Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

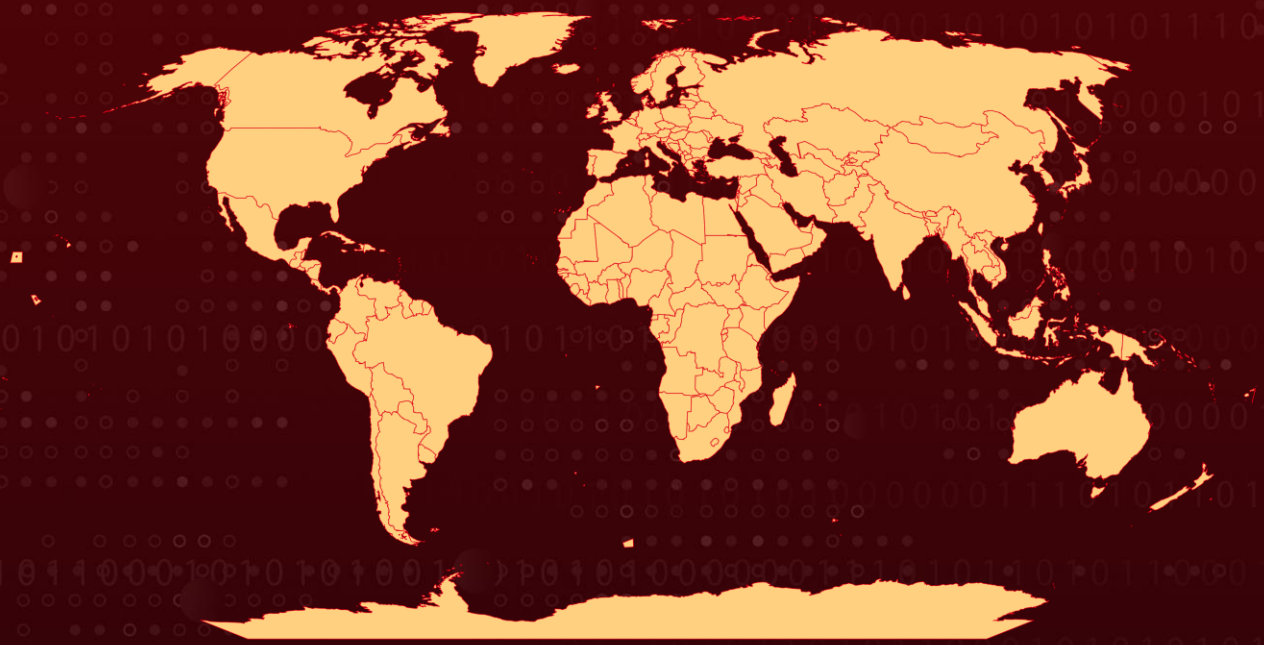
DanaBot Stealer: Multistage MaaS Malware Resurfaces

Date of Publication	Admiralty Code	TA Number
December 06, 2023	A1	TA2023491

Summary

First appeared: 2018
Targeted Industry: individuals, businesses, and government organizations
Malware: DanaBot
Attack: DanaBot is a covert malware designed for the discreet theft of sensitive data for financial gain. Unlike ransomware, its focus is on prolonged persistence rather than immediate disruption. Functioning as a malware-as-a-service (MaaS) platform, DanaBot is versatile, targeting individuals, businesses, and government organizations alike. Its deployment since 2018 has been associated with encompassing credential theft, financial fraud, and DDoS attacks.

Attack Regions



Attack Details

#1 DanaBot is a covert malware designed to steal sensitive data for financial gain. Operating discreetly, it places emphasis on long-term persistence. DanaBot Stealer, an evolving stealer malware, is distributed through phishing campaigns, employing a multi-level infection process to achieve successful compromise and evade detection.

#2 DanaBot stealer has recently adapted its distribution strategy to phishing campaigns, making it a notable email-based threat. The malware employs a malicious attachment as the primary vector for downloading and executing its payload. The deployment process involves multiple stages, each with distinct sources for its payload. The initial stage payload takes the form of an obfuscated JavaScript file designed to evade static detections. This file activates the CMD and subsequently triggers PowerShell, initiating the download of a second-stage malware.

#3 The second stage payload is retrieved from the Discord Content Delivery Network (CDN), leveraging the perceived legitimacy of Discord as a service for unhindered access to the payload. The third stage payload is obtained from an FTP server under the control of the threat actor, residing at a specific IP address. This payload encompasses additional files and scripts, facilitating subsequent execution and data exfiltration.

#4 In July, DanaBot v.3 was released introducing significant changes such as price restructuring and dedicated customer support. It offers increased flexibility for threat actors with new subscription structures, including stealer, stealer plus HVNC, stealer and PostGrabber, API, personal server, and personal support. The DanaBot Tor site provided panel setup instructions and bot customization options.

#5 The Cactus ransomware operators are utilizing Danabot malware, distributed through malvertising, to assist in their malicious activities. Recently, **Cactus ransomware** group were also discovered capitalizing on Qlik sense vulnerabilities.

#6 DanaBot Stealer maintains persistence on infected systems by creating entries in the Windows registry, ensuring it is executed every time the system is started or a user logs in, allowing the malware to continue operating even after system reboots or logins. To elude detection, threat actors consistently alter techniques for delivering payloads at each stage.

