Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

PowerExchange Backdoor and Web Shells Breach at UAE Government Agency

Date of Publication	Admiralty Code	TA Number
May 26, 2023	A1	TA2023247

Summary

First appeared: April, 2023
Attack Region: UAE
Affected Platform: Windows
Malware: PowerExchange
Targeted Industry: Government
Attack: A high-severity attack targeted a UAE government agency, utilizing a custom PowerShell backdoor named PowerExchange and web shells on Microsoft Exchange servers.

Attack Regions

Attack Details

#1 A series of attacks targeted a government agency in the United Arab Emirates, involving the use of several known threats and a custom PowerShell-based backdoor called PowerExchange. The attacks were attributed to an Iranian threat actor, and the severity level was considered high. The infection chain started with email phishing, where a user opened a malicious zip file containing a disguised executable file.

#2 This dropper installed and executed the final payload, which created a persistent backdoor on the compromised system. The PowerExchange backdoor utilized the Exchange Web Services (EWS) API to connect to the victim's Microsoft Exchange server, enabling communication through email-based commands. The backdoor supported various commands for data exfiltration and executing further malicious actions.

#3 The investigation also uncovered the presence of other implants, such as web shells, on Microsoft Exchange servers and domain controllers. The web shells, including ExchangeLeech, had the capability to harvest credentials and execute commands. The attack is believed to have been carried out by the suspected threat actor APT34.

Recommendations

Patch and update systems: Regularly apply security patches and updates to all software and systems, including Windows platforms and Microsoft Exchange servers. Promptly addressing known vulnerabilities can prevent attackers from exploiting them.

Enhance email security measures: Strengthen email security by implementing robust spam filters, anti-phishing technologies, and email filtering solutions. Train employees to recognize and report suspicious emails, particularly those with malicious attachments or links.

Implement network monitoring and access controls: Deploy comprehensive network monitoring tools and intrusion detection systems to detect any unusual or malicious activity. Monitor Exchange server logs and network traffic for signs of compromise. Enforce strong access controls, such as least privilege, to restrict unauthorized access to critical systems.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1007 System Service Discovery
T1204 User Execution	T1566 Phishing	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1505 Server Software Component	T1083 File and Directory Discovery	T1505.003 Web Shell	T1132 Data Encoding
T1132.001 Standard Encoding	T1041 Exfiltration Over C&C Channel	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1566.001 Spearphishing Attachment	T1204.002 Malicious File	T1053 Scheduled Task/Job	T1053.005 Scheduled Task
T1059.001 Powershell	T1036 Masquerading	T1036.004 Masquerade Task or Service	T1036.005 Match Legitimate Name or Location
T1135 Network Share Discovery	T1570 Lateral Tool Transfer		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	f18575065970ef36e613ffa046f381fe9b01b3e9 2ba23d9115fb1c1d4c5899d34dc4772631d77eda 2b995ce4656db7257451080111705d5b98b45df3 68299DF5D8CE52845A8FC10598F138840094181C d82aad3222664ec9fb112808dfabbb56de9aa770 70aaa46784a2abd8af5628cb94f876d57fe8d154 fd3750d809f6ff9cf2b49d7a63f8f3fa0a457f61

