Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

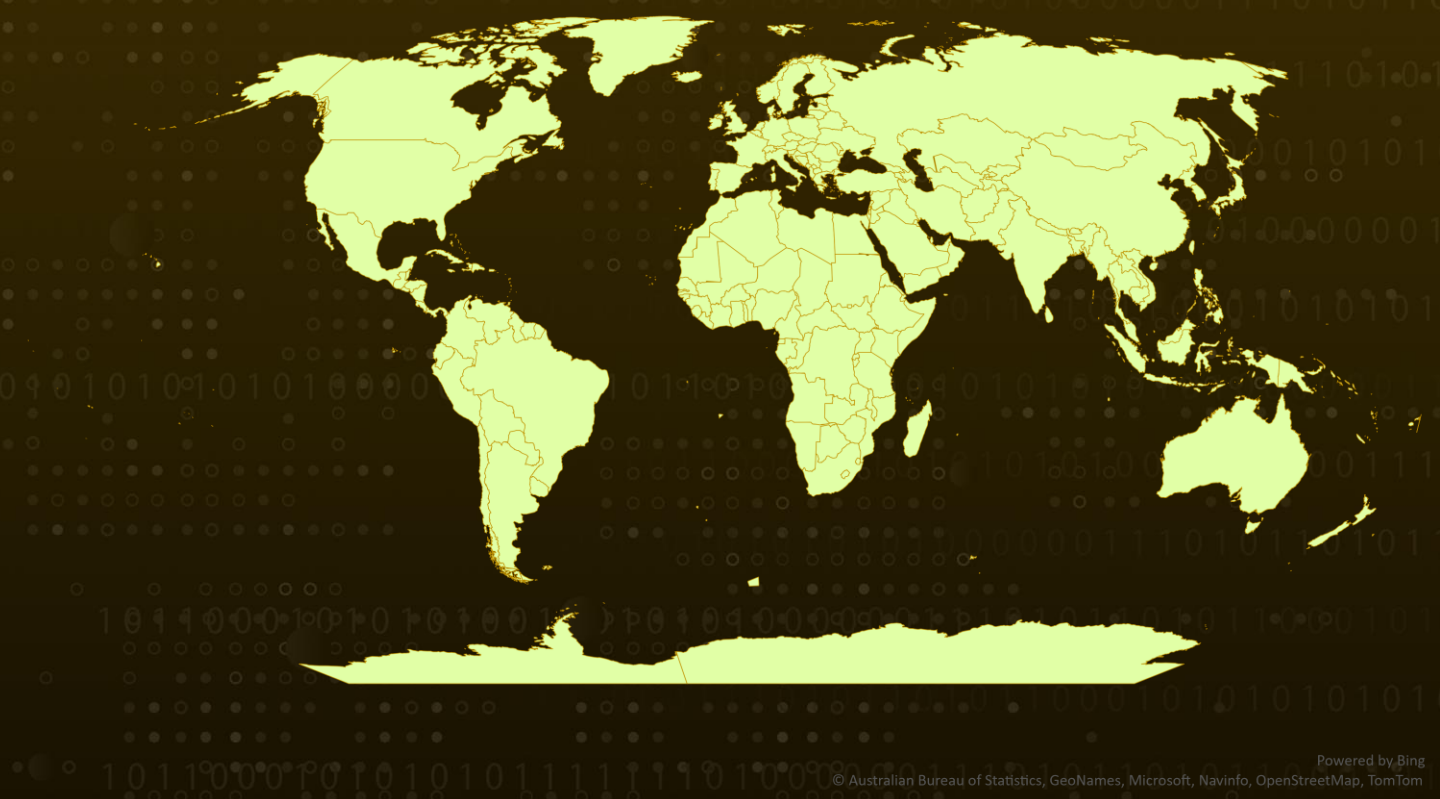
BadSpace Backdoor Infiltrates via Fake Browser Updates

Date of Publication	Admiralty Code	TA Number
June 19, 2024	A1	TA2024234

Summary

First Seen: May 2024
Malware: BadSpace (aka WarmCookie, QUICKBIND)
Affected Platform: Windows
Attack Region: Worldwide
Attack: A new Windows backdoor named BadSpace has emerged, exploiting legitimate but compromised websites to spread through fake browser updates. This campaign's command-and-control (C2) servers are connected to the notorious SocGholish malware.

