Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

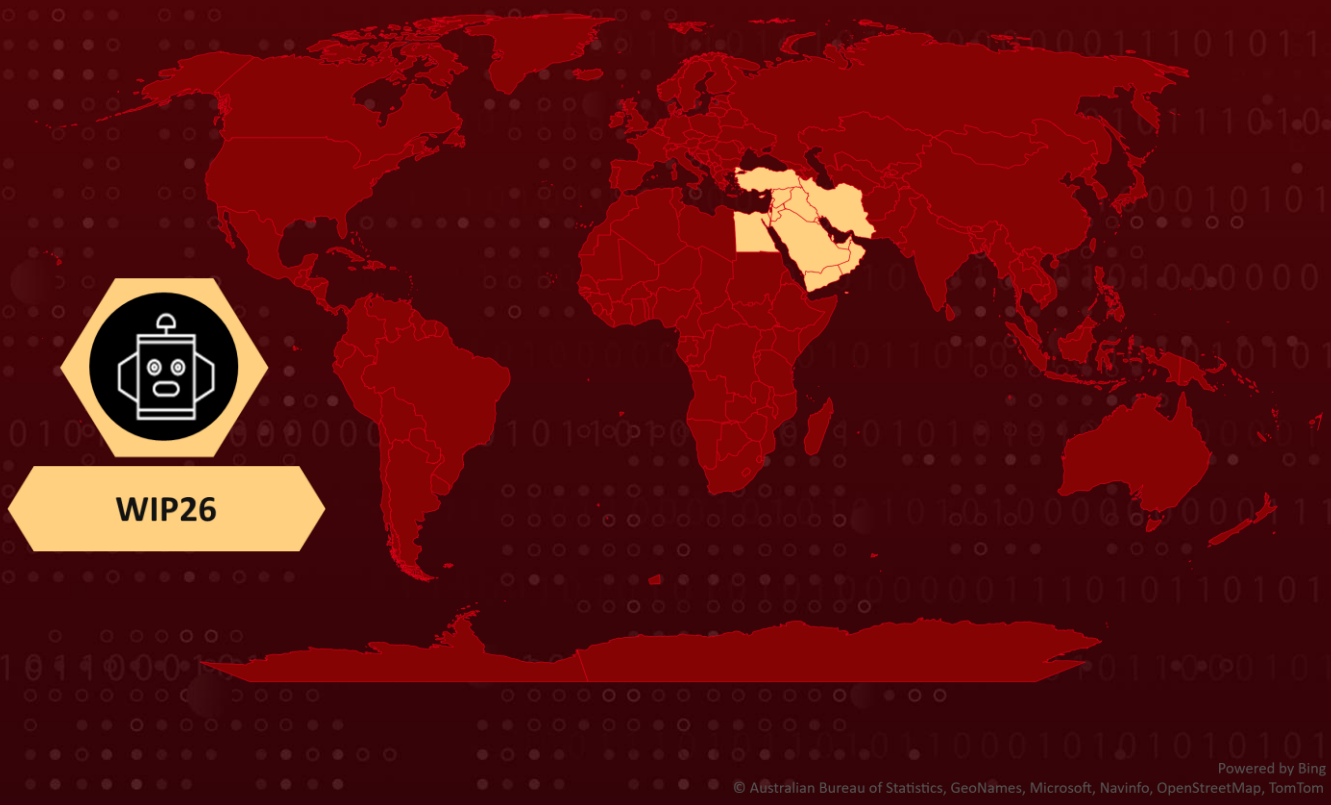
WIP26 attacks Middle Eastern telecom service providers

Date of Publication	Admiralty code	TA Number
February 21, 2023	A1	TA2023093

Summary

First Appearance: 2022
Actor Name: WIP26
Target Industries: Telecommunications.
Target Region: Middle East.

Actor Map



Actor Details

#1

The WIP26 operation commences by precisely selecting employees to receive WhatsApp messages containing Dropbox links to a malware loader. The employees are enticed into downloading and executing the loader, which then deploys backdoors that employ Microsoft 365 Mail and Google Firebase instances as command-and-control servers.

#2

The archives housed both the documents and a disguised malware loader (PDFelement.exe) masquerading as the legitimate PDFelement application. CMD365's main function is to execute instructions from a command-and-control server hosted on a Microsoft 365 Mail instance. This capability was leveraged for various activities, such as reconnaissance, elevating privileges, staging malware, and exfiltrating data.

