Grandoreiro Malware Campaign: A Global Threat to Banking Security

By Ameer Owda

Published: 2024-06-07 · Archived: 2026-04-06 01:34:46 UTC

The Grandoreiro banking trojan was first observed in 2016. This threat is described as a highly sophisticated and adaptive Windows-based banking trojan. Grandoreiro uses a Malware-as-a-Service (MaaS) model, making it easily accessible to various cybercriminals. Its latest wave affected Central and South America, Africa, Europe and the Indonesia-Pacific region, targeting more than **1,500 banks** in more than **60 countries**.

Banks targeted by the Grandoreiro malware, distributed by countries (X Force)

Grandoreiro uses advanced techniques to infiltrate systems and evade detection. These techniques include bypassing **User Account Control (UAC)**, parsing Outlook .pst files to extract email addresses, using HTTP in Command and Control (C2) communications, creating link files in system startup folders to ensure continuity, hijacking browser sessions, and stealing cookie data and credentials from web browsers such as Google Chrome.

Description of the Grandoreiro Malware Campaign

The Grandoreiro banking trojan has reemerged as a significant global threat to banking security, following a resurgence in March 2024 despite law enforcement efforts to dismantle its operations.

For more details, see the Grandoreiro Malware Campaign on SOCRadar Platform's Campaigns page

This sophisticated Windows-based malware, first detected in 2016, has targeted over 1,500 banks across more than 60 countries, employing advanced techniques to infiltrate systems and avoid detection. It uses a Malware-as-a-Service (MaaS) model, making it accessible to a broad spectrum of cybercriminals.

The phishing emails employed in the campaign frequently mimic legitimate organizations, including Mexico's Tax Administration Service (SAT), Mexico's Federal Electricity Commission (CFE), and the South African Revenue Service (SARS). These emails typically contain links that direct recipients to **ZIP files infected with malware**.

Sample email impersonating CFE, Mexico's Federal Electricity Commission

Grandoreiro Malware Capabilities

Grandoreiro employs several sophisticated techniques to compromise systems, including abusing elevation control mechanisms, email account discovery, application layer protocol communication, boot or logon autostart execution, browser session hijacking, and stealing credentials from web browsers.

The malware's unique loader checks the legitimacy of the victim, gathers basic information, and then executes the Grandoreiro trojan. To bypass automated scanning, it employs a **CAPTCHA pop-up** and evades detection by increasing the size of the executable. The malware uses a complex decryption process, involving multiple layers of encryption and custom algorithms, to obtain the plaintext strings required for its operation.

Grandoreiro collects extensive data from infected machines, including IP addresses, operating system details, and information about installed software, all of which are sent to the C2 server. To avoid DNS-based blocking, it uses DNS over HTTPS and employs a **Domain Generation Algorithm (DGA)** to determine active C2 domains. Encrypted requests are sent to the C2 server to retrieve the final payload.

Grandoreiro DGA visualization

Impact of the Grandoreiro Malware Campaign

The impact of the Grandoreiro campaign has been devastating, resulting in financial fraud and significant monetary losses. It affected various sectors such as banking, finance, manufacturing, public administration, telecommunications, and energy and utilities.

The chart below depicts the top countries that have been targeted by the Grandoreiro malware:

Malware infections in early May, distributed by countries

Mitigation Strategies

To combat Grandoreiro, organizations should implement a multi-layered defense strategy, including email and phishing defense, network traffic surveillance, blocking DGA domains, Windows registry surveillance, enhanced endpoint security, and user education programs.

In the event of an infection, critical steps include identifying and removing infected systems, updating and patching systems, monitoring and hardening network security, user account and access management, regular audits and monitoring, and incident response planning. In the face of the re-emergence of Grandoreiro, the following are important countermeasures and defense strategies that organisations should take:

- **Email and Phishing Defence**
- - Deploy sophisticated email filtering systems, blocking emails from suspicious domains.
  - Provide regular training to employees to raise awareness about recognizing phishing emails.
- - Conduct regular training sessions to raise awareness of phishing and educate users on safe browsing habits.
  - Encouraging verification of email senders and URLs before clicking or downloading attachments.
- **Network Traffic Surveillance**
- - Implement anomaly detection systems that can detect abnormal traffic patterns.
  - Using network fragmentation, controlling the spread of malware, and providing isolation against suspicious activities.

- **Blocking DGA Domains**
- Using DNS filtering solutions, block domains created by Grandoreiro's Domain Generation Algorithm (DGA).
- Proactively monitor and block new malicious domains by utilizing threat intelligence services.
- **Windows Registry Surveillance**
- Regularly audit Windows registry entries to detect and remove unauthorized changes.
- Monitor registry changes in real time using automated tools.
- **Enhanced Endpoint Security**
- Ensuring that all endpoints are equipped with up-to-date antivirus and anti-malware software.
- Providing advanced threat detection and remediation by implementing Endpoint Detection and Response (EDR) solutions.

These strategies are critical to building an effective line of defense against complex and adaptive threats such as Grandoreiro.

Conclusion

The resilience and adaptability of the Grandoreiro banking trojan, even after a major law enforcement operation, underscore the need for robust cybersecurity measures. Organizations must adopt advanced threat detection, regular audits, user education, and comprehensive endpoint protection to effectively counter this persistent threat.

