Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

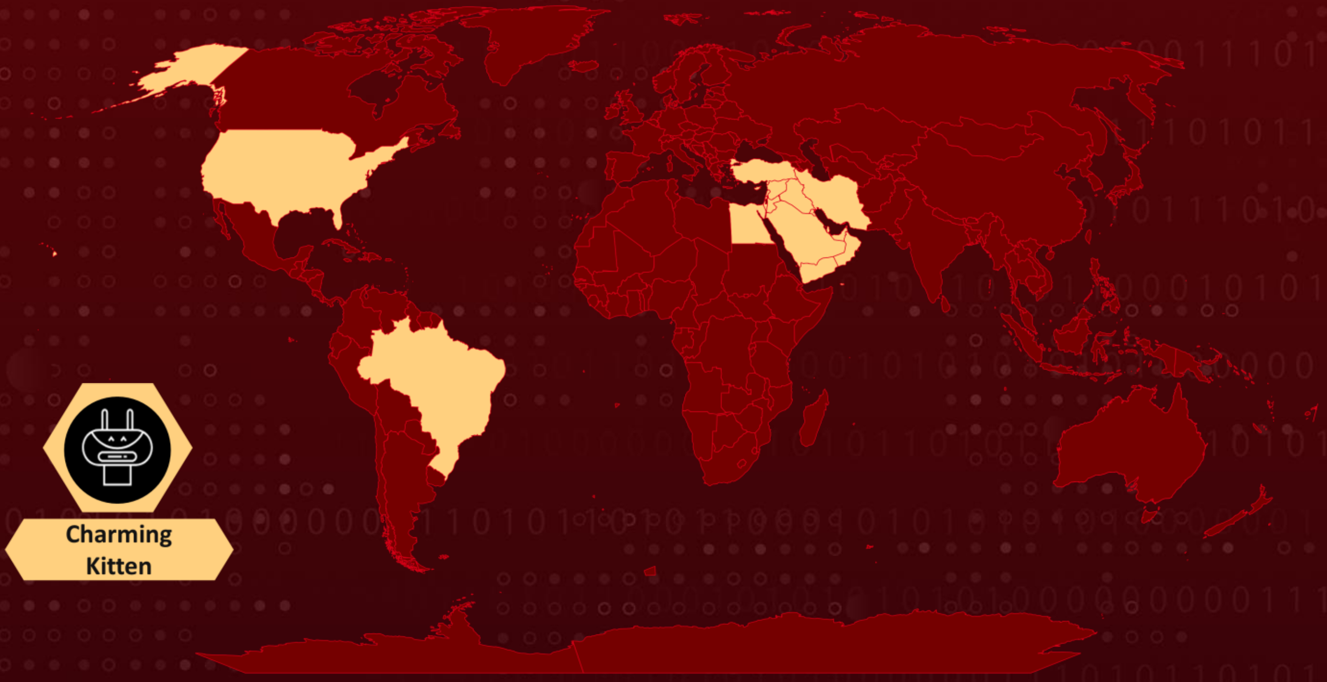
Charming Kitten's 'Sponsor' Strikes 34 Organizations in Brazil, Israel, and U.A.E

Date of Publication	Admiralty Code	TA Number
September 12, 2023	A1	TA2023367

Summary

Attack Began: March 2021
Malware: Sponsor Backdoor
Threat Actor: Charming Kitten (aka Ballistic Bobcat, Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, Charming Kitten, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)
Targeted Industries: Automotive, Communications, Engineering, Financial Services, Healthcare, Insurance, Law, Manufacturing, Retail, Technology, Telecommunications, Research, Education, Government, Media, and Pharmaceuticals
Attack Region: Brazil, the Middle East, and the United States.
Attack: Charming Kitten, also known as Ballistic Bobcat, orchestrated a sophisticated campaign aimed at 34 diverse targets across Brazil, Israel, and the United Arab Emirates. This operation employed a novel backdoor, which was identified as 'Sponsor'.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✓	✓	✓

Attack Details

#1 The Iranian threat actor, widely recognized as Charming Kitten (also known by aliases such as Ballistic Bobcat, Magic Hound, and APT 35), has been associated with a recent surge of cyberattacks spanning from March 2021 to June 2022. These attacks were directed towards 34 distinct entities, primarily situated in Brazil, Israel, and the United Arab Emirates.

#2 The adversaries leveraged a previously undisclosed backdoor, aptly named 'Sponsor,' which specifically targeted educational institutions, government agencies, and healthcare organizations, along with individuals such as human rights activists and journalists.

#3 Charming Kitten gained initial access by exploiting well-documented vulnerabilities (CVE-2021-26855) in publicly accessible Microsoft Exchange servers. This was preceded by thorough system and network scans to identify potential vulnerabilities, which were subsequently exploited.

#4 Throughout the Sponsoring Access campaign, Charming Kitten deployed an array of open-source tools like RevSocks, Mimikatz, and Plink, which facilitated activities such as data exfiltration, system monitoring, network infiltration, and maintaining access to compromised systems. Batch files were also deployed to the victims' systems prior to implementing the Sponsor backdoor.

#5 The Sponsor backdoor developed in C++, is engineered to collect host information and execute instructions received from a remote server. The results of these operations are then relayed back to the controlling server, encompassing tasks such as command execution, file downloads, and the update of a roster of attacker-controlled servers.

#6 The Sponsor backdoor harnesses Windows APIs to obtain current usernames and gather system data such as the operating system build and power source status, which is subsequently transmitted to the command-and-control server via port 80. Charming Kitten continues to operate according to a scan-and-exploit model, diligently seeking out potential targets with unpatched vulnerabilities in publicly exposed Microsoft Exchange servers.

