Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Charming Kitten's Latest Malware Arsenal and Targeting Strategies

Date of Publication	Admiralty Code	TA Number
July 07, 2023	A1	TA2023291

Summary

First Appearance: May 2023
Attack Region: Middle East, United States
Actor Name: Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, TarhAndishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)
Affected Platform: macOS, Windows
Malware: GorjolEcho, NokNok, CharmPower (also known as GhostEcho or POWERSTAR), BellaCiao
Targeted Industries: Foreign affairs, Think Tanks, and Nuclear security
Attack: Charming Kitten, an adaptable threat actor, has shifted to new malware tactics and targets by employing LNK infection chains and utilizing cloud hosting providers. This evolution in their approach poses a significant threat in the realm of cyber espionage.

Attack Regions

Attack Details

#1

Charming Kitten, also known as Magic Hound, APT 35, TA453, is an active and highly adaptable threat actor that has recently made significant changes to its malware tactics and targeting strategies. One notable development is its shift from using Microsoft Word documents with macros to LNK infection chains.

#2

To achieve its goals of unauthorized reconnaissance, Charming Kitten has been employing sophisticated techniques such as benign messages and multi-persona impersonation. It specifically targets experts in Middle Eastern affairs and nuclear security, leveraging timely events like the JCPOA negotiations to gather intelligence and influence foreign policies.

#3

Charming Kitten's adaptability is evident in its use of cloud hosting providers to deliver malware. By leveraging platforms like Google Scripts, Dropbox, and CleverApps, the threat actor aims to complicate tracking and minimize the chances of detection by threat hunters. This multi-cloud approach demonstrates Charming Kitten's determination and the effort it invests in targeting victims.

#4

A new PowerShell backdoor called GorjolEcho is deployed through Charming Kitten's novel infection chain and establishes persistence on compromised systems. GorjolEcho enables the threat actor to conduct intrusive activities such as information exfiltration and potential module downloads for espionage purposes. It represents Charming Kitten's latest iteration in collecting intelligence from highly targeted individuals.

#5

In addition to GorjolEcho, Charming Kitten has also developed a Mac-specific infection chain named NokNok. This demonstrates the threat actor's adaptability and determination to target victims across different platforms. NokNok believed to be a port or evolution of GorjolEcho, serves as an initial foothold for Charming Kitten's intrusions on Mac systems.

#6

Charming Kitten is associated with Iran's Islamic Revolutionary Guard Corps (IRGC) and has been operating since around 2011. Recently, Volexity drew attention to their usage of an upgraded variant of a Powershell implant called CharmPower (also known as GhostEcho or POWERSTAR). In another instance, Charming Kitten was accused of deploying a fresh strain of malware named BellaCiao, which targeted multiple victims across the United States, Europe, the Middle East, and India during April.

Recommendations

Enhanced Email Security: Strengthen Email Security: Enhance email security measures to combat Charming Kitten's use of benign messages. Implement advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts.

Deploy Endpoint Protection: Utilize robust endpoint protection solutions that include behavior-based detection, advanced malware scanning, and real-time threat intelligence. Regularly update and patch operating systems and applications to address known vulnerabilities exploited by Charming Kitten.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0011 Command and Control	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0001 Initial Access	TA0009 Collection	TA0008 Lateral Movement
TA0011 Command and Control	TA0043 Reconnaissance	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1059 Command and Scripting Interpreter	T1590 Gather Victim Network Information	T1547 Boot or Logon Autostart Execution	T1082 System Information Discovery
T1218 System Binary Proxy Execution	T1102 Web Service	T1566 Phishing	T1036 Masquerading
T1204 User Execution	T1059.005 Visual Basic	T1204.001 Malicious Link	T1059.001 PowerShell
T1055 Process Injection	T1547.009 Shortcut Modification	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information
T1059.007 JavaScript	T1132.001 Standard Encoding	T1132 Data Encoding	T1071.001 Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	144.217.129[.]176
Host Name	library-store[.]camdvr[.]org, filemanager.theworkpc[.]com, fuschia-rhinestone.cleverapps[.]io
SHA256	464c5cd7dd4f32a0893b9fff412b52165855a94d193c08b114858430c26a9f1d, ddead6e794b72af26d23065c463838c385a8fdff9fb1b8940cd2c23c3569e43b, 1fb7f1bf97b72379494ea140c42d6ddd53f0a78ce22e9192cfba3bae58251da4, e98afa8550f81196e456c0cd4397120469212e190027e33a1131f602892b5f79, 5dc7e84813f0dae2e72508d178aed241f8508796e59e33da63bd6b481f507026, b6916b5980e79a2d20b4c433ad8e5e34fe9683ee61a42b0730effc6f056191eb, acfa8a5306b702d610620a07040262538dd59820d5a42cf01fd9094ce5c3487c

References

https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware

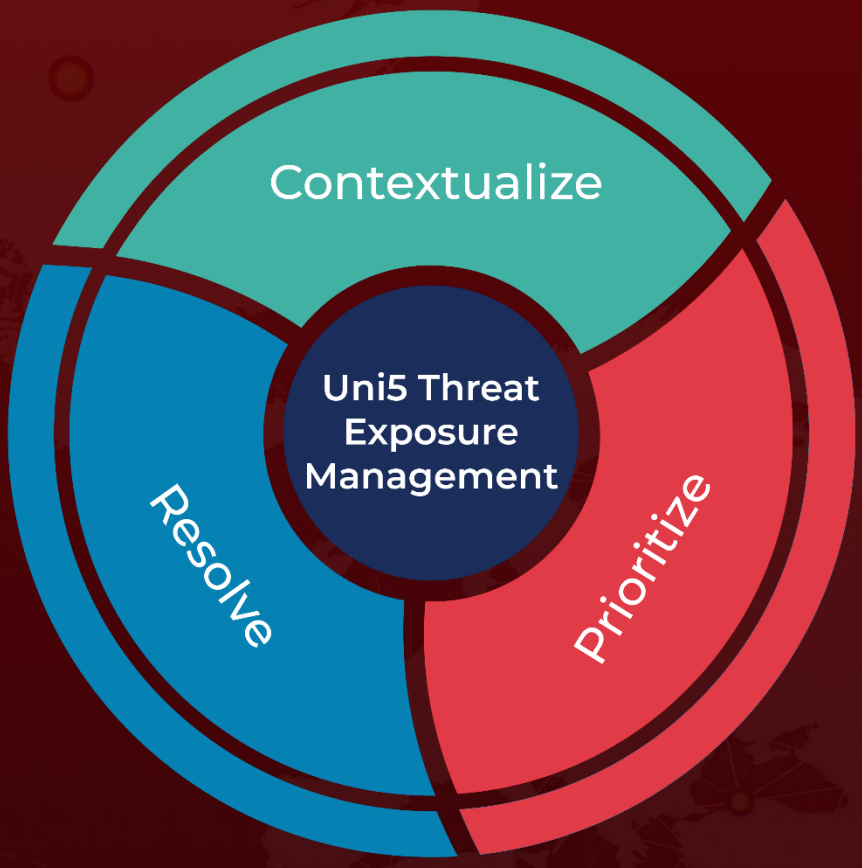
https://www.hivepro.com/charming-kitten-hackers-utilize-new-tactics-with-bellaciao-malware/

https://www.hivepro.com/iranian-apts-new-data-extraction-tool-hyperscrape/

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

July 07, 2023 • 5:30 AM

More at www.hivepro.com