HYBRID MALWARE & WORMS

In this report I will be explaining computer worms and hybrid malware, exploring the modern variant of malware called TrickBot, its complex worm capabilities and its hybrid modular activities.

Hybrid Malware

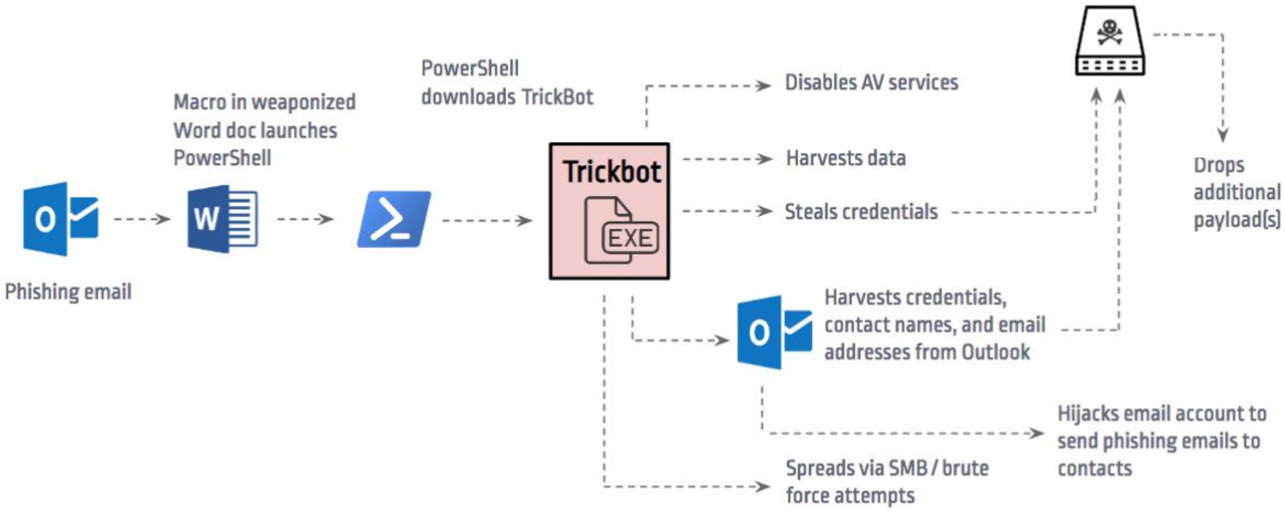
Modern malware can be best described as hybrid malware, it can be combination of Trojan, Rootkit or self-replicating worm all built into a single cyberattack package. During the first stages of an attack, after a user opens an email attachment, the first components of the attack is installed, this is usually to send information about the user to the attacker, information such as operating system information, network size, what vulnerabilities are present, what security is being used. This is sent back to the command and control server, there the attacker has many options. The attack method can also be thought as hybrid, as the option can be there to use a executable or script attack, or if java is installed a jar file can be dropped, mostly these decisions are made to evade security measures.

Origins:

In the past viruses came in one payload, usually did only one thing were easily caught. Combining two are more malware types such as a worms ability to live in live memory and to spread to different networks while using the viruses ability to alter program code made malware more effective. By separating malware into modules (dll files), made it more reusable. The usual method now for installing malware, would be an exe installer would load the separate dll files into live memory when needed.

TrickBot: Modular Approach.

Its main appeal to cybercriminals is its versatility, with its modular design, with a wide range of plugins allowing it to perform a wide range of tasks.


PowerShell downloads TrickBot
Macro in weaponized Word doc launches PowerShell
Phishing email
Trickbot
EXE
Disables AV services
Harvests data
Steals credentials
Drops additional payload(s)
Harvests credentials, contact names, and email addresses from Outlook
Hijacks email account to send phishing emails to contacts
Spreads via SMB / brute force attempts

The first stage of infection is a user clicking on an attachment in an email used malicious spam campaigns. A macro in a downloaded document launches PowerShell and executes a script which downloads TrickBot onto the users system. TrickBot comes with an exe installer, the modules are downloaded separately usually in dynamic link library files. Each of these files can be loaded into live memory as when needed.

When a system is infected, it decrypts and downloads several modules, each module has its own specific task.

- **Disables Av services**
  One of the first tasks is to disable antivirus software, so it can remain persistence and go undetected while carrying out its business.

