Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

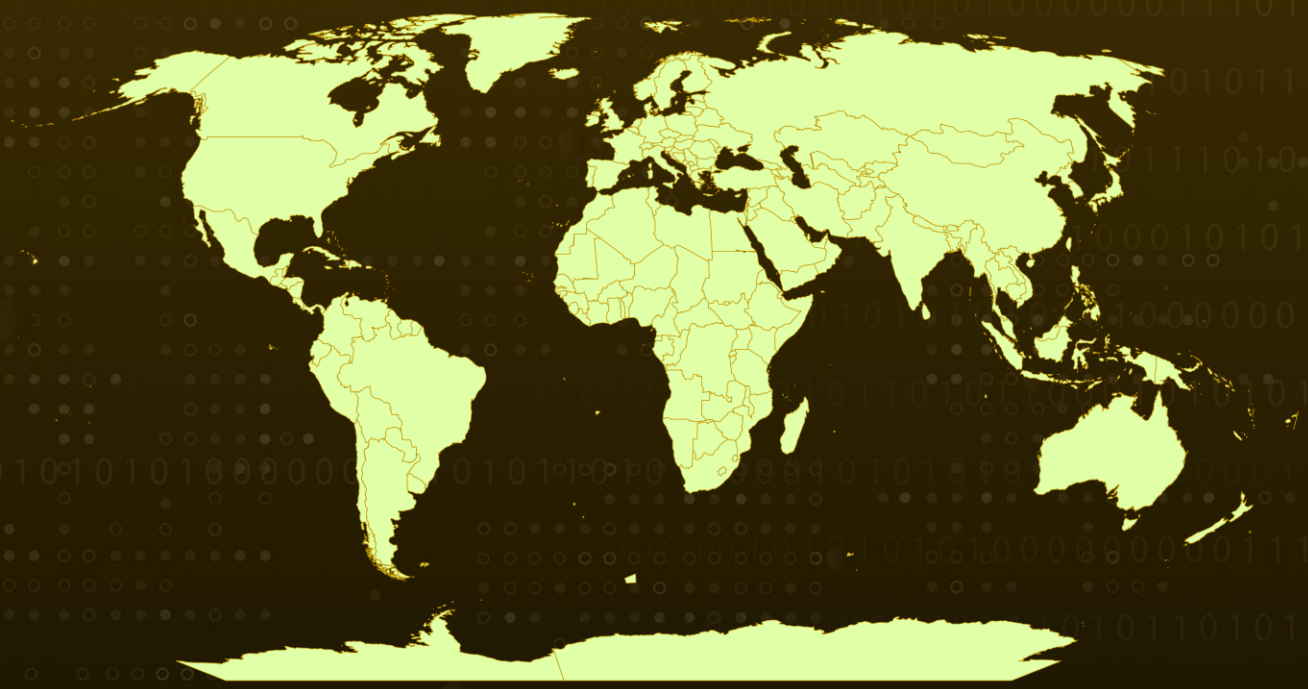
Millenium RAT the $30 Access Ticket to Data Theft

Date of Publication	Admiralty Code	TA Number
November 8, 2023	A1	TA2023452

Summary

Active Since: 2022
Malware: Millenium RAT
Attack Region: Worldwide
Affected Platform: Windows
Attack: The Millenium RAT, a Win32 executable built on .NET, specifically version 2.4, is available on GitHub for a one-time fee of $30, granting lifetime access. Notably, this RAT is actively developed and has been intricately designed to discreetly collect sensitive user data, evade advanced anti-analysis techniques, establish persistence in compromised systems, and enable remote control.

Attack Regions



Attack Details

#1 The Millenium RAT, a Win32 executable built on .NET, specifically version 2.4, can be found on GitHub and is available for purchase for $30, granting lifetime access. Notably, this RAT is actively under development, as evidenced by the recent release of version 2.5, without a clear indication of its pricing.

#2 This malicious software represents a sophisticated array of nefarious functionalities intricately designed to discreetly collect sensitive user data, evade detection through advanced anti-analysis techniques, establish persistence within the compromised system, and enable remote control over it.

#3 Furthermore, a Millenium RAT builder offers customization options to tailor the RAT to specific requirements. The Millenium RAT may have evolved from an open-source Telegram RAT known as the ToxicEye RAT. Upon execution, the RAT establishes a connection with a URL to obtain location-based information and employs module handle checks to detect the presence of a Sandbox environment.

#4 The RAT possesses the capability to self-install and uninstall, and it can execute a range of commands to manipulate the compromised system, exfiltrate data, or engage in other malicious activities. Periodically, it checks for new commands delivered via the Telegram bot API.

Recommendations

Behavior-Based Monitoring: Deploy behavior-based monitoring to detect unusual activity patterns, including suspicious processes attempting unauthorized network connections, which is a common behavior of RATs.

