Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

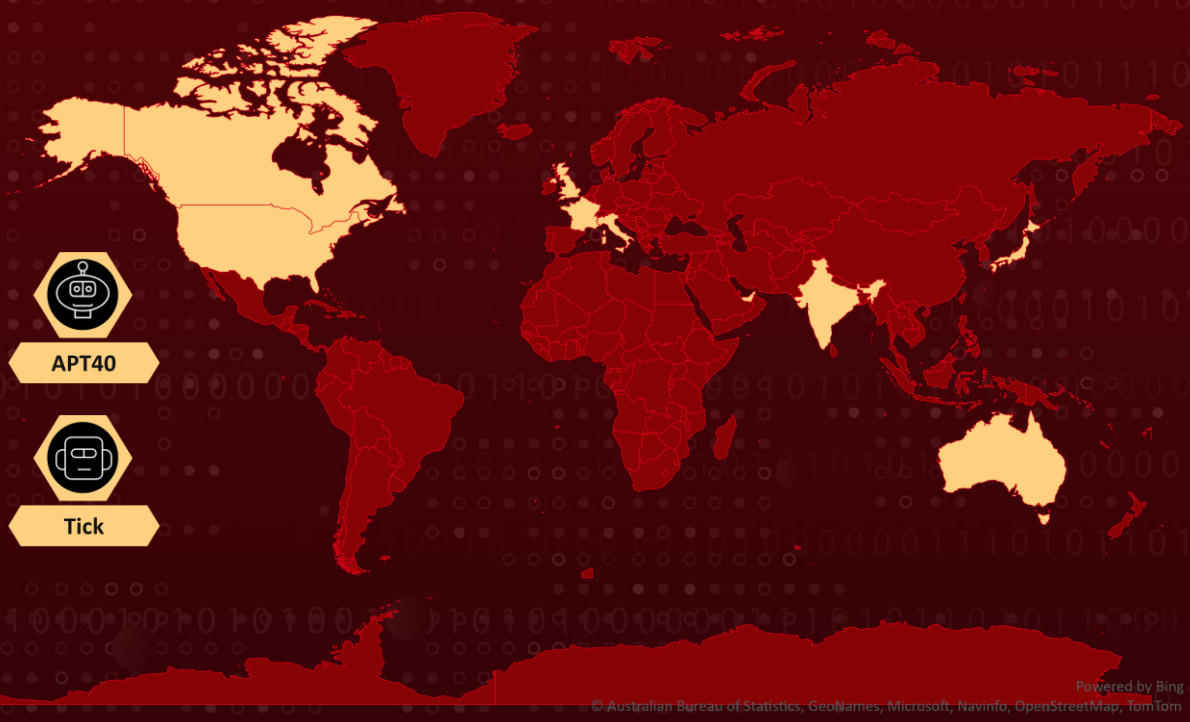
Chinese Threat Actors Leverage Phishing and GuLoader to Distribute Remcos RAT

Date of Publication	Admiralty Code	TA Number
January 24, 2023	A1	TA2023042

Summary

Campaign observed: November 2022
Threat Actor: APT40, TICK
Attack Countries: Australia, Canada, France, India, Italy, Japan, Singapore, South Korea, UAE United States, and United Kingdom
Attack Sector: Banks, Diversified Financial Services, Energy Equipment & Services, Government Entities, Industrial Conglomerates, Insurance, Internet & Direct Marketing, IT Services, Retail, Storage & Peripherals, Technology Hardware, Trading & Distributors.
Attack: Chinese threat actors are conducting phishing campaigns to deploy Remcos RAT and GuLoader.

Attack Regions



Attack Details

#1

The malicious campaign described involves the distribution of a malicious PDF file through email, via phishing. The PDF file in this case redirects victims to a legitimate cloud-based platform, where they are prompted to download a ZIP file. Inside the ZIP file is a shortcut link, which when executed, uses PowerShell to download a heavily obfuscated VBS script known as GuLoader.

#2

GuLoader is an advanced malware downloader that uses a polymorphic shellcode loader to evade detection from traditional security solutions. The shellcode itself is encrypted and later heavily obfuscated, making static analysis difficult. The majority of malware downloaded by GuLoader is commodity malware, with AgentTesla, FormBook, and NanoCore being the most prominent. This time, it is deploying Remcos RAT on the victim machine. Remcos RAT has been operating since 2016. This RAT was originally promoted as genuine software for remote control of Microsoft Windows from XP onwards by a German security firm. Although the security firm claims that the program is only available to those who intend to use it for legal purposes Remcos RAT is now widely used in multiple malicious campaigns by threat actors.

