CyberCave

APT-34

Threat Intelligence As Code

PROFILING IRANIAN OFFENSIVE THREAT ACTOR

TLP: White

September 2022

cybercave.com.sa

EXECTIVE SUMMARY:

APT-34 a.k.a. Twisted Kitten, Cobalt Gypsy, Crambus, Helix Kitten, OilRig, APT34, IRN2, ATK40, G0049, Evasive Serpens, is an Iranian threat group operating primarily in the Middle East by targeting organizations in this region that are in a variety of different industries; however, this group has occasionally targeted organizations outside of the Middle East as well.

It also appears APT-34 carries out supply chain attacks, where the threat group leverages the trust relationship between organizations to attack their primary targets. The group is an active and organized threat group, which is evident based on their systematic targeting of specific organizations that appear to be carefully chosen for strategic purposes. Attacks attributed to this group primarily rely on social engineering to exploit the human rather than software vulnerabilities, however, on occasion this group has used recently patched vulnerabilities in the delivery phase of their attacks.

The lack of software vulnerability exploitation does not necessarily suggest a lack of sophistication, as the group has shown maturity in other aspects of their operations. Such maturities involve:

- Organized evasion testing used theduring development of their tools.
- Use of custom DNS tunneling protocols for command and control (C2) and data exfiltration.
- Custom web-shells and backdoors used to persistently access servers. They relies on stolen account credentials for lateral movement.

After the group gains access to a system, they use credential dumping tools, such as Mimikatz, to steal credentials to accounts logged into the compromised system. The group uses these credentials to access and to move laterally to other systems on the network.

After obtaining credentials from a system, operators in this group prefer to use tools other than their backdoors to access the compromised systems, such as remote desktop and putty. APT-34 also uses phishing sites to harvest credentials to individuals at targeted organizations to gain access to internet accessible resources, such as Outlook Web Access. Since at least 2014, an Iranian threat group tracked by FireEye as APT34 has conducted reconnaissance aligned with the strategic interests of Iran. The group conducts operations primarily in the Middle East, targeting financial, government, energy, chemical, telecommunications and other industries. Repeated targeting of Middle Eastern financial, energy and government organizations leads FireEye to assess that those sectors are a primary concern of APT34. The use of infrastructure tied to Iranian operations, timing and alignment with the national interests of Iran also lead FireEye to assess that APT34 acts on behalf of the Iranian government.

Associated Malware:

The group used the following malwares Quadagent, Twoface, Helminth, OopsIE, Karkoff, Fox Panel, HighShell, Glimpse, Webmask, RunningBee, HyperShell, ISMAgent, Poison Frog, PhpSpy, ThreeDollars, Neptun, Pickpocket, ValueVault, and Longwatch.

Targeting Region/Sector:

As we mentioned the threat group was initially observed targeting financial organizations,government telecommunication and education agencies across the Middle Eastern region and the US, but gradually it moved to other regions and sectors.

Financial

Government

Telecommunications

Education

APT34 campaign:

Cobalt Gypsy

OilRig

Twisted Kitten

APT34

IRN2

Sea turtle

Helix Kitten

ATK40

Cutting Kitten

Crambus

Fox Kitten

Associated Malware:

This group is known to use various malware and tools to collect strategic information that would benefit the economic and geopolitical interests of the state of Iran. Also, Iran considers cyber-attacks as an offensive weapon against its rival countries. The cyberattacks linked to the group are not that advanced or sophisticated, but highly persistent with their victim choice, which is directly or indirectly connected to Iran's military, financial, and political interests

Threat Actor Time Line

2014

Since 2014, the group's attacks were focused on Middle Eastern banks and government entities since 2014. Later, their primary targets changed, but the trend of targeting critical infrastructure and governmental entities remained the same.

2016

In October 2016, the group was observed to be targeting government entities in Middle Eastern countries and the U.S., along with several airlines from Middle Eastern countries.

2017

Between 2017 to 2018, the group focused more on Western-Asian and North American organizations working in Education, Information Technology and Government sector.

2017

Delivers Digitally Signed Malware, Impersonates University of Oxford In recent attacks they set up a fake VPN Web Portal and targeted at least five Israeli IT vendors, several financial institutes, and the Israeli Post Office.

