Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

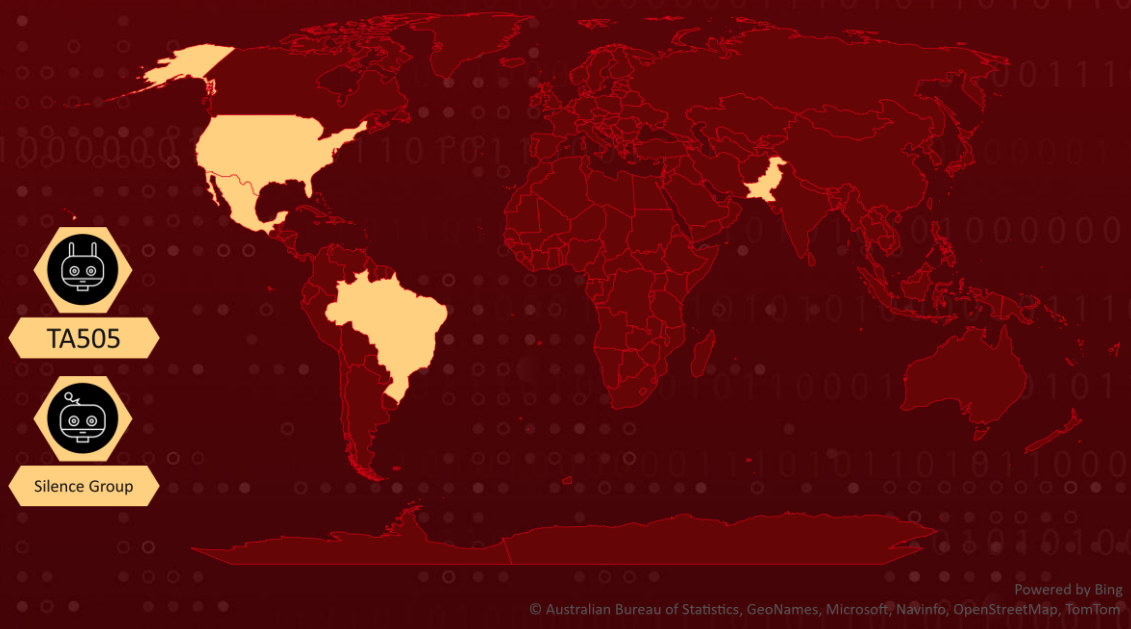
Truebot exploits vulnerability in Netwrix to deploy Clop Ransomware

Date of Publication	Admiralty Code	TA Number
December 12, 2022	B1	TA2022293

Summary

Active Since: 2017
Attack Countries: USA, Mexico, Pakistan, and Brazil
Threat Actors: TA505, Silence Group
Attack Industries: Education
Attack: As part of a double-extortion attack, Clop ransomware targets its victims with a botnet called TrueBot.

Attack Regions



CVE

CVE	NAME	PATCH
CVE-2022-31199	Netwrix Remote Code Execution Vulnerability	✓

Attack Details

#1 In 2017, Truebot was discovered to be linked to the Silence group and has affected more than 1,500 systems worldwide with shellcode, Cobalt Strike beacons, Grace malware, the Teleport tool, and Clop ransomware. A recent study has linked it to TA505.

#2 There are two different Truebot botnets discovered recently; one is distributed worldwide, with a specific focus on Mexico, Pakistan, and Brazil, while the other is focused on the US. In recent attacks, the Raspberry Robin worm and a now-patched vulnerability in Netwrix Auditor have been exploited to deliver malware.

#3 Truebot malware is a downloader malware that spreads through infected systems, collects information on targets, and deploys malicious payloads. The attacker's command and control (C2) receives the collected data.

#4 An unknown custom tool called Teleport was used to exfiltrate stolen data. Teleport commands reveal that the attackers use the tool to collect files from the victim's OneDrive and Downloads folders, as well as from their Outlook email messages. This could result in double extortion using Clop ransomware.

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

TA0001 Initial Access	TA0005 Defense Evasion	TA0011 Command and Control	TA0002 Execution
TA0003 Persistence	TA0042 Resource Development	TA0008 Lateral Movement	TA0043 Reconnaissance
TA0009 Collection	TA0007 Discovery	TA0040 Impact	TA0006 Credential Access
T1566 Phishing	T1190 Exploit Public-Facing Application	T1200 Hardware Additions	T1070 Indicator Removal
T1070.001 Clear Windows Event Logs	T1573 Encrypted Channel	T1059 Command and Scripting Interpreter	T1562 Impair Defenses
T1136 Create Account	T1587 Develop Capabilities	T1587.001 Malware	T1021 Remote Services
T1203 Exploitation for Client Execution	T1590 Gather Victim Network Information	T1592 Gather Victim Host Information	T1210 Exploitation of Remote Services
T1005 Data from Local System	T1083 File and Directory Discovery		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	092910024190a2521f21658be849c4ac9ae6fa4d5f2ecd44c9055cc353a26875 1ef8cdbd3773bd82e5be25d4ba61e5e59371c6331726842107c0f1eb7d4d1f49 2d50b03a92445ba53ae147d0b97c494858c86a56fe037c44bc0edabb902420f7 55d1480cd023b74f10692c689b56e7fd6cc8139fb6322762181daead55a62b9e 58b671915e239e9682d50a026e46db0d775624a61a56199f7fd576b0cef4564d 6210a9f5a5e1dc27e68ecd61c092d2667609e318a95b5dade3c28f5634a89727

