Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

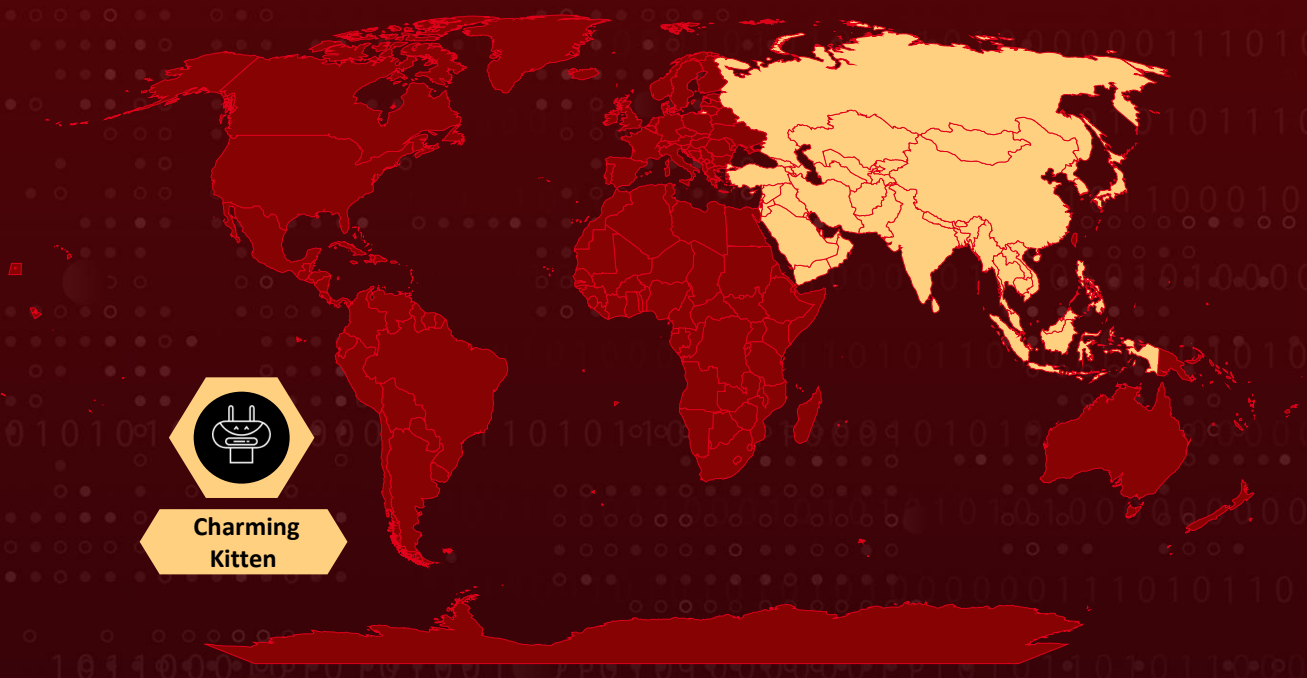
BellaCPP: The New C++ Variant of BellaCiao Malware

Date of Publication	Admiralty Code	TA Number
December 26, 2024	A1	TA2024473

Summary

Attack Began: 2024
Malware: BellaCiao, BellaCPP
Targeted Region: Asia
Affected Platform: Windows
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)
Attack: A new variant of the BellaCiao malware, called BellaCPP, has recently been identified, rewritten in C++ instead of its original .NET implementation. This shift highlights efforts by attackers to create more versatile and harder-to-detect malware. BellaCPP operates as a Windows service, using DLL files and domain generation algorithms to establish covert communication channels. Attributed to the Charming Kitten APT group, this variant underscores the need for robust cybersecurity measures to counter evolving threats.

Attack Regions



Attack Details

#1

Recently, researchers identified a new variant of the BellaCiao malware, called BellaCPP, rewritten in C++ instead of its original .NET implementation. This discovery highlights a shift in tactics by threat actors, demonstrating their efforts to create more versatile and difficult-to-detect malware. BellaCPP was first identified on a compromised system in Asia, where its predecessor, the .NET-based BellaCiao, had already been deployed. This suggests that the malware may be part of a coordinated and layered attack strategy.

#2

BellaCPP operates as a Windows service, leveraging a DLL file named "adhapl.dll." The malware installs itself in the C:\Windows\System32 directory and uses an export function called "ServiceMain" to execute its payload. It decrypts specific strings during runtime, loads a secondary DLL named "D3D12_1core.dll," and generates domain names based on predetermined patterns. These capabilities indicate that BellaCPP is designed to establish covert communication channels potentially for command-and-control purposes while evading detection.