2018

On January 2018 ,8, Unit 42 observed the OilRig threat group carry out an attack on an insurance agency based in the Middle East

2019

We identified three new malware families and a reappearance of PICKPOCKET, malware exclusively observed in use by APT34. The new malware families, which we will examine later in this post, show APT34 relying on their PowerShell development capabilities, as well as trying their hand at Golang.

2019

New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East.

2020

OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory.

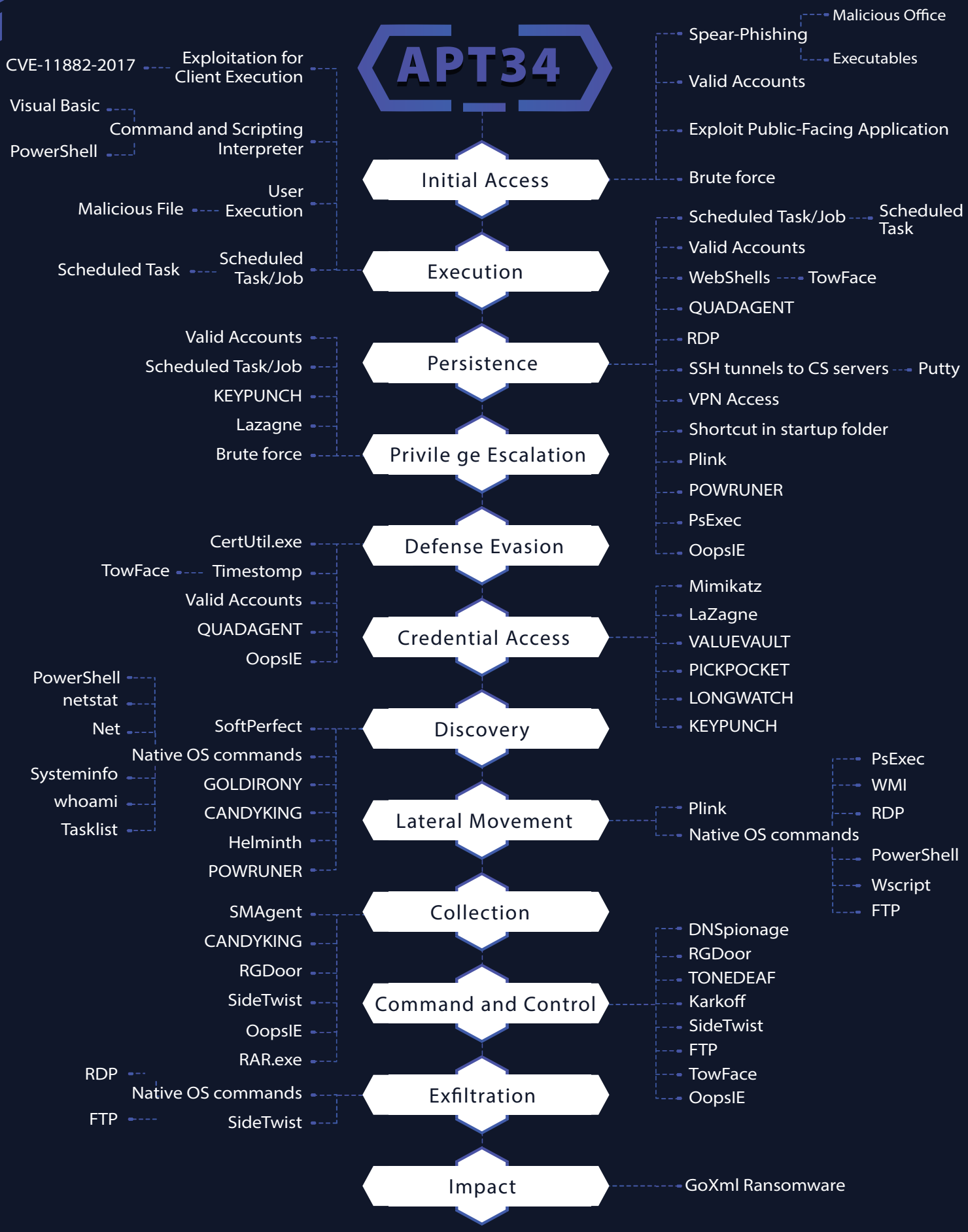
2021

A new APT34 espionage operation involves Lebanon Government

2022

1- in May 2022, Spear phishing has been observed, this spear phishing attack targeted a Jordanian diplomat, with the sender pretending to be a colleague from the IT department of the same governmental organization.

