DANABOT A BANKING TROJAN

Social Engineering Attack

Prof. Umarani Chellapandy

Chethan NP
Master of Computer Application
In
Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India

***Abstract*:** This paper features about Danabot, which is a malicious. The emails containing a malicious URL that is sent to a Word Document which contains macros embedded with a powershell script. The embedded script was loaded to potential victims in Australia, via verifying the client's IP geolocation. If there are results as successful, the second stage malware (DanaBot) would be sent.
This bot is a trojan which includes such as banking web site injections and other stealer functionality.
This malware connects using raw TCP connections to port 443 and downloads additional modules

I. INTRODUCTION

In the past several years, banking trojans have been some of the more prevalent malware. First seen in May 2018 targeting customers in Australia, Danabot has added to this barrage of banking trojans. And only several months after its initial sightings, it has increased its reach through campaigns in Europe and the US.

Danabot, like its perceived precursor Reveton, is a modular banking trojan coded in Delphi. Its operators can easily develop new modules and deploy them to infected machines. It stands out among other banking trojans because of this modularity, which allows it to include additional functionality on top of the more traditional web injection and information-stealing capabilities. For example, some Danabot samples incorporate modules that list cryptocurrency-related processes and provide RDP access.
Like other campaigns that distribute prevalent banking trojans, Danabot campaigns use socially engineered spam email, with lures that refer to e-toll account statements, invoices, and shipment tracking codes. Danabot campaigns, however, employ additional mechanisms to deliver its payload. Instead of carrying malicious attachments, some of its spam emails include links to Word documents with malicious macros. Other campaign emails include links to ZIP files containing malicious JavaScripts. Both these macros and JavaScripts download Danabot from multiple domains.

The actors behind Danabot are currently unknown. With continued improvements to its modularity as well as the modules themselves, its usage will likely increase among campaign operators.

II. DESCRIPTION ON DANABOT

DanaBot is a banking trojan, written in programming language know as Delphi, they are capable of stealing credentials and hijacking infected systems. It is spread via spam emails masquerading as invoices with malicious attachment that, when they are executed, a legitimate system administration tool retrieve and execute its modules.

III. WORKING

To distribute Danabot, campaign operators send spam emails that employ common social-engineering methods. The emails have realistic lures that discuss e-toll account statements, invoices, and shipment tracking codes, all designed to entice unsuspecting users into clicking links on the emails.

Danabot campaign operators use multiple domains to hinder takedown efforts. They use different domains for initial payload delivery, command-and-control (C&C), and exfiltration (drop sites).

Once Danabot successfully embeds itself, a downloader component starts an AES-encrypted connection to a command-and-control node. It first reports details about the infected machine and obtains additional instructions for reconnaissance, paving the way for attackers to customize succeeding stages of the attack.

The main Danabot implant is a DLL file saved in a hidden folder. This main implant updates regularly and uses a variety of persistence mechanisms to automatically load with the OS through *rundll32.exe*. If cleanup attempts fail to remove it completely, this implant can reappear with new components.

Danabot connects to hardcoded C&C IP addresses on TCP port 443 to download components that typically include a VNC viewer, a stealer module, and a sniffer module. It also obtains configuration files, such as lists of cryptocurrency processes and files that operators want to monitor.

The Danabot stealer module obtains private information from a number of email, messaging, FTP, and web browsing apps: Windows Live Mail, Outlook, Trillian, WS_FTP, FileZilla, Chrome, Firefox, and Opera. It can also obtain system information, list files, and capture screenshots. Other Danabot modules found in the wild provide TOR browsing and RDP capabilities, enabling stealthier and more robust C&C communication.

DanaBot is composed of three components:

1. Loader module: downloads and loads mainly required component
2. Main component: This helps in configures, and loads modules
3. Modules: various malware functionality

