Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

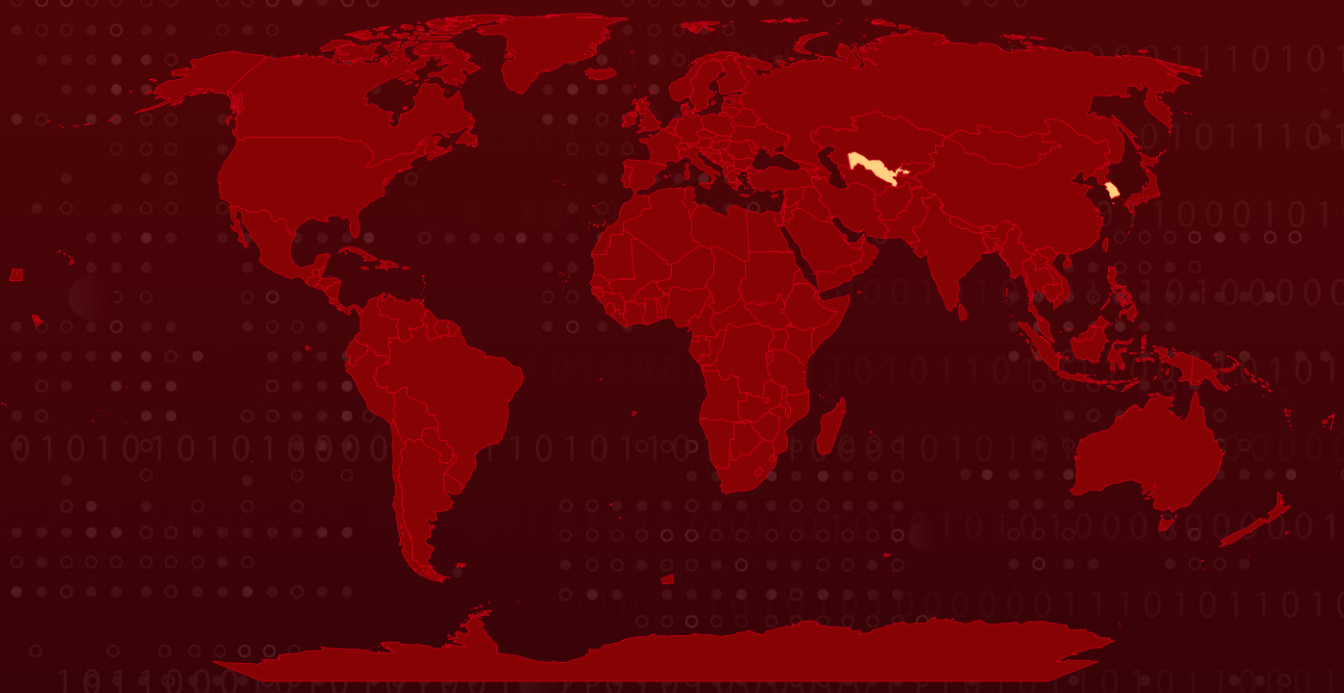
SugarGh0st RAT: A Customized Gh0st Variant in Cyber Espionage

Date of Publication	Admiralty Code	TA Number
December 4, 2023	A1	TA2023485

Summary

Attack Began: August 2023
Attack Region: Uzbekistan and South Korea
Malware: SugarGh0st RAT, Gh0st RAT (Farfli, Ghost RAT, PCRat)
Targeted Industries: Government
Attack: A malicious campaign deploying the customized SugarGh0st RAT, likely orchestrated by a Chinese-speaking threat actor targeting the Uzbekistan Ministry of Foreign Affairs and South Korean users. SugarGh0st, a variant of Gh0st RAT, exhibits advanced features for remote control, keylogging, and espionage.

Attack Regions



Attack Details

#1 A malicious campaign, likely originating from August 2023, introducing a new remote access trojan (RAT) called "SugarGh0st." The threat actor appears to target the Uzbekistan Ministry of Foreign Affairs and users in South Korea. SugarGh0st is identified as a customized variant of the infamous Gh0st RAT, known for over a decade, with modified commands and communication protocol.

