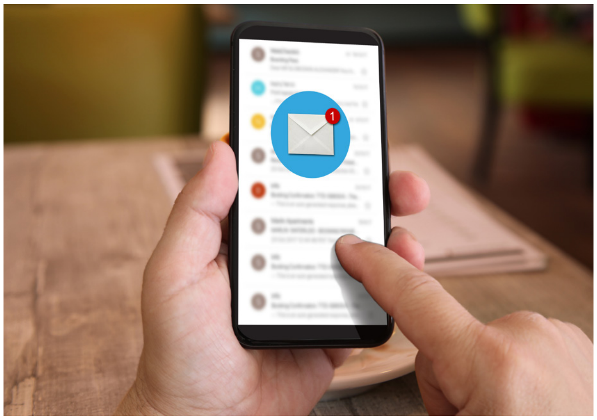
Vidar InfoStealer

Author: Nick Sundvall

Overview

From 25 to 30 June, we observed a malicious spam (malspam) email campaign distributing Vidar malware. Vidar is a trojan and information stealer (infostealer) that was first observed in December 2018.[1] It is a variant of the Arkei infostealer.



Customer Impact

Threat actors can reportedly purchase Vidar in online forums for $250.[2] It has the ability to steal credit cards, usernames, passwords, and files, as well as take screenshots of the user's desktop.[3] It can also steal wallets for cryptocurrencies such as Bitcoin and Ethereum.

Two-factor authentication (2FA) is an additional security layer for user accounts, typically requiring a one-time use code in addition to a password to sign in to an account. Vidar specifically targets the 2FA software Authy in order to bypass this added hurdle for gaining access to an account.[2]

Campaign Analysis

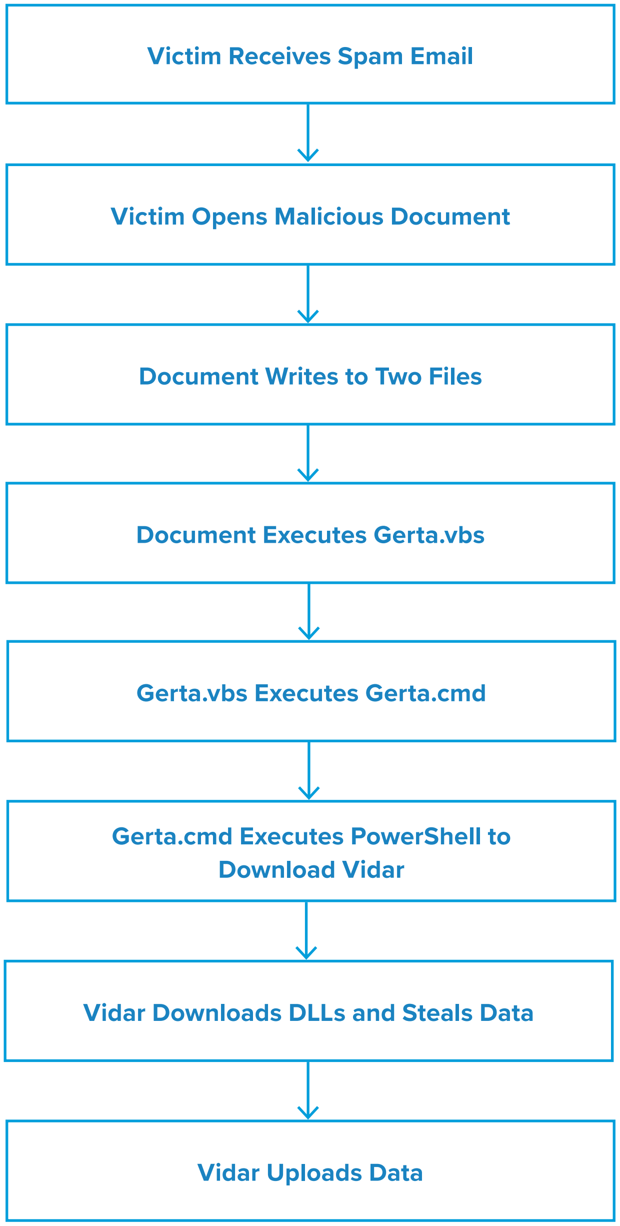
In this campaign, the threat actor sent emails with multiple subjects referencing a successful payment, such as "Confirmation of Payment" and "Your Transaction was Approved." Each email had a generic message body that resembled an invoice, with "Payment receipt attached" at the end. Every email we observed had an attached DOC file named *25.06Feo.doc*.

Attack Chain

Unlike typical malspam attacks, wherein the malware runs when the user opens the file, Vidar does not execute until the user closes the file. The attached DOC file uses the Visual Basic for Applications (VBA) method *Document_close()* to write two files - *Gerta.vbs and Gerta.cmd* - into *C:\programdata*. It executes *Gerta.vbs*, which runs *Gerta.cmd*, then launches a PowerShell script.

Throughout their execution, the scripts utilize many "sleep" commands, presumably as an anti-analysis technique to appear inactive. The PowerShell then downloads and runs the executable file *Poserto.exe*.

From here, Vidar downloads several dynamic link-library (DLL) files that it uses for stealing the data. Vidar then grabs all of the data it can access, puts it in a ZIP file, and sends it back to its command and control (C2). After sending the data, Vidar deletes itself from the infected computer.



Victim Receives Spam Email
Victim Opens Malicious Document
Document Writes to Two Files
Document Executes Gerta.vbs
Gerta.vbs Executes Gerta.cmd
Gerta.cmd Executes PowerShell to Download Vidar
Vidar Downloads DLLs and Steals Data
Vidar Uploads Data

Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for Vidar. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

- Exercise caution if it is necessary to open emails with generic subject lines.
- Always be suspicious of unexpected emails, especially regarding financial or delivery correspondence, documents, or links.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.
- Never configure Microsoft Office to enable macros by default. Many malware families use macros as an infection vector.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.

Endnotes

1. https://any.run/malware-trends/vidar
2. https://fumik0.com/2018/12/24/lets-dig-into-vidar-an-arkei-copycat-forked-stealer-in-depth-analysis/
3. https://isc.sans.edu/forums/diary/What+data+does+Vidar+malware+steal+from+an+infected+host/25398/

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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