Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

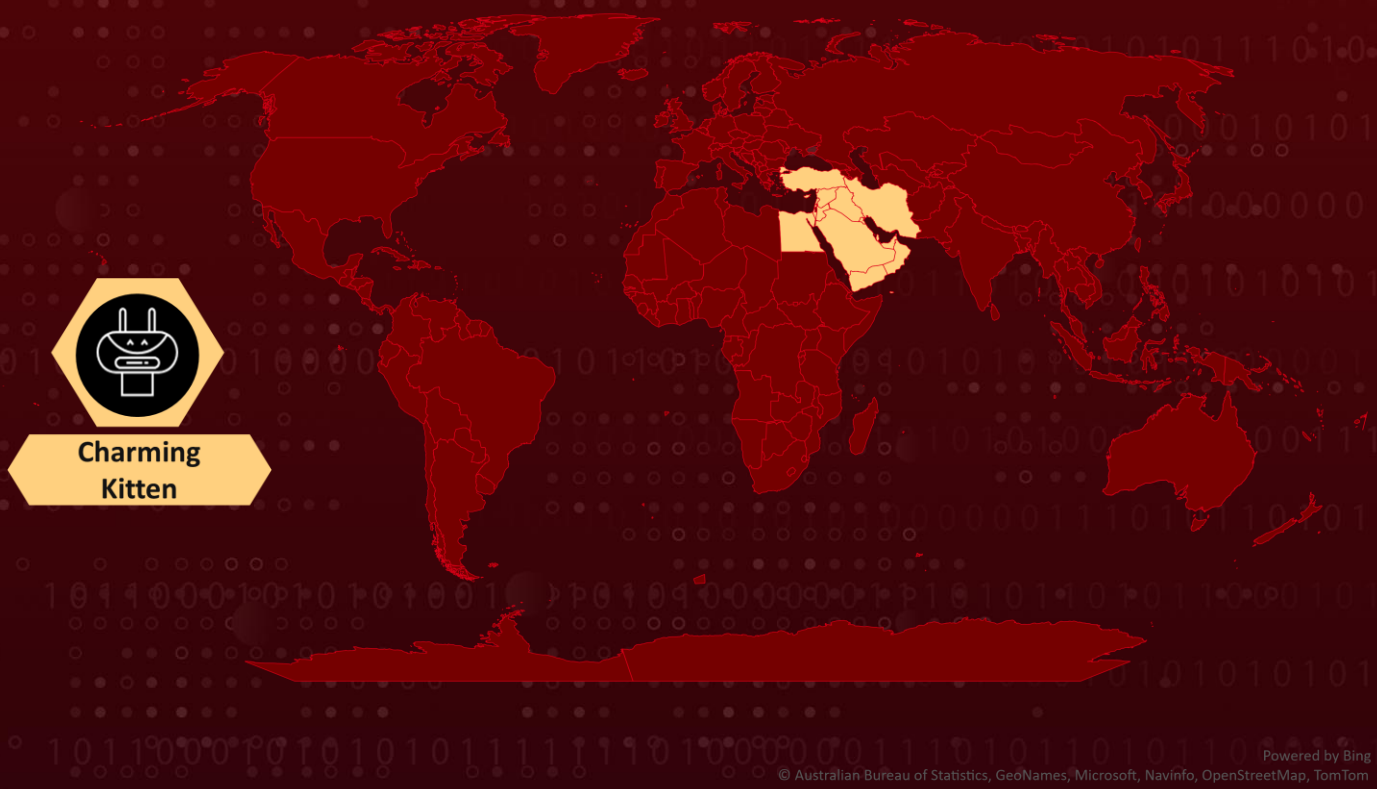
Iranian Threat Actor Adapts Tactics to Stay One Step Ahead

Date of Publication	Admiralty Code	TA Number
February 20, 2024	A2	TA2024065

Summary

Attack Commenced: January 2024
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, Ballistic Bobcat, CharmingCypress)
Malware: POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLASS
Attack Region: Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen
Targeted Industries: Politics, Government, Think Tanks, NGOs, Journalists
Attack: Charming Kitten, an Iranian threat actor, has recently been linked to a series of attacks targeting the Middle East. This campaign involves deploying a new backdoor called BASICSTAR through a deceptive webinar portal.

Attack Regions



Attack Details

#1 The Iranian threat actor, known as Charming Kitten (aka CharmingCypress, TA453, APT 35), has been implicated in a recent series of attacks targeting Middle East policy experts. This campaign involves the use of a new backdoor named BASICSTAR, implemented through the creation of a deceptive webinar portal.