#2 The attack involves two infection chains utilizing Windows Shortcuts embedded with malicious JavaScript to deliver and execute SugarGh0st. The actor, suspected to be Chinese-speaking with low confidence, deploys decoy documents in Uzbek and Korean languages to lure victims. The campaign involves phishing emails with malicious attachments sent to specific targets.

#3 SugarGh0st, a new variant of Gh0st RAT, exhibits customization in reconnaissance, utilizing specific Open Database Connectivity (ODBC) registry keys and evading detection. It maintains core features like remote control, keylogging, webcam access, and downloading arbitrary binaries. Two infection chains are observed, one utilizing a customized DLL loader and the other leveraging DynamicWrapperX for shellcode injection.

#4 The RAT establishes C2 communication with hardcoded domains, engaging in regular heartbeats and transmitting system information. SugarGh0st functions as a comprehensive backdoor, executing remote control commands, keylogging, process manipulation, file operations, and even clearing event logs for stealth.

#5 The actor can control the victim's machine extensively, performing tasks such as taking screenshots, accessing the camera, and initiating remote shell sessions. The RAT uses distinct commands for various actions, demonstrating a high level of functionality and adaptability.

#6 Overall, the campaign employs sophisticated techniques, indicating a potential Chinese-speaking threat actor targeting specific geopolitical interests in Uzbekistan and South Korea. The use of a customized Gh0st RAT variant underscores the ongoing evolution of malware for surveillance and espionage purposes.

Recommendations

Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.

Enhance Endpoint Security: Deploy advanced endpoint security solutions, such as endpoint detection and response (EDR) tools, to identify and respond to malicious activities promptly. Keep security software, including antivirus and endpoint protection, up to date to defend against known threats.

Email Filtering and Gateway Security: Implement robust email filtering solutions to detect and block phishing emails. Consider using advanced threat protection tools to identify and neutralize malicious attachments and links.

Network Monitoring and Intrusion Detection: Deploy network monitoring and intrusion detection systems to detect unusual or suspicious activities. Anomalies in network traffic and behavior can be indicative of a security incident.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0009 Collection	TA0006 Credential Access
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0011 Command and Control
T1059.007 JavaScript	T1106 Native API	T1059 Command and Scripting Interpreter	T1056 Input Capture
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204.002 Malicious File	T1204 User Execution
T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information	T1036.007 Double File Extension	T1574.002 DLL Side-Loading

T1218.011 Rundll32	T1218 System Binary Proxy Execution	T1036 Masquerading	T1574 Hijack Execution Flow
T1070 Indicator Removal	T1070.004 File Deletion	T1547.001 Registry Run Keys / Startup Folder	T1059.005 Visual Basic
T1055 Process Injection	T1056.001 Keylogging	T1560 Archive Collected Data	T1059.003 Windows Command Shell

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8584094f79fce97321ee82ca5da41b6830ecc6a0921bcaddb8dd337827cd7d1a, 3436135bb3839521e7712882f0f6548aff78db66a1064408c49f820a0b85d980, c758eed6660786097b63ac6748236b5b6084783703ea7ee2111e8f0bcaa3652e, 6dff111b6adc9e33bed20eae99bec779f1c29dd55895a71125cfbe3c90950eb2, 7c87451261dfce64fda987eb395694b5330fd958466c46c931440cd9dc227505, ddac61f918ed87b49ef15d05873e7f52b919758aef713145f6a7d538c714fa2e, f3ea4611c72d57eabf381d5639c3c8d1840cb005ed811f3038410fb2e04978c1, 9d9a0af09fc9065bacabf1a193cad4386b5e8e5101639e07efa82992b723f3b0, 5ad182c913f0b5cb6a34126137c335110d4c9472f5c745cb7a438d108b03b27c, 38c815729f34aef6af531edf3f0c3f09635686dbe7e5db5cb97eca5b2b5b7712, adb4eb33213fa81c8b6cc013a6f4a43fa8b70eb8027433cf4339b532cb6e84cf, 2e543adb701afd40affcb4c51bd8246398b0210bee641ca9aeffcca893c9e4a5, 7cacdc84a0d690564c8471a4f58ab192ef7d9091ab0809933f616010bbf6846a, 66982ebd5ebb75633723c7057a1e948ac3aafe3ff808397eb0c55c853c82f9e6,

