Grandoreiro Malware: Spear Phishing, Outlook Exploits, and More

By Flashpoint Intel Team

Published: 2024-08-01 · Archived: 2026-04-05 14:42:29 UTC

Grandoreiro, a banking trojan that once preyed on Latin American financial institutions, has reemerged. Previously thought to have been shut down in a joint operation spearheaded by the Federal Police of Brazil, Flashpoint analysts have observed new reports of the malware targeting victims in North America, Europe, Asia, and Africa. Now that this once-regional threat has gone global, it is essential that organizations understand how the trojan works and learn how to protect against it.

Understanding How Grandoreiro Works

The focus of Grandoreiro is to steal financial information, steal credentials, and make unauthorized money transfers. Grandoreiro is primarily disseminated through spear phishing, using malicious links or email attachments for initial infection. However, after this, the malware uses a unique module that enables it to spread even further by utilizing local installations of Microsoft Outlook.

This is accomplished by leveraging email templates sent to Outlook by the command and control (C2) server. The malware then uses a legitimate component to access the local Outlook namespace. It then systematically scans through the victim's inbox and filters out unwanted email addresses. These harvested emails are then sent the email template acquired from the C2 server.

Next, Grandoreiro distributes phishing emails that contain links to ZIP archives or MSI installer files masquerading as PDF documents. These files harbor the Grandoreiro loader which is primed to infect additional systems and perpetuate the malware's distribution.

The Grandoreiro Loader

The custom loader is written in Borland Delphi. To avoid antivirus scanning, the Grandorero loader is bloated to over 100 MB. When the custom loader executes, it requires user interaction in the form of a fake Adobe Acrobat captcha to prevent execution in sandbox environments.

After this, additional anti-analysis checks will occur. The malware uses standard process enumeration APIs and searches for an extensive list of analysis tools and other sandbox indicators.

Example of a sandbox environment check code block for Grandoreiro malware

If the target machine passes the anti-analysis check, the malware then acquires basic information about the victim. This includes the target's public IP address and location. Afterwards, it then collects machine information such as

the username, computer name, OS version, installed antivirus, if Outlook is installed, the number of cryptocurrency wallets installed, the number of specialty banking software, and other information. All of this is packaged into a single string and sent to the C2 server.

The C2 is hard coded as an encrypted string within the loader. Once the beacon packet is sent, the C2 responds with a location to download the next stage payload and the size of the payload. This payload is RC4 decrypted and executed.


Grandoreiro Malware string decryption | Flashpoint

Flowchart for Grandoreiro's string decryption within the loader

The Grandoreiro Stealer

Like the loader, the main payload is also written in Borland Delphi and is bloated to over 100 MB. It begins by looking for the presence of a .cfg file in both the local directory and in the C:Publicdirectory. This config file contains information on which functions are enabled. If this .cfg file is not present, Grandoreiro will create one. Additionally, it creates an XML file that contains the executable's location and the infection date. Both files' contents are encrypted using Grandoreiro's custom string encryption algorithm.

Additional Malware Capabilities

Grandoreiro primarily targets financial data, login credentials, and facilitates illicit monetary transactions. However, this strain of malware requires threat actor interaction and does not perform independent actions like other infostealers or banking trojans. Using Grandoreiro, threat actors can perform additional actions such as:

1. Disabling mouse inputs and blocking the screen for the infected target.
2. Establishing remote control to steal money without disruption.
3. Creating fake login screens or leveraging keylogging features to steal credentials.
4. Downloading and executing additional malware.

How to Defend against It

Grandoreiro malware is written to target both financial institutions and individuals. Therefore, it is essential that readers take the proper precautions to repel or mitigate targeting attempts. Here are some ways you can protect yourself:

- **Rely on a comprehensive source of threat intelligence:** Threat actors are constantly improving their tactics and tools. Having access to detailed threat intelligence will help security teams stay informed on the latest malware changes and trends.
- **Heightened email vigilance**: Exercise extreme caution when handling unsolicited emails, especially those containing links or attachments. Scrutinize the sender's address and verify the legitimacy of any links.
- **Keep antivirus and security software up-to-date:** Ensure that all security tools are maintained and configured to perform regular scans.

- **User education:** Organizations should schedule regular and comprehensive security awareness training to educate employees about the risks of spear phishing and the importance of adhering to security best practices.
- **Implement multi-factor authentication (MFA):** Use MFA for critical systems and accounts to add an extra layer of security. This will make it more difficult for attackers to gain unauthorized access even if they steal user credentials.

Protect against Emerging Threats Using Flashpoint

The resurgence of Grandoreiro underscores the dynamic and ever-evolving landscape of cybercrime. Threat actors will continually adapt, refine their tactics, and expand their reach. While Grandoreiro presents a formidable challenge for organizations, understanding its distribution vectors, evasion techniques, and capabilities empowers security teams to protect themselves.

Sign up for a demo and see how Flashpoint helps customers stay ahead of emerging threats. Customers can find a more in-depth analysis in the Flashpoint Ignite platform.
