مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malware Campaign - BellaCPP: A New Variant of BellaCiao Malware

Tracking #:432316685
Date:30-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a threat actor deploying BellaCPP, a newly discovered C++ variant of the BellaCiao malware, to target systems.

TECHNICAL DETAILS:

The threat actor known as Charming Kitten (also known as APT35, CALANQUE, ITG18, and others) has been observed deploying a new C++ variant of the BellaCiao malware, named BellaCPP. This variant was found on a compromised machine in Asia, co-infected alongside the original BellaCiao malware.

- **BellaCiao**: Originally documented in April 2023, BellaCiao is a custom dropper malware family used in cyber attacks against the U.S., Middle East, and India.
- It leverages social engineering and exploits known vulnerabilities in applications like Microsoft Exchange Server and Zoho ManageEngine to establish unauthorized access.
- **BellaCPP**: The C++ version of BellaCiao, identified as a DLL file ("adhapl.dll"), contains similar functionality to the original malware, including the ability to load additional payloads (e.g., "D3D12_1core.dll") for creating SSH tunnels. Notably, BellaCPP lacks the web shell feature that allows BellaCiao to upload/download files and run commands.
- **Threat Landscape**: This malware represents an evolution of Charming Kitten's bespoke malware arsenal. The group's activities continue to focus on highly targeted attacks, leveraging vulnerabilities and custom-built tools for sustained cyber intrusions. BellaCPP uses domains previously attributed to Charming Kitten.

Indicators of Compromise (IOCs):

Indicator	Type
222380fa5a0c1087559abbb6d1a5f889	md5
14f6c034af7322156e62a6c961106a8c	md5
44d8b88c539808bb9a479f98393cf3c7	md5
e24b07e2955eb3e98de8b775db00dc68	md5
8ecd457c1ddfbb58afea3e39da2bf17b	md5
103ce1c5e3fdb122351868949a4ebc77	md5
28d02ea14757fe69214a97e5b6386e95	md5
4c6aa8750dc426f2c676b23b39710903	md5
ac4606a0e10067b00c510fb97b5bd2cc	md5
ac6ddd56aa4bf53170807234bc91345a	md5
36b97c500e36d5300821e874452bbcb2	md5
febf2a94bc59011b09568071c52512b5	md5
systemupdate.info	domain

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures
- **Patch Vulnerabilities**: Ensure all publicly accessible applications, especially Microsoft

Exchange and Zoho ManageEngine, are up to date with the latest security patches.

- **Monitor Suspicious Activity**: Look for signs of unauthorized file execution, unusual traffic, or SSH tunnels on network systems.
- **Network Segmentation and Access Control**: Restrict lateral movement within the network and apply strict access control policies to limit the potential impact of successful intrusions.
- Implement robust email filtering and user awareness training to mitigate social engineering risks
- Deploy and maintain up-to-date endpoint detection and response (EDR) solutions

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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