CROWDSTRIKE

eSENTIRE

CASE STUDY

Threat Dissection: Trickbot

THREAT TYPE:

Modular malware

FUNCTIONALITY:

banking trojan, reconnaissance, exfiltration, dropper for other malware

FIRST DISCOVERED:

2016

INFECTION MECHANISMS:

Phishing, man-in-the-browser, known vulnerabilities such as EternalBlue and other malware droppers such as Emotet

TRADITIONAL DETECTION CHALLENGES:

Infections are not noticeable to the end user. Trickbot is modular and customizable, giving the threat actor many options to evade detection. Some modules can disable endpoint security tools.

CONTAINMENT AND REMEDIATION CHALLENGES:

A threat actor can deploy many different modules through scheduled tasks that are designed for stealth and persistence in a network (expiration times for tasks, new IP addresses, sandbox checking, etc.). Infected hosts are recommended to be completely reimaged as a result.

POTENTIAL EFFECTS:

- Theft of sensitive data
- Business disruption due to ransomware
- Financial losses incurred for incident response and restoration
- Regulatory penalties
- Reputational harm

BACKGROUND

Trickbot malware was first observed in the wild in 2016, being utilized as a banking trojan similar to Emotet and Dyre. It has since evolved to become one of the most prominent types of modular malware, meaning it is highly customizable in functionality and how it is deployed.

Since 2016, there has been significant reporting on the sophisticated and ongoing development behind Trickbot. This has been linked to what CrowdStrike researchers call the Wizard Spider cybercrime organization, believed to be based in Russia.[1]

While highly capable as a stealthy internal reconnaissance and data exfiltration tool for threat actors, the more concerning development is that Trickbot is increasingly being used as a backdoor to deploy ransomware. Multiple sources have reported a developing connection between Trickbot, Emotet and Ryuk ransomware.

Threat researchers have observed considerable dwell time between initial infection of Trickbot and the distribution of Ryuk. One of the prevailing theories is that the perpetrators behind Trickbot have developed an “access-as-a-service” business model and are selling backdoors to other threat actors looking to distribute ransomware.[2]

There are two especially insidious implications of this apparent malware partnership. First, ransomware attacks can now be delivered with incredible precision. Historically ransomware campaigns have involved casting a wide and indiscriminate net, with threat actors relying on the law of averages to take effect and result in profits. With Trickbot’s persistence and reconnaissance utility, a victim’s network can be vetted before the ransomware is deployed, allowing threat actors to target specific aspects of the network or sensitive data that can be especially profitable.

The second implication is that it allows threat actors to effectively monetize their attacks twice. Sensitive data can be identified and exfiltrated using Trickbot and subsequently be sold on the black market. Once this is accomplished, the threat actor can either sell their access to victim networks to other cybercriminals or exploit the victims further by deploying ransomware.

This “unholy alliance,” as one reporter described it, further underscores the need for advanced threat detection and more importantly, rapid response as a means to mitigate the risk posed by modular malware like Trickbot.[3]

COMMON TRICKBOT MODULES[4]

DATA THEFT

LoaderDll/InjectDll: Monitors for website activity and uses web injects (e.g. pop ups and extra fields) to steal information.

Sinj: This file contains information on Trickbot targets and it uses redirection attacks (also known as web fake injections).

Dinj: This file contains information on TrickBot targets and it uses server side web injections.

Mailsearcher: A module to search for and collect mail files on disk to send back to the C2 server.

SYSTEM/NETWORK RECONNAISSANCE

Systeminfo: Harvests system information so that the attacker knows what is running on the affected system.

NetworkDll: Leveraged to map out the victim's network.

loader.dll: A module to ensure other modules are successfully loaded.

CREDENTIAL AND USER INFORMATION HARVESTING

ModuleDll/ImportDll: Harvests browser data (e.g. cookies and browser configurations).

DomainDll: Uses LDAP to harvest credentials and configuration data from domain controller by accessing shared SYSVOL files.

OutlookDll: Harvests saved Microsoft Outlook credentials by querying several registry keys.

SqulDll: Force-enables WDigest authentication and utilizes Mimikatz to scrape credentials from LSASS.exe. The worming modules use these credentials to spread TrickBot laterally across networks.

Pwgrab: Steals credentials, auto-fill data, history and other information from browsers as well as several software applications.

LATERAL MOVEMENT AND PROPAGATION

WormDll and ShareDll: These are worming modules that abuse Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) to move laterally across networks.

TabDll: Uses the EternalRomance exploit (CVE-2017-0147) to spread via SMBv1.

spreader_x64: A module that spreads TrickBot by exploiting EternalBlue and uses mimikatz to perform credential threat.

TrickBooster: Harvests email addresses from an infected host, sends out malspam emails and deletes sent messages to remain hidden.

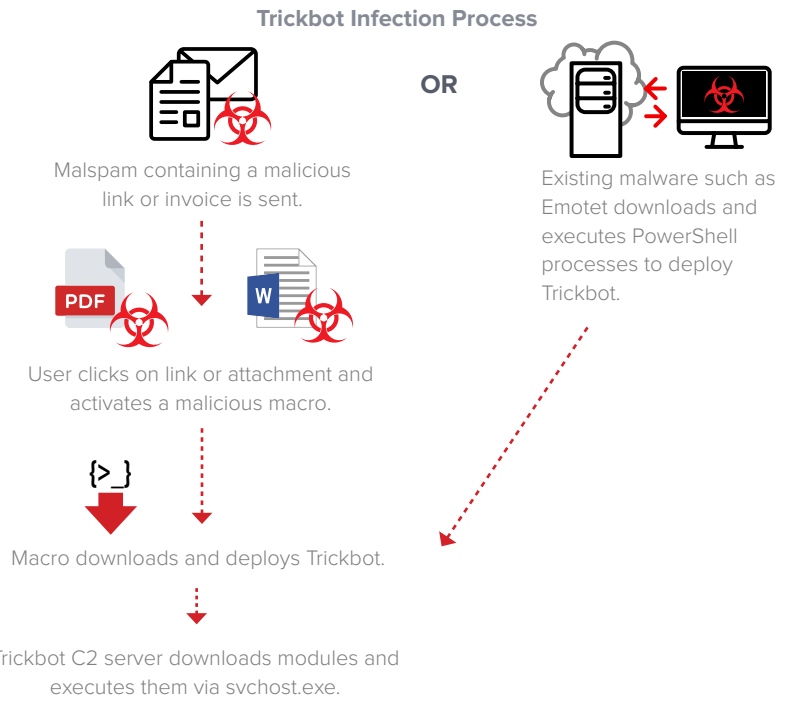
HOW DOES TRICKBOT WORK?