#2 Charming Kitten employs sophisticated social-engineering tactics in its phishing efforts, engaging targets in lengthy email conversations before introducing links to malicious content. Depending on the victim's operating system, distinct applications are delivered. Windows users receive an infection chain culminating in the deployment of POWERLESS, a PowerShell backdoor featuring AES-encrypted command-and-control communication.

#3 This includes functionalities such as downloading additional executables for audio recording, browser information theft, persistence, and keylogging. Meanwhile, macOS victims experience an infection chain culminating in NOKNOK. Charming Kitten specifically targets high-profile individuals in the Middle East, utilizing malware like EYEGLASS capable of extracting sensitive information from compromised hosts.

#4 The group is believed to be affiliated with Iran's Islamic Revolutionary Guard Corps (IRGC). Charming Kitten persists in distributing various backdoors, showcasing its commitment to ongoing cyber operations. Despite the public exposure, Charming Kitten adapts its tactics and methods to maintain its cyber raid.

Recommendations

- **Email Security:** Implement robust email filtering solutions to detect and block phishing attempts, especially those involving deceptive webinar portals. Encourage the use of multi-factor authentication (MFA) to add an extra layer of security for email accounts.
- **Anomaly Detection:** Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.
- **Implement Network Security Measures:** Employ robust network security measures, including firewalls and intrusion detection/prevention systems, to help prevent unauthorized access and the spread of ransomware within the network.

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	T1555.003 Credentials from Web Browsers	T1018 Remote System Discovery	T1140 Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information	T1001 Data Obfuscation	T1566.002 Spearphishing Link	T1059.001 PowerShell
T1036 Masquerading	T1055 Process Injection	T1123 Audio Capture	T1105 Ingress Tool Transfer
T1070.004 File Deletion	T1204.002 Malicious File		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	ae67cd9c37127821e7768801dda7e8fb, c79d85d0b9175cb86ce032543fe6b0d5, 266305f34477b679e171375e12e6880f, c3fe93fc9133c0bc4b441798b9bcf151, 9b6c308f106e72394a89fac083de9934,

TYPE	VALUE
MD5	bd41c99df6945650727f871c6ed3f95b, 859a9e523c3308c120e82068829fab84, ac4e5a1df9c2ec889be088159e28ddb1, a2729e8e105b76808da741263fc394be
SHA1	e2ec9b77e3feb0c8f30f314ed15da2bbcde25ddc, 195e939e0ae70453c0817ebca8049e51bbd4a825, 607137996a8dc4d449185586ecfbe886e120e6b1, 87f36a0279b31a4a2f9b1123674e3dea130f1554, 27b38cf6667936c74ed758434196d2ac9d14deae, 1f16544eb41f4b5146cee457504b8b13d10a91e1, 5bdec05bdca8176ae67054a3a7dc8c5ef0ac8deb, 16f58fdb4443a963cea36de8c8500539e28d053d, 01966af573124d90608167a5d544ac59b6c994ea
SHA256	1690cff04de44a26440d4fd15d0a0c11f64d3db670607ef658938690436b6636, 37bb42720bfc1cf5d0e9d7b66be134b6431055ed8bdfd384f61ab7ac061d26eb, 2d99755d5cd25f857d6d3aa15631b69f570d20f95c6743574f3d3e3e8765f33c, 35f062f46f42dce06804cc4e7b456c528618d650edcf1cf7f806c016e88b3d19, f1ee5dd179f66f597edfeb4b2c73c6adb4b7b6d4dcfb0bef33ee5c285148d085, 1feade2bbd4dbc0b2052213d792b83c969928a150dce332746a6b5426ac93e4f, a8622dccb40a9fe9c2123f661e32e0a6bc40e95c88c9c2b764e603ce5eccb311, 42477f0236e648f6e981db279406ca5f2a37a26cdf2baf472c41cb7f85f046e8, 11f0e38d9cf6e78f32fb2d3376badd47189b5c4456937cf382b8a574dc0d262d, 9ef84d6a709adbd6f29813ee145dbf542a69150e5ab4261e0d58de7ee371a8ef, c6f91e5585c2cbbb8d06b7f239e30b271f04393df4fb81815f6556fa4c793bb0, f6f0f682668f78dbecfc30a0e0c76b6a3d86298869fb44b39adf19fdcdca5762, 1ffc0bb577e4605059143a5cca213fbe0762c320c74174fe3c2a8f4878c85fc0, 13b659e009577ab7890157ce00cc5c3641049f46135d5be2b1c17ca88a1490f9, fdc5d6caaaa4fb14e62bd42544e8bb8e9b02220e687d5936a6838a7115334c51, 07384ab4488ea795affc923851e00ebc2ead3f01b57be6bf8358d7659e9ee407,

