Attack Graph Response to US-CERT Alert (AA22-264A)

By Francis Guibernau

Published: 2022-09-23 · Archived: 2026-04-05 17:41:13 UTC

On September 21, 2022, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA) that provides insight information on recent cyber operations against the Government of Albania in July and September 2022.

In July 2022, Iranian actors identifying as “HomeLand Justice” launched a destructive cyber-attack against the Government of Albania which rendered websites and services unavailable. An FBI investigation indicates Iranian state cyber actors acquired initial access to the victim’s network approximately 14 months before launching the destructive attack, which included both a ransomware-style file encryptor and a disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content.

Between May and June 2022, Iranian state cyber actors conducted lateral movements, network reconnaissance, and credential harvesting from Albanian government networks. In July 2022, the actors launched ransomware on the networks, leaving an anti-Mujahideen E-Khalq (MEK) message on desktops. When network defenders identified and began to respond to the ransomware activity, the cyber actors deployed a version of ZeroCleare destructive malware.

On July 18, 2022, HomeLand Justice claimed credit for the attack on the Albanian government infrastructure. On July 23, 2022, Homeland Justice posted videos of the cyber-attack on their website. From July to August 2022, Homeland Justice posted videos of the cyber-attack on their website and promoted on social media accounts Albanian Government information for release.

In September 2022, Iranian cyber actors launched another wave of cyber-attacks against the Government of Albania, using similar TTPs and malware as the cyber-attacks in July. These were likely done in retaliation for public attribution of the cyber-attacks in July and severed diplomatic ties between Albania and Iran.

According to the following report from Microsoft, released on September 8, 2022, the adversary responsible for the initial access and exfiltration of information is linked to OilRig, also known as APT34. This adversary is closely linked to Iran’s Ministry of Intelligence and Security (MOIS). Additionally, the Microsoft Detection and Response Team (DART) details that the DEV-0133 adversary, publicly known as Lyceum, was responsible for testing the victim’s infrastructure.

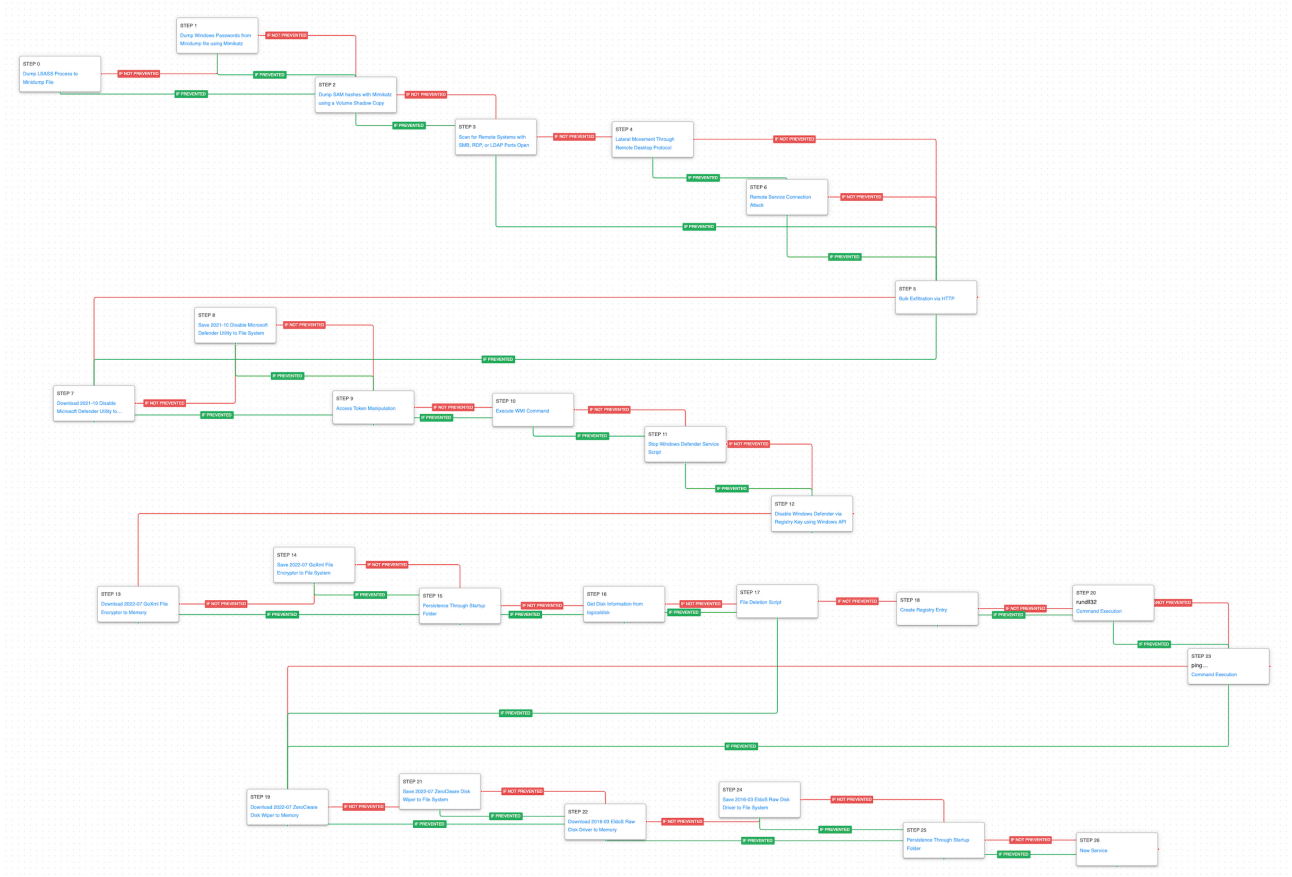
Lyceum is an adversary previously reported by SecureWorks in August 2019. The adversary is suspected of being closely linked to APT33 and OilRig.

