LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Trickbot

01/09/2020

Report #: 202001091000

Agenda

- Overview
- Attack vectors and initial execution
- Persistence and propagation
- References
- Questions

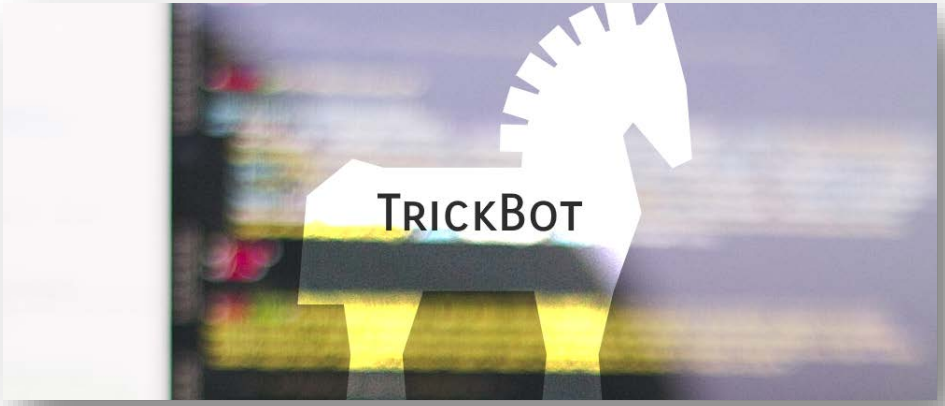


Image courtesy of ZDNet

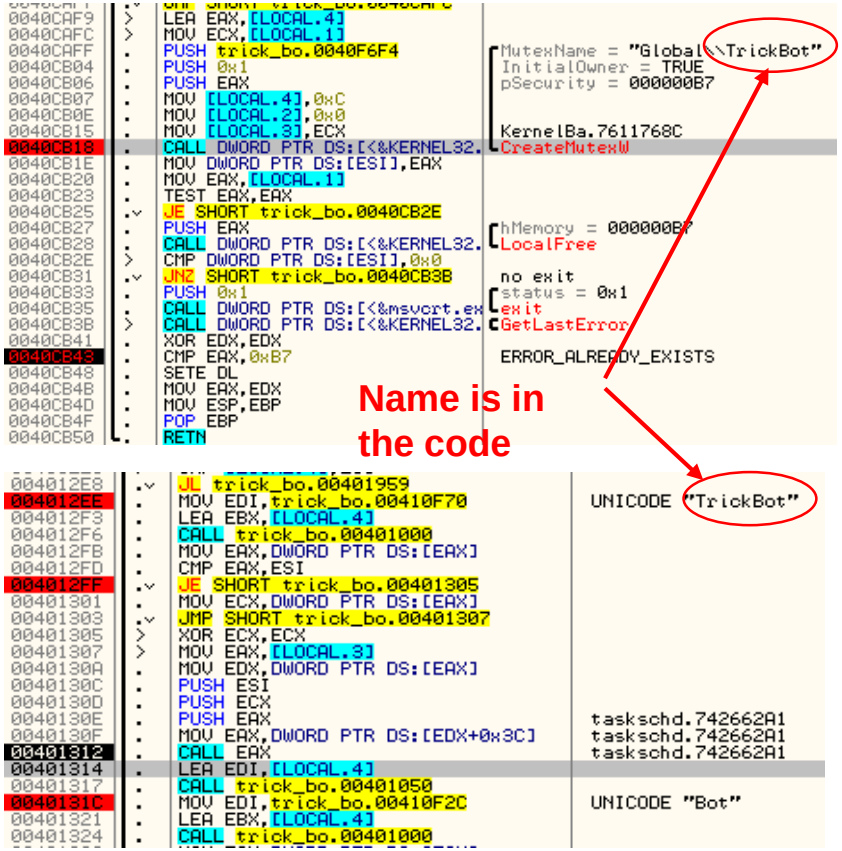
Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- AKA Trickster, TrickLoader and TheTrick
- Modular malware, described as a banking trojan
- Similar to Dyreza, an old credential-stealer
  - Probably operated and maintained by the same group - code similarities and circumstances
- Used by: Wizard Spider (likely Russian cybercriminals)
- What separates TrickBot from the crowd?
  - Constantly evolving (and increasingly powerful)
  - Frequently used to target a variety of organizations
  - Nothing that TrickBot does is unique
    - Aggregate capabilities make it a powerful tool
- Offered as Access-as-a-Service
- Frequently used to target healthcare organizations and providers
  - Often utilized in combination with other malware in multi-staged attacks



Images courtesy of Malwarebytes

Attack vectors and initial execution

- TrickBot uses standard attack vectors for infection:
  - Malvertising – The use of advertising – legitimate or fake – to surreptitiously deliver TrickBot to victim system
  - SpearPhishing – E-mails with malicious links or attachments that specifically target organizational leadership
  - Network vulnerabilities – SMB (Server Message Block) and RDP (Remote Desktop Protocol) are common
  - Secondary payload – Sometimes dropped by other malware (second stage), often Emotet
- Execution – multiple layers
  - First layer contains encrypted payload
    - Attempts to conceal TrickBot from detection
    - Uses AES or ECC encryption
  - Second layer is the main bot loader
    - Will deploy either 32-bit or 64-bit payload