IV. ANALYSIS DIAGRAM

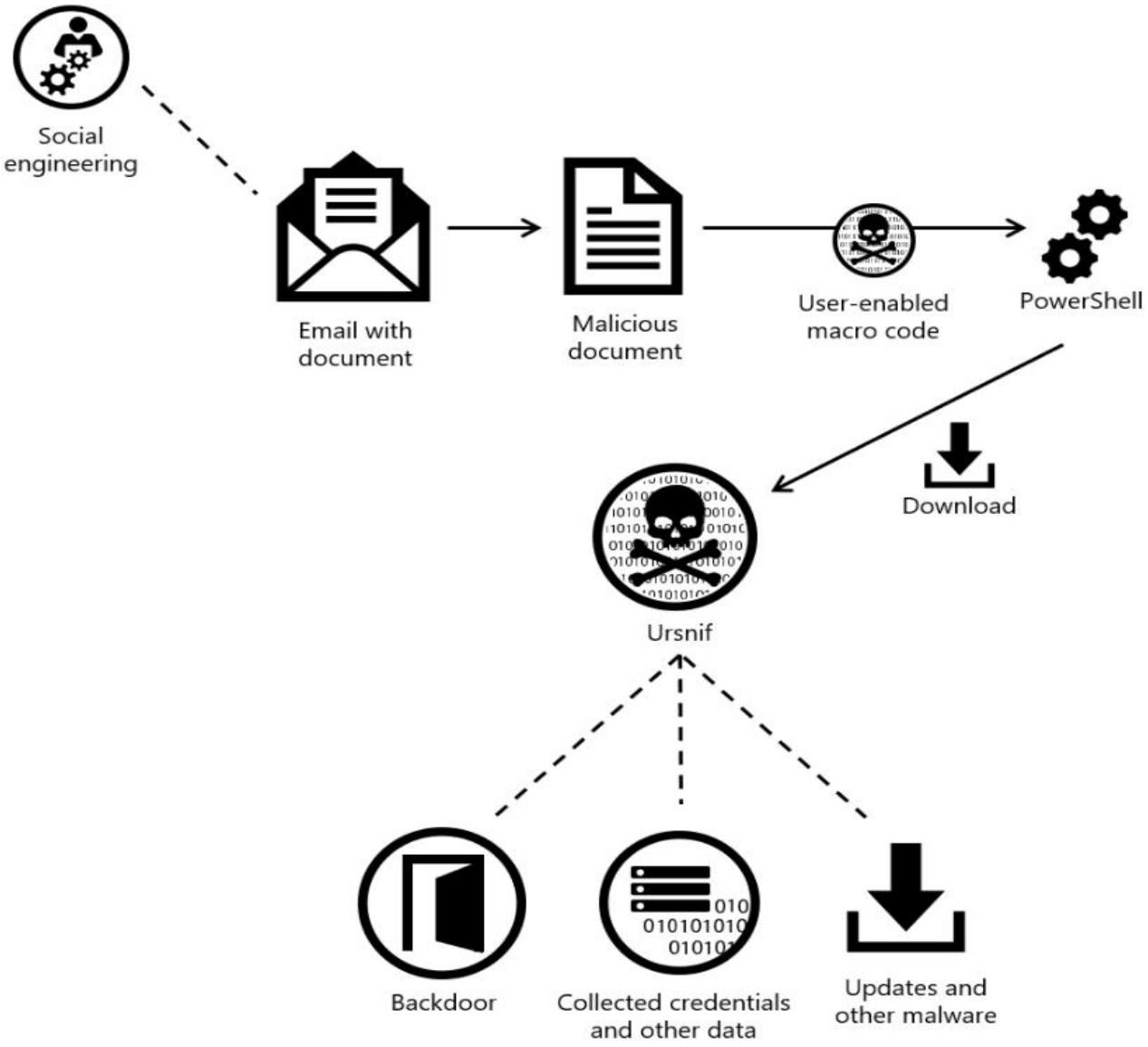

Figure-02

V. MALWARE FUNCTIONALITY

DanaBot is a Trojan that includes banking site web injections and stealer functions. This consists of a component that downloads an encrypted file containing the functional DLL. The DLL, will connects using TCP connections to port 443 and downloads additional required modules including:

- VNCDLL.dll - "VNC"
- StealerDLL.dll - "Stealer"
- ProxyDLL.dll - "Sniffer"

This malware also manages downloads configuration files such as:

- Targeted sites for the Sniffer module
- Banking web injects
- Lists of cryptocurrency processes and files to monitor

It also helps in uploading files to the command and control (C&C) server including:

- Detailed system information
- Screenshot of the user's desktop
- List of files on the user's hard disk

All uploads and downloads are encrypted with the Microsoft CryptAPI AES256 algorithm.

VI. FLOW DIAGRAM

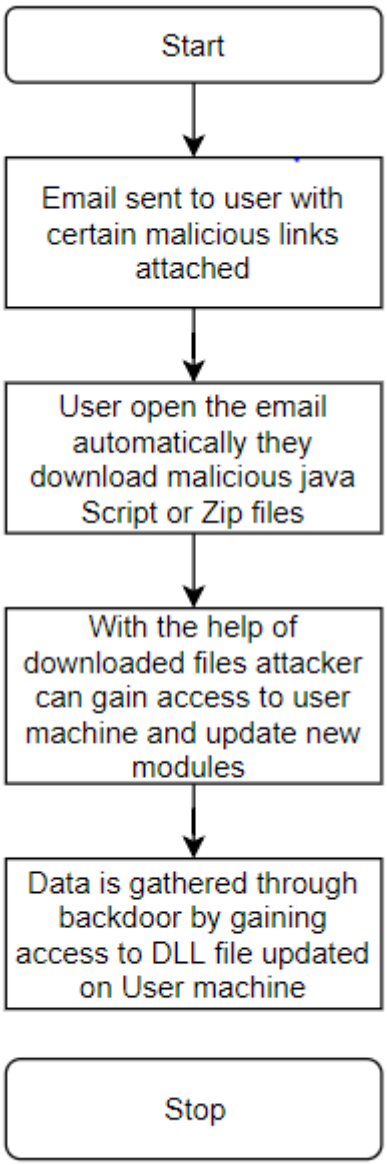

Figure-02

VII. DETECTION MECHANISM

Antivirus detects following malware:

- Trojan:JS/Danabot (delivery)
- Trojan:Win32/Danabot (implant/module)
- Trojan:Win64/Danabot (implant/module)

Endpoint detection and response (EDR)
Alerts with the following are detected:

- Possible Danabot infection
- Detected malware URLs used by Danabot
- Malicious documents are detected based on indication provided by O365

Attack surface reduction rules
These rules can block or audit activity associated with this threat:

- Block all Office applications from creating child processes
- Block Office applications from creating executable content
- Block JavaScript or VBScript from launching downloaded executable content.

VIII. INDICATORS OF COMPROMISE

Monitoring for indicators of compromise enables organizations to better detect and respond to security compromises. Collecting and correlating IOCs in real time means that organizations can more quickly identify security incidents that may have gone undetected by other tools and provides the necessary resources to perform forensic analysis of incidents. If security teams discover recurrence or patterns of specific IOCs they can update their security tools and policies to protect against future attacks as well.
Here are certain malicious hashes, domains and C&C servers.

Domains:
1. job.hitjob[.]it
2. vps.hitjob[.]it
3. pph.picchio-intl[.]com
4. dcc.fllimorettinilegnaegiardini[.]it
5. icon.fllimorettinilegnaegiardini[.]it
6. team.hitweb[.]it
7. latest.hitweb[.]it

Malicious Hashes:
1. 98C70361EA611BA33EE3A79816A88B2500ED7844
2. 0DF17562844B7A0A0170C9830921C3442D59C73C
3. B816E90E9B71C85539EA3BB897E4F234A0422F85
4. B1FF7285B49F36FE8D65E7B896FCCDB1618EAA4B
5. 5F085B19657D2511A89F3172B7887CE29FC70792
6. 4075375A08273E65C223116ECD2CEF903BA97B1E
7. 28139782562B0E4CAB7F7885ECA75DFCA5E1D570

C&C servers used by DanaBot:
1. 84.54.37[.]102
2. 89.144.25[.]243
3. 89.144.25[.]104
4. 192.71.249[.]51
5. 178.209.51[.]211
6. 185.92.222[.]238

IX. MITIGATION

Be careful about unsolicited email messages, abstain from clicking attachments and opening attachments except if certain that they're safe and dependably ensure yourself with solid antivirus software.
Apply these mitigations to reduce the impact of this threat.

- ✓ Enable and manage cloud-delivered prevention and automatic sample submission. These capabilities use artificial intelligence and machine learning to quickly identify.
- ✓ Encourage users to use Microsoft Edge and other web browsers that support SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware.
- ✓ Turn on network protection to block connections to malicious domains and IP addresses.
- ✓ Train end users to limit the use of accounts with local or domain admin privileges.
- ✓ Do not allow macros for everything, allow macros from trusted locations. See the latest security baselines for Office and Office 365.
- ✓ Turn on attack surface reduction rules, including rules that can block advanced macro activity and suspicious script activity.

X. CONCLUSION

It is becoming difficult to address today's malware threats. This paper provides an explanation about Danabot a banking trojan, Working and flow of malware delivery mechanism is explained. Analysis of the mechanism to avoid this malware distribution is explained and couple of mitigation. Few Malicious hashed are given in this paper.

XI. REFERENCES

[1] https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0

[2] https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

[3] https://www.proofpoint.com/us/threat-insight/post/hancitor-ruckguv-reappear

[4] https://0ffset.wordpress.com/2018/08/12/post-0x16-hancitor-stage-1/

[5] https://www.proofpoint.com/us/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler

[6] http://malware-traffic-analysis.net/2016/04/20/index.html

[7] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/func_hashes.py

[8] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/loader_func_hashes.txt

[9] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/main_func_hashes.txt

[10] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/decrypt_str_ida.py

[11] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/loader_strings.txt

[12] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/main_strings.txt

[13] https://github.com/EmergingThreats/threatresearch/blob/master/danabot/24_hours_of_ips.txt

[14] https://www.eshlomo.us/ursnif-gozi-trojan-malware

XII. BIOGRAPHY

Prof. Umarani Chellapandy
Faculty & Guide Department of Computer Science & IT-MCA
Jain (Deemed-to-be University) Bangalore, India

Chethan NP
Master of Computer Application in Information Security Management Systems
Jain (Deemed-to-be University) Bangalore, India