Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

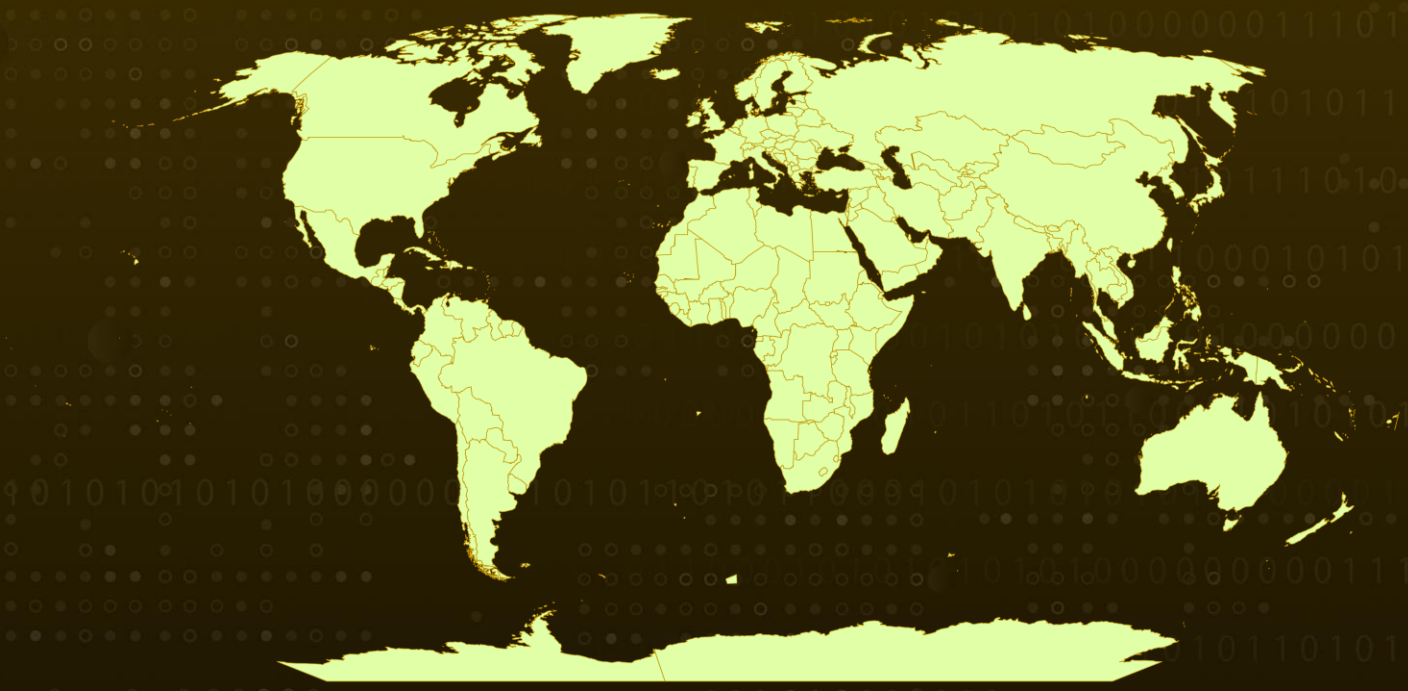
Korean Word Processor Scam Alert: Orcus RAT Lurking in Cracked Versions

Date of Publication	Admiralty Code	TA Number
January 20, 2023	A1	TA2023035

Summary

First appeared: April 1, 2016
Attack Region: Worldwide
Attack: Orcus RAT is being circulated on file-sharing websites as a cracked version of a popular Korean word processor, such as Microsoft Office Word. Along with an Orcus RAT variant, XMRig CoinMiner is disguising itself as a cracked version of Hangul Word Processor 2022.

Attack Regions



Attack Details

#1

Orcus RAT, formerly known as Schnorchel, first appeared in April 2016 and allows for remote control of infected systems. Intruders are attempting to deploy a variant of Orcus RAT along with XMRig CoinMiner, disguised as a cracked version of Hangul Word Processor 2022, in an ongoing campaign. The malicious programs were distributed and infected via several file-sharing sites.

#2

When the downloaded compressed file is decompressed, an obfuscated PowerShell command is executed, followed by the actual installer application. Before proceeding with the installation process, the virus collects and communicates basic information, such as the infected system's login and IP address, via the Telegram API.

#3

The new version of Orcus RAT has a sophisticated mechanism for evading detection by antivirus software, as well as using PowerShell commands on the task scheduler to install updates regularly. Being cautious is essential to avoiding this hazard, as this malware is actively being spread.