TYPE	VALUE
File Path	C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Handler\ v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]Handler[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]Roles\ v4[.]0_1[.]0[.]0[.]0_9cbc39238c01012f\System[.]Web[.]Roles[.]dll C:\Users\Public\System[.]Web[.]Handler[.]dll C:\Windows\temp\temp[.]ps1 C:\Users\Public\temp[.]ps1 C:\Windows\System32\System[.]Web[.]TransportClient[.]dll C:\Windows\System32\inetsrv\System[.]Web[.]TransportClient[.]dll C:\Windows\Mirosoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]TransportClient\ v4[.]0_1[.]0[.]0[.]0__9cbc39238c01012f\System[.]Web[.]TransportClient[.]dll C:\Windows\Microsoft[.]NET\assembly\GAC_MSIL\System[.]Web[.]ServiceAuthentication\ v4[.]0_1[.]0[.]0[.]0__ff08ceb7abd6adf3\System[.]Web[.]ServiceAuthentication[.]dll C:\Users\Public\MicrosoftEdge\autosave[.]exe C:\Users\Public\MicrosoftEdge\wsdl[.]ps1 C:\Users\Public\MicrosoftEdge\Microsoft[.]Exchange[.]WebServices[.]dll C:\Users\Public\MicrosoftEdge\config[.]conf
URLs	hxxps://enmckkb0t0v3[.]x[.]pipedream[.]net?n=my
File Name	Brochure[.]zip Brochure[.]exe MicrosoftEdgeUpdateService

References

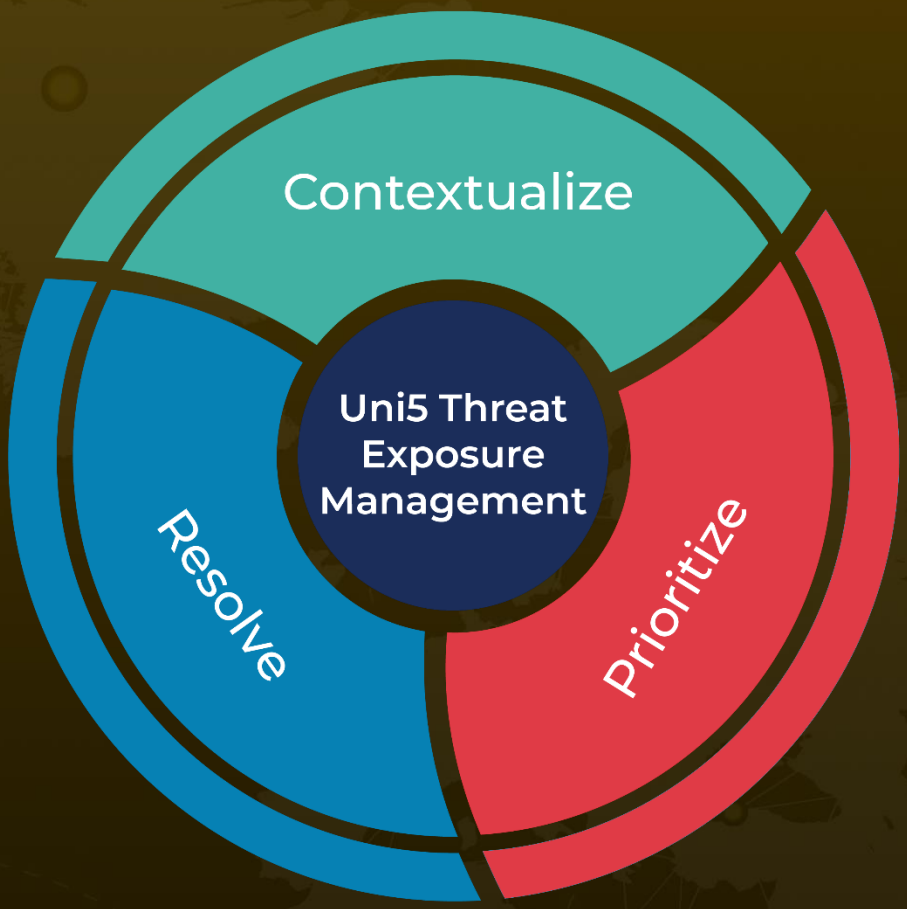
https://www.bleepingcomputer.com/news/security/new-powerexchange-malware-backdoors-microsoft-exchange-servers/

https://www.blackhatethicalhacking.com/news/hackers-use-new-powerexchange-malware-to-target-microsoft-exchange-servers/

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

May 26, 2023 • 4:30 AM

More at www.hivepro.com