Like most attacks, initial infection typically occurs from a malspam email containing a malicious productivity attachment, such as a Word or Excel file cleverly disguised as legitimate communications from reputable businesses or known contact. The victim unknowingly enables malicious macro commands to run PowerShell and ultimately downloads the malware from the threat actor's command and control (C2) server.

Trickbot infection is possible through other means. It has been observed being deployed by other types of malware such as Emotet and Ursnif, which often follows a similar initial infection methodology. Following initial infection, Trickbot can propagate throughout the network by stealing credentials, utilizing exploits such as EternalBlue or by modules that automatically send malspam emails to harvested email addresses from the compromised host's account.

Another particularly advanced feature of Trickbot: the malware takes specific and automatic action against endpoint security measures. Following download, Trickbot looks to tamper with the policies of Windows Defender (Microsoft's native endpoint security platform) via PowerShell commands, disabling functions like behavior monitoring, scanning, automatic remediation and more.

The malware then redeploys itself in the infected machine's memory where it begins to establish persistence through scheduling tasks and downloading modules from the C2 server. Modules are delivered as Dynamic Link Libraries (DLL) via the svchost.exe process name, file types that allow for instructions to be disseminated to multiple programs. What happens from here depends on the goals of the attacker. See the table to the right for examples of various Trickbot modules and their functions.



SOC CASE STUDY: TRICKBOT DETECTION AND RESPONSE WITH esNETWORK AND esENDPOINT

In January 2020, an eSentire manufacturing customer was initially alerted to suspicious network activity, which prompted further investigation by analysts from eSentire's Security Operations Center (SOC). Nine minutes later, a host was observed sending unusual outbound communications, at which point SOC analysts took action and placed TCP disruptions on both the internal host and the IP it was communicating with in order to halt the activity via esNETWORK. The host itself was isolated from the rest of the network as well via esENDPOINT. The SOC updated the customer with the latest development in the incident.

At this point, the threat appeared to be limited to a single compromised workstation with no observed indicators of compromise on the rest of the customer network. Furthermore, there was no risk of lateral movement with the host quarantined, which was fortunate because deeper forensic endpoint investigation revealed that the host was attempting to spread via the known EternalBlue exploit less than 20 minutes following the SOC's actions to isolate the threat.

Trickbot was identified as the malware responsible for the activity with the initial infection traced back to human error from an employee who clicked on a link from a malspam email. Further investigation did reveal that a limited amount of the employee's personal information (saved passwords and shipping address from a web browser auto-fill function) was exfiltrated before eSentire blocked the connection. eSentire recommended to the client that the end user change their passwords and their workstation be completely reimaged to ensure no traces of malware remained.

Swift investigation and response within less than 10 minutes of the initial threat detection was critical in containing this particular Trickbot incident. If reaction to the threat was slower by just 17 minutes, (a relative blink of an eye in the context of the typical workday in the average IT organization) there is a good chance this Trickbot infection would have been able to spread throughout the network. This underscores the speed security teams must operate at to stop advanced threats. Success is measured in seconds and minutes, but unfortunately, most organizations are lagging far behind with the mean time to contain a data breach at 73 days.[5] eSentire cloud-delivered Managed Detection and Response (MDR) closes this gap for 750+ customers globally with our SOC averaging 35 seconds to initial triage and 20 minutes for the containment and remediation of threats.

TRICKBOT ATTACK TIMELINE

2020-01-18 9:38 UTC — SOC sends alert for unusual network traffic.

9:47 UTC — SOC sends second malware alert for observed outbound POSTs to a malicious C2 server. eSentire blocks the network connection and isolates the host to prevent further spread.

10:04 UTC — Further investigation reveals the compromised host attempting to spread via EternalBlue exploit. Attempts were unsuccessful because of earlier quarantine actions from eSentire's SOC. No evidence of compromise in the rest of the customer's network.

12:20 UTC — Deeper forensic investigation into the earlier POST request reveals a limited amount of web browser data was exfiltrated from the victim workstation. The customer was notified of this new discovery along with remediation recommendations via email.

13:55 UTC — SOC debriefs the customer on the incident via conference call, fully resolving the incident.

ADDITIONAL READING

Security Primer TrickBot, Center for Internet Security: https://www.cisecurity.org/white-papers/security-primer-trickbot/

TrickBot, MITRE ATT&CK Framework: https://attack.mitre.org/software/S0266/

The Unholy Alliance of Emotet, TrickBot and the Ryuk Ransomware,Decipher:
https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

REFERENCES

[1] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware

[2] https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

[3] https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

[4] https://www.cisecurity.org/white-papers/security-primer-trickbot/, https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data, https://success.trendmicro.com/solution/1122411-trickbot-s-newly-released-modules-makes-it-even-trickier

[5] Ponemon 2019 Cost of a Data Breach Study

eSENTIRE