Fact Sheet: TrickBot Malware

SUMMARY

TrickBot malware—first identified in 2016—is a Trojan developed and operated by a sophisticated group of cybercrime actors. The cybercrime group initially designed TrickBot as a banking trojan to steal financial data. Through continued development and new functionality, TrickBot has become a highly modular, multi-stage malware that provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. Since TrickBot's inception, the cybercrime group has used the malware to attack individuals and businesses globally across a wide range of sectors.

KEY TAKEAWAYS

TrickBot Operators

- Are a sophisticated cybercrime group known by several aliases in open-source reporting, including
  - Wizard Spider (CrowdStrike),[1]
  - UNC1878 (FireEye), and
  - Gold Blackburn (Secureworks).[2]
- Employ malware from other 'trusted' cybercrime actors, including Emotet[3] and Bokbot.[4, 5]
- Enable high impact "big game hunting" ransomware attacks.
- Have a toolset capable of using the entire cyber kill chain, from delivery to post-exploitation.[6]

Initial Access

- The TrickBot operators typically achieve initial access through the following infection vectors: spearphishing, spam campaigns, malvertising, and network vulnerabilities (e.g., Server Message Block).
  - Spearphishing campaigns use tailored emails that contain malicious links or documents that contain macros, which—if enabled—execute malware.

Execution

- The TrickBot operators may
  - Execute TrickBot as either a first- or second-stage payload;
  - Deploy additional malware (e.g., Ryuk[7] and Conti ransomware, Emotet downloader); and
  - Load TrickBot into networks using other malware to achieve additional objectives.

Capabilities

- TrickBot may be used
  - To exfiltrate data (e.g., email, credentials, point-of-sale info);
  - For cryptomining; and
  - For host enumeration (e.g., reconnaissance of Unified Extensible Firmware Interface or Basic Input/Output System [UEFI/BIOS] firmware).[8]
    - For host enumeration, the operators deliver TrickBot in modules containing a configuration file with specific tasks.

[1] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
[2] https://www.secureworks.com/research/threat-profiles/gold-blackburn
[3] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
[4] https://www.crowdstrike.com/blog/wizard-spider-lunar-spider-shared-proxy-module/
[5] https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/
[6] https://www.crowdstrike.com/blog/wizard-spider-adversary-update/
[7] https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
[8] https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/#background

ADDITIONAL REFERENCES

CISA Alert AA21-076A: TrickBot Malware *(to be published March 17, 2021)*

Multi-State Information Sharing and Analysis Center (MS-ISAC) Security Primer — TrickBot

CISA Alert AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector

CISA and MS-ISAC's Joint Ransomware Guide

CISA Tip: Avoiding Social Engineering and Phishing Attacks

Federal Bureau of Investigation Public Service Announcement: High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations

FireEye Blog: A Nasty Trick: From Credential Theft Malware to Business Disruption

FireEye Blog: It's Your Money and They Want It Now — The Cycle of Adversary Pursuit

Malwarebytes Blog: Trojan.TrickBot

Microsoft Security Blog: TrickBot Disrupted

MITRE ATT&CK: Wizard Spider

National Institute of Standards and Technology Special Publication 1800-26 – Data Integrity

National Cyber Security Centre (United Kingdom) Advisory: TrickBot

Palo Alto — Unit 42: TrickBot Campaign

SANS Threat Analysis Rundown Recap: The Return of UNC1878

CONTACT INFORMATION

- 1-888-282-0870
- Central@cisa.gov (UNCLASS)
- NCCIC@dhs.sgov.gov (SIPRNET)
- NCCIC@dhs.ic.gov (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://www.surveymonkey.com/r/CISA-cyber-survey.