- **Harvests data**
  TrickBot collects all different types of data from system and network information, email accounts, tax information etc.

- **Steals credentials**
  TrickBot main purpose was as password stealer, its upgraded module grab's credentials, is used to authenticate remote serves using Putty and Remote Desktop Protocol (RDP).

- **Spreads via SMB / brute force attempts**
  As we have already explored, its self-propagation worm module is used to spread TrickBot to other machines on the same network.

- **Drops additional payloads**
  With its modular design, additional payloads is easily implemented and download. TrickBot often downloads Ryuk ransomware, which locks machines across the network.

- **Backdoor**
  Like any large scale software program, modules can be added, changed or updated to adapt to changing needs.

Like any large scale software program, modules can be added, changed or updated to adapt to changing needs. TrickBot keeps evolving, finding new ways to infect hosts, avoid detection and it's difficult to remove, maybe it's why cybercriminals like it so much.

Computer Worms

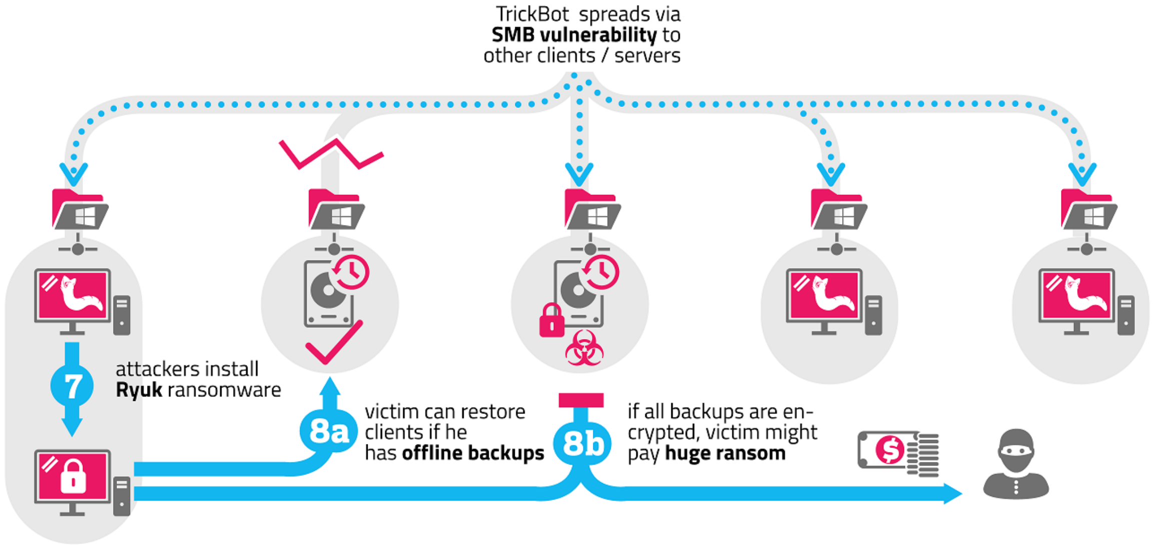
Definition: A computer worm is defined as a malicious program which resides on a single computer, searchers for other clients and servers, replicates itself and spreads throughout the network. A worm is a standalone piece of code, it does not affect other files

TrickBot: Modular Worm

Traditionally the TrickBot malware was a banking Trojan, or information stealer, that all changed with the Wannacry campaign in 2017. Wannacry was a worm which distribrited ransomware indiscriminately infecting older unpatched windows operating systems. It exploited a vulnerability in Windows Server Block (SMB) v1 Protocol, which is a communication protocol windows used for client-server sharing of resources.

TrickBot: Mworm

Trickbot authors seen the benefits of speed and effectiveness and created its own worm spreading module which they called Mworm. Using the same exploited vulnerability in the SMB Protocol to propagate across the network and increase system level privileges on host machines.


TrickBot spreads via **SMB vulnerability** to other clients / servers
7
attackers install **Ryuk** ransomware
8a
victim can restore clients if he has **offline backups**
8b
if all backups are en-crypted, victim might pay **huge ransom**

Mworm would transfer the TrickBot executable in an unencrypted form to a vulnerable domain controller. It runs in the Domain Controlled and remains persistent on an infected host. As the executable was unencrypted, allowing antivirus software to easily detect it.