Attack Regions



Attack Details

#1 In late May 2024, a new Windows backdoor, dubbed BadSpace (also known as WarmCookie or QUICKBIND), surfaced, exploiting legitimate but compromised websites to propagate itself under the guise of fake browser updates.

#2 The attackers injected malicious code into these compromised websites, including those built on WordPress, to harvest device information from first-time visitors. This information includes IP addresses, user agents, and location data.

#3 The collected data is then transmitted to a hard-coded domain via an HTTP GET request, triggering a deceptive Google Chrome update pop-up that delivers a JScript downloader, subsequently installing the backdoor on the victim's system.

#4 The command-and-control (C2) servers utilized in this campaign have been linked to the notorious SocGholish malware (also known as FakeUpdates). BadSpace incorporates anti-sandbox techniques and ensures persistence by setting up scheduled tasks. It is capable of collecting system information and executing commands to take screenshots and delete the scheduled tasks.

Recommendations

Behavior-Based Detection: Use endpoint detection and response (EDR) solutions that can detect unusual behaviors indicative of a backdoor like BadSpace, such as unauthorized access attempts or anomalous system activities.

Content Security Policy (CSP): Deploy CSP headers on web servers to restrict the sources from which browsers can load content, thereby preventing the execution of unauthorized scripts that may deliver BadSpace.

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0011 Command and Control	TA0010 Exfiltration
T1566 Phishing	T1204 User Execution	T1204.001 Malicious Link	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1082 System Information Discovery	T1053 Scheduled Task/Job	T1113 Screen Capture
T1059.003 Windows Command Shell	T1036 Masquerading	T1562 Impair Defenses	T1105 Ingress Tool Transfer
T1059.007 JavaScript	T1059.006 Python		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2b4d7ed8d12d34cbf5d57811ce32f9072845f5274a2934221dd53421c7b8762b, f3fed82131853a35ebb0060cb364c89f42f55e357099289ca22f7af651ee2c48, 255cc818a2e11d7485c1e6cc1722b72c1429b899304881cf36c95ae65af2e566, c64cb9e0740c17b2561eed963a4d9cf452e84f462d5004ddbd0e0c021a8fdabc, 9786569f7c5e5183f98986b78b8e6d7afcad78329c9e61fb881d3d0960bc6a15, c7fc0661c1dabd6efd61eaf6c11f724c573bb70510e1345911bdb68197e598e7, 2a311dd5902d8c6654f2b50f3656201f4ceb98c829678834edaeae5c50c316f5, 0da87bff1a95de9fc7467b9894a8d8e0486dfd868c2c7305e83951babacde642, 6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f, 2a5a12cc4ef2f0f527cc072243aa27d3e95e48402ef674e92c6709dc03a0836a, 2a4451ef47b1f4b971539fb6916f7954f80a6735cf75333fa9d19b169c31de2e, 9bc4c44b24f4ba71a1c7f5dd1c8135544218235ae58efa81898e55515938da6a, 475edfbb2b03182ef7c42c1bc2cc4179b3060d882827029a6e67c045a0c1149b, 676cbcaa74ee8e43abaf0a2767c7559a8f4a7c6720ecc5ae53101a16a3219b9a, 770cafb3fe795c2f13eb44f0a6073b8fe4fb3ee08240b3243c747444592d85ff, 84519a45da0535087202b576391d1952a4cc81213f0e470db65f1817b65ee9d7, a5f16fa960fe0461e2009bd748bc9057ef5cd31f05f48b12cfd7790fa741a24e, a725883bd1c39e48ab60b2c26b5692f7334a3e4544927057a9ffbdabfeedf432, ad2333e1403e3d8f5d9bd89d7178e85523fa7445e0a05b57fd9bc35547ec0d98,