TYPE	VALUE
SHA256	21f19d87d2169c82efd76ddb1baa024a1e59b93f82d28f276de853fc3ef8b20e, 362fde3362e307af3787b9bf0b5c71f87b659a3217e054c4d0acea8b9e6d74b0, ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e, 9783c0eee31ce6c5f795ecf387025af5d55208ff2713c470af2042721ab38606, 410d7dc973d188cd0d962a59f48deb1cfc73adf37857765e90194f6e878d4488, bd0a1efe07fcb4af4bec1b2881a0711f0be34044680ad8cff958a68a70d4a914, ff0f28f96bbb6c80fc3823fe71d5e07e1a05b06986e82a2fbe324d68ba5ab2ea
IPv4	103[.]148[.]245[.]235, 103[.]108[.]67[.]191
Hostname	account[.]drive-google-com[.]tk, login[.]drive-google-com[.]tk

References

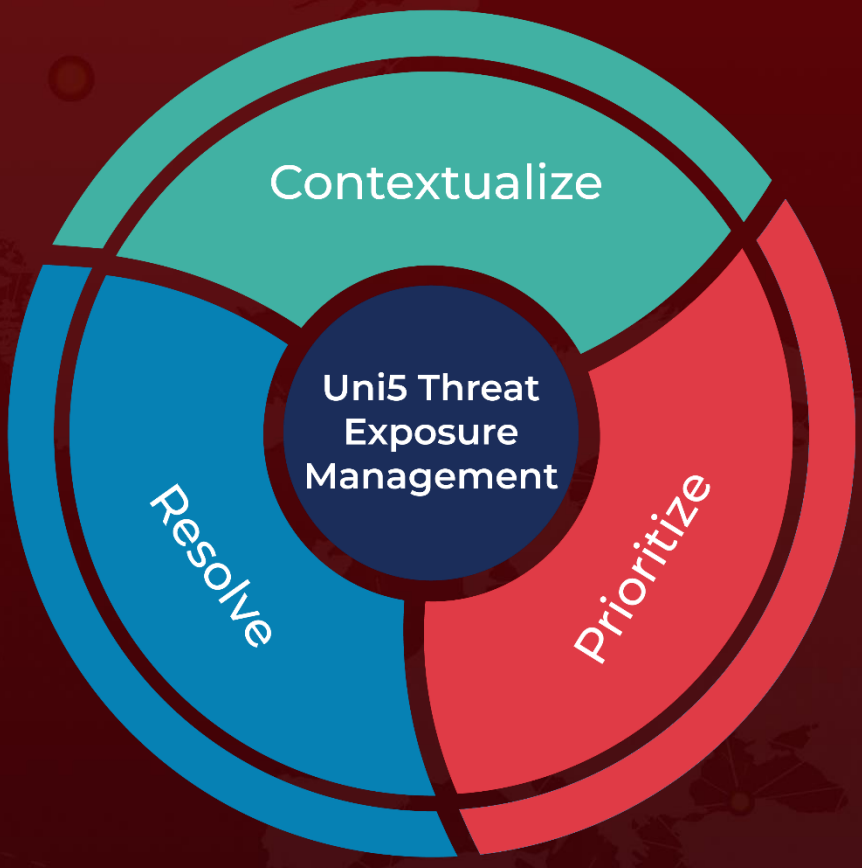
https://blog.talosintelligence.com/new-sugargh0st-rat/

https://attack.mitre.org/software/S0032/

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 4, 2023 . 5:30 AM

More at www.hivepro.com