Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

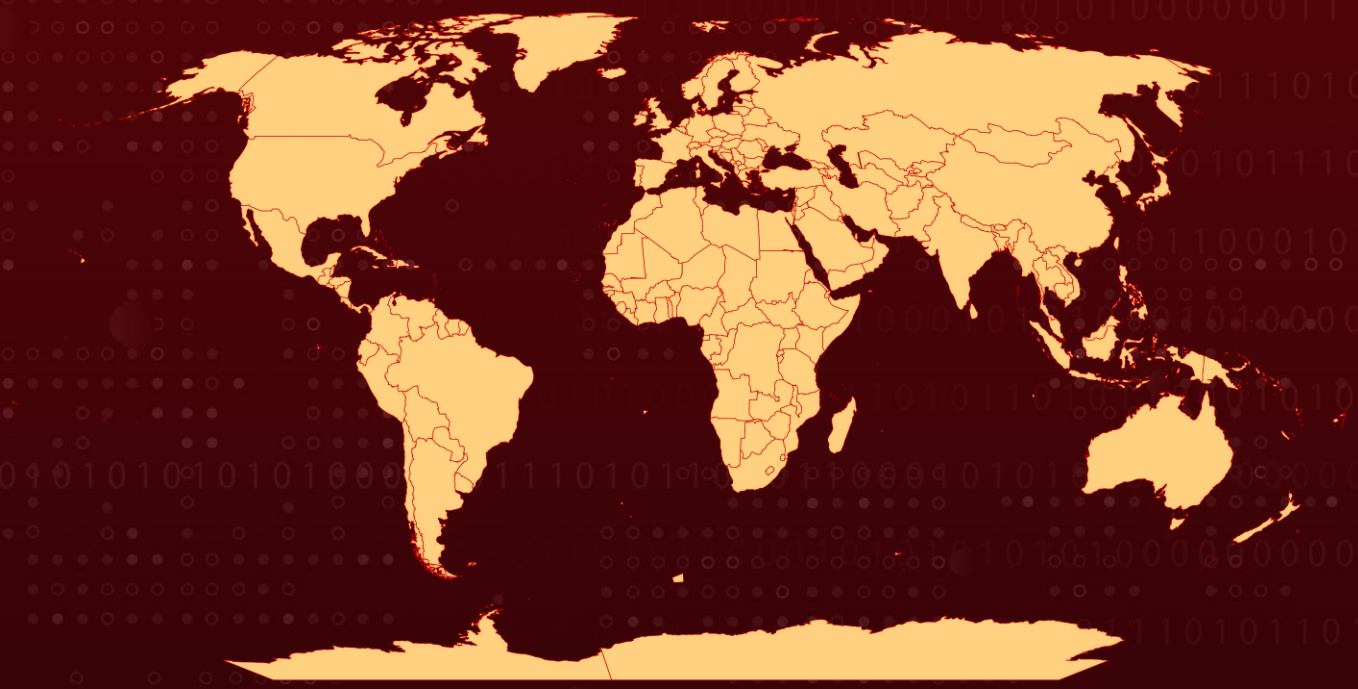
New Zaraza Bot Malware Steals Login Credentials from 38 Web Browsers via Telegram

Date of Publication	Admiralty Code	TA Number
April 18, 2023	A1	TA2023191

Summary

First Appearance: March 18, 2023
Target Countries: Worldwide
Malware: Zaraza bot
Affected Products: 38 different web browsers (Chrome, Firefox, Safari, Edge, and Opera)
Attack: A new credential-stealing malware named Zaraza bot uses Telegram as its command and control, targeting 38 web browsers and exfiltrating sensitive data for potential identity theft and financial fraud.

Attack Regions



Attack Details

#1 A new variant of credential stealing malware named Zaraza bot that uses Telegram as its command and control server. The malware uses a 64-bit binary file compiled using C#, targets 38 different web browsers, including popular ones like Google Chrome and Microsoft Edge, and exfiltrates login credentials from online bank accounts, cryptocurrency wallets, email accounts, and other high-value websites.

#2 The stolen data is sent to a Telegram server where attackers can access it immediately. The malware has been traced back to Russian hackers and communicates in plain Russian language. The Telegram channel used by the malware is live, and the credentials collected can be sold on the underground market or used in follow-on attacks.