On July 11, 2022, AttackIQ released two attack graphs that seek to emulate different aspects of OilRig’s operations against multiple sectors around the globe.

AttackIQ has released a new fully featured attack graph that emulates the tactics, techniques, and procedures (TTPs) used by Iranian nation-state adversaries against the government of Albania.

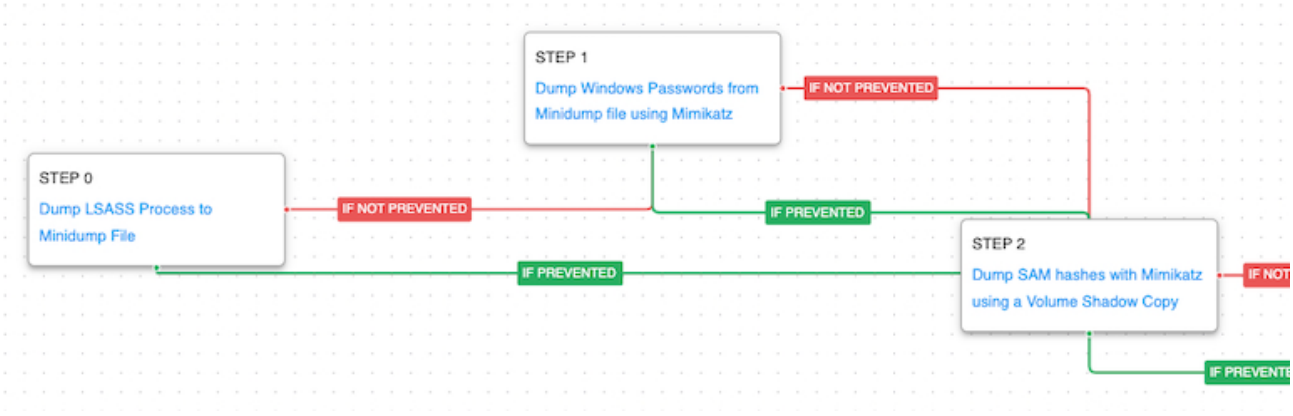
Testing previously released attack graphs pertaining to this kind of threat in conjunction with this newly released attack graph can help validate your security program performance in reducing risk. By using the AttackIQ Security Optimization Platform, security teams will be able to:

- Evaluate security control performance against malicious techniques that lead to the mass encryption of critical services.
- Assess their security posture against an actor that doesn't need to bring down additional backdoors to successfully infiltrate your network.
- Continuously validate detection and prevention pipelines beyond the initial access exploits as new zero-days are discovered



(Click for Larger)

[US-CERT AA22-264A] Iranian Ransomware and Disk Wiping Attack against Government of Albania

