Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

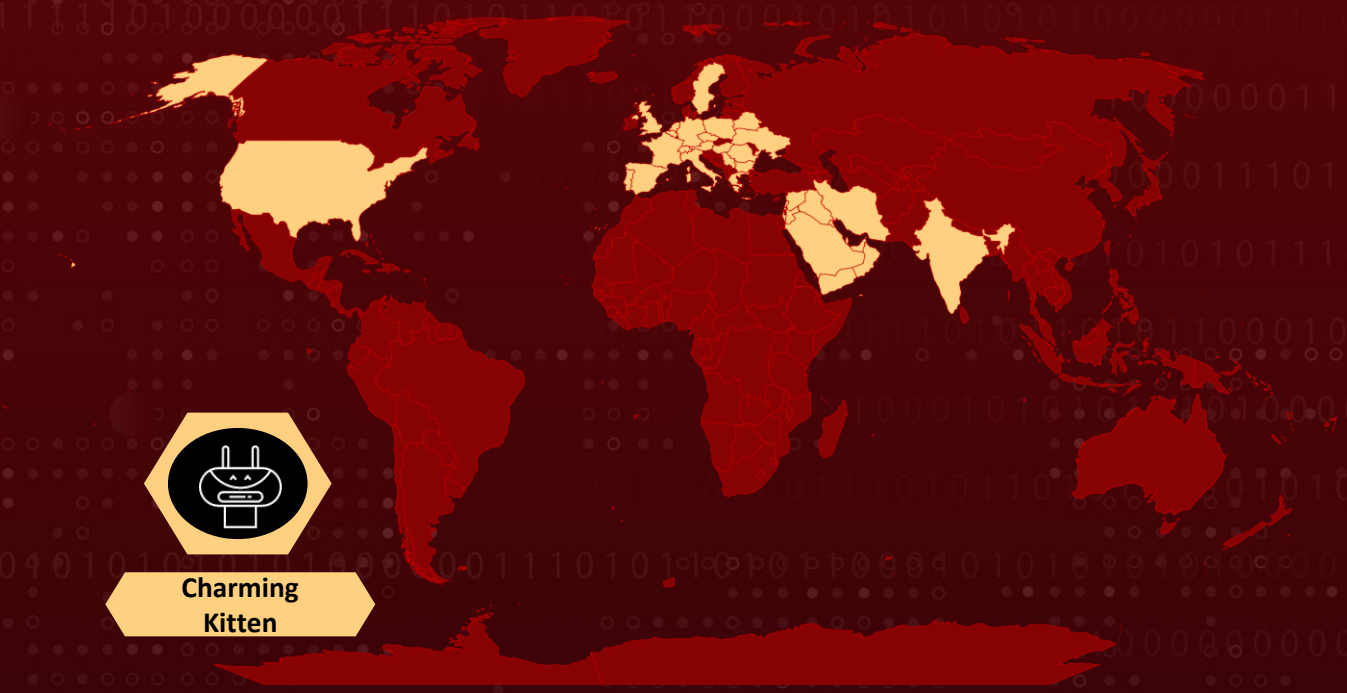
Charming Kitten Hackers Utilize New Tactics with BellaCiao Malware

Date of Publication	Admiralty Code	TA Number
April 27, 2023	A1	TA2023201

Summary

First Appearance: June 21, 2020
Threat Actor: Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)
Target Countries: US, Europe, the Middle East, and India.
Malware: BellaCiao, tailored
Target Industries: Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications
Attack: Iranian APT group, Charming Kitten, is using a new, sophisticated malware called BellaCiao to target specific victims in multiple regions, employing unique communication tactics with its command-and-control infrastructure.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	PATCH	Zero-day	CISA KEV
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	Zoho ManageEngine	✓	✗	✓

Attack Details

#1 The Charming Kitten group, an Iranian state-sponsored advanced persistent threat (APT) group associated with the Islamic Revolutionary Guard Corps (IRGC), has modernized its tactics, techniques, and procedures. The group has been using a new, complex, and tailored malware called BellaCiao to target specific victims in the US, Europe, the Middle East, and India.

#2 The malware exhibits a unique communication approach with its command-and-control infrastructure. Charming Kitten is exploiting publicly disclosed proof-of-concepts (PoCs) quickly to achieve its goals, using automated scanners to discover and compromise vulnerable systems.

#3 Threat actors identify a remote code execution vulnerability that impacts as many companies as possible, and using automated scanners, vulnerable systems are discovered and automatically compromised (spray-and-pray tactic). The malicious payload is typically a webshell to enable remote administration access.

#4 The initial (opportunistic and fully automated) compromise is followed by a manual triage phase to determine the best approach to benefit from an attack. The group also uses custom-developed malware named “tailored” to evade detection, making it more challenging to detect and defend against its attacks.

