Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

State-Sponsored Hackers Target Middle Eastern and African Governments

Date of Publication	Admiralty Code	TA Number
June 20, 2023	A2	TA2023271

Summary

First appeared: June 2023
Attack Region: Middle East and Africa
Targeted Sectors: Government.
Attack: Persistent cyber-espionage attacks, targeting governmental entities in the Middle East and Africa, have been unleashed by a group known as CL-STA-0043. This group has employed unprecedented methods to infiltrate networks.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 Governmental entities in the Middle East and Africa have become the targets of persistent cyber-espionage assaults, employing unprecedented and uncommon methods to steal credentials and extract Exchange emails. The collective responsible for these attacks is tracked CL-STA-0043 (where "CL" denotes cluster and "STA" represents state-sponsored motivation).

#2 The infection chain is set in motion through the exploitation of vulnerable on-premises Internet Information Services (IIS) and Microsoft Exchange servers, facilitating the infiltration of target networks. Once inside, the assailants embarked on a process of reconnaissance, meticulously mapping the network and identifying critical resources. Their primary goal revolved around locating administrative accounts.

#3 In their pursuit of this information, the attackers made attempts to employ various tools such as the Ladon web scanning tool, custom network scanners, Nbtscan, and Portscan. Notably, CL-STA-0043 employed a relatively new suite of penetration testing tools known as "Yasso." Among the intriguing techniques observed in these attacks was the precise exfiltration of targeted data from compromised Exchange servers.

#4 A variation of this method had previously been reported as being utilized by Hafnium. This activity involves the exploitation of the Exchange Management Shell or PowerShell scripts to pilfer emails and PST files that match specific keywords deemed important by the threat actors.

Recommendations

Strengthen on-premises security: Enhance the security of Internet Information Services (IIS) and Microsoft Exchange servers to mitigate vulnerabilities and reduce the risk of unauthorized access.

Implement comprehensive network monitoring: Deploy advanced monitoring systems to detect and respond to cyber-espionage attacks, including reconnaissance activities, in real time. This will help identify and neutralize threats before they can exploit critical resources.

Enforce robust email security practices: Implement stringent measures to protect against targeted email attacks, such as spear-phishing and credential theft. This includes enforcing multi-factor authentication, email encryption, and regular security awareness training for employees to enhance their email security hygiene.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0010 Exfiltration	TA0011 Command and Control	T1059 Command and Scripting Interpreter	T1129 Shared Modules
T1055 Process Injection	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1497 Virtualization/Sandbox Evasion
T1497.001 System Checks	T1082 System Information Discovery	T1083 File and Directory Discovery	T1124 System Time Discovery
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1590 Gather Victim Network Information	T1190 Exploit Public-Facing Application
T1543 Create or Modify System Process	T1068 Exploitation for Privilege Escalation	T1212 Exploitation for Credential Access	T1010 Application Window Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6b37aec6253c336188d9c8035e90818a139e3425c6e590734f309bd45021f980 77a3fa80621af4e1286b9dd07edaa37c139ca6c18e5695bc9b2c644a808f9d60 73b9cf0e64be1c05a70a9f98b0de4925e62160e557f72c75c67c1b8922799fc4 E781ce2d795c5dd6b0a5b849a414f5bd05bb99785f2ebf36edb70399205817ee 0f22e178a1e1d865fc31eb5465afbb746843b223bfa0ed1f112a02ccb6ce3f41 291bc4421382d51e9ee42a16378092622f8eda32bf6b912c9a2ce5d962bcd8f4 aa99ae823a3e4c65969c1c3aa316218f5829544e4a433a4bab9f21df11d16154 ddcf878749611bc8b867e99d27f0bb8162169a8596a0b2676aa399f0f12bcbd7 bcd2bdea2bfecd09e258b8777e3825c4a1d98af220e7b045ee7b6c30bf19d6df

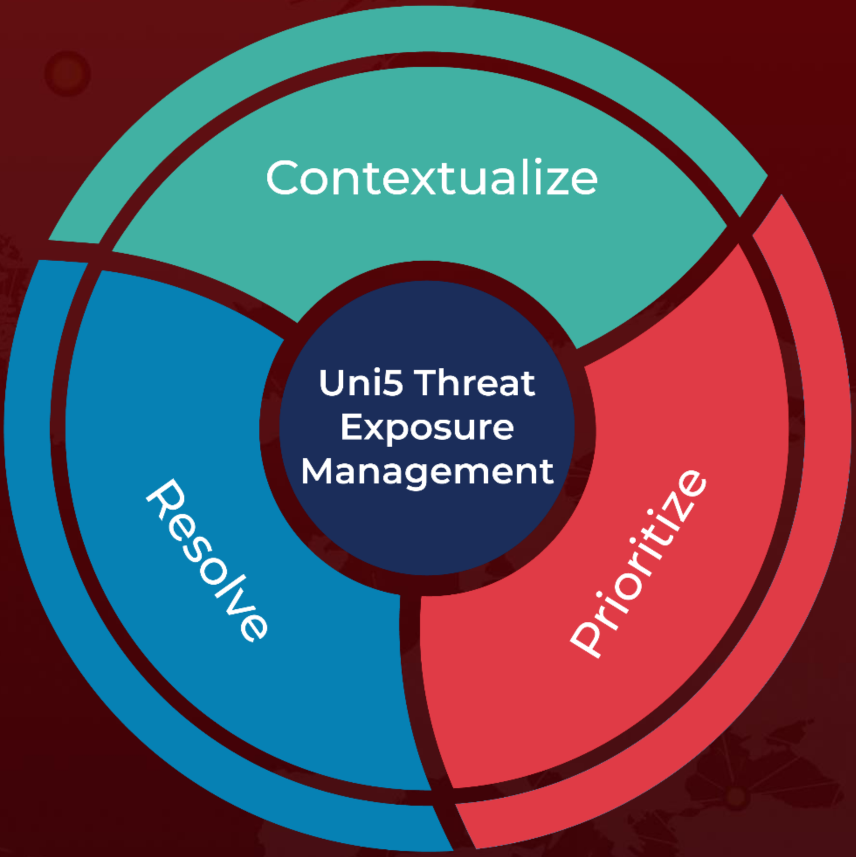
References

https://www.paloaltonetworks.com/blog/security-operations/through-the-cortex-xdr-lens-uncovering-a-new-activity-group-targeting-governments-in-the-middle-east-and-africa/#post-296259-_3tgjtn57dmzm

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

June 20, 2023 • 6:57 AM

More at www.hivepro.com