SECURITY ADVISORY

CYBER STASH

April, 2023

Multiple CVEs

BellaCiao Dropper Malware

Context

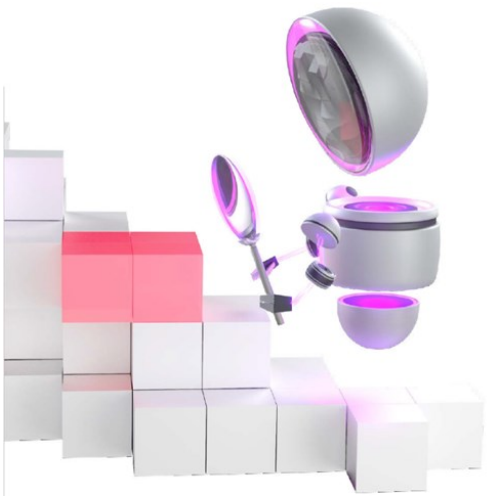
An Iranian state-sponsored hacking group Charming Kitten, also known as APT35/APT42 or Mint Sandstorm, has been identified as deploying a new strain of malware named BellaCiao, which has targeted victims in various countries, including the U.S., Europe, India, Turkey, and others. The campaign aims to exploit vulnerabilities in Microsoft Exchange servers to gain unauthorized access and deploy malicious payloads for espionage, data theft, and potentially ransomware attacks.

BellaCiao is a dropper malware designed to deliver additional malicious payloads to compromised devices based on instructions from the threat actors. Its primary objective is to establish persistence and maintain stealth while awaiting further instructions. The malware is customized for each victim (including hardcoded information such as company name, specially crafted subdomains, or associated public IP address) ensuring tailored implants and evading detection mechanisms. A second variant drops the Plink tool and PowerShell script hardcoded locations. The PowerShell scripts execute the Plink tool for establishing a reverse proxy connection to the C2 to enable interaction with the PowerShell web server.

Mitigation

Patch software: To prevent BellaCiao malware, regularly update your software and systems with the latest security patches. Give special attention to vulnerable apps that are exposed to the Internet.

Implement application controls: Establish strict controls for how each application interacts with its environment and the internet. Limit access and permissions to prevent unauthorized actions or communications that may compromise the software's security.



Block communication: Implement restrictions on communication with high-risk countries, Autonomous System Numbers (ASNs), Top-Level Domains (TLDs), and Threat Intelligence Data.

Investigate Anomalous DNS Traffic: By continuously monitoring DNS requests and responses, you can quickly detect and investigate any anomalies, enabling timely action to mitigate potential threats.

Technical Details

Tactics, Techniques and Procedures

The notable TTPs related to the BellaCiao Dropper Malware are:

T1190 -Exploit Public-Facing Application

Suspected that the threat actors utilized a Microsoft Exchange Exploit Chain such as ProxyShell, ProxyNot-Shell or OWASSRF

T1089 - Disabling Security Tools/Impair Defenses: Disable or Modify Tools

Upon deployment, BellaCiao attempts to disable Microsoft Defender using a PowerShell command, which reduces the effectiveness of the built-in security protection.

T1036 - Masquerading

To establish persistence, BellaCiao creates new service instances using legitimate process names specific to Microsoft Exchange servers. This technique, known as masquerading, helps malware blend in with legitimate processes.

T1203 - Exploitation for Client Execution

The threat actors attempted to download two IIS backdoors from a specific URL. The first backdoor, IIS-Raid, is a native IIS module that processes requests and executes commands based on specific headers. The second backdoor is a .NET IIS module designed for credential exfiltration.

T1035 - System Services: Service Execution

BellaCiao is a dropper malware that delivers other malware payloads onto the victim's computer system. The executable is written to specific locations on the system and runs as a service, using names resembling legitimate Microsoft Exchange services.

T1568 - Dynamic Resolution

BellaCiao employs a unique approach to receive instructions from the command and control (C2) server. It performs a DNS request every 24 hours to resolve a victim-specific subdomain, comparing the resolved IP address with a hardcoded IP address to receive further instructions.

T1105 - Ingress Tool Transfer

Based on the comparison of IP addresses, BellaCiao determines the operations to perform for webshell deployment. Different segments of the IP address are parsed to identify the folder, subfolder, and file-name to use for webshell deployment.

T1102 - Web Service

The dropped .aspx webshell supports operations such as upload, download, and command execution. Requests to the webshell must have a User-Agent string starting with a secret code followed by the requested operation.

T1219 - Remote Access Tools

In the second variant of BellaCiao, Plink (a command-line tool) and a PowerShell script are dropped. The PowerShell script uses Plink to establish a reverse proxy connection to the C2 server, enabling interaction with a PowerShell web server.

T1086 - Command and Scripting Interpreter: PowerShell

The PowerShell web server implemented by BellaCiao's second variant supports various operations, including command execution, script execution, file download/upload, web log manipulation, reporting server start time, reporting current time, beeping, and stopping the web server.

Threat Intelligence

APT35/Mint Sandstorm/PHOSPHORUS also referred to as Charming Kitten is a state-sponsored advanced persistent threat (APT) group orchestrated by the Islamic Revolutionary Guard Corps (IRGC) of Iran. Researchers from Bitdefender, a cybersecurity firm, have linked the group to the deployment of BellaCiao malware. Notably, the malware's name, "BellaCiao," references an Italian folk song associated with resistance fighting, possibly indicating the group's intended messaging or inspiration.

Charming Kitten has become a prominent figure in the information security landscape since 2014. The group is renowned for its targeted operations aimed at political dissidents, activists, journalists, and those opposing oppressive regimes. While social engineering and spear phishing are its main tools, it has also showcased advanced techniques, including the impersonation of respected researchers and activists.

References

Public Intelligence

https://www.pcrisk.com/removal-guides/26598-bellaciao-malware

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

https://www.hivepro.com/wp-content/uploads/2023/04/Charming-Kitten-Hackers-Utilize-New-Tactics-with-BellaCiao-Malware_TA2023201.pdf