2- In July 2020, The Threat Actor targeting Albania government with distractive and ransomware Cyber Attack .



Based on the above TTPs we will deep dive intro each TTPs and Corrleted with MITER framework and propose some detection ,recommendetion and mitigation.

Let's Start...

INITIAL ACCESS CARD

Tactics, techniques, and procedures (TTP):

Initial Access card:

Spear Phishing: groups usually send phishing messages containing malicious office or executable attachments to victims from partner organizations that already had a relationship with the recipient or social media site (Lindekin).

Mitigation:

Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
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)
User training	Users can be trained to identify social engineering techniques and spearphishing emails.

Detection:

Detection Name	New Lolbin Process by Office Applications
CyberCave	[1],[2],[3]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Initial Access card:

Valid Account: Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Mitigation:

Password Policies	Applications and appliances that utilize default username and password should be changed immediately after the installation, and before deployment to a production environment.
Privileged Account Management	Audit domain and local accounts as well as their permission levels routinely to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account
User Account Management	Regularly audit user accounts for activity and deactivate or remove any that are no longer needed.
User training	Users can be trained to identify social engineering techniques and spearphishing emails.

Detection:

Logon Session Creation	Monitor for newly constructed logon behavior that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Correlate other security systems with login information (e.g., a user has an active login session but has not entered the building or does not have VPN access)
Logon Session Metadata	Look for suspicious account behavior across systems that share accounts, either user, admin, or service accounts. Examples: one account logged into multiple systems simultaneously; multiple accounts logged into the same machine simultaneously; accounts logged in at odd times or outside of business hours
User Account Authentication	Monitor for an attempt by a user that may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

Tactics, techniques, and procedures (TTP):

Initial Access card:

Exploit Public-Facing Application:

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior.

Mitigation:

Application Isolation and Sandboxing	Application isolation will limit what other processes and system features the exploited target can access.
Exploit Protection	Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application.
Privileged Account Management	Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system.
Network Segmentation	Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure.
Vulnerability Scanning	Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.

Detection:

Application Log Content	Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation.
Network Traffic Content	Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.

Tactics, techniques, and procedures (TTP):

Initial Access card:

Brute-Force:

Using brute force Password Spraying techniques to gain access to accounts like Outlook Web Access, VPN, Citrix application etc.

Mitigation:

Password Policies	Having a strong password policy is the simplest and most effective way of thwarting a brute-force attack.
Multi-factor Authentication	Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information
Locking Accounts	Lock out accounts after a defined number of incorrect password attempts.
Using CAPTCHAS	Using CAPTCHAS to prevent any automation tool trying to brute-force your services.

Detection:

Application Log Content:	Monitor authentication logs for system and application login failures of Valid Accounts
User Account Authentication	Monitor for an attempt by a user to gain access to a network or computing resource, often by the use of domain authentication services, such as the System Security Services Daemon (sssd) on Linux.

EXECUTION CARD

Tactics, techniques, and procedures (TTP):
Execution card:

Exploitation for Client Execution– CVE-11882-2017:

Taking advantage of cve-11882-2017 vulnerability which leverage for A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory.

Mitigation:

Application Isolation and Sandboxing	Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. Other types of virtualization and application micro segmentation may also mitigate the impact of client-side exploitation. Risks of additional exploits and weaknesses in those systems may still exist.
Exploit Protection	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior

Detection:

Detection Name	EXPLOIT Equation Editor Exploit (CVE-11882-2017)
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Execution card:

Command and Scripting Interpreter|PowerShell | VBScript :

Using various types of scripting for execution like scripts, or PowerShell.

Mitigation:

Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
Execution Prevention	Use application control where appropriate
Disable or Remove Feature or Program	It may be possible to remove PowerShell from systems when not needed or turn off to unneeded VM components, but a review should be performed to assess the impact to an environment

Detection:

Detection Name	Malicious PowerShell, VBs
CyberCave	[1],[2],[3]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Execution card:

User Execution – Malicious File

Using macro-enabled documents that required targets to click the "enable content" button to execute the payload on the system

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Detection:

Detection Name	Dump Office Macro Files from Commandline, Outlook C2 Macro Creation
CyberCave	[1],[2]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Execution card:

Scheduled Task:

Creating scheduled tasks that run a VBScript to execute a payload on victim machines.