#3 The malware is capable of decrypting encrypted credentials stored by web browsers. The infection flow of Zaraza bot involves extracting login credentials and capturing screenshots, which are then transmitted to the bot server. The malware is compiled using C# and contains obfuscated code to make detection and debugging difficult.

Recommendations

- Implement multi-factor authentication (MFA) for all user accounts and enforce the use of strong passwords to add an extra layer of security and prevent Zaraza bot from stealing credentials.
- Segment your network to limit the lateral movement of Zaraza bot or any other malware, using firewalls, VLANs, or other network segmentation techniques. Keep software and security systems up-to-date, regularly update web browsers, operating systems, and security software to patch known vulnerabilities and protect against malware attacks.
- Preventive measures include keeping all security patches and antivirus software updated, using signatures or heuristics to detect malicious software, blocking code execution through application control or script blocking, managing privileged accounts, and utilizing capabilities to prevent suspicious behavior patterns.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0002 Execution	TA0007 Discovery	TA0010 Exfiltration
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0042 Resource Development	TA0006 Credential Access	T1584 Compromise Infrastructure	T1027 Obfuscated Files or Information
T1055 Process Injection	T1140 Deobfuscate/Decode Files or Information	T1584.005 Botnet	T1113 Screen Capture
T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter	T1555 Credentials from Password Stores	T1005 Data from Local System
T1592 Gather Victim Host Information	T1555.003 Credentials from Web Browsers	T1102 Web Service	T1078 Valid Accounts
T1486 Data Encrypted for Impact	T1552 Unsecured Credentials	T1106 Native API	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	41D5FDA21CF991734793DF190FF078BA
SHA1	b50a8e2a7998e17286d2e18d1cf3f7e4e84482c6
SHA256	2cb42e07dbdfb0227213c50af87b2594ce96889fe623dbd73d228e46572f0125

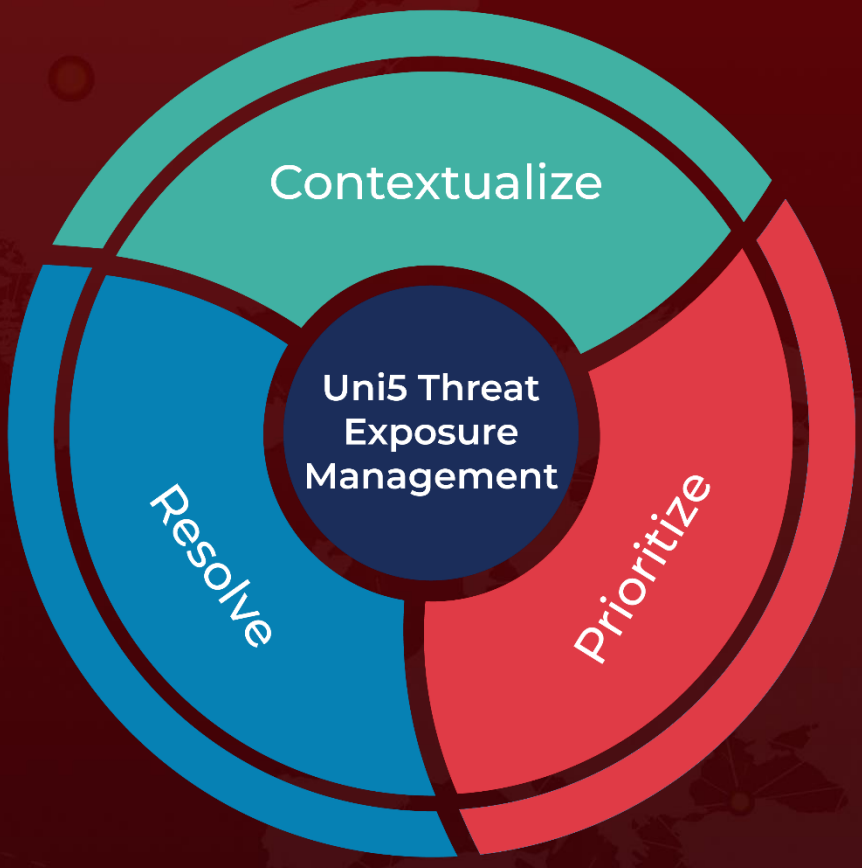
References

https://www.uptycs.com/blog/zaraza-bot-credential-password-stealer

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

April 18, 2023 • 1:50 AM

More at www.hivepro.com