TYPE	VALUE
SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f, 1e7d2390a64abf51291d58a4104341664ec3c4f9989e07bdf612ecbe53f1231c, b0f0aeded0aa68cfa17353faaf2093d35237758cdb668fff91f915092c9696ed, 10460becafe4a67b959d9eaa09fb391d4ed46c083843ca3ab28c36e803760e41, bd7db9d9617c6108ed363cc2622594e9fd6932ed2c25f403bd1cc83bc9a21a1d, cfd340b4b4b3698f87acd1bebe8bec3d3ff48bfd6513a73c9aa3975d2cfe84c3, ea308c76a2f927b160a143d94072b0dce232e04b751f0c6432a94e05164e716d, a288618325a42a22fc642a73c5f5a39409a229e7f7aedec0043839b1e1483266, 56cd102b9fc7f3523dad01d632525ff673259dbc9a091be0feff333c931574f7, e4e7f08d9a9a662b5615e8fcbb6cd3c711ecab6341a60562bbeff9ccca43f7e0, 8803b8faa6e6ee4c3cdf31b6d6b4af104be8650e2ff63a9b9818b3e2596fdc5b
IPv4	49[.]13[.]15[.]66, 144[.]217[.]117[.]74, 149[.]28[.]133[.]236
Domains	rasaneh-iiis[.]org, www[.]defaultbluemarker[.]info, beginningofgraylife[.]ddns[.]net, yellowparallelworld[.]ddns[.]net, defaultbluemarker[.]info, www[.]rasaaneh-iiis[.]org

References

https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/

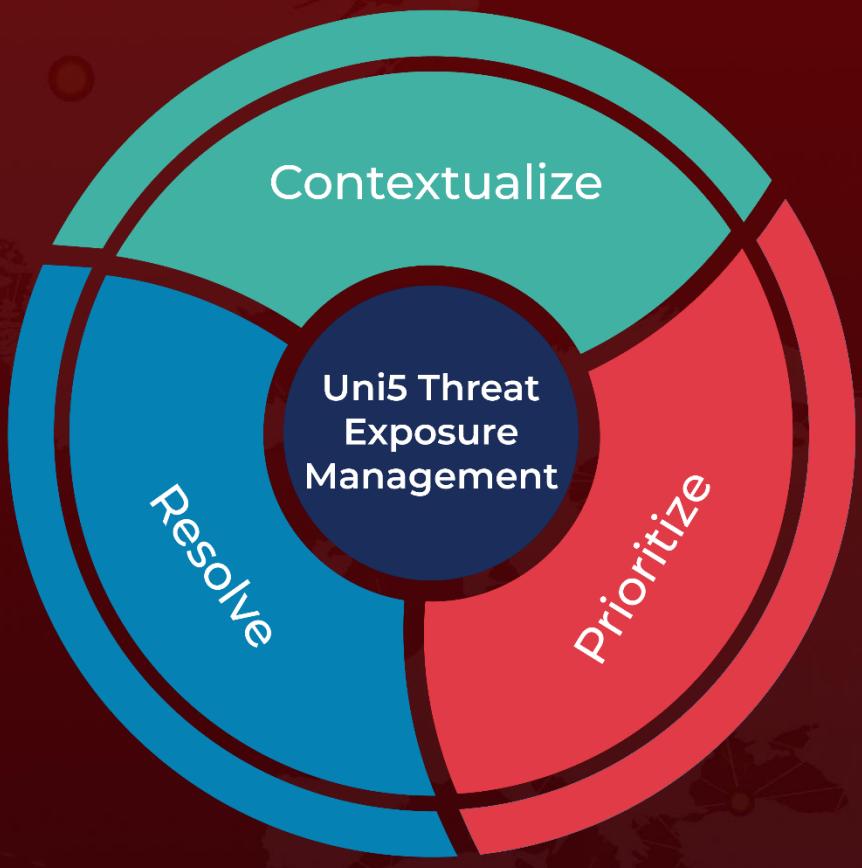
https://github.com/volexity/threat-intel/blob/main/2024/2024-02-13%20CharmingCypress/iocs.csv

https://www.hivepro.com/threat-advisory/charming-kittens-latest-malware-arsenal-and-targeting-strategies/

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

February 20, 2024 • 4:00 PM

More at www.hivepro.com