


Breakdown of a Targeted DanaBot Attack

 fortinet.com/blog/threat-research/breakdown-of-a-targeted-danabot-attack.html

March 1, 2019



A FortiGuard SE Team Threat Analysis Report

On Feb 5th, 2019, the FortiGuard SE team discovered a targeted attack aimed at an unknown individual working for a government department in Queensland State in Australia. Within a span of a few days, we had observed additional activity targeting various members of this organization, specifically in the form of spearphishing attacks. We can safely surmise that it is very likely that this threat was specifically targeting this organization at this time for reasons unknown to us.

The threat being delivered is known as DanaBot. It is a modular banking Trojan that has been historically linked to combining operations with other malware operators, such as those behind Gootkit. Other modules associated with DanaBot include remote desktop through VNC, information stealing, and keylogging. While it appears that this recent attack may be looking to establish a foothold in the network, the reasons behind this are currently unknown.

Following the Attack Chain

The attack begins with a seemingly innocuous email:

As can be seen, this email was sent in early February through a legitimate free email service available to everyone. In addition, the sender has not been registered as a spam-related email address, which adds to the analysis that this is a specifically targeted attack.

The link in the email (hxxp://users.xxxx.com.au/soniamatas/9302030002_993.zip?33505757) also points to an ISP that offers file hosting services.

Based on our telemetry for this server, the DanaBot authors' method of operation appears to be concentrated in Australia. In this most recent case, it is focused on a .gov.au email address, which coincides with this latest attack.

The link leads to a zip archive that contains a single .VBS file. Once deobfuscated, a shortcut link to a popular website is created in the temp folder, and after that, the script downloads a file from hxxp://corp.invest.preferredweb.org/dMJbnufMVu.php into the same temp folder and names it as *inv.exe*.

This domain has seen a recent surge in activity:

Also, most of the visitors come from Australia.

The domain itself was recently registered (February 03), as can be observed in the screenshot below.

Data shows that while the server was registered through a registrar in the United States, it was ultimately hosted by what appears to be a Russian webhosting service, as evidenced by the Russian name servers.

It's clear that the DanaBot authors also follow basic operational security practices, as indicated by their low visitor numbers. Aside from sending targeted emails, they also prevent anyone outside of Australia from downloading the malware. This may be in hopes of preventing security researchers, law enforcement agencies, and other curious onlookers from finding their campaigns.

In addition, the threat first contacts certain IP addresses to check for a valid Internet connection. This is a failsafe system for the malware in the very case of it's being analyzed (i.e. sandbox/isolated network) to avoid and thwart further analysis. If there is no connection, the threat will not continue to run.

Upon initiation, Danabot connects to a variety of benign IP addresses belonging to seemingly randomly-selected organizations to see if it is online. Other IP addresses not known to be Danabot C2 were not investigated due to time constraints, as well the difficulty of analyzing banking Trojans in the allocated timeframe before publication.

A New Attack?

During the time of our initial analysis, as early as in the first week of February, the threat itself was completely new. Interestingly, the recorded compilation time of the threat was actually ahead of the time it was downloaded. This suggests that it is most likely because the threat was compiled in a time zone ahead of the United States.

The threat can also create a service for persistence purposes, as well as build custom directories and files to hold collect data. The threat can also inject malware into other processes, such as winlogon.exe, explorer.exe, and svchost.exe. Functionality on older systems include rootkit capabilities, including the ability to hide newly created services along with the directories the threat uses.

Using a custom tool to reveal hidden services yields the following.

As mentioned, because of the embedded rootkit, browsing the folder does not reveal anything.

However, if the folder name is known, it is possible to manually navigate to the DanaBot directory.

DanaBot Modularity

Because of its modularity, DanaBot is known to install different modules, such as a remote desktop through VNC, information stealing, keylogging, and as expected, injecting malware into banking web pages, which ultimately makes it one of the more advanced and evolved banking Trojans.

Technical Details

Overview

9302030002_993.zip (detected as: VBS/Agent.QQN!tr.dldr)

- Size: 2135 bytes
- MD5: B827896DCA0E874A976595D027E27D0E
- SHA256:
CE96E325F79BA07871489DB205E9ACA9FAC5AB3C15BDCA60E562CBAB65CC6447

9302030002_993.vbs (detected as: VBS/Agent.QQN!tr.dldr)

- Size: 5294 bytes
- MD5: 1E0E503EF61BCF30CED17777FFD263DE
- SHA256:
4D542B11FF7B3DFAB52D4C9E64AE209EF9AFBDFCEA1910CA24815EEC54944F21

inv.exe (detected as: W32/Generic.AC.4399AE!tr)

- Size: 455168 bytes
- MD5: 75FD221DEA39A4AEA27998F4FB071041
- SHA256:
1991548C135E4653CD18F969102A3225661AE70102AC7C3D5FF8A69E75FFB644
- creates %temp%\inv.dll

inv.dll (detected as: W32/Danabot.!!tr)

- Size: 286224 bytes
- MD5: AB2C3D293C442C351A0B04CE9F4DEA3F
- SHA256:
F2EA70B5131E88D8B9B354D618E03B35A2B3FFFE980CF6B871E1BE3A88625BFE9

MITRE ATT&CK – Tactics and Techniques

This analysis shows how DanaBot functionality maps to the MITRE ATT&CK model.