Least Privilege Principle (PoLP): Adhere to the principle of least privilege (PoLP) by restricting user permissions to only those required for their specific roles, limiting the impact of malware that relies on elevated privileges.

Network Segmentation: Segment your network into isolated zones to limit lateral movement for attackers and reduce the impact of a breach. Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0010 Exfiltration	TA0040 Impact	T1566 Phishing	T1204.002 Malicious File
T1547.001 Registry Run Keys / Startup Folder	T1497 Virtualization/Sandbox Evasion	T1498 Network Denial of Service	T1056 Input Capture
T1555.003 Credentials from Web Browsers	T1552.001 Credentials In Files	T1057 Process Discovery	T1083 File and Directory Discovery
T1033 System Owner/User Discovery	T1497 Virtualization/Sandbox Evasion	T1113 Screen Capture	T1119 Automated Collection
T1041 Exfiltration Over C2 Channel	T1048 Exfiltration Over Alternative Protocol	T1485 Data Destruction	T1021 Remote Services
T1056.001 Keylogging			

Indicators of Compromise (IOCs)

TYPE	VALUE
File Path	C:\Users\Username\AppData\Roaming\SoftwareLogs, C:\Users\Username\AppData\Roaming\GoogleChromeUpdateLog
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run

TYPE	VALUE
File Name	Update[.]exe, BrowserPasswords[.]txt, BrowserDownloads[.]txt, CreditCards[.]txt, BrowserCookies[.]txt, Browser data[.]zip
URL	hxxp://ip-api.com/json/
SHA256	6d207c1e954f9d60f693e17e63df73fb8e954d02544b5d52b8b18c4ab86a267e
SHA1	f4d698ece0ff6af36c1a2e9108ea475518df0aa7
MD5	eba4be8ed0e9282976f8ee0b04fb2474

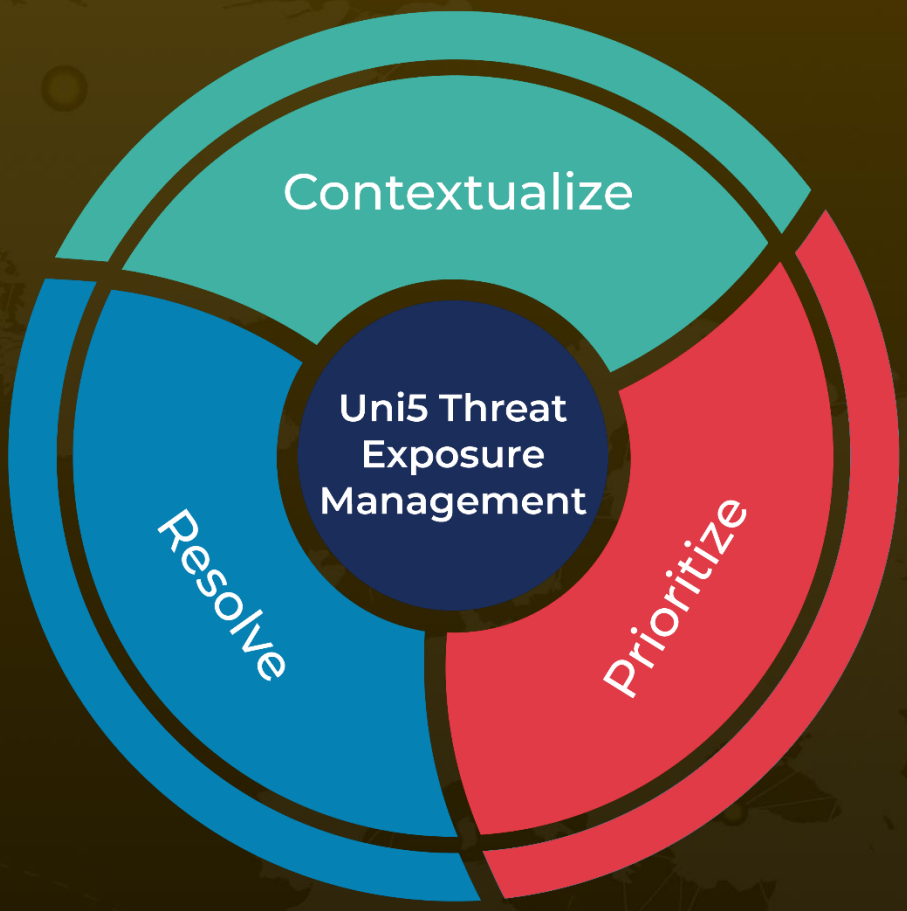
References

https://www.cyfirma.com/outofband/unveiling-a-new-threat-the-millenium-rat/

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

November 8, 2023 • 4:30 AM

More at www.hivepro.com