Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

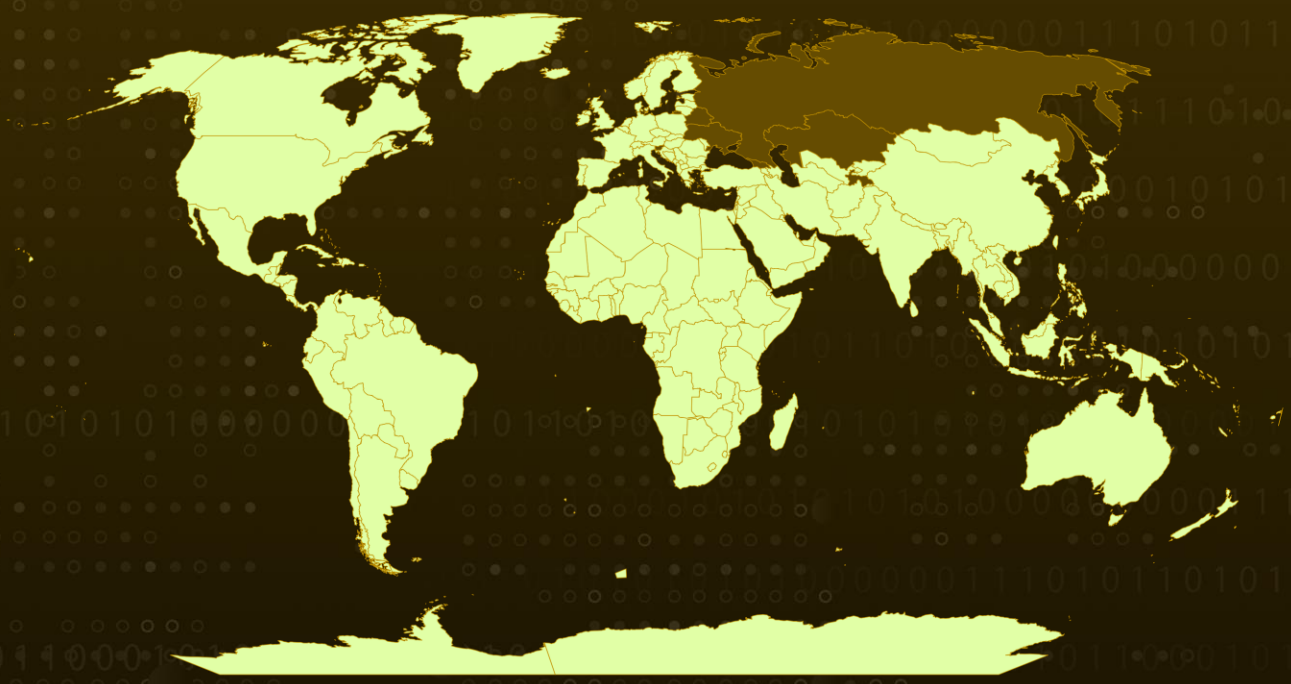
Pikabot A Stealthy Backdoor with Ingenious Evasion Tactics

Date of Publication	Admiralty Code	TA Number
May 25, 2023	A2	TA2023246

Summary

First seen: 2023
Malware: Pikabot
Attack Region: Worldwide (excluding Georgia, Kazakhstan, Cyrillic, Tajikistan, Russia, Ukraine, Belarus, and Slovenia).
Attack: Pikabot, a sophisticated backdoor active since 2023, evades analysis with anti-analysis measures like the "sleep" function, uses NtContinue API, employs language-based execution cessation, and shows connections to Qakbot trojan.

Attack Regions



Attack Details

#1 Pikabot, an insidious backdoor, has been operational since the start of 2023. This malicious software consists of distinct modules: a loader and a core component responsible for executing the majority of tasks. Using a command-and-control server, Pikabot can receive various commands, including injecting arbitrary shellcode, DLLs, or executable files.

#2 Pikabot employs a code injector to decrypt and injects its core module, incorporating multiple anti-analysis mechanisms. The core module and its injector also leverage the ADVobfuscator, an open-source string obfuscation tool. Pikabot shares identical dissemination tactics, marketing strategies, and malicious behaviors with the Qakbot trojan.

#3 The Pikabot core module incorporates several measures to evade analysis, including a notable technique known as the "sleep" function. This function introduces a delay in Pikabot's execution. Instead of using commonly utilized Windows API functions, Pikabot employs the NtContinue API function to set a timer.

#4 Additionally, if the system's language matches any of the following: Georgian, Kazakh, Uzbek, Tajik, Russian, Ukrainian, Belarusian, or Slovenian, Pikabot will cease its execution. There are indications that Pikabot could be linked to Qakbot, as they share similarities in distribution methods, design elements, and campaign identifiers.

