Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

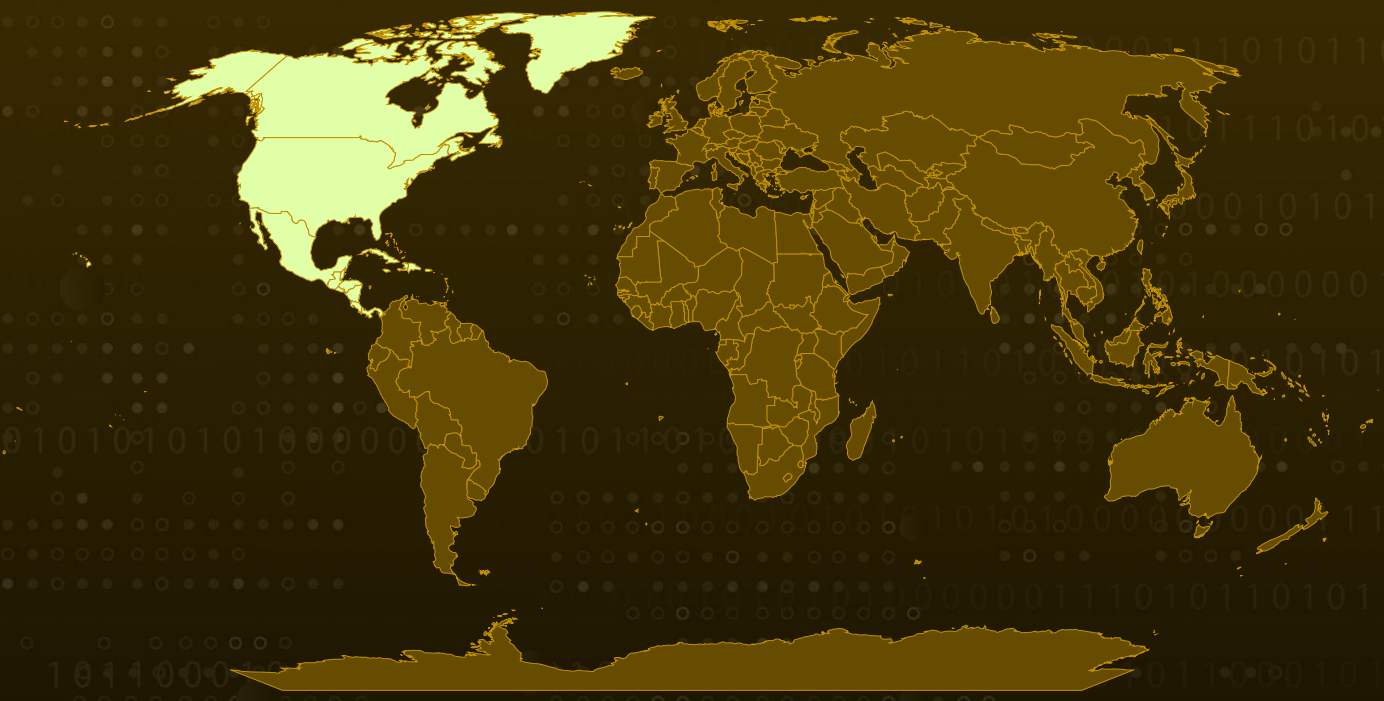
CRON#TRAP: Leveraging Emulated Environments for Covert Cyber Operations

Date of Publication	Admiralty Code	TA Number
November 08, 2024	A2	TA2024424

Summary

Malware: PivotBox, Chisel
Targeted Region: North America
Attack: A new phishing campaign known as CRON#TRAP is leveraging sophisticated techniques to deploy a tailored TinyCore Linux instance on Windows systems via QEMU. The campaign represents a significant evolution in cyber threat tactics, utilizing legitimate virtualization technology to enhance stealth and establish persistent backdoors on compromised systems.

Attack Regions



Attack Details

#1 A new phishing campaign known as CRON#TRAP is leveraging sophisticated techniques to deploy a customized TinyCore Linux instance using QEMU on compromised Windows systems. This campaign utilizes a multi-stage attack process, beginning with phishing emails disguised with “OneAmerica survey” themes.

#2 Phishing email prompts users to download a large ZIP file (approximately 285 MB) containing a Windows shortcut (LNK) file, which, when executed, initiates the installation of a hidden Linux environment. The hidden files are extracted to the user profile directory, where a batch file is executed.

#3 The batch file renders a "server error" static image from a remote URL and initiates the QEMU process in background, thereby launching the emulated environment. The Linux instance is referred as “PivotBox” and is preloaded with chisel backdoor. Chisel is pre-configured to connect to C2 server and is loaded on system startup. The attackers configured multiple persistence mechanisms within the PivotBox.

#4 The CRON#TRAP campaign represents a significant evolution in cyber threats, utilizing phishing to deliver a sophisticated attack environment that enables stealthy and persistent intrusions. This setup not only facilitates covert operations but also underscores the effectiveness of employing legitimate virtualization technology to evade detection, marking a new frontier in the tactics used by cybercriminals.

Recommendations

Be Vigilant: Implement advanced email filtering and conduct regular employee training on recognizing phishing attempts. Utilize tools that track and alert on unusual download sizes while employing sandboxing for suspicious files to mitigate risks.

Endpoint Monitoring: Monitor common malware staging directories, especially script-related activity in user’s home directories. Implement application whitelisting to permit only approved applications to run on the system, enhancing security by blocking unauthorized software.