#3

Researchers noted several similarities between BellaCPP and the original BellaCiao, particularly in their domain generation algorithms and network communication techniques. These overlaps, combined with evidence of both versions being found on the same machine, point toward their likely use by the Charming Kitten advanced persistent threat (APT) group. Charming Kitten, also known as Phosphorus or APT35, is widely believed to be linked to Iranian state-sponsored cyber operations. Researchers attribute this variant to the group with medium-to-high confidence based on its behavior and characteristics.

#4

The emergence of BellaCPP highlights the evolving threat landscape, where attackers are adopting new programming languages and methods to improve their malware's stealth and effectiveness. By rewriting the malware in C++, the attackers can better evade detection and analysis tools designed for .NET-based threats. This adaptation underscores the importance of robust cybersecurity measures, including behavioral analysis, network monitoring, and endpoint protection, to detect and mitigate such sophisticated attacks.

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint detection and response (EDR) solutions across all systems to detect and block suspicious activities, such as unauthorized DLL files or unusual service behaviors. These solutions should be configured to monitor for anomalies like the creation of hidden services or the loading of unknown DLLs.

Regularly Update and Patch Software: Ensure that all systems are kept up to date with the latest security patches and software updates. Attackers often exploit vulnerabilities in outdated software, so maintaining a proactive patch management strategy can minimize the risk of exploitation.

Network Monitoring and Threat Detection: Employ continuous network monitoring to detect any unusual or suspicious network traffic. In particular, monitor for domain-generation algorithms (DGAs) and other indicators of command-and-control (C2) communication commonly used by advanced persistent threats (APTs) like Charming Kitten.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**TA0010** Exfiltration	**TA0002** Execution	**TA0011** Command and Control
TA0003 Persistence	**T1059.001** PowerShell	**T1041** Exfiltration Over C2 Channel	**T1027** Obfuscated Files or Information
T1071.004 DNS	**T1071** Application Layer Protocol	**T1568.002** Domain Generation Algorithms	**T1568** Dynamic Resolution
T1543.003 Windows Service	**T1543** Create or Modify System Process	**T1059** Command and Scripting Interpreter	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	327a1f32572b4606ae19085769042e51, 34eb579dc89e1dc0507ad646a8dce8be, b3bde532cfbb95c567c069ca5f90652c, 29362dcdb6c57dde0c112e25c9706dcf, 882f2de65605dd90ee17fb65a01fe2c7, 5f4284115ab9641f1532bb64b650aad6, 0fea857a35b972899e8f1f60ee58e450, 20014b80a139ed256621b9c0ac4d7076, 7f0ee078c8902f12d6d9e300dabf6aed, 63647520b36144e31fb8ad7dd10e3d21, 8096e00aa7877b863ef5a437f55c8277, 12ab1bc0989b32c55743df9b8c46af5a, 50dc5faa02227c0aefa8b54c8e5b2b0d, e760a5ce807c756451072376f88760d7, b03c67239e1e774077995bac331a8950, ba69cc9f087411995c64ca0d96da7b69, 051552b4da740a3af5bd5643b1dc239a, edfb8d26fa34436f2e92d5be1cb5901b, 3e86f6fc7ed037f3c9560cc59aa7aacc, ae4d6812f5638d95a82b3fa3d4f92861, 67677c815070ca2e3ebd57a6adb58d2e, 17a78f50e32679f228c43823faabedfd, b9956282a0fed076ed083892e498ac69, 1b41e64c60ca9dfadeb063cd822ab089
SHA1	dccdfc77dd2803b3c5a97af0851efa0aa5bbeeeb, 2D22F3744A9DADA4638486FB26B3404364C1418B, 1DD27A926E98C9305BD1689A9F7C33E0E3070D4B, 2873D5C7B215A68BF02697BA169078919AEEE474, 0431FE37BF744D5416E2F2A3220C5DC696E0FDA3, 9F6C7D3F02F6E214F56C3A3FC218A564FB8CB3C0, D0EB6CB3CA82D2D2E1D30AF4DFE7ED744111C6D7, 7697329BD6AFAA0874E8EF1AE81AD27BAA1863EC, D3D67296C8FE2B10A3626EEEE0B9BCC26157DE99, AC5B30AEA5F5C36FF6918A7545740F7FB4301650, 7995FC3EE9A9A97561774D1652A768D9586C259A, 74D53B909C75C5850C0C0EAAD71AD98CA3546064,
SHA256	0F696B7505255119B3CA53F57C2F829FC282D227D7A1577E698687A199800EF1, 8DD77DFD8DA749741FA9AADBE82E62B273C1C3565DEBBB753FAFEDB18A9F50C0, D967148E4289FD6B831C4BC9EC5BB808A384BD7D334FB2D1AB3A498F680315C7,