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	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1574 Hijack Execution Flow	**T1105** Ingress Tool Transfer	**T1204** User Execution	**T1059** Command and Scripting Interpreter
T1055 Process Injection	**T1102** Web Service	**T1113** Screen Capture	**T1056** Input Capture

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	516a2bde694b31735c52e013d65de48d 6a1fc56b4ce8a62f1ebe25bf7bbe2dbd 74bdc2a8d48a6a4833aac4832e38c3b9 ccf2d6c69a4e016cd19fa4ee7bc341ec 7303e2f671f86909527d8514e1f1f171 9c11f58ed5e7b2806042bc9029a5cca8 d3c271624e23c125b77dd774ffa4af5d bd1301fb0bd0f7d2e75f090894423be0
Domains	minecraftrpgserver[.]com xmr.2miners[.]com minecraftrpgserver[.]com
URLs	hxxps://api.telegram[.]org/bot5538205016:AAH7S9IGtFpb6RbC8W2TfNkjD7Cj_3qxCnI/sendMessage hxxps://docs.google[.]com/uc?export=download&id=1GWm1TFpqTxungXVH0vlktkat5HilyBOJ hxxps://docs.google[.]com/uc?export=download&id=1FgV6vUZZX3XkERFlXDpKQHoo8qYL9r4z hxxps://docs.google[.]com/uc?export=download&id=1T3Kp_aH5-D8F5OS1qv40IPIUXoz3orh4 hxxps://docs.google[.]com/uc?export=download&id=1N75CXe7da3gN7DW2eM4X0w1Rb9XJr7Mx

TYPE	VALUE
URLs	hxxps://docs.google[.]com/uc?export=download&id=1qz1trnHId7cJZsjDnN0r7nSjaLbhw4sN hxxps://docs.google[.]com/uc?export=download&id=1TgGYGUuCp2MC31UKtaOrlEDOIqbvYArO hxxps://docs.google[.]com/uc?export=download&id=1kNCUUyEMYVhfp2rypg-3COmlrnAjBeyd hxxps://docs.google[.]com/uc?export=download&id=1VgEmuFjDFKXL-zVaaO903BHdoJN3Jr8M hxxps://docs.google[.]com/uc?export=download&id=1l4cygNMQxj-oyPPPFq65x1ALk9duhd7D hxxps://docs.google[.]com/uc?export=download&id=1bPnNN92VXIoGEWl-AAiYq_KAjqZA9Boe hxxps://docs.google[.]com/uc?export=download&id=1DkEj9fNfDssSj0qNhpQUn1U-bHogDRrv hxxps://docs.google[.]com/uc?export=download&id=1-B3960J-kcD_v9PaVP0gYyGpZVWDTHOw hxxps://docs.google[.]com/uc?export=download&id=11oXcLJflmBUXZAycZ3mbTiqNctbmox0b

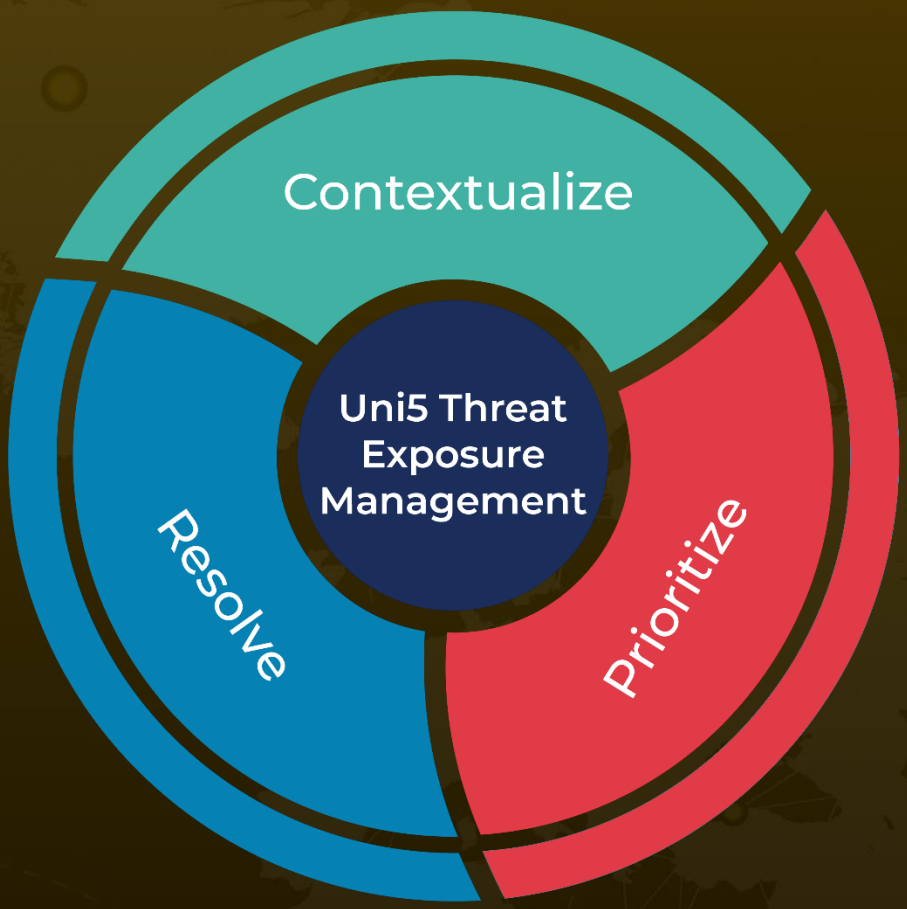
References

https://asec.ahnlab.com/en/45462/

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

January 20, 2023 . 5:55 AM

More at www.hivepro.com