Trickbot: Nworm

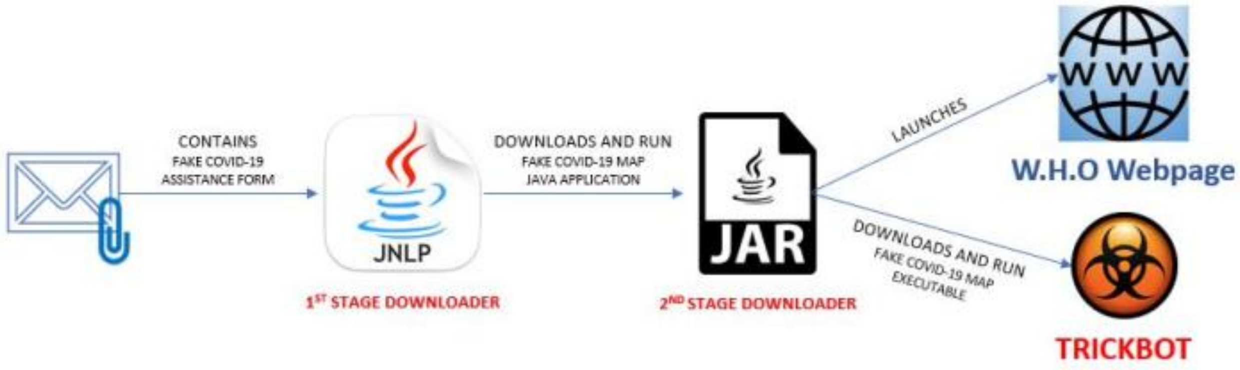
An update to mworm was seen by researches in April 2020, this new modular function is called Nworm. This Nworm was updated evade detection, its executable is encrypted its HTTP communication is also encrypted, it does not remain persistent on an infected host.

TrickBots latest campaigns.

TrickBot is focusing on the current coronavirus outbreak, to target users who are seeding information on the pandemic.

Google has seen a spike in Covid-19 phishing emails and spam targeting Gmail users disguised as a WHO (World Health Organization) messages looking for donations.

Another infection method is an email claiming to be from a volunteer organization, helping those seeking financial aid during the covid-19 pandemic. What makes this rather new is downloads a Java Network Launch Protocol (JNLP) file.



The client has to have Java running on their machine, if they double click this JNLP file, it downloads a JAR file, which will launch a W.H.O Webpage while also downloading TrickBot.

Help prevent TrickBot Infections.

Modern malware is changing all the time, to help protect your computer systems and networks here is some helpful tips:

- To prevent TrickBot infections it is best to have the latest version of the Windows 10 and run the latest windows updates.
- Don’t open any suspicious emails with attachments.
- Disable the use of SMBv1 the network communication protocol, and update to SMBv2.
- Use an Intrusion Detection System (IDS) system on your network, and keep up to date with the latest signatures.
- Keep up to date with the latest security news, learn about new TrickBot infections and how they are implemented.

REFERENCES

Hybrid Malware

https://www.cyclonis.com/trickbot-malware-new-tricks-coronavirus-themed-samples-fool-security-products-target-telecommunication-companies/

https://kc.mcafee.com/corporate/index?page=content&id=KB92380

https://www.bleepingcomputer.com/news/security/trickbot-banking-trojan-now-steals-rdp-vnc-and-putty-credentials/

https://blog.f-secure.com/what-is-trickbot/

https://www.greenviewdata.com/blog/trickbot-trojan-fake-bank-america-and-amazon-email

Computer worms

https://www.secureworks.com/research/wcry-ransomware-analysis

https://searchnetworking.techtarget.com/definition/Server-Message-Block-Protocol

https://unit42.paloaltonetworks.com/goodbye-mworm-hello-nworm-trickbot-updates-propagation-module/

https://cyberflorida.org/2020/06/03/nworm-new-trickbot-module/

https://www.binarydefense.com/trickbot-ono-new-tricks/

TrickBots latest campaigns

https://www.bankinfosecurity.com/covid-19-phishing-emails-mainly-contain-trickbot-microsoft-a-14149

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trickbot-disguised-as-covid-19-map/

Prevent TrickBot Infections.

https://www.cisecurity.org/white-papers/security-primer-trickbot/