Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

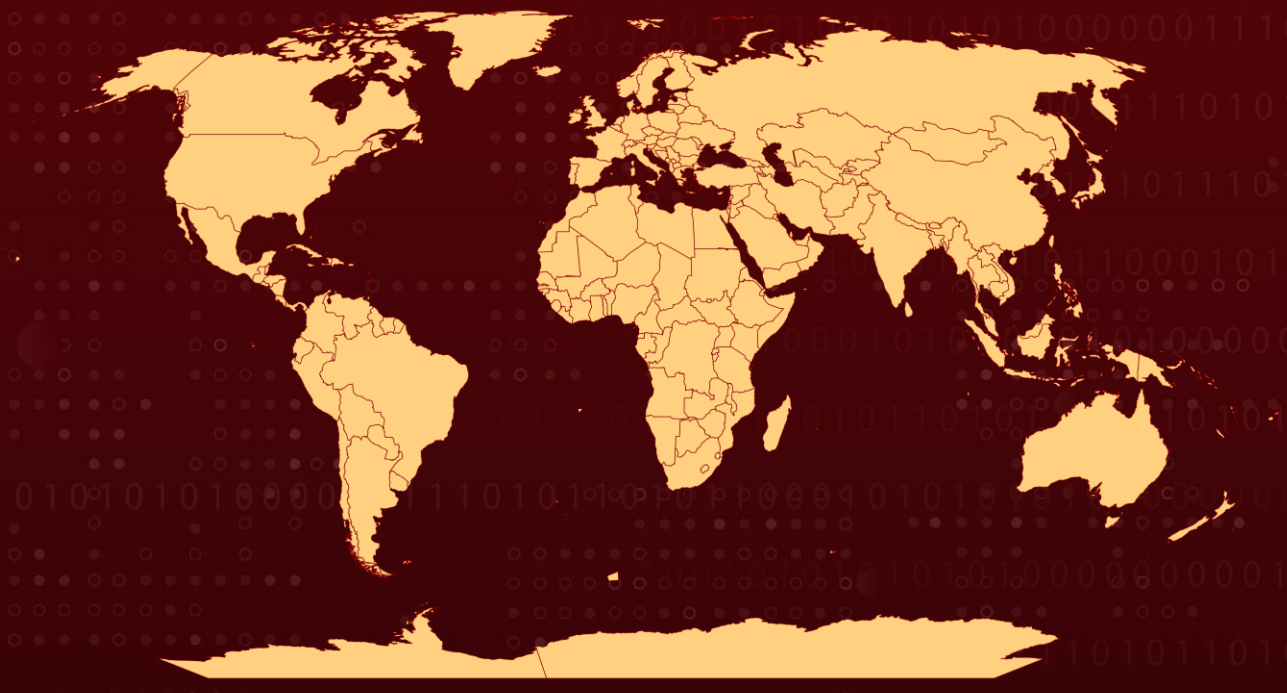
Mylobot: A Sophisticated Botnet Malware Targeting Computers Worldwide

Date of Publication	Admiralty Code	TA Number
February 21, 2023	A1	TA2023094

Summary

First Appearance: October 20, 2017
Target Countries: Worldwide
Malware: Mylobot
Affected Platform: Windows
Attack: Mylobot is a sophisticated botnet malware that can turn an infected computer into a proxy by taking full control of it, and it is designed to evade detection and remain persistent on infected machines.

Attack Regions



Attack Details

#1 Mylobot is a Windows-targeting malware and was first discovered in 2017. It has not received much attention since then, but it is noteworthy for its ability to transform the infected system into a proxy. The number of unique infected systems per day has decreased from a peak of 250,000 in 2020 to currently observing over 50,000 unique infected systems daily.

#2 The malware has three different stages. The first stage is a dropper that embeds an encrypted resource, performs anti-debug checks, and decodes a long base64 encoded string. The resulting shellcode creates a new process and does process hollowing to run the decrypted PE file.

#3 The second stage contains two resources: an encrypted PE file and a small 4-byte RC4 key. The program uses the key to decrypt the PE file in memory and executes one of its exported functions. The third stage writes itself on disk and turns the infected computer into a proxy. It injects itself into a newly created process and maps the raw file in memory. The program then runs the exported function in the new process and terminates itself.

