Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

# Grandoreiro Trojan: An Evolving Threat to Global Banking

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 20, 2024 | A1 | TA2024196 |

# Summary

**Attack Began:** March 2024
**Targeted Regions:** LATAM, Europe, North America, regions of Africa and Indo-Pacific
**Malware:** Grandoreiro Banking Trojan
**Targeted Industries:** Finance
**Affected Platform:** Windows
**Attack:** The Grandoreiro banking Trojan, initially targeting Latin America, has evolved to attack financial institutions globally, now targeting over 1500 banks in 60 countries. The latest variant can harvest email addresses from infected Outlook clients to send further phishing emails, underscoring the need for enhanced global security measures.

## Attack Regions

# Attack Details

**#1**

The Grandoreiro banking Trojan is an advanced malware primarily focused on the financial sector, especially in Latin America. First identified in 2017, it has since evolved, adopting new techniques and expanding its reach to other regions, including Europe, North America, Central America, South America, Africa, Indo-Pacific and global islands. This malware aims to steal financial data, manipulate transactions, and carry out other malicious activities.

**#2**

Despite an INTERPOL joint operation in January 2024 that disrupted a Grandoreiro malware operation, the trojan has returned to large-scale operations since March 2024. Operated as a Malware-as-a-Service (MaaS), Grandoreiro has undergone significant updates, particularly in its decryption and domain generating algorithms.

**#3**

A notable feature of the latest variant is its ability to use Microsoft Outlook clients on infected machines to propagate further phishing emails. It now targets over 1500 global banks across 60 countries, with campaigns impersonating government entities in Mexico, Argentina, and South Africa.

**#4**

Grandoreiro's infection campaigns typically involve phishing emails pretending to be from government agencies, leading recipients to download malware disguised as PDFs. The malware loader evades detection through its size and CAPTCHA pop-ups. Once installed, it verifies victims, communicates with its server, and downloads the main banking trojan payload, which targets various banking applications globally.

**#5**

Grandoreiro can harvest email addresses from Outlook clients to send phishing emails, enhancing its spread. It collects addresses from various sources and crafts convincing emails using templates from its server. The malware acts stealthily, deleting sent messages and operating when users are inactive to avoid detection. Grandoreiro represents a sophisticated and evolving threat, expanding its targeting and infection capabilities globally. Enhanced vigilance and security measures are crucial in combating this threat across affected regions.

# Recommendations

**Enhance Email Security:** Deploy advanced email filtering solutions to detect and block phishing attempts and malware attachments before they reach users' inboxes. Additionally, enable multi-factor authentication (MFA) for email accounts to add an extra layer of security.

**Implement Endpoint Protection:** Deploy comprehensive endpoint protection platforms (EPP) that include behavior analysis and real-time threat detection capabilities. Ensure all systems and software are kept up-to-date with the latest security patches.

**Registry Monitoring for Persistence:** Regularly monitor registry Run keys (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run andHKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ) for unauthorized modifications, which may indicate persistent threats.

**Consider DNS Blocking:** Take proactive measures by blocking pre-calculated Domain Generation Algorithm (DGA) domains via DNS. This can disrupt the malware's ability to communicate with its command-and-control servers.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0010<br>Exfiltration | TA0040<br>Impact | TA0011<br>Command and Control | TA0043<br>Reconnaissance |
| TA0007<br>Discovery | TA0003<br>Persistence | TA0004<br>Privilege Escalation | TA0009<br>Collection |
| TA0001<br>Initial Access | TA0002<br>Execution | TA0005<br>Defense Evasion | T1071.004<br>DNS |
| T1497<br>Virtualization/Sandbox Evasion | T1059<br>Command and Scripting Interpreter | T1059.006<br>Python | T1592<br>Gather Victim Host Information |
| T1568.002<br>Domain Generation Algorithms | T1568<br>Dynamic Resolution | T1568.003<br>DNS Calculation | T1114<br>Email Collection |