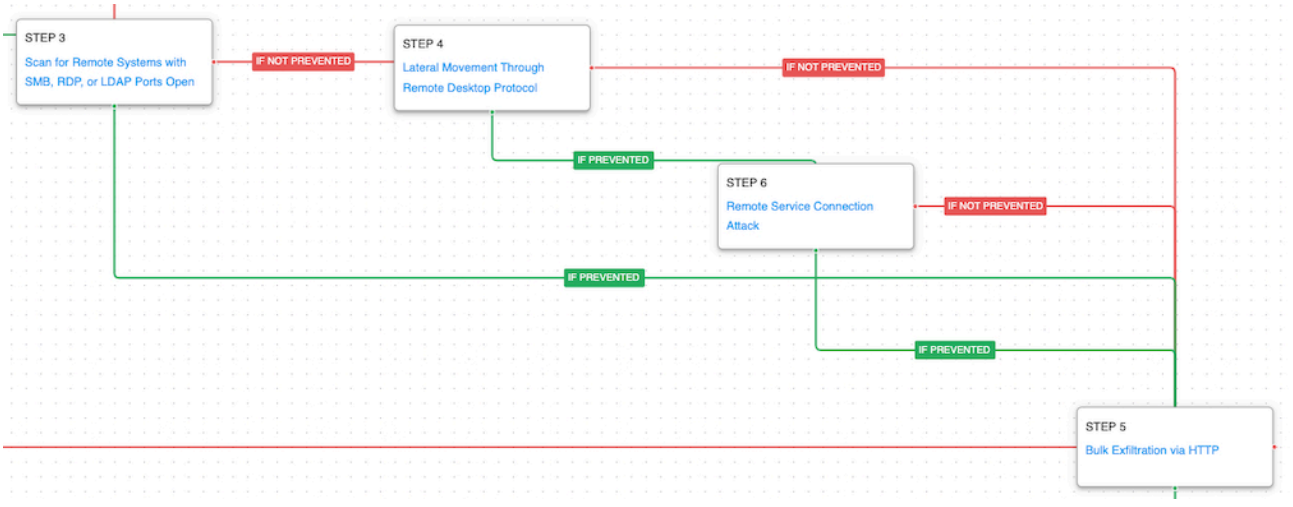


(Click for Larger)

The Iranian actors first exploited a common vulnerability in SharePoint and dropped a series of webshells to begin their attack. Our attack graph begins after their initial access has been established and the threat actor needs to gain access to additional credentials to move laterally and expand the scope of their attack.

OS Credential Dumping: LSASS Memory (T1003.001): LSASS memory is dumped to disk by creating a minidump of the `lsass.exe` process. This process is used for enforcing security policy on the system and contains many privileged tokens and accounts that are targeted by threat actors. `Mimikatz` is then used to dump the credentials from that minidump file.

OS Credential Dumping: Security Account Manager (T1003.002): A Volume Shadow Copy is used to be able to dump the SAM registry hive that is typically locked for access when Windows is running. Mimikatz is again used to dump the credentials from this registry hive.



(Click for Larger)

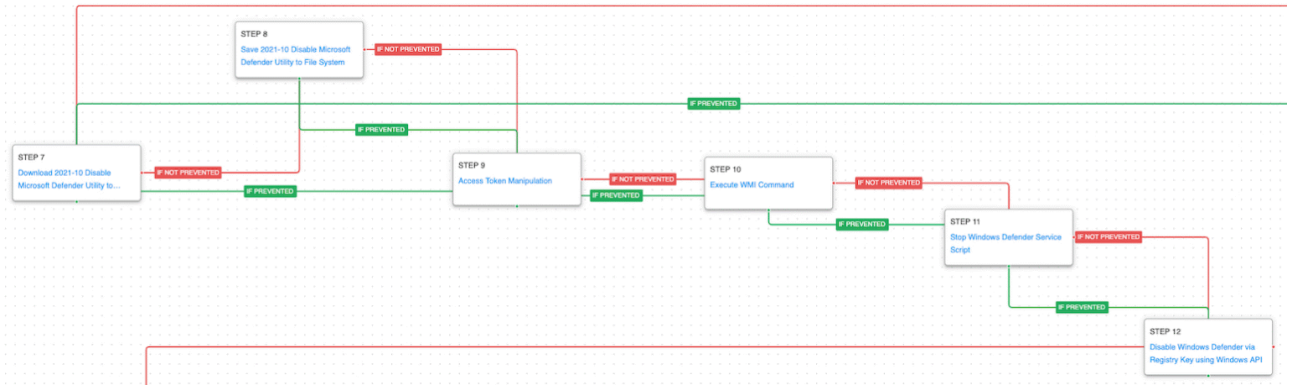
With the dumped credentials the actors can now begin to move about the network. They first leveraged a network scanner to identify other hosts of interest based on their remote services. Then they moved laterally using Remote Desktop Protocol (RDP) and File Transfer Protocol (FTP). Finally, they exfiltrated gigabytes of data using HTTP requests to the Exchange server.