TYPE	VALUE
SHA256	ba4c8be6a1eb92d79df396eea8658b778f4bc0f010da48e1d26e3fc55d83e9c7, b6ac7f6e3b03acd364123a07b2122d943c4111ac4786bb188d94eae0e5b22c02, bb74c6fc0323956dd140988372c412f8b32735fb0ed1ad416e367d29c06af9cc, c437e5caa4f644024014d40e62a5436c59046efc76c666ea3f83ab61df615314, ccde1ded028948f5cd3277d2d4af6b22fa33f53abde84ea2aa01f1872fad1d13
Domains	uhsee[.]com, kongtuke[.]com, omeindia[.]com, assets.work-for[.]top
IPv4	80[.]66[.]88[.]146, 185[.]49[.]69[.]41, 45[.]9[.]74[.]135
Mutex	32ac0087-89d0-4ea5-89af-26a8d08e87ce, f92e6f3c-9cc3-4be0-966c-1be421e69140, 91f785f4-2fa4-4c85-954d-b96768ca76f2
File Path	%ALLUSERSPROFILE%\RtlUpd\RtlUpd.dll, %APPDATA%\RtlUpd\RtlUpd.dll

References

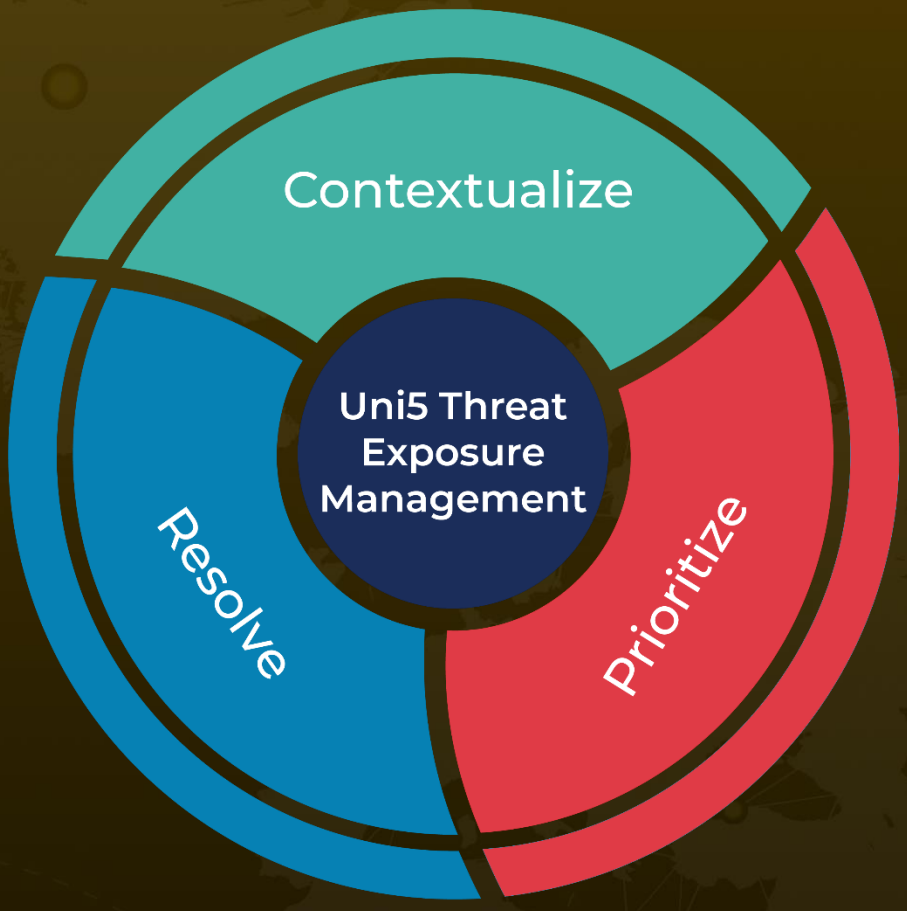
https://www.gdatasoftware.com/blog/2024/06/37947-badspace-backdoor

https://www.elastic.co/security-labs/dipping-into-danger

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

June 19, 2024 • 5:30 AM

More at www.hivepro.com