Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

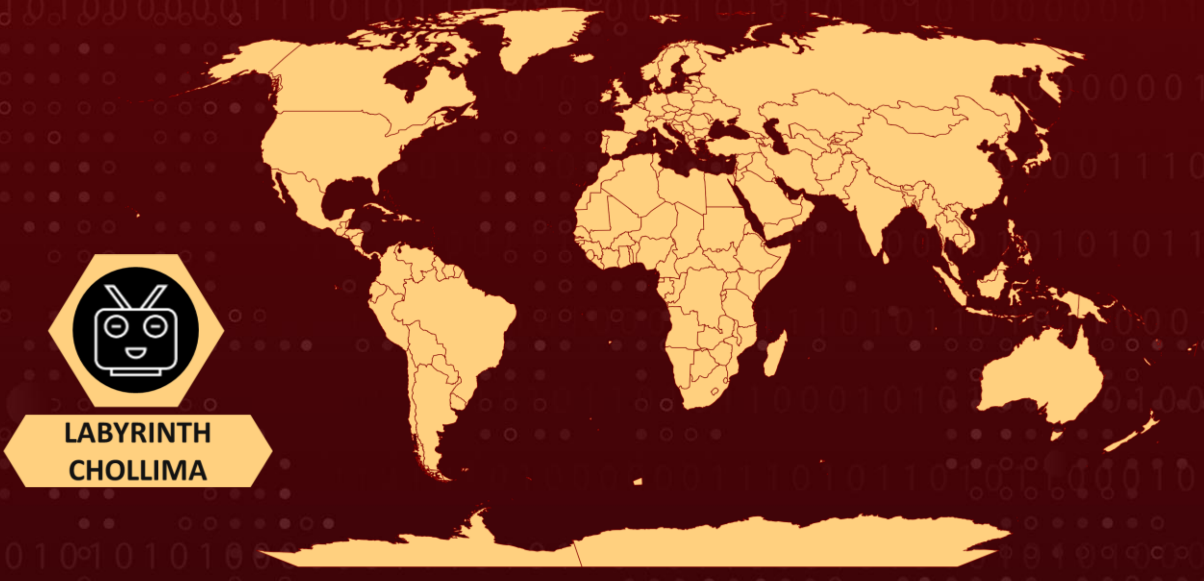
SmoothOperator Campaign Trojanizes 3CXDesktopApp

Date of Publication	Admiralty Code	TA Number
March 31, 2023	A1	TA2023167

Summary

Attack began: March 22, 2023
Actor: LABYRINTH CHOLLIMA (aka HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Lazarus Group)
Malware: ICONIC Stealer or SUDDENICON
Attack Region: Worldwide
Targeted Industries: Automotive, Food & Beverage, Hospitality, Managed Information Technology Service Provider (MSP), Manufacturing
Attack: The 3CX desktop app trojanized via a multi-stage supply attack chain in the SmoothOperator campaign.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	CISA KEV	PATCH
CVE-2023-29059	Arbitrary code execution in 3CXDesktopApp	3CX DesktopApp for Windows Versions: 18.12.407, 18.12.416 & 3CX DesktopApp for macOS Versions: 18.11.1213	✗	✗

Attack Details

#1

The SmoothOperator campaign conducted a supply chain attack targeting downstream customers via rigged installers of a popular conferencing software. The first stage uses a trojanized 3CXDesktopApp, followed by ICO files pulled from Github, ultimately leading to an infostealer dubbed ICONIC Stealer aka SUDDENICONDLL. 3CXDesktopApp is compromised and actively exploited with embedded malicious code (CVE-2023-29059).

#2

The malevolent DLL, which has been sideloaded, includes instructions and a payload encrypted within another DLL using a blob. The shellcode is also present in this blob, which endeavors to retrieve ICO files from GitHub that encompass several URIs for download. The payload is eventually loaded and installed into the targeted environment. The malign behavior comprises beaconing to infrastructure under the control of the attacker, deployment of second-stage payloads, and, in a few instances, direct manipulation of the keyboard.