Mitigation:

Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges
Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM.
Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process.
User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

Detection:

Detection Name	Scheduled Task Creation, cheduled Task WScript VBScript
CyberCave	[1],[2]
GitHub	Click Here

PERSISTENCE

Tactics, techniques, and procedures (TTP):
Persistence card:

WebShell TowFace| SEASHARPEE:

According to Unit42, TwoFace is a two-staged (loader+payload) webshell, written in C# and meant to run on webservers with ASP.NET.

Mitigation:

Disable or Remove Feature or Program	Consider disabling functions from web technologies such as PHP's eval() that may be abused for web shells.
User Account Management	Enforce the principle of least privilege by limiting privileges of user accounts so only authorized accounts can modify the web directory.

Detection:

Detection Name	Detect Tow-Face WebShell
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Persistence card:

QUADAGENT:

A PowerShell script backdoor which uses DNS tunneling to communicate with the C2.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.

Detection:

Detection Name	Detect QUADAGENT Malware
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Persistence card:

Remote Desktop (RDP): Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system.

Mitigation:

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.
Public accessibility	Do not expose RDP directly to the internet. RDP should be accessible only from within trusted networks.
Disabled unused services	If RDP is not used on your Windows systems, disable the service altogether.

Detection:

Detection Name	Publicly Accessible RDP Service.
CyberCave	[1],[2]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Persistence card:

Putty & Plink:

Legitimate tools that function as clients for a number of communications protocols such as SSH protocol to allow authorized users to open remote shells on other devices.

Mitigation:

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.
Public accessibility	Do not expose SSH directly to the internet. SSH should be accessible only from within trusted networks.
Disabled unused services	If SSH is not used on your Windows systems, disable the service altogether.

Detection:

Logon Session Creation	Monitor for suspicious connections across systems that using bruteforce or user enumeration.
User Account Authentication	Monitor for an attempt by a user to gain access to a network or computing resource, often by the use of domain authentication services, such as the System Security Services Daemon (sssd) on Linux.
Detection Name	Suspicious Plink Remote Forwarding
CyberCave	[1],[2]
GitHub	[1],[2]

Tactics, techniques, and procedures (TTP):

Persistence card:

Shortcut in startup folder:

Adversaries may achieve persistence by adding a program to a startup folder.

Mitigation:

User Account Management	Limit permissions for who can create symbolic links in Windows to appropriate groups such as Administrators and necessary groups for virtualization. This can be done through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create symbolic links

Detection:

Detection Name	Startup Folder File Write
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Persistence card:

POWRUNER :

A PowerShell script that sends and receives commands to and from the C2 server.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.

Detection:

PowerShell Version	Ensure Use of PowerShell version 5 (or higher)
Script Execution	monitor for any attempts to enable scripts running on a system would be considered suspicious.
Process Creation	Monitor for newly executed processes that may abuse PowerShell commands and scripts for execution.

Tactics, techniques, and procedures (TTP):

Persistence card:

PsExec:

A free Microsoft tool that can be used to execute a program on another computer. It is used by IT administrators and attackers.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to block processes created by PsExec from running.
Privileged Account Management	Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level.
Restrict File and Directory Permissions	Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Detection:

Detection Name	PsExec Tool Execution,
CyberCave	[1],[2]
GitHub	Click Here

PRIVILEGE ESCALATION

Tactics, techniques, and procedures (TTP):

Persistence card:

LaZagne:

A post-exploitation, open-source tool used to recover stored passwords on a system.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files

Detection:

Detection Name	Credential Dumping by LaZagne
CyberCave	[1],[2]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Persistence card:

KEYPUNCH:

A key logger that logs user keystrokes to capture credentials as the user types them.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.

Detection:

Update Windows	Insure your system up to date.
Process Creation	Monitor for newly constructed processes and/or command-lines for applications that may be used by an adversary.
Avoid Downloading untrusted software	Insure all software that installed in your PC's is legitimate and not cracked.

DEFENSE EVASION

Tactics, techniques, and procedures (TTP):

Defense evasion card:

CertUtil tool:

A command-line utility that can be used to obtain certificate authority information and configure Certificate Services.

Mitigation:

Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known protocols like FTP can be used to mitigate activity at the network level
Restrict File and Directory Permissions	Ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level.