#3

The email campaign to deliver GuLoader and Remcos RAT to the victim machine is believed to be active since the end of November 2022. The threat actor is using Linux/Ubuntu Server at IP “194[.]180[.]48[.]211” and deploys malicious obfuscated and encrypted scripts there. The PDF file is sent as an attachment in the email to the victim, which redirects the user to a cloud-based mega drive to download a ZIP file that contains a shortcut (LNK) file. On execution, the shortcut link runs PowerShell to download the highly obfuscated VBS script from the server identified as GuLoader which injects the malicious code into the legitimate browser Internet Explorer file “ieinstal.exe” to connect with C2 server.

#4

The motives of these campaigns include exploiting the weakness in the systems, carrying out lateral movement into the organization, and executing malware/trojan implants. Recent trends show that Chinese nation-state threat actor groups have been observed to leverage tried and tested malware with new techniques to target governments and organizations to exfiltrate sensitive information and gain maximum benefits with low investment in the early phase of campaigns before executing the next stage of cyber-attacks.

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	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1566 Phishing	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.005 Visual Basic	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1012 Query Registry	T1082 System Information Discovery
T1071 Application Layer Protocol	T1571 Non-Standard Port		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	FA29A3514315DAA300A2F51EFFED36B7 7B458417E456EDFB8816B9F063DD7F4A 4937FCED9860DEE34E4A62036D7EB3E4 2BEA6452110DC15A82C1CE2338AE9303 10F6D31ED0ACFECD2D1EF65C5DC538E0 F37664C2B8D6CAC837ED746DD16CCA4A EE7FEE3FDF1CE0BC40F209AAD8C7BC25
URLs	http[:]//194[.]180[.]48[.]211/lmp/” http[:]/194[.]180[.]48[.]211/tvic/ http[:]/194[.]180[.]48[.]211/Axel/
IPV4	194[.]180[.]48[.]211 178[.]237[.]33[.]50
IPV4:Port	45[.]81[.]39[.]21:28465 84[.]21[.]172[.]49:4890 37[.]0[.]14[.]209:6299

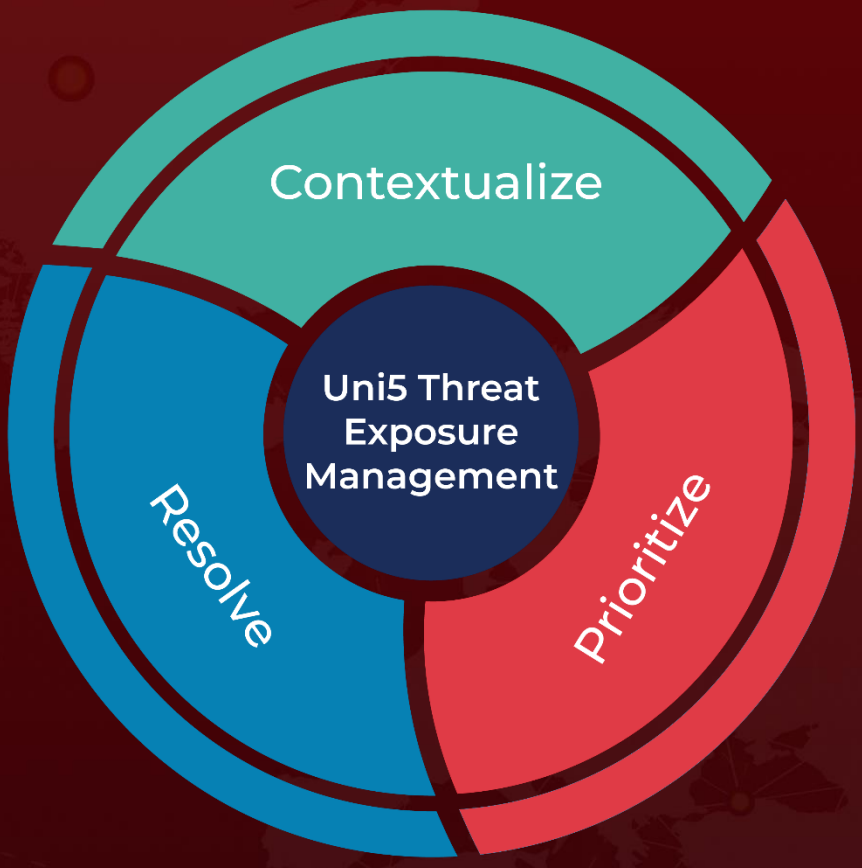
References

https://www.cyfirma.com/outofband/guloader-deploying-remcos-rat/

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 24, 2023 . 2:20 AM

More at www.hivepro.com