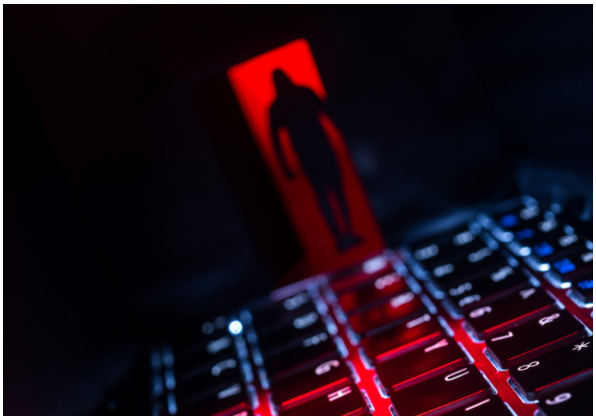
DanaBot Banking Trojan

Author: James Barnett



Overview

On 19 April, security researcher Brad Duncan reported a malicious spam campaign that used compressed Windows link files (LNK) to deliver DanaBot malware.[1] DanaBot is a relatively advanced banking trojan with a modular design that allows for multiple vectors of attack.

Customer Impact

DanaBot's modules include a remote desktop client, a credential stealer, a keylogger, and scripts that manipulate the victim's web browser to inject malware into banking web pages.[2]

According to ESET researchers, DanaBot's author(s) broadened its distribution (expanding in Europe) and functionalities (harvesting email addresses and sending spam) in 2018.[3] This year, they report that the banking trojan has new internal features, including:

- Layered, encrypted command and control (C2) communication,
- A new loader component,
- Ability to achieve persistence through the loader rather than the main module,
- New campaign identifiers.[4]

Campaign Analysis

The newly reported DanaBot campaign used a professional meeting theme to entice victims to open malicious email attachments. The emails used the subject line "Inner City CRR Network Meeting" and included body text indicating that a meeting agenda was attached to the email.

The actual email attachments were ZIP archive files whose names began with "nMeeert" and ended with 4-5 random digits. These attachments contained LNK files that would download and execute the DanaBot binary when opened.

Attack Chain

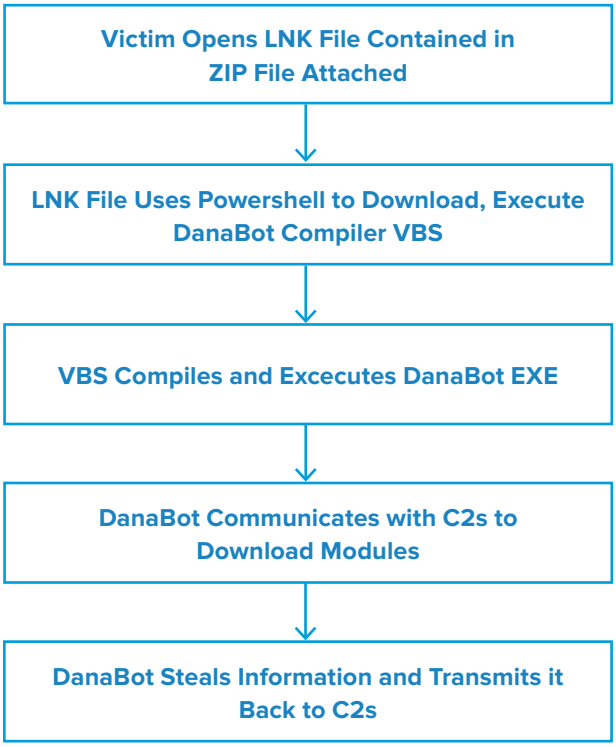
When the victim opens the LNK file contained within the ZIP attachment, it silently launches the Windows command line and uses it to execute Powershell commands. These commands download a Visual Basic Script (VBS) file from a remote location, place it in the victim's temp directory, and then execute it.

Upon execution, the VBS file compiles the core DanaBot EXE payload and uses rundll32.exe to execute it. DanaBot then communicates with its C2 servers using TCP connections on port 443 to download additional modules that expand its capabilities. DanaBot loads these modules, uses them to steal files and information from the victim, and then transmits the stolen data back to the attacker's C2s.

Vulnerabilities & Mitigation

Malicious email attachments are the primary infection vector for DanaBot. Infoblox recommends the following actions to reduce the risk of this type of infection:

- Be cautious of emails from unfamiliar senders and do not open unexpected attachments before inspecting them.
- 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.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not open attachments that are unexpected or from unfamiliar senders.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g. by phone or in person) before opening them.



Endnotes

1. 1. https://twitter.com/malware_traffic/status/1119331956217585664
2. https://www.fortinet.com/blog/threat-research/breakdown-of-a-targeted-danabot-attack.html
3. https://www.welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/
4. https://www.welivesecurity.com/2019/02/07/danabot-updated-new-cc-communication/