Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Grandoreiro Banking Trojan Attacks Industries in Spanish-Speaking Countries

Date of Publication	Admilarity Code	TA Number
August 24, 2022	A1	TA2022180

Summary

Grandoreiro banking trojan is a campaign that has been active since at least 2016 and targets a variety of businesses in Mexico and Spain, including automotive, chemical production, and others. Threat actors' mimic government officials in spear-phishing emails to entice victims to deploy "Grandoreiro." The trojan is built in Delphi and employs techniques such as binary padding to inflate binaries, Captcha implementation for sandbox evasion, and command-and-control (C&C).

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1036** Masquerading	**T1140** Deobfuscate/Decode Files or Information	**T1562** Impair Defenses
T1553 Subvert Trust Controls	**TA0004** Privilege Escalation	**TA0003** Persistence	**T1547** Boot or Logon Autostart Execution
TA0001 Initial Access	**T1566** Phishing	**TA0009** Collection	**T1113** Screen Capture
TA0011 Command and Control	**T1105** Ingress Tool Transfer	**T1102** **Web Service**	

Technical Details

#1

The infection chain starts with a spear-phishing email written in Spanish that includes an embedded link that, when clicked, redirects the victim to a website that downloads a malicious ZIP archive on the victim's Device.

#2

The ZIP archive is bundled with the Grandoreiro Loader module and a PDF Icon to persuade the victim into execution. The ZIP archive contains the following files:

1. A31136.xml: This is not an XML file, but rather a portable executable with the original name "Extensions.dll" and a valid certificate.
2. infonpeuz52271VVCYX.exe: This is the Grandoreiro Loader module. When launched, it has overall control of downloading, extracting, and executing the final 400MB 'Grandoreiro' payload from a remote HTTP File Server(HFS), as well as communicating with the command- and-control system.

#3

The final payload maintains persistence on the system by utilizing the Run Registry key, which allows the payload to be executed on startup. Another active Grandoreiro operation with an additional anti-sandbox approach necessitates manually filling out a Captcha before the malware can be executed on the victim's PC.

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	970f00d7383e44538cac7f6d38c23530 724f26179624dbb9918609476ec0fce4 2ec2d539acfe23107a19d731a330f61c 6433f9af678fcd387983d7afafae2af2 56416fa0e5137d71af7524cf4e7f878d 7ea19ad38940ddb3e47c50e622de2aae e02c77ecaf1ec058d23d2a9805931bf8 6ab9b317178e4b2b20710de96e8b36a0 5b7cbc023390547cd4e38a6ecff5d735 531ac581ae74c0d2d59c22252aaac499
Domains	http[:]//barusgorlerat[.]me http[:]//damacenapirescontab[.]com http[:]//assesorattlas[.]me http[:]//perfomacepnneu[.]me
URLs	35[.]181[.]59[.]254/info99908hhzzb.zip 35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012 35[.]181[.]59[.]254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494 52[.]67[.]27[.]173/deposito(1110061313).zip 54[.]232[.]38[.]61/notificacion(flfit48202).zip 54[.]232[.]38[.]61/notificacion(egmux24178).zip 15[.]188[.]63[.]127/$TIME 167[.]114[.]137[.]244/$TIME 15[.]188[.]63[.]127:36992/zxeTYhO.xml 15[.]188[.]63[.]127:36992/vvOGniGH.xml 15[.]188[.]63[.]127[:]36992/eszOscat.xml 15[.]188[.]63[.]127:36992/YSRYIRIb.xml 167[.]114[.]137[.]244:48514/eyGbtR.xml

TYPE	VALUE
URLs	barusgorlerat[.]me/MX/ assesorattlas[.]me/MX/ assesorattlas[.]me/AR/ atlasassessorcontabilidade[.]com/BRAZIL/ vamosparaonde[.]com/segundona/ mantersaols[.]com/MEX/MX/ premiercombate[.]eastus.cloudapp.azure.com/PUMA/

References

https://www.zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 24, 2022 • 1:17 AM

More at www.hivepro.com