Network Service Discovery (T1046): This scenario uses `nmap` to scan for hosts that are open on ports “ that would identify remotely accessible hosts to the attacker.

Remote Services: Remote Desktop Protocol (T1021.001): Remote Desktop is the built-in remote access utility used by Windows. This scenario attempts to remotely connect to another accessible asset with stolen credentials.

Remote Services (T1021): This scenario can be configured with the IP address of a remote FTP server and credentials to simulate the network traffic observed in the authentication of an internal FTP server.

Exfiltration Over C2 Channel (T1041): A large amount of data is exfiltrated over HTTP requests mimicking the data exfiltration method used by the Iranian actors when they stole a large amount of email data using their webshells.



(Click for Larger)

The actors wanted to impair the defenses of their compromised systems to limit the ability for the victim to detect their activity or recover from the future destruction actions. The first brought their own custom utility that would disable Windows Defender in order to reduce the likelihood that their follow up actions would be detected or prevented. The tool would elevate their privileges before checking if Windows Defender was enabled using a WMI command, and then stopping the service before modifying registry keys to prevent it from being re-enabled at reboot.

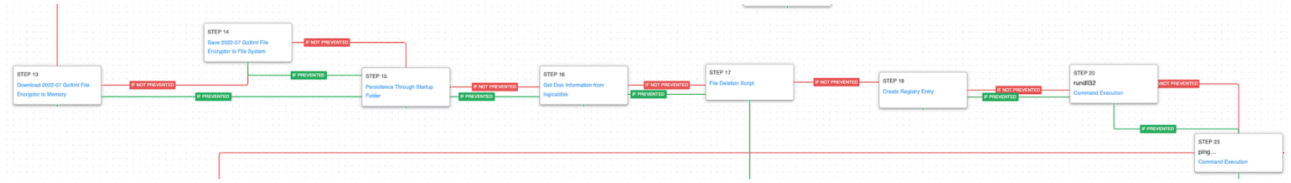
Ingress Tool Transfer (T1105): This scenario downloads to memory and saves to disk in two separate scenarios to test network and endpoint controls and their ability to prevent the delivery of the `disable-defender.exe` binary.

Access Token Manipulation (T1134): This scenario lists active access tokens that could be impersonated by another process. This method is commonly used to escalate privileges.

Windows Management Instrumentation (WMI) (T1047): WMI is a native Windows administration feature that provides a method for accessing Windows system components. This scenario gets the status of Windows Defender by calling “ `MSFT_MpPreference Get DisableRealtimeMonitoring` ”

Service Stop (T1489): The Windows Defender service is stopped with a “ `net stop` ” command.

Impair Defenses: Disable or Modify Tools (T1562.001): The registry key `HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware` is set to `1` that will disable Windows Defender from being enabled at next reboot.



(Click for Larger)

With the system defenses degraded, the actor moved on to launching a ransomware attack. The file cryptor was brought down to the system and persistence establishing using the Startup folder. A batch script would be executed that disabled System Recovery for all the drives and delete their Recycle Bin directories. Volume Shadow Copies would then be removed before finally executing the ransomware binary. The desktop background is changed to a ransomware calling card picture. `RunDll32` is used to for the background to update and then `ping` is used to delay in the batch script before killing itself and removing its artifacts.

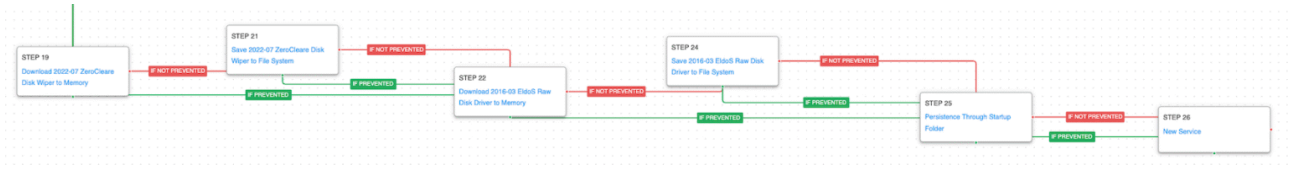
Logon Autostart Execution: Startup Folder (T1547.001): The Startup folder is a directory associated with the Windows Start Menu that can be used to launch a process at Windows logon. This scenario creates a binary file in this directory that would execute at next logon for users.

Windows Management Instrumentation (WMI) (T1047): This scenario executes the `logicaldisk` command to retrieve details on the system's disks.

Inhibit System Recovery (T1490): Runs `vssadmin.exe` to delete a recent Volume Shadow Copy created by the attack graph.