ATT&CK TTP Summary

Initial Access

Spearphishing – a link is provided in the email that points to an archive containing a malicious VBS script to continue on to the next stage of infection.

Execution

Regsvr32 – DanaBot file

Rundll32 – DanaBot file

Scripting – VBS file

Service Execution – custom startup service

User Execution – phishing link, unzipping archive, executing VBS file

Persistence

Hidden Files and Directories – DanaBot files

New Service – execute on startup

Privilege Escalation

New Service – rootkit

Defense Evasion

Hidden Files and Directories – Danabot files

Obfuscated Files or Information – data files, keylogging file

Process Injection – explorer, winlogon, services, browser

Rootkit – hiding files, directories, custom service

Rundll32 – launching DanaBot dll

Scripting - VBS

Discovery

Process Discovery – For injection

Exfiltration

Data Encrypted – SSL + custom

Exfiltration over Command and Control Channel – SSL port 443

Command and Control

Commonly Used Port – TCP port 443

Standard Application Layer Protocol – HTTPS

Known Defenses and Mitigations

Initial Access: FortiMail or other mail solutions can be used to block specific file types. FortiMail can also be configured to send attachments to the FortiSandbox solution (ATP) either on-premise or in the cloud to determine if a file displays malicious behavior. FortiGate firewalls with Anti-Virus enabled alongside a valid subscription will detect and block this threat if configured to do so.

Execution: *User Awareness Training* – Since it has been observed that this threat has been delivered via spearphishing distribution mechanisms, it is crucial that end users within an organization are made aware of various types of attacks delivered via this method. This can be accomplished through regularly occurring training sessions and impromptu tests using predetermined templates by internal security departments within an organization. Simple user awareness training on how to spot emails with malicious attachments or links could stop the initial access into the network. If user awareness training fails, and the user opens the attachment or link, FortiClient running with the latest up to date virus signatures will detect and block files associated with this threat. The files analyzed in this report are detected as VBS/Agent.QQN!tr.dldr, W32/Generic.AC.4399AE!tr, W32/Danabot.I!tr.

Exfiltration & C&C: FortiGates located in all your ingress and egress points with the Web Filtering service enabled and up-to-date definitions and or Botnet Security will detect and block any observable outbound connections if configured correctly.

It is important to note that attacks continue to become more sophisticated and can sometimes circumvent your security defenses for a number of reasons. This is why it is important to ensure you have the ability to detect anomalous activity that could be malicious. Lastly, our Enterprise Bundle will address this attack as well as others. Our Enterprise Bundle consolidates all the cyber security services you need to protect and defend against all the cyber-attack channels from the endpoint to the cloud, including IoT devices, providing you the integrated defense to tackle today's advanced threats. Including the technologies needed to address today's challenging risk, compliance, management, and visibility and Operational Security (OT) concerns.

Indicators Of Compromise (IOCs)

DanaBot only contacts the IP addresses listed below to determine its online status. These addresses appear to have been selected randomly, and it is important to emphasize that there is no indication of any vulnerabilities or exploits associated with these addresses or the DanaBot malware whatsoever. However, by identifying some or all of this list of addresses in your outbound records, you could potentially validate whether or not your organization have been infected by this malware.

91.112.46.201:443

52.245.17.2:443

61.165.173.178:443

26.64.30.13:443

38.229.153.189:443

61.184.194.124:443

89.144.25.243:443

93.145.247.149:443

140.155.223.170:443

147.28.140.161:443

171.16.126.45:443

178.209.51.211:443

192.71.249.51:443

226.188.219.5:443

234.53.54.120:443

NOTE: The FortiGuard Labs team has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit cyberthreatalliance.org.

Learn more about [FortiGuard Labs](#) and the FortiGuard Security Services [portfolio](#). [Sign up](#) for our weekly FortiGuard Threat Brief.

Know your vulnerabilities – get the facts about your network security. A [Fortinet Cyber Threat Assessment](#) can help you better understand: Security and Threat Prevention, User Productivity, and Network Utilization and Performance.

Read about the FortiGuard [Security Rating Service](#), which provides security audits and best practices.