#3

The malicious actor disguised the open-source tool Chisel as the Media Player Classic program, which was signed with an invalid certificate under the name "Rare Ideas LLC." They also exchanged encrypted and Base64-encoded information between the C2 server and CMD365. In addition, CMDEmber leveraged a Google Firebase Realtime Database instance as a C2 server. Furthermore, the Launcher.exe sample for CMDEmber was a .NET application that imitated the Opera browser.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
WIP26	Unknown **MOTIVE** Information theft and espionage	Middle East	Telecommunications

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration	TA0040 Impact
T1102 Web Service	T1036 Masquerading	T1106 Native API	T1199 Trusted Relationship
T1053 Scheduled Task/Job	T1547 Boot or Logon Autostart Execution	T1566 Phishing	T1059 Command and Scripting Interpreter
T1189 Drive-by Compromise	T1056 Input Capture	T1010 Application Window Discovery	T1518 Software Discovery
T1518.001 Security Software Discovery	T1213 Data from Information Repositories	T1210 Exploitation of Remote Services	T1041 Exfiltration Over C2 Channel
T1486 Data Encrypted for Impact	T1033 System Owner/User Discovery	T1497 Virtualization/Sandbox Evasion	T1012 Query Registry

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	B8313A185528F7D4F62853A44B64C29621627AE7 8B95902B2C444BCDCCB8A481159612777F82BAD1 3E10A3A2BE17DCF8E79E658F7443F6C3C51F8803 A7BD58C86CF6E7436CECE692DA8F78CEB7BA56A0 6B5F7659CE48FF48F6F276DC532CD458BF15164C
URLs	hxxps[:]//gmall-52fb5-default-rtdb.asia-southeast1.firebasedatabase[.]app/ hxxps[:]//go0gle-service-default-rtdb.firebaseio[.]com/ hxxps[:]//graph.microsoft[.]com/beta/users/3517e816-6719-4b16-9b40-63cc779da77c/mailFolders hxxps[:]//www.dropbox[.]com/s/6a8u8wlpvv73fe4/ hxxps[:]//www.dropbox[.]com/s/hbc5yz8z116zbi9/ hxxps[:]//socialmsdnmicrosoft.azurewebsites[.]net/AAA/ hxxps[:]//socialmsdnmicrosoft.azurewebsites[.]net/ABB/ hxxps[:]//socialmsdnmicrosoft.azurewebsites[.]net/ABB/ hxxps[:]//socialmsdnmicrosoft.azurewebsites[.]net/AMA/ hxxps[:]//socialmsdnmicrosoft.azurewebsites[.]net/AS/ hxxps[:]//akam.azurewebsites[.]net/api/File/Upload
IPV4	193.29.56[.]122

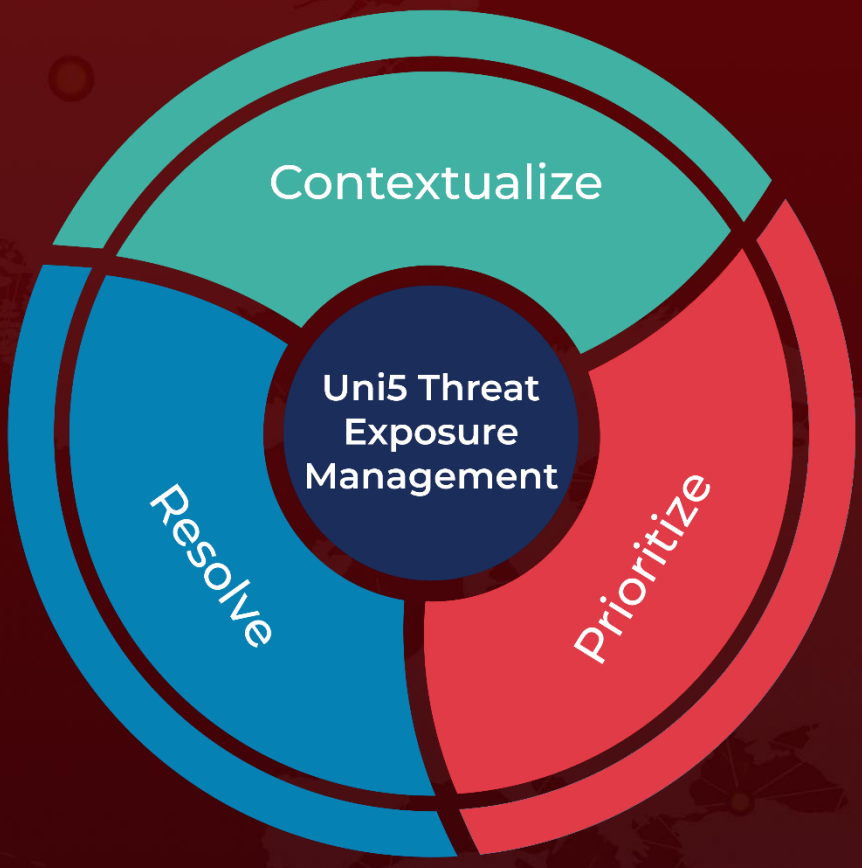
References

https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 21, 2023 . 4:15 AM

More at www.hivepro.com