Modify Registry (T1112): The "`HKEY_CURRENT_USER\Control Panel\Desktop`" registry key is modified that changes the background image for the current user.

System Binary Proxy Execution: Rundll32 (T1218.011): `RunDll32` is another native system utility that can be used to execute DLL files and a specific export inside the file. This scenario executes `RunDll32` and passes "`user32.dll,UpdatePerUserSystemParameters`" which will force the system to refresh a user's setting including the desktop background.



(Click for Larger)

In response to the victim's efforts to remediate their incident, the actors moved on to deploying a disk wiping malware in retaliation. This was a modified version of their ZeroCleare wiper that uses the EldoS Raw Disk Driver to wipe drives at the lowest level.

Create or Modify System Process: Windows Service (T1543.003): Creates a new service called "RawDisk3" using the native `sc.exe` utility. This is the service named used when the driver starts.

Opportunities for Extending the Attack Graph

While we did not include one of many different ransomware file encryption scenarios to this attack graph, customers can add one of the many different Collect and Encrypt File scenarios to the graph or run it individual in a separate assessment to test similar ransomware tools like Locky and Ryuk.

Detection and Mitigation Opportunities

With so many different techniques being used by threat actors, it can be difficult to know which to prioritize for prevention and detection opportunities. AttackIQ recommends first focusing on the following techniques emulated in our scenarios before moving on to the remaining techniques.

1. OS Credential Dumping: Security Account Manager (T1003.002)

Description:

Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either through in-memory techniques or through the Windows Registry where the SAM database is stored. The SAM is a database file that contains local accounts for the host, typically those found with the net user command. Enumerating the SAM database requires SYSTEM level access

1a. Detection:

Using an EDR or SIEM product, you can detect when suspicious creations of shadow copies are observed as well as Mimikatz usage with the created shadow copy.

Note: it would be advised to correlate these two rules together in a SIEM product to create an Alert when creation of shadow volumes is observed alongside Mimikatz usage.

Detecting Suspicious Shadow Copy creations:

```
Process Name = “powershell.exe”
Command Line CONTAINS (“Get-WMIObject Win32_ShadowCopy” AND “Create”)
```

Detecting Mimikatz usage:

```
Process Name = (“powershell.exe” OR “cmd.exe”)
Command Line CONTAINS (“lsadump::sam”)
```

1b. Mitigations:

MITRE ATT&CK Recommends the following mitigations for OS Credential Dumping: Security Account Manager (T1003.002):

- M1028 – Operating System Configuration
- M1027 – Password Policies
- M1026 – Privileged Account Management
- M1017 – User Training

2. Impair Defenses: Disable or Modify Tools (T1562.001)

Description:

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take the many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information

2a. Detection:

Using an EDR or SIEM product, you can detect when Microsoft Defender Registry Key's Value for "DisableAntiSpyware" has been set to 1, disabling the security control:

```
Process Name = "reg.exe"
Command Line CONTAINS ("HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" AND "DisableAntiSpyware"
AND "REG_DWORD /d 1")
```

2b. Mitigations:

MITRE ATT&CK Recommends the following mitigations for Impair Defenses: Disable or Modify Tools (T1562.001):

- M1022 – Restrict File and Directory Permissions
- M1024 – Restrict Registry Permissions
- M1018 – User Account Management

3. Create or Modify System Process: Windows Service (T1543.003)

Description:

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions

3a. Detection:

Using an EDR or SIEM product, you can detect when sc.exe is being used to create possibly suspicious services. In this case, the service the threat actor has been seen creating is named "RawDisk3"

```
Process Name = ("cmd.exe" OR "powershell.exe")
Command Line CONTAINS ("sc create" AND "RawDisk3" AND start="demand")
```

3b. Mitigations:

MITRE ATT&CK Recommends the following mitigations for **Create or Modify System Process: Windows Service (T1543.003):**

- M1018 – User Account Management
- M1028 – Operating System Configuration
- M1047 – Audit
- M!040 – Behavior Prevention on Endpoint
- M1045 – Code Signing

Wrap-up

In summary, this attack graph will evaluate security and incident response processes and support the improvement of your security control posture against an actor who intends to destroy their target. With data generated from continuous testing and use of this attack graph, you can focus your teams on achieving key security outcomes, adjust your security controls, and work to elevate your total security program effectiveness against a known and dangerous threat.

AttackIQ stands at the ready to help security teams implement this attack graph and other aspects of the AttackIQ Security Optimization Platform, including through our co-managed security service, AttackIQ Vanguard.