Recommendations

Update Out-of-Support Versions: If you are using an older or out-of-support version of Exchange Server, Microsoft has released patches for these versions too. Prioritize the installation of the appropriate patches or updates for your specific Exchange Server version.

Application Whitelisting: Consider implementing application whitelisting to allow only authorized applications to run on systems, reducing the risk of unapproved malware like Sponsor Backdoor executing.

Implement Granular Access Controls: Establish fine-grained access controls that align with user roles and responsibilities. This approach ensures that users only have access to the specific resources necessary for their tasks, reducing the risk of unauthorized access.

Real-time Monitoring and Compliance Checks: Implement real-time monitoring and compliance checks within your Web Application Firewall (WAF) to promptly identify, respond to, and mitigate suspicious or malicious activities targeting the Exchange Server while ensuring alignment with industry regulations and internal security standards.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	T1595 Active Scanning
T1587.001 Malware	T1588.002 Tool	T1190 Exploit Public-Facing Application	T1059.003 Windows Command Shell
T1569.002 Service Execution	T1543.003 Windows Service	T1078.003 Local Accounts	T1140 Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information	T1555.003 Credentials from Web Browsers	T1018 Remote System Discovery	T1001 Data Obfuscation

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	098b9a6ce722311553e1d8ac5849ba1dc5834c52, 5aee3c957056a8640041abc108d0b8a3d7a02ebd, 764eb6ca3752576c182fc19cff3e86c38dd51475, 2f3eda9d788a35f4c467b63860e73c3b010529cc, e443dc53284537513c00818392e569c79328f56f, c4bc1a5a02f8ac3cf642880dc1fc3b1e46e4da61, 39ae8ba8c5280a09ba638df4c9d64ac0f3f706b6, a200be662cdc0ece2a2c8fc4dbbc8c574d31848a, 5d60c8507ac9b840a13ffdf19e3315a3e14de66a, 50cfb3cf1a0fe5ec2264ace53f96fadfe99cc617, 1aae62acee3c04a6728f9edc3756fabd6e342252, 519ca93366f1b1d71052c6ce140f5c80ce885181, 4709827c7a95012ab970bf651ed5183083366c79, 99c7b5827df89b4fafc2b565abed97c58a3c65b8, e52aa118a59502790a4dd6625854bd93c0deaf27
File Path	%SYSTEMDRIVE%\inetpub\wwwroot\aspnet_client\, %USERPROFILE%\AppData\Local\Temp\file\, %USERPROFILE%\AppData\Local\Temp\2\low\, %USERPROFILE%\Desktop\, %USERPROFILE%\Downloads\a\, %WINDIR%\, %WINDIR%\INF\MSExchange Delivery DSN\, %WINDIR%\Tasks\, %WINDIR%\Temp\%WINDIR%\Temp\crashpad\1\Files
IPv4	162.55.137[.]20, 37.120.222[.]168, 198.144.189[.]74, 5.255.97[.]172

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855

Recent Breaches

https://www.gilead.com/
https://www.who.int/

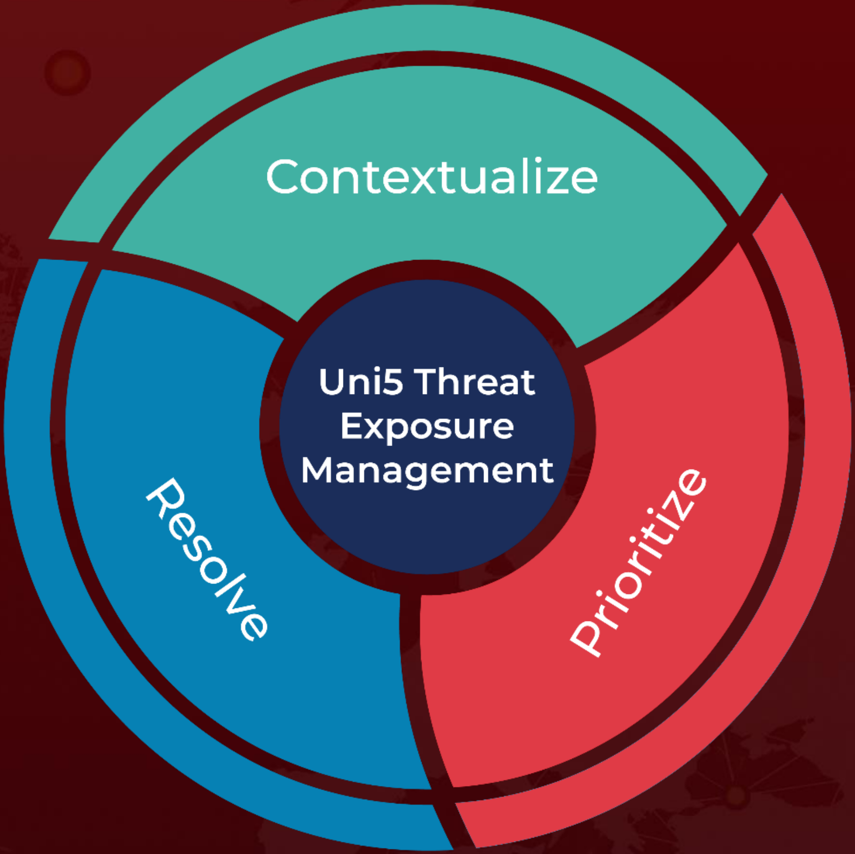
References

https://www.welivesecurity.com/en/eset-research/sponsor-batch-filed-whiskers-ballistic-bobcats-scan-strike-backdoor/

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

September 12, 2023 • 10:30 PM

More at www.hivepro.com