Recommendations

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0010 Exfiltration	T1592 Gather Victim Host Information	T1566 Phishing	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.007 JavaScript	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1204 User Execution	T1204.002 Malicious File	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	T1622 Debugger Evasion	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories

T1055 Process Injection	T1055.012 Process Hollowing	T1218 System Binary Proxy Execution	T1218.011 Rundll32
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1217 Browser Information Discovery	T1083 File and Directory Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1071.002 File Transfer Protocols	T1573 Encrypted Channel	T1104 Multi-Stage Channels
T1020 Automated Exfiltration	T1564.003 Hidden Window	T1070 Indicator Removal	T1070.004 File Deletion
T1070.007 Clear Network Connection History and Configurations	T1027 Obfuscated Files or Information	T1027.009 Embedded Payloads	T1027.010 Command Obfuscation
T1087 Account Discovery			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	dd54705e88abe160e5febcf9f92b92ba, fcf058c84afcf6059cd9cbf2ccdb566d, Oaaa1867a920a77e8c3a83561f861d71, 2E129B351FF75498DC75871E5E395DFA, 09e1729b0917b448f60e9520f8b6c844, e4313b13d3b2a0cebdcc417f5f7b7644, 92ee9e2a75be2bcb0b37fe557eb7b263, ce956d5aa11b9fb152e7bad48c7a82fe
URL	hxxps[:]//cdn[.]discordapp[.]com/attachments/1176544174691061881/1176597937829822/t4[.Jexe
IP	195.185.1115[.]195

TYPE	VALUE
SHA256	3d673d0427cceb8e8a11c3548eeb0fb26530768b34f5585fb5101cbe5b517599, 2c588f6f3378d320082379ee8c215259b8d9a1952a95b20efce6acd1d1e78148, cObd0a1412e37290b94108298ac49ee0d209502e631deale1151451b3ec8e881, 534DC0D2088821521A8C83AAB5100987C930F6BA4CBBB69A4036B571885717CO, 333aa54b7532b181164520f69a680eaee344c2f483a02239898a64126d26a6d9, 1005847cbd6771df9dd81e6cd5a40686cd6454bd644fc93347e3e56e668a464b, 1a7138679e397d208d99923d7e4edc38b56d7bfe76ce71971700f1eaecfb7e8d, Ode8b287ddc4c9674a7dfb915cc86960d5a9a14ff27e3aeed0fc79a611714ba0

References

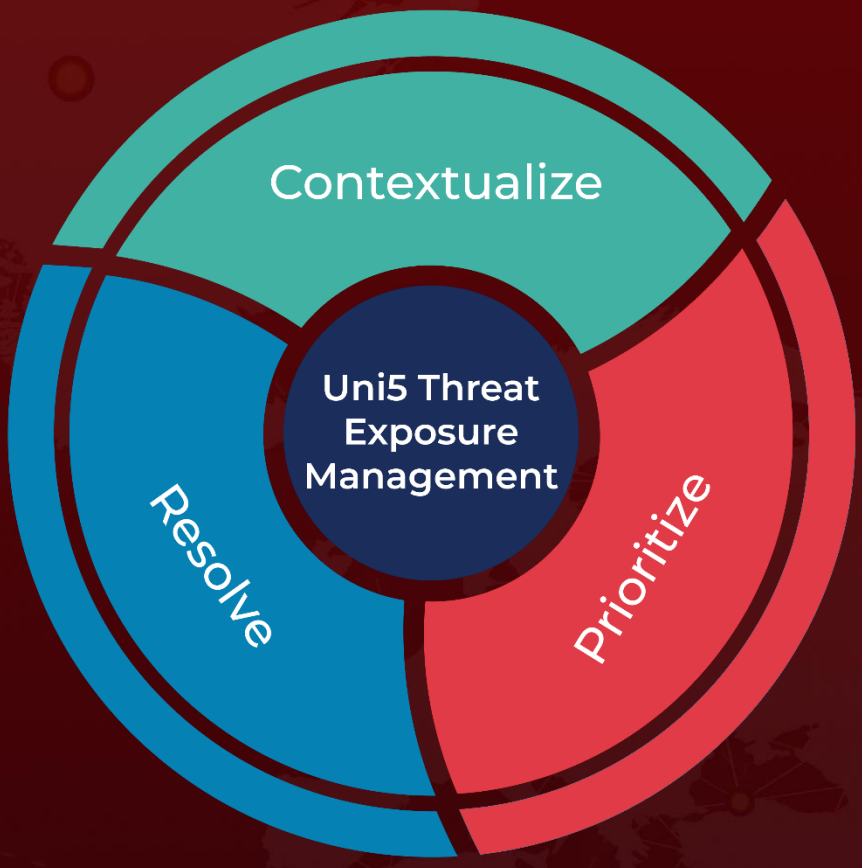
https://www.cyfirma.com/outofband/danabot-stealer-a-multistage-maas-malware-re-emerges-with-reduced-detectability/

https://www.hivepro.com/threat-advisory/cactus-ransomware-exploits-vulnerabilities-in-qlik-sense/

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 06, 2023 . 5:40 AM

More at www.hivepro.com