#4 Mylobot communicates with the command and control server using a unique network fingerprint that involves more than 1000 hard-coded domains, mostly ending with the top-level domain (TLD) .ru or .com. Once the malware connects to the command and control server, it turns the infected computer into a proxy that can handle many connections and relay traffic sent through the server. The infected machine can be used to download and run other malware samples. The malware is noisy and produces thousands of DNS requests, and its size and complexity suggest that it is part of a larger botnet.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
T1059 Command and Scripting Interpreter	T1106 Native API	T1562 Impair Defenses	T1027 Obfuscated Files or Information
T1055 Process Injection	T1608 Stage Capabilities	T1496 Resource Hijacking	T1090 Proxy
T1132 Data Encoding	T1218 System Binary Proxy Execution	T1055.012 Process Hollowing	T1105 Ingress Tool Transfer
T1140 Deobfuscate/Decode Files or Information	T1012 Query Registry	T1005 Data from Local System	T1057 Process Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	84733af3b60b966042d5cd17e12fd8d90650e0731297d203bd913dc5c663b91c 11fc02dd825c8e67d58cc40a47e3f4c572097bd58c6aae80591a5fb73b9167f2 392f1054815c5f805d50b60ea261210012bdda386158a1da92d992a929eb77c2 03b2164da6318fff63b6cad2fc613c3d885bd65432a7b8744c2b1709f2f9a479 69a36e6f12b4e9b9cd15528a068385f2311b0c540336c142aabdd73c2a2e2015 a63a5639d0cb6a10f7af5bd0dd30ca1800958a0f5bb47f358b6d37f51d0f0a31 2ae61c8c2a8e83cde33f38b89599032a6fb455256aa414a15f2724c94d3460d2 40cfb7b7fad1602276ebf3fa63514ba91be6186d5d3bd190f593bdec0b6d8d64 cfde42903367d77ab7d5f7c2a8cfc1780872d6f1bfac42e9c2577dfd4b6cdeb2 fcdb7247aa6e41ff23dc1747517a3682e5a89b41bfd0f37666d496a1d3faa4ba ad53ad1d3e4ac4cc762f596af8855fd368331d9da78f35d738ae026dd778eb9f

TYPE	VALUE
IPV4	89[.]39[.]105[.]47 89[.]38[.]96[.]140 89[.]38[.]96[.]14 217[.]23[.]12[.]80 178[.]132[.]3[.]12 168[.]119[.]15[.]229 89[.]38[.]98[.]48 49[.]12[.]128[.]181 37[.]48[.]112[.]111 109[.]236[.]82[.]28 49[.]12[.]128[.]180 144[.]76[.]8[.]93 194[.]88[.]106[.]18 95[.]211[.]203[.]197 89[.]39[.]104[.]201 95[.]168[.]169[.]43 95[.]211[.]198[.]102 91[.]229[.]23[.]112 217[.]23[.]13[.]104 95[.]211[.]140[.]149 62[.]112[.]11[.]245 178[.]132[.]2[.]82 116[.]202[.]114[.]236 217[.]23[.]12[.]50 89[.]39[.]104[.]58 89[.]38[.]98[.]47 194[.]88[.]105[.]108 109[.]236[.]83[.]166 109[.]236[.]91[.]239 89[.]39[.]107[.]92 190[.]2[.]134[.]165 217[.]23[.]8[.]12 89[.]39[.]104[.]62 89[.]39[.]107[.]82

References

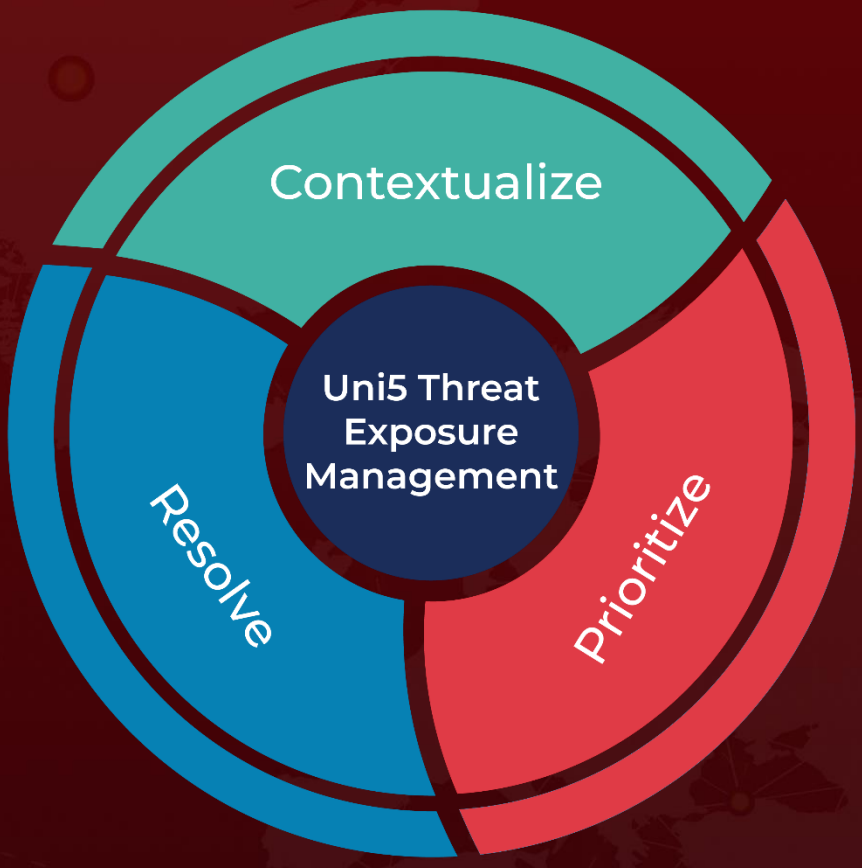
https://www.bitsight.com/blog/mylobot-investigating-proxy-botnet

https://thehackernews.com/2023/02/mylobot-botnet-spreading-rapidly.html

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

February 21, 2023 . 11:00 PM

More at www.hivepro.com