Recommendations

BellaCiao malware is often delivered through software vulnerabilities, so it's crucial to keep your software and systems up-to-date with the latest security patches. Regularly check for updates from the software vendor and install them as soon as they become available.

Implement a defense-in-depth architecture that involves multiple layers of security measures to protect against a variety of threats, including modern attacks such as the BellaCiao malware. This approach should involve reducing the attack surface by limiting entry points and promptly patching vulnerabilities.

Use multi-layered security measures, implement multi-layered security measures to reduce the risk of BellaCiao malware infecting your systems. This includes using anti-virus and anti-malware software, firewalls, intrusion detection and prevention systems, and strong access controls.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0010 Exfiltration	TA0005 Defense Evasion	TA0001 Initial Access
T1071.001 Web Protocols	T1071 Application Layer Protocol	T1190 Exploit Public-Facing Application	T1027 Obfuscated Files or Information
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1584 Compromise Infrastructure	T1203 Exploitation for Client Execution
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1059.001 Power Shell	T1071.004 DNS
T1104 Multi-Stage Channels	T1505 Server Software Component	T1505.003 Web Shell	T1048 Exfiltration Over Alternative Protocol
T1505 Server Software Component	T1036 Masquerading	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	284cdf5d2b29369f0b35f3ceb363a3d1 2daa29f965f661405e13b2a10d859b87 3fbea74b92f41809f46145f480782ef9 5a487c41efa2f3055d641591d601977c 7df50cb7d4620621c2246535dd3ef10c 95c6fdc4f537bccca3079d94e65bc0b0 c450477ed9c347c4c3d7474e1f069f14 c6f394847eb3dc2587dc0c0130249337 e7149c402a37719168fb739c62f25585 f56a6da833289f821dd63f902a360c31

TYPE	VALUE
SHA256	2aa1bbbe47f04627a8ea4e8718ad21f0d50adf6a32ba4e6133ee46ce2cd13780 ca57391cdbac224f159e858425d231d068aa76316e0345cb8d58c716b9eff587
SHA1	736ba9daf63a2add3217c79fa9d83088358f7012
Domains	mail-updateservice[.]info maill-support[.]com mailupdate[.]com mailupdate[.]info msn-center[.]uk msn-service[.]co twittsupport[.]com
IPV4	188[.]165[.]174[.]199 88[.]80[.]148[.]162

Patch Links

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

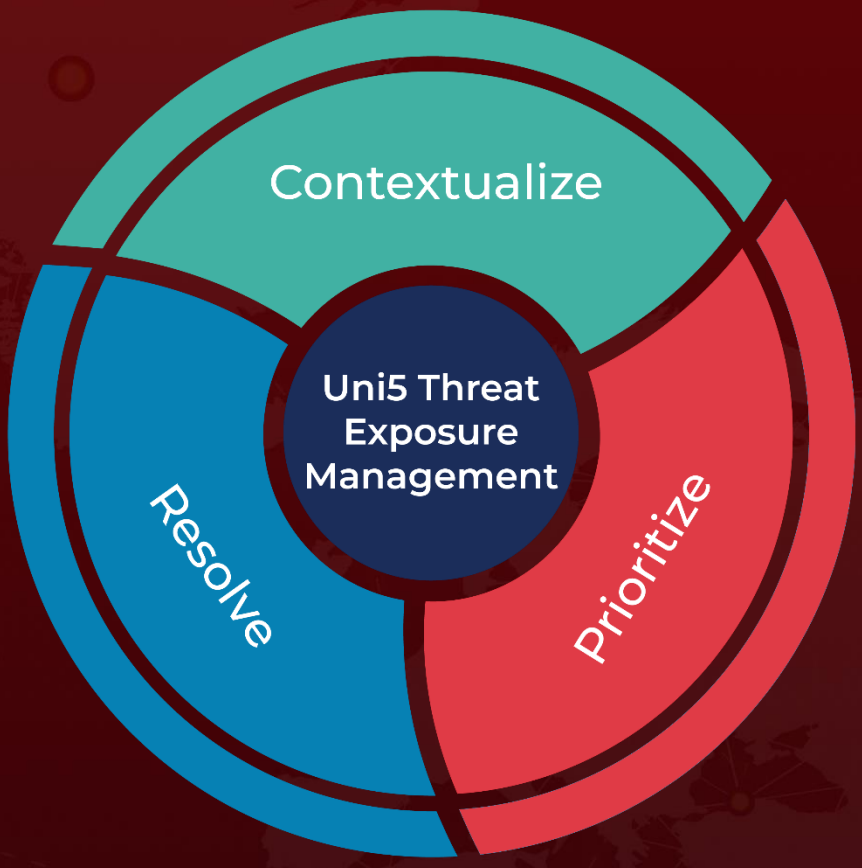
References

https://businessinsights.bitdefender.com/unpacking-bellaciao-a-closer-look-at-irans-latest-malware

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

April 27, 2023 • 2:30 AM

More at www.hivepro.com