Detection:

Detection Name	Certutil Encode, Suspicious Certutil Command
CyberCave	[1],[2]
GitHub	Click Here

CREDENTIAL ACCESS

Tactics, techniques, and procedures (TTP):

Credential access card:

Mimikatz: A credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.

Mitigation:

Active Directory Configuration	Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication
Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing
Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping
Operating System Configuration	Consider disabling or restricting NTLM. Consider disabling WDigest authentication

Detection:

Detection Name	Mimikatz Command Line, Possible Mimikatz Zerologon Attempt
CyberCave	[1],[2]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Credential access card:

VALUEVAULT:

A Golang compiled version of the "Windows Vault Password Dumper" browser credential theft tool.

Mitigation:

Password Policies	Organizations may consider weighing the risk of storing credentials in web browsers. If web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in web browsers.
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.

Detection:

Detection Name	APT34 VALUEVAULT Malware
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Credential access card:

PICKPOCKET:

A credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
Password Policies	Organizations may consider weighing the risk of storing credentials in web browsers. If web browser credential disclosure is a significant concern, technical controls, policy, and user training may be used to prevent storage of credentials in web browsers.

Detection:

Command Execution	Monitor executed commands and arguments that may acquire credentials from web browsers by reading files specific to the target browser.
Disabled local admin	Disable the debug right for local administrators on all servers and workstation
Disable the WDigest	Identify web browser files that contain credentials such as Google Chrome's Login Data database file: AppData\Local\Google\Chrome\User Data\Default\Login Data. Monitor file read events of web browser files that contain credentials, especially when the reading process is unrelated to the subject web browser.

Tactics, techniques, and procedures (TTP):

Credential access card:

LONGWATCH:

A key logger that outputs keystrokes to a log.txt file in the Windows temp folder.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Detection:

Windows Registry Key Modification	Monitor for changes made to windows registry keys or values for unexpected modifications
Disabled local admin	Disable the debug right for local administrators on all servers and workstation
OS API Execution	Monitor for API calls to the SetWindowsHook, GetKeyState, and GetAsyncKeyState. and look for common keylogging API calls

DISCOVERY

Tactics, techniques, and procedures (TTP):

Discovery card:

SoftPerfect:  A scanner tool can pings computers, scans ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell.

Mitigation:

Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Disable or Remove Feature or Program	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
Network Intrusion Prevention	Use network intrusion detection/prevention systems to detect and prevent remote service scans.
Network Segmentation	Ensure proper network segmentation is followed to protect critical servers and devices.

Detection:

Detection Name	Suspicious using of softperfect network scanner tool
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Discovery card:

Netstat:

A networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network.

Mitigation:

NOTE:	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection:

Detection Name	Mounted Windows Admin Shares with net.exe, Net.exe Execution
CyberCave	[1],[2]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Discovery card:

Systeminfo:

A Windows utility that can be used to gather detailed information about a computer.

Mitigation:

NOTE:	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection:

Detection Name	Suspicious Execution of Systeminfo
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Discovery card:

Whoami:

A command that displays user, group and privileges information for the user who is currently logged on to the local system.

Mitigation:

NOTE:	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection:

Detection Name	Mounted Windows Admin Shares with net.exe, Net.exe Execution
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Discovery card:

Tasklist:

A utility that displays a list of applications and services with their Process IDs (PID) for all tasks running on either a local or a remote computer.

Mitigation:

NOTE:	This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection:

Detection Name	Suspicious Execution of Systeminfo
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):

Discovery card:

GOLDIRONY:

Network Scanner tool.

Mitigation:

Disable or Remove Feature or Program	Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.
Network Intrusion Prevention	Use network intrusion detection/prevention systems to detect and prevent remote service scans.
Network Segmentation	Ensure proper network segmentation is followed to protect critical servers and devices.

Detection:

Command Execution	Monitor executed commands and arguments that may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.
Network Traffic Flow	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.

Tactics, techniques, and procedures (TTP):

Discovery card:

CANDYKING:

A tool used to capture a screenshot of user's desktop.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.

Detection:

Command Execution	Monitor executed commands and arguments that may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.
OS API Execution	Monitoring for screen capture behavior will depend on the method used to obtain data from the operating system and write output files. Detection methods could include collecting information from unusual processes using API calls used to obtain image data, and monitoring for image files written to disk, such as CopyFromScreen, xwd, or screencapture.

