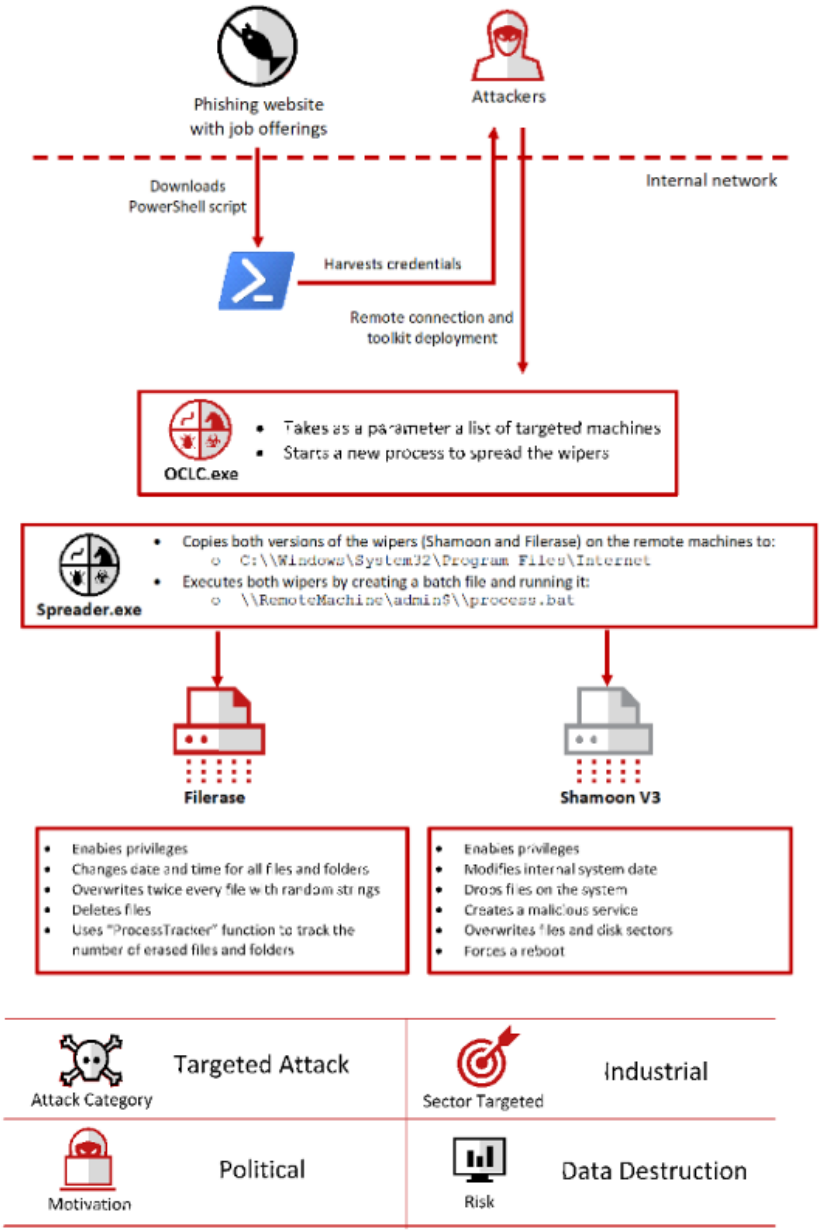

Figure 1. Diagram from McAfee showing a typical APT33 spearfishing attack.

Remediations

Included are detections and mitigations mapped to MITRE ATT&K specific to the indicators of compromise GoodCorp's IT and Security teams have found.

Also included is an ATT&K Navigator showing the actions needed to address what we know so far about this breach against MITRE's collection of techniques used by APT.

Note that this report is based on incomplete knowledge about the recent breach. Additional indicators of compromise will surely come to light and should make up the core of a more comprehensive final plan.

M1047 Audit
System scans can be performed to identify unauthorized archival utilities.

DS0009 Process Creation
Monitor for newly constructed processes and/or command-lines that aid in compression or encrypting data that is collected prior to exfiltration, such as 7-Zip, WinRAR, and WinZip.

DS0022 File Creation
Monitor newly constructed files being written with extensions and/or headers associated with compressed or encrypted file types. Detection efforts may focus on follow-on exfiltration activity, where compressed or encrypted files can be detected in transit with a network intrusion detection or data loss prevention system analyzing file headers.

M1038 Execution Prevention
se application control where appropriate. VBA macros obtained from the Internet, based on the file's Mark of the Web (MOTW) attribute, may be blocked from executing in Office applications (ex: Access, Excel, PowerPoint, Visio, and Word) by default starting in Windows Version 2203.

DS0017 Command Execution
Monitor executed commands and arguments that may abuse Visual Basic (VB) for execution.

DS0011 Module Load
Monitor for the loading of modules associated with VB languages (ex: vbscript.dll).

DS0012 Script Execution
Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

1054 Software Configuration
Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross-domain) to perform similar message filtering and validation. Furthermore, policies may enforce/install browser extensions that protect against IDN and homograph attacks.

M1017 User Training
Users can be trained to identify social engineering techniques and spear phishing emails with malicious links, including phishing for consent with OAuth 2.0. Users may also perform visual checks of the domains they visit; however, homographs in ASCII and IDN domains may render

manual checks difficult. Phishing and other cybersecurity training may raise awareness to check URLs before visiting the sites.

