Dreambot Banking Trojan Targets Czech and Slovenian Speakers

Author: Jonathan Armer

Overview

On 7 November, we observed two email campaigns distributing the banking trojan Dreambot, which is a variant of Ursnif.[1] Threat actors have distributed Dreambot since 2016, targeting financial customers in Australia, Italy, Switzerland, the U.K., the U.S., Poland, and Canada.[2]

Customer Impact

Dreambot extends Ursnif's functionality with the ability to communicate over Tor, which can make it more difficult for security teams to detect the malware's activity on their networks.[2]

Dreambot targets financial institutions' customers to steal authentication information.[3] Additionally, it can:[4]

- log keystrokes
- inject into web pages
- extract web form data
- extract email data
- take screenshots

Campaign Analysis

In the campaigns we observed, the emails are written in Czech or Slovenian and reference the user's financial information. Threat actors distribute Dreambot through email attachments or emails containing a link to a file. The file is either a Microsoft Office document or a ZIP containing a Microsoft Office document or JavaScript file.

- The DOCX file retrieves a template containing Visual Basic for Applications (VBA) code from a compromised server.
- Alternatively, the encrypted ZIP contains a Microsoft Office DOC file containing VBA code.

The VBA code executes PowerShell commands to download Dreambot from a compromised WordPress website.

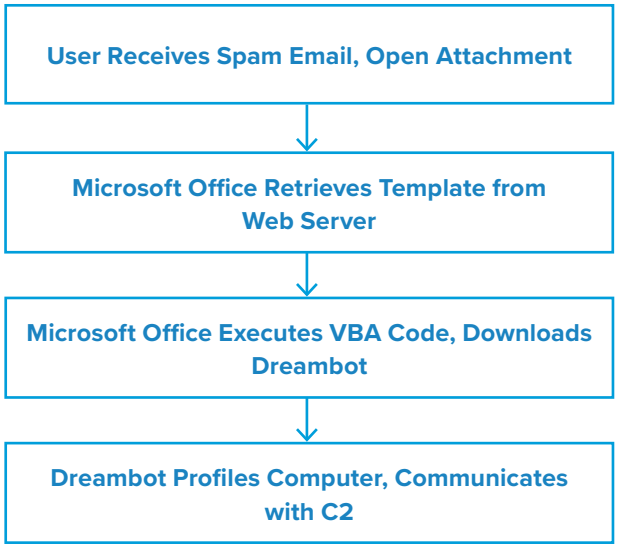
Linking to a template with VBA code and encrypting a ZIP file containing a document with the VBA code are techniques to prevent email attachment scanners from detecting malicious activity. The DOCX file only contains a reference to the template with VBA code and only retrieves the it when opened. Without retrieving the additional file, the DOCX will appear benign.

For the second technique, without the decryption password, the file in the ZIP cannot be extracted to scan.

Attack Chain

When the email recipient opens the DOCX attachment, Microsoft Office downloads the externally linked template. Office then applies the template and opens the DOCX file. This triggers the VBA code in the template.

The VBA code runs PowerShell commands to download and execute Dreambot using Regsvr32.exe. The malware injects itself into Explorer.exe and runs CMD.exe commands to profile the user's computer. Dreambot then sends this information to its command and control (C2) server.



Vulnerabilities & Mitigation

We recommend the following methods to prevent and mitigate infections from Dreambot:

- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully before opening it.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Always be suspicious of unexpected emails, especially regarding financial or delivery correspondence, documents, or links.
- Do not enable macros in a Microsoft Office attachment, especially if the file's only apparent contents are directions to enable macros.

Endnotes

1. https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree
2. https://www.proofpoint.com/us/threat-insight/post/ursnif-variant-dreambot-adds-tor-functionality
3. https://www.lac.co.jp/english/report/2017/10/16_alert_01.html
4. http://benkow.cc/DreambotSAS19.pdf

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com