For more information about the Grandoreiro Malware Campaign and many more campaigns, you can visit our Campaigns page on SOCRadar LABS.

SOCRadar LABS, Campaigns page

YARA RULES

Below is a YARA Rule, which may be used for the detection of Grandoreiro malware. You can find YARA Rules related to various malware with SOCRadar's Threat Hunting Rules.

```
rule Windows_Trojan_Grandoreiro_51236ba2 {
   meta:
        author = "Elastic Security"
        id = "51236ba2-fdbc-4c46-b57b-27fc1e135486"
        fingerprint = "c3082cc865fc177d8cbabcfcf9fb67317af5f2d28e8eeb95eb04108a558d80d4"
        creation_date = "2022-08-23"
        last_modified = "2023-06-13"
        description = "Grandoreiro rule, target loader and payload"
        threat_name = "Windows.Trojan.Grandoreiro"
        reference_sample = "1bdf381e7080d9bed3f52f4b3db1991a80d3e58120a5790c3d1609617d1f439e"
```

```
        severity = 100
        arch_context = "x86"
        scan_context = "file, memory"
        license = "Elastic License v2"
        os = "windows"
    strings:
        $antivm0 = { B8 68 58 4D 56 BB 12 F7 6C 3C B9 0A 00 00 00 66 BA 58 56 ED B8 01 00 00 00 }
        $antivm1 = { B9 [4] 89 E5 53 51 64 FF 35 00 00 00 00 64 89 25 00 00 00 00 BB 00 00 00 00 B8 01 00 00 00
        $xor0 = { 0F B7 44 70 ?? 33 D8 8D 45 ?? 50 89 5D ?? }
        $xor1 = { 8B 45 ?? 0F B7 44 70 ?? 33 C3 89 45 ?? }
    condition:
        all of them
}
```

Indicators of Compromise (IOCs)

MD5 Hashes:

- 5ba143b5cef7e0505de283091c288e35
- 6b9217ef9cbd2b29bfc353261566be1a
- 7b6defb3ec63cc0c4b8ff21bba79c830
- cf48f1fecfe2efbb3071e9c3eb2140e0
- e02c77ecaf1ec058d23d2a9805931bf8
- 970f00d7383e44538cac7f6d38c23530
- 5b7cbc023390547cd4e38a6ecff5d735
- 56416fa0e5137d71af7524cf4e7f878d
- 2ec2d539acfe23107a19d731a330f61c
- 3b5c1137198d2aecfbc288f1d5693b4e
- 1c913e1918f175e135f03146819cd743
- 121a870dd7cdd01fc2baa6897d376492

SHA1 Hashes:

- 8db589e61c6a9aeb47cd35570318b321866a415d
- 987d02620b4f57a667771f03ebb4c89ed3bf7cc8
- ceafe62c098f30e369eb7dac19dc04e66248fa90
- e68804f8fed07df2bfd3f85d38db673f92d9137e
- c91b333502f6f43aef47441bbf06e7912cef8143
- 3c928e286997daab447e0cfe13988dad9923fd96

SHA256 Hashes:

- 2d3ec83c7a50990b13221e9018fe0c2b0b7fd6d1534160adf56f5df836e46537
- 880db8383100c53c408224a003b312b6d57954ef42d3663ec80e4157ba003a01
- e2dc1f6e45a7be302736e1b42bb97e6a7877f82e081389b7a8195ea22cf6a10c

- 794ad887a11149f438ecc886b5dfc6fa0503c26b8e63f48cf0bf2dcc2cdc58bb
- 45992c4d15aa21aa0a6a29bcc306a25cb13b7c6bebe8d5de5f51cd325259b285
- 25acc903388cf6e4d65c0d8295da8688ece1be4a6e6bec9e5d467f91f6026a4a

Domains and IP Addresses:

- vamosparaonde.com
- perfomacepnneu.me
- mantersaols.com
- damacenapirescontab.com
- barusgorlerat.me
- atlasassessorcontabilidade.com
- assesorattlas.me
- http://vamosparaonde.com/segundona/
- http://mantersaols.com/MEX/MX/
- http://barusgorlerat.me/MX/
- http://atlasassessorcontabilidade.com/BRAZIL/
- http://assesorattlas.me/MX/
- http://assesorattlas.me/AR/
- http://167.114.137.244:48514/eyGbtR.xml
- http://167.114.137.244/$TIME
- http://15.188.63.127/$TIME
- http://15.188.63.127:36992/YSRYIRIb.xml
- http://15.188.63.127:36992/vvOGniGH.xml
- http://15.188.63.127:36992/zxeTYhO.xml
- http://35.180.117.32/$FISCALIGENERAL3489213839012
- http://35.181.59.254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494
- http://35.181.59.254/info99908hhzzb.zip
- http://52.67.27.173/deposito
- http://54.232.38.61/notificacion
- http://15.188.63.127:36992/zxeTYhO.xml”
- http://premiercombate.eastus.cloudapp.azure.com/PUMA/

CVE Identifiers:

- CVE-2022-34233

While we strive to provide accurate and up-to-date information about malware threats, it is important to exercise caution when handling potential malware links or Indicators of Compromise (IOCs). Please only access such links or IoCs from trusted sources and take appropriate security measures to protect your system.