M1049 Antivirus/Antimalware
Anti-virus can be used to detect and quarantine suspicious files automatically. Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted.

M1021 Restrict Web-Based Content
Determine if certain websites that can be used for spear phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

M1042 Disable or Remove Feature or Program
follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing. Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notifications for allowing add-ins. For some add-in types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor prevents VBA code from executing.

M1057 Data Loss Prevention
Data loss prevention can detect and block sensitive data being sent over unencrypted protocols.

M1031 Network Intrusion Prevention
Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.

DS0022 File Access
Monitor for suspicious files (i.e. .pdf, .docx, .jpg, etc.) viewed in isolation that may steal data by exfiltrating it over an existing command and control channel.

DS0029 Network Traffic
Monitor for newly constructed network connections that are sent or received by untrusted hosts. Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g. extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated with traffic patterns (e.g. monitor anomalies in the use of files that do not normally initiate connections for the respective protocol(s)). Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

M1053 Data Backup

Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

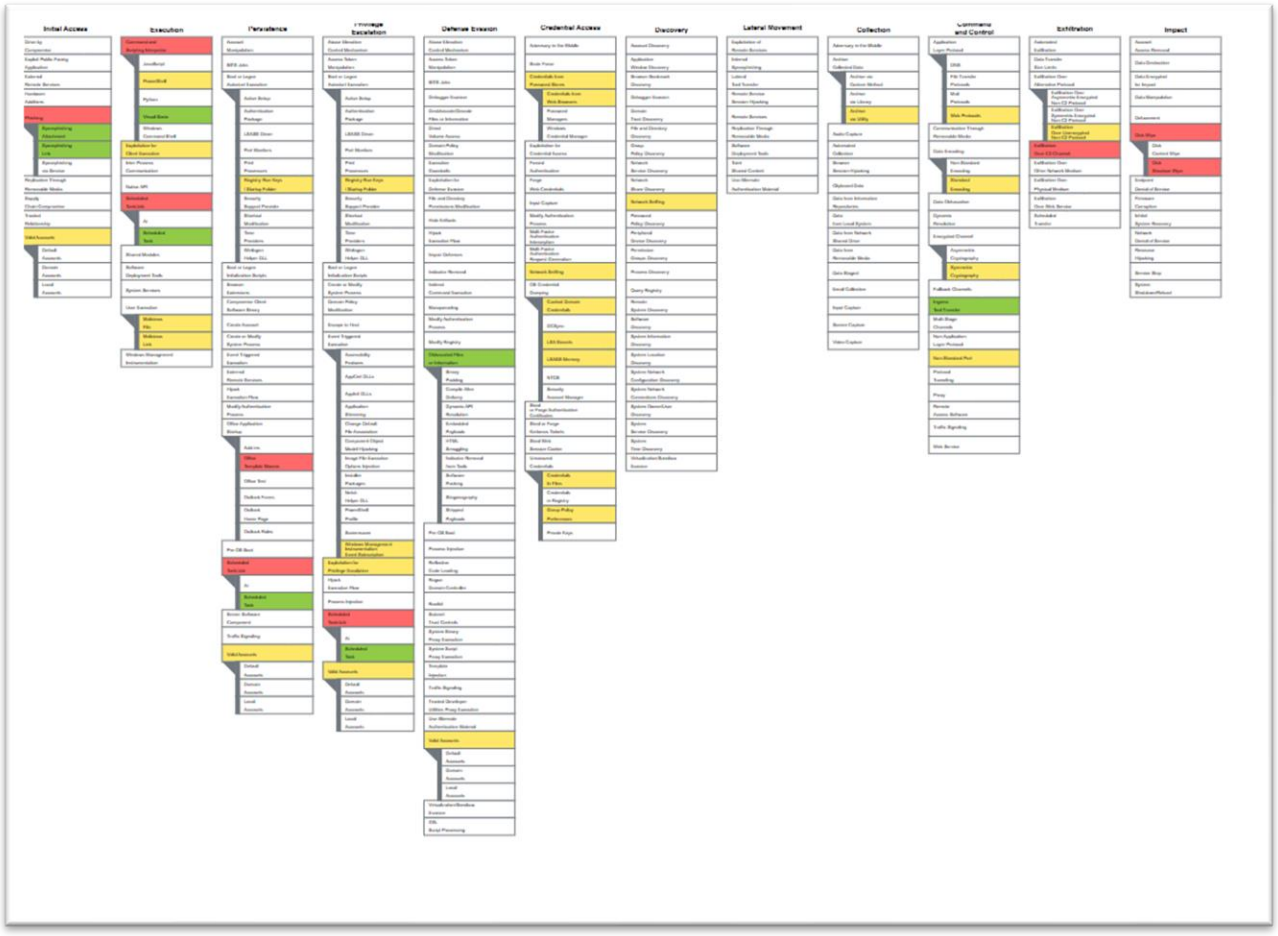

Figure 2. MITRE Navigator. The red shows indicators of compromise found so far in this incident. The yellow shows APT33's techniques identified by MITRE. The green shows the techniques shared by both. Good-Energy should focus on implementing the mitigations and detections for the yellow items. The red and green mitigations and detections are included in this report.

--End--