| | | | |
|---|---|---|---|
| T1056.001<br>Keylogging | T1056<br>Input Capture | T1529<br>System Shutdown/Reboot | T1217<br>Browser Information Discovery |
| T1562.006<br>Indicator Blocking | T1562<br>Impair Defenses | T1059.007<br>JavaScript | T1027<br>Obfuscated Files or Information |
| T1573<br>Encrypted Channel | T1140<br>Deobfuscate/Decode Files or Information | T1547.001<br>Registry Run Keys / Startup Folder | T1547<br>Boot or Logon Autostart Execution |
| T1566.001<br>Spearphishing Attachment | T1566.002<br>Spearphishing Link | T1566<br>Phishing | T1071<br>Application Layer Protocol |
| T1036<br>Masquerading | T1204<br>User Execution | T1027.013<br>Encrypted/Encoded File | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| SHA256 | 97f3c0beef87b993be321b5af3bf748cc8e003e6e90cf5febf69dfd81e85f581,<br>afd53240a591daf50f556ca952278cf098dbc5b6c2b16c3e46ab5a0b167afb40,<br>f8f2c7020b2d38c806b5911acb373578cbd69612cbe7f21f172550f4b5d02fdb,<br>10b498562aef754156e2b540754bf1ccf9a9cb62c732bf9b661746dd08c67bd1,<br>55426bb348977496189cc6a61b711a3aadde155772a650ef17fba1f653431965,<br>bfcd71a4095c2e81e2681aaf0239436368bc2ebddae7fdc8bb486ffc1040602c,<br>3f920619470488b8c1fda4bb82803f72205b18b1ea31402b461a0b8fe737d6bd,<br>84572c0de71bce332eb9fa03fd342433263ad0c4f95dd3acd86d1207fa7d23f0,<br>29f19d9cd8fe38081a2fde66fb2e1eff33c4d4b5714ef5cada5cc76ec09bf2fa, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 2ab8c3a1a7fe14a49084fbf42bbdd04d6379e6ae2c74d801616e2b9cf8c8519c, 70f22917ec1fa3a764e21f16d68af80b697fb9d0eb4f9cd6537393b622906908, fb3d843d35c66f76b1b1b88260ad20096e118ef44fd94137dbe394f53c1b8a46, 6772d2425b5a169aca824de3ff2aac400fa64c3edd93faaabd17d9c721d996c1 |
| URLs | hxxps[:]//onwfacttasunslahf[.]norwayeast[.]cloudapp[.]azure[.]com?_task=mail&_action=get&_mbox=INBOX&_uid=19101&_token=rbrJMXNUOQvrlaWOOxGAyj7vcufaFN3r&_part=1.2.3&_embed=1&_mimeclass=image, hxxps[:]//pjohconstruccionescpaz[.]com?docs/xml/WCA161006TN9/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp.azure[.]com/?PDF-XML-71348793, hxxps[:]//officebusinessaccount[.]eastus[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//servicerevenueza[.]southeastasia[.]cloudapp[.]azure[.]com/?PDF-XML-<eight digit number>, hxxps[:]//hilcfacdigitaelpichipt[.]norwayeast[.]cloudapp.azure[.]com/?docs/pdf/15540f02-d006-4e3b-b2de-6873baff3b2a, hxxps[:]//pjohconstruccionescpaz[.]com/?8205-23069071&tokenValue=92b768ccface4e96cee662517800b208f88ff796 |
| Emails | gruposat[@]gob[.]mx, root[[@]]zpmbnoxf[.]crazydocuments[.]com, marcasat[@]gob[.]mx , assistance[@]gov[.]za , ^root[@]yhsp\d{2}\[.]rufnag\[.]com$ |
| Domains | Rufnag[.]com, pjohconstruccionescpaz[.]com |
| IPv4 | 18[.]231[.]181[.]227, 18[.]231[.]158[.]159, 15[.]229[.]211[.]175, 15[.]228[.]245[.]103 |

# References

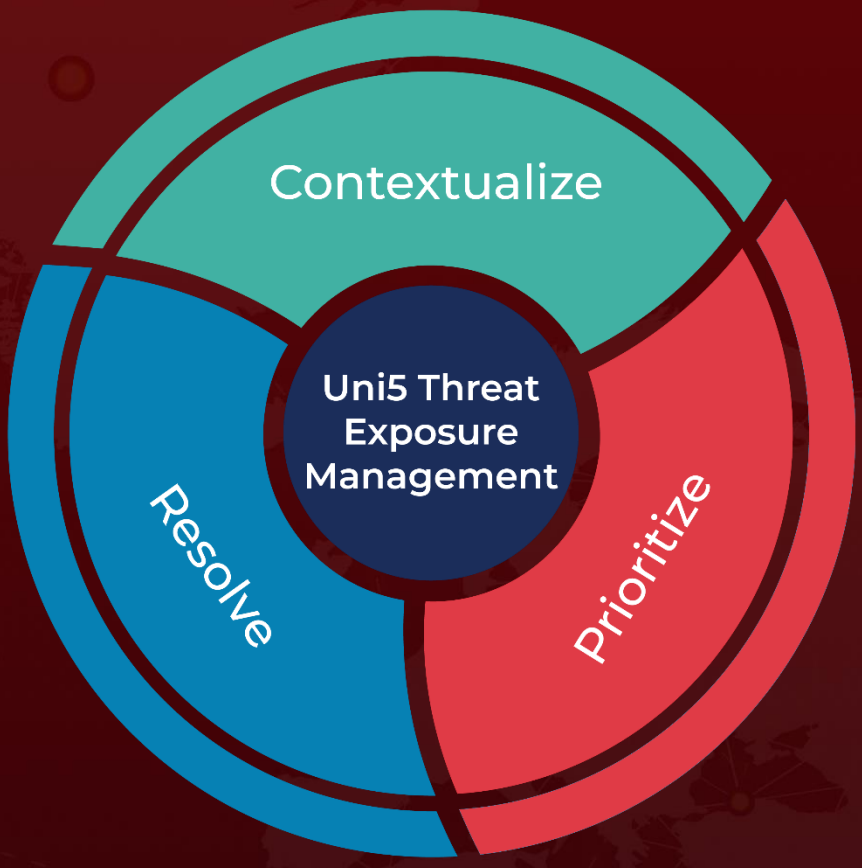

https://securityintelligence.com/x-force/grandoreiro-banking-trojan-unleashed/

https://www.interpol.int/en/News-and-Events/News/2024/Disrupting-a-Grandoreiro-malware-operation

# 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

**May 20, 2024 • 10:30 PM**



More at www.hivepro.com