TYPE	VALUE
SHA256	68a86858b4638b43d63e8e2aaec15a9ebd8fc14d460dd74463db42e59c4c6f89 72813522a065e106ac10aa96e835c47aa9f34e981db20fa46a8f36c4543bb85d 7a64bc69b60e3cd3fd00d4424b411394465640f499e56563447fe70579ccdd00 7c79ec3f5c1a280ffdf19d0000b4bfe458a3b9380c152c1e130a89de3fe04b63 7e39dcd15307e7de862b9b42bf556f2836bf7916faab0604a052c82c19e306ca 97d0844ce9928e32b11706e06bf2c4426204d998cb39964dd3c3de6c5223fff0 bf3c7f0ba324c96c9a9bff6cf21650a4b78edbc0076c68a9a125ebcba0e523c9 c3743a8c944f5c9b17528418bf49b153b978946838f56e5fca0a3f6914bee887 c3b3640ddf53b26f4ebd4eedf929540edb452c413ca54d0d21cc405c7263f490 c6c4f690f0d15b96034b4258bdfaf797432a3ec4f73fbc920384d27903143cb0
URLs	hxxp://179[.]60[.]150[.]34:80/download/file.ext hxxp://179[.]60[.]150[.]53:80/download/msruntime.dll hxxp://179[.]60[.]150[.]53:80/download/GoogleUpdate.dll hxxp://tddshht[.]com/chkds.dll hxxp://nefosferta.com/gate.php hxxp://185[.]55.[.]243[.]110/gate.php hxxp://gbpooolfhbrb[.]com/gate.php hxxp://88[.]214[.]27[.]100/gate.php hxxp://hiperfdhaus.com/gate.php hxxp://88[.]214[.]27[.]101/gate.php hxxp://jirostrogud[.]com/gate.php
IPv4	45[.]227[.]253[.]102

Patch Details

Upgrade to version 10.5
Link
https://bishopfox.com/blog/netwrix-auditor-advisory

References

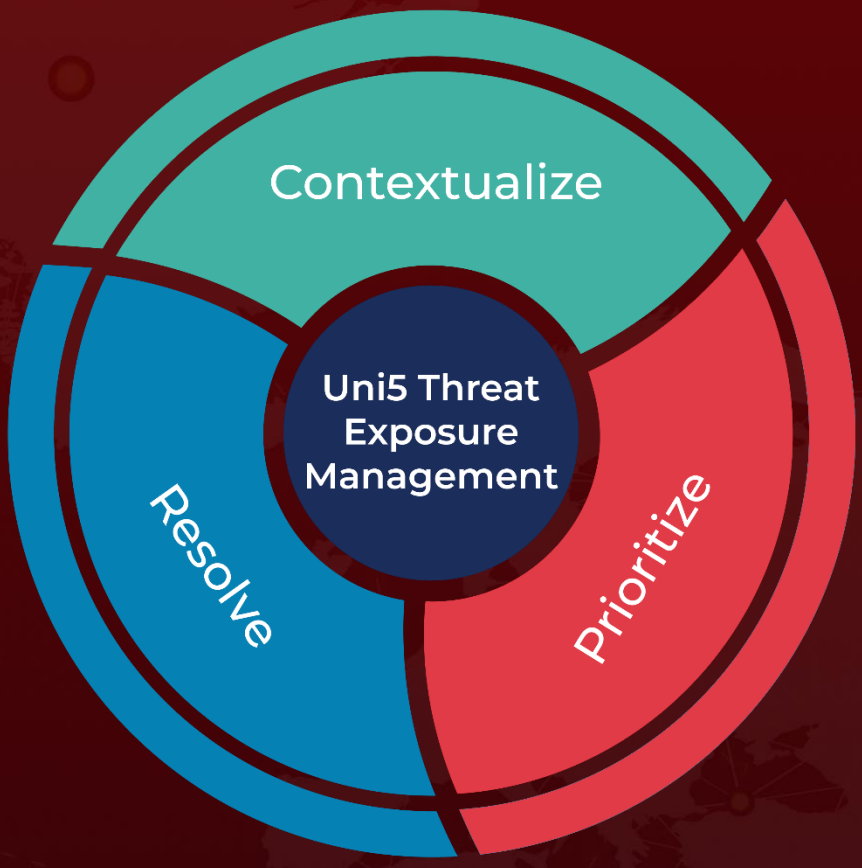
https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

https://otx.alienvault.com/pulse/639390c75bce2382e17867e5/

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 12, 2022 • 5:45 AM

More at www.hivepro.com