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	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	T1091 Replication Through Removable Media	T1059 Command and Scripting Interpreter
T1543 Create or Modify System Process	T1543.003 Windows Service	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1056 Input Capture	T1071 Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	github[.]com/IconStorages/images https[://]www.3cx[.]com/blog/event-trainings/ https[://]akamaitechcloudservices[.]com/v2/storage https[://]azureonlinestorage[.]com/azure/storage https[://]msedgepackageinfo[.]com/microsoft-edge https[://]glcloudservice[.]com/v1/console https[://]pbxsources[.]com/exchange https[://]msstorageazure[.]com/window https[://]officestoragebox[.]com/api/session https[://]visualstudiofactory[.]com/workload https[://]azuredeploystore[.]com/cloud/services https[://]msstorageboxes[.]com/office https[://]officeaddons[.]com/technologies https[://]sourceslabs[.]com/downloads https[://]zacharryblogs[.]com/feed https[://]pbxcloudeservices[.]com/phonesystem https[://]pbxphonenetwork[.]com/voip https[://]msedgeupdate[.]net/Windows https[://]sbmsa[.]wiki/blog/_insert

TYPE	VALUE
Emails	cliego.garcia@proton[.]me philip.je@proton[.]me
SHA1	cad1120d91b812acafef7175f949dd1b09c6c21a bf939c9c261d27ee7bb92325cc588624fca75429 20d554a80d759c50d6537dd7097fed84dd258b3e 769383fc65d1386dd141c960c9970114547da0c2 3dc840d32ce86cebf657b17cef62814646ba8e98 9e9a5f8d86356796162cee881c843cde9eaedfb3
SHA256	dde03348075512796241389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405 92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61 b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983 5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290 e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec

References

https://www.sentinelone.com/blog/smoothoperator-ongoing-campaign-trojanizes-3cx-software-in-software-supply-chain-attack/

https://www.3cx.com/blog/news/desktopapp-security-alert/

https://www.tenable.com/blog/3cx-desktop-app-for-windows-and-macos-reportedly-compromised-in-supply-chain-attack

https://www.crowdstrike.com/blog/crowdstrike-detects-and-prevents-active-intrusion-campaign-targeting-3cxdesktopapp-customers/

https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp

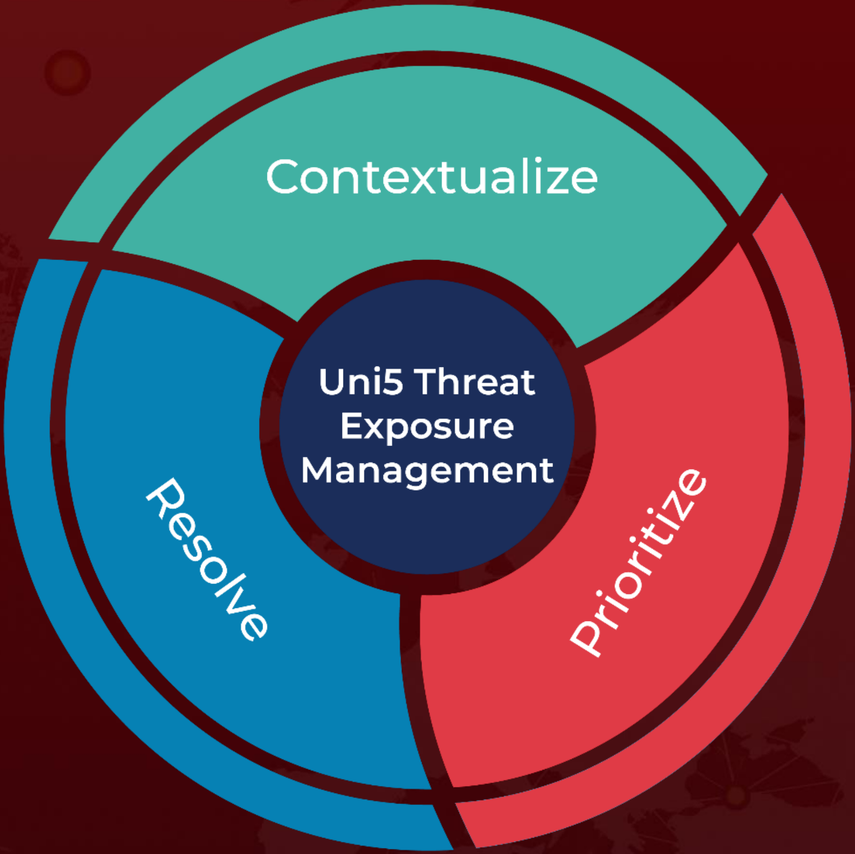
https://thehackernews.com/2023/03/3cx-supply-chain-attack-heres-what-we.html

https://attack.mitre.org/groups/G0032/

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

March 31, 2023 • 7:42 AM

More at www.hivepro.com