Network Monitoring: Use network monitoring to detect traffic to malicious domains and IPs linked to known malware servers. Look for connections attempting to contact command-and-control (C2) servers associated with this campaign.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0011 Command and Control	**TA0010** Exfiltration	**T1566.001** Phishing: Spearphishing Attachment	**T1132** Data Encoding
T1572 Protocol Tunneling	**T1071.001** Application Layer Protocol: Web Protocols	**T1072** Software Deployment Tools	**T1041** Exfiltration Over C2 Channel
T1204.002 User Execution: Malicious File	**T1204.001** User Execution: Malicious Link	**T1059.003** Command and Scripting Interpreter: Windows Command Shell	**T1059.001** Command and Scripting Interpreter: PowerShell
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1218** System Binary Proxy Execution	**T1564.006** Hide Artifacts: Run Virtual Instance
T1564.001 Hide Artifacts: Hidden Files and Directories			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	18[.]208[.]230[.]174
URLs	github[.]com/yaniraenrica/testing/raw/main/resolvd.zip, github[.]com/rustyshackleford72/testing/raw/main/cheezel-client, github[.]com/gregtunny/data/raw/refs/heads/main/ch.zip, forum.hestiacp[.]com/uploads/default/original/2X/9/9aae76309a614c85f880512d8fe7df158fec52cc.png
SHA256	CE26AAC9BA7BE60BFB998BA6ADD6B34DA5A68506E9FEA9844DC44BAFE3CAB676, 0618BB997462F350BC4402C1A5656B38BEDC278455823AC249FD5119868D3DF4, 9FFAD9CF6D93B21BB0CA15DE9AB9E782E78F2B6356D05FB55FB95F55BEC9FC04, 002f9cd9ffa4b81301d003acd9fb3fbba1262e593b4f2e56a085b62a50e76510, 5A8BC06587CE40B3A8D8DD4037D0EF272EFC64A69E21F6689FFE3F5FBB04A468, 4C91070877C6D116F5A27EFADDBBFBC339455628E9D6585A4EA5F9B6972BF92B, BC7A34379602F9F061BDB94EC65E8E46DA0257D511022A17D2555ADBD4B1DD38, 3E6A47DA0A226A4C98FB53A06EC1894B4BFD15E73D0CEA856B7D2A001CADA7E9, 9A33EA831EDF83CB8775311963F52299F1488A89651BD3471CC8F1C70F08A36C, 82A9747485FDD60360D28CD73671F171A8312B7D68B26FE1E2D472EB97C4FE59, F4229128EF642D299F7AB5FBCB6DE75A17D12F30F22A3985044C8B1B44F1768F, 6903BDF7F4A22ECFDDBAEE0B16E3DEE85DBB169AA446094BB3D1B75526677B6C

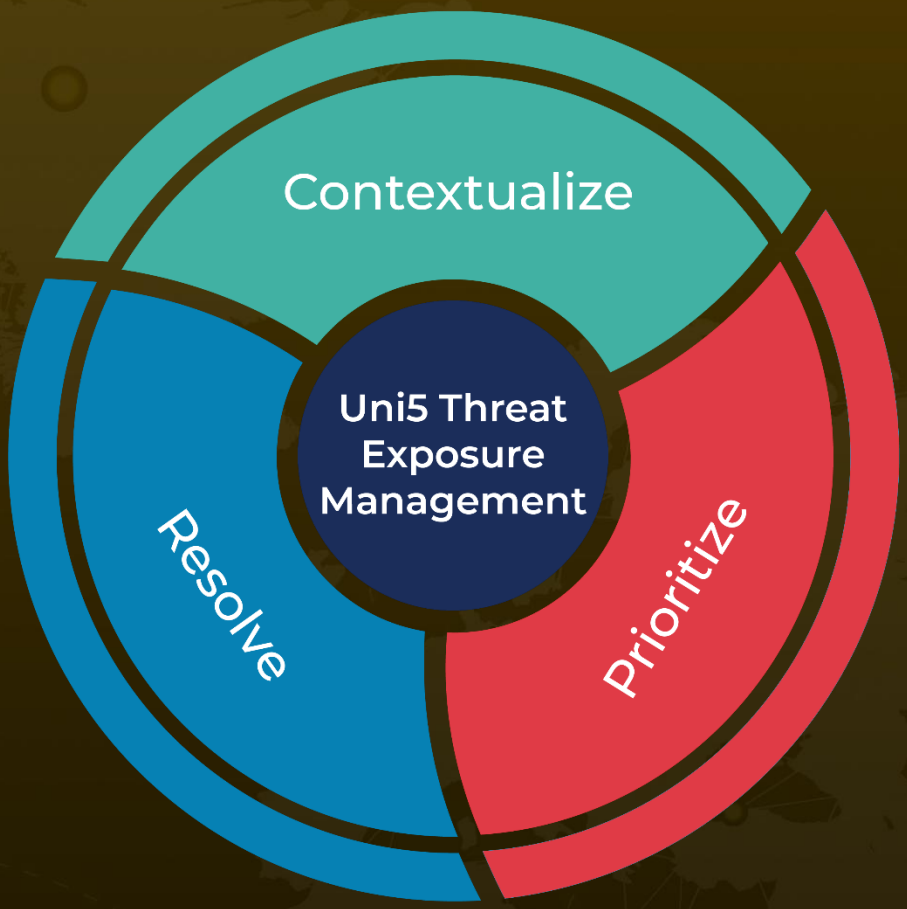
References

https://www.securonix.com/blog/crontrap-emulated-linux-environments-as-the-latest-tactic-in-malware-staging/

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

November 08, 2024 . 10:00 AM

More at www.hivepro.com