COLLECTION

Tactics, techniques, and procedures (TTP):
Collection card:

OopsIE:

A trojan used by OilRig to remotely execute commands as well as upload/download files to/from victims.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.

Detection:

Detection Name	APT34 OopsIE Trojan
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Collection card:

RGDoor:

A malicious Internet Information Services (IIS) backdoor developed in C++ language.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.

Detection:

Detection Name	RGDoor.
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Collection card:

Rar.exe

A winrar tool that compress data to RAR files (e.g., sensitive documents) which is collected prior to exfiltration

Mitigation:

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

Detection:

Detection Name	Data Compressed - rar.exe, Winrar Compressing Dump Files
CyberCave	[1],[2]
GitHub	Click Here

COMMAND AND CONTROL

Tactics, techniques, and procedures (TTP):
Command and control card:

Helminth:

A backdoor that has at least two variants - one written in VBScript and PowerShell that is delivered via a macros in Excel spreadsheets, and one that is a standalone Windows executable.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.

Detection:

Detection Name	Helminth Backdoor
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Command and control card:

ISMAgent:

A fallback DNS tunneling mechanism used when the C2 server is not reachable over HTTP.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Filter Network Traffic	Consider filtering DNS requests to unknown, untrusted, or known bad domains and resources. Resolving DNS requests with on-premise/proxy servers may also disrupt adversary attempts to conceal data within DNS packets.
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.

Detection:

Detection Name	Malware ISMAgent C2 DNS
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Command and control card:

Side-Twist:

A backdoor developed in the C++ language.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.

Detection:

Detection Name	APT34 SideTwist Backdoor
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Command and control card:

TONEDEAF:

A backdoor that communicates with Command and Control servers using HTTP or DNS.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.
Filter Network Traffic	Consider filtering DNS requests to unknown, untrusted, or known bad domains and resources. Resolving DNS requests with on-premise/proxy servers may also disrupt adversary attempts to conceal data within DNS packets.

Detection:

Detection Name	Detect TONEDEAF Malware APT34
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Command and control card:

Karkoff:

A malware that uses base64 encoding to initially obfuscate the C2 communications.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.

Detection:

Detection Name	APT34 Karkoff Malware
CyberCave	[1]
GitHub	Click Here

Tactics, techniques, and procedures (TTP):
Command and control card:

DNSPIONAGE:

A malware that uses HTTP and DNS communication with the attackers infrastructure.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
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.
Filter Network Traffic	Consider filtering DNS requests to unknown, untrusted, or known bad domains and resources. Resolving DNS requests with on-premise/proxy servers may also disrupt adversary attempts to conceal data within DNS packets.

Detection:

Detection Name	APT34 DNSPIONAGE malware
CyberCave	[1]
GitHub	Click Here

EXFILTRATION

Tactics, techniques, and procedures (TTP):
Exfiltration card:

File Transfer Protocol (FTP):

A utility commonly available with operating systems to transfer information over the File Transfer Protocol (FTP).

Mitigation:

Data Loss Prevention	Data loss prevention can detect and block sensitive data being sent over unencrypted protocols.
Filter Network Traffic	Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.
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.

Detection:

Detection Name	Suspicious ftp.exe
CyberCave	[1]
GitHub	Click Here

IMPACT

Tactics, techniques, and procedures (TTP):
Impact card:

GoXml Ransomware:

A custom tool built on SMB protocol called "Mellona.exe" to spread destructive ransomware.

Mitigation:

Behavior Prevention on Endpoint	On Windows 10, various Attack Surface Reduction (ASR) rules can be enabled to prevent the execution of potentially malicious executable files (such as those that have been downloaded and executed by Office applications/scripting interpreters/email clients or that do not meet specific prevalence, age, or trusted list criteria).
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Data Backup	Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data

Detection:

Detection Name	Detect GoXml Ransomware
CyberCave	[1]
GitHub	Click Here

RESOURCES

Resources

- https://attack.mitre.org/groups/G0049/
- https://github.com/blackorbird/APT_REPORT/blob/master/Threat%20Group%20Cards.pdf
- https://www.cisa.gov/uscert/ncas/alerts/aa264-22a
- https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
- https://malpedia.caad.fkie.fraunhofer.de/actor/oilrig

@cyber_cave_sa

cybercave.com.sa