Recommendations

Strengthen Anti-Malware Defenses: Given Pikabot's advanced evasion techniques and potential ties to Qakbot, it is crucial to enhance anti-malware defenses. Organizations should invest in robust cybersecurity solutions capable of detecting and mitigating such sophisticated threats. Employing behavior-based analysis can help identify and neutralize Pikabot.

Heighten User Awareness and Vigilance: Educating users about the risks posed by sophisticated malware like Pikabot is paramount. Additionally, users should exercise caution when opening email attachments or clicking on unfamiliar links to minimize the risk of infection.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1129 Shared Modules	**T1574** Hijack Execution Flow	**T1547.001** Registry Run Keys / Startup Folder	**T1574.002** DLL Side-Loading
T1055 Process Injection	**T1027** Obfuscated Files or Information	**T1036** Masquerading	**T1112** Modify Registry
T1218 System Binary Proxy Execution	**T1218.010** Regsvr32	**T1218.011** Rundll32	**T1497** Virtualization/Sandbox Evasion
T1056 Input Capture	**T1057** Process Discovery	**T1082** System Information Discovery	**T1083** File and Directory Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery	**T1571** Non-Standard Port	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	92153e88db63016334625514802d0d1019363989d7b3f6863947ce0e490c1006 a48c39cc45efea110a7c8edadcb6719f5d1ebbeebb570b345f47172d393c0821 8ee9141074b48784c89aa5d3cd4010fcf4e6d467b618c8719970f78fcc24a365 a9db5aca01499f6ce404db22fb4ba3e4e0dc4b94a41c805c520bd39262df1ddc 347e2f0d8332dd2d9294d06544c051a302a2436da453b2ccfa2d7829e3a79944
URLs	hxxps://129.153[.]135.83:2078 hxxps://132.148.79[.]222:2222 hxxps://45.154.24[.]57:2078 hxxps://45.85.235[.]39:2078 hxxps://94.199.173[.]6:2222

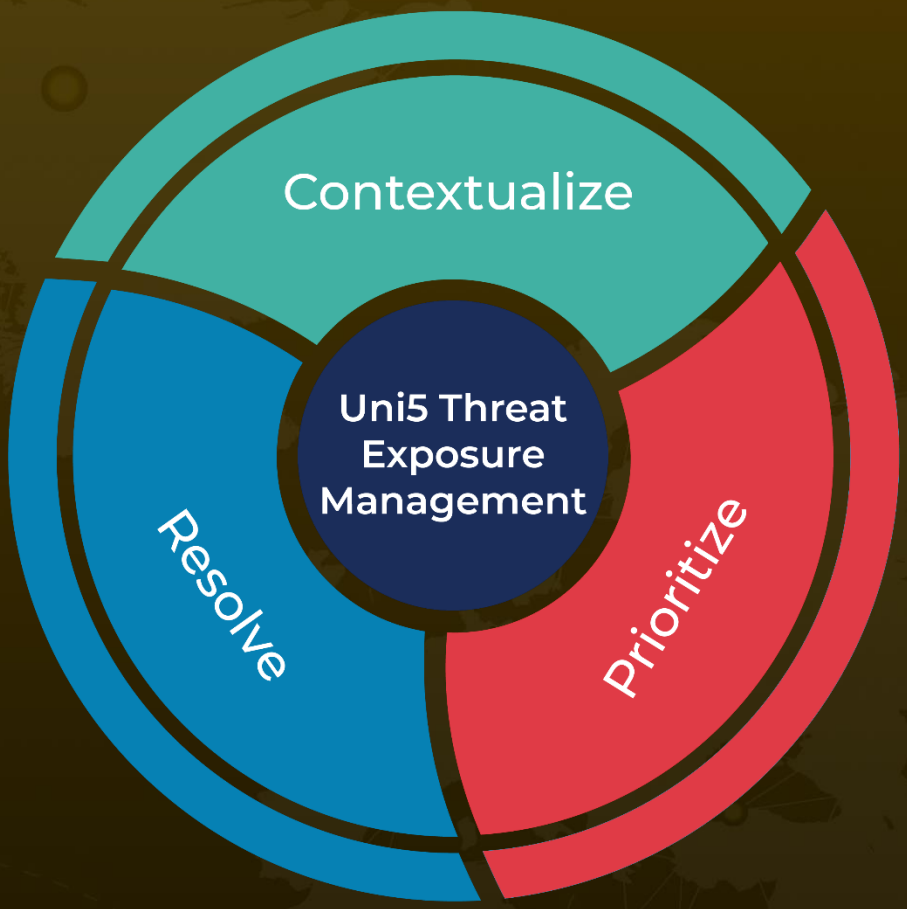
References

https://www.zscaler.com/blogs/security-research/technical-analysis-pikabot

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

May 25, 2023 • 5:43 AM

More at www.hivepro.com