TYPE	VALUE
SHA256	81B6911BEC25C314C256E3E04E1826169359BFCBBED76ACD14F18A05BAF0A28A, 6A5F8868456CE708C7D6318C10A27BFB576DA1A02FF8F8575D2007F5C2F88E54, B2B3E8B3DA25215FF5DC3965DA852A27FEFDE958C6D06DDFFE36087BD0F6D1A5, C8AC671B0AB1BDDABB229A0F28D0E52B2EFBCC7415254CEB720452FA4AC7942A, 1BCB35DEB900C2C12F2B96071A24023A026FFB09464CFD446F8BF6D928C1365E, 5ECBFC037A992FA71B6DA1229308840692589F019F5FFD77EFAEFECD322179F1, 5F2C954DC7B35C4D31084CE43D7E5F88FFD803F848DBDD77F3112ACA01325D06, e4e3f09c4257269cef6cfbebc83c8a60376ce5e547080502e3e408a3f9916218, 7E761786FF674DE0ADCBD62ED6ADCB5237B2E23D5E6E2A4799F23037463513C5
File Name	Adhapl[.]dll
Domain	systemupdate[.]info

References

https://securelist.com/bellacpp-cpp-version-of-bellaciao/115087/

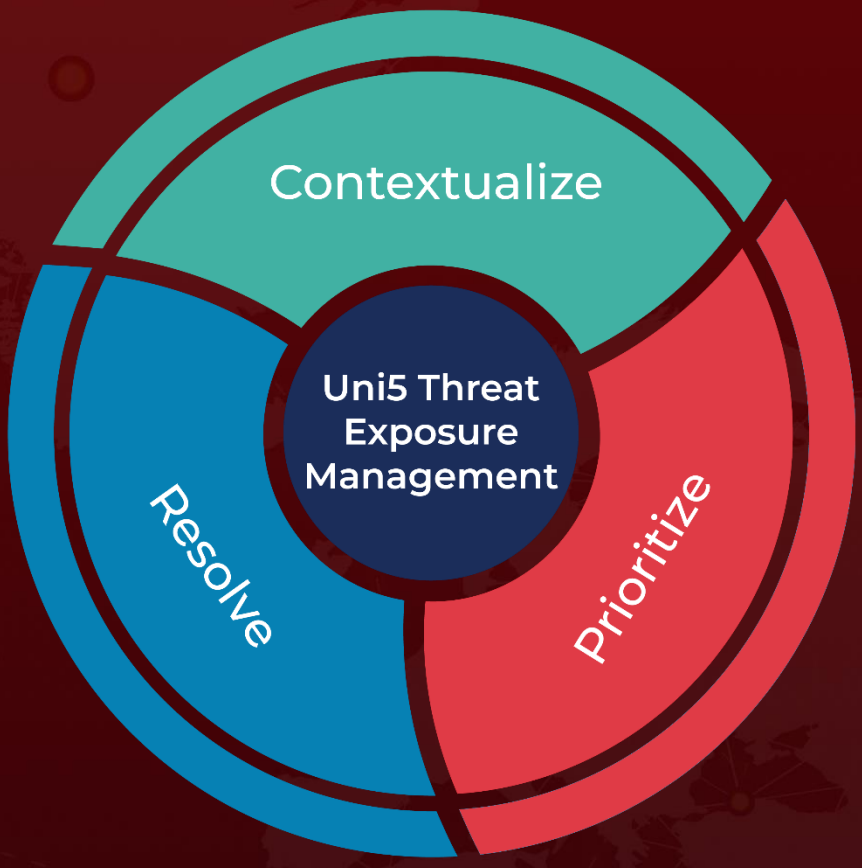
https://www.hivepro.com/charming-kittens-latest-malware-arsenal-and-targeting-strategies/

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

December 26, 2024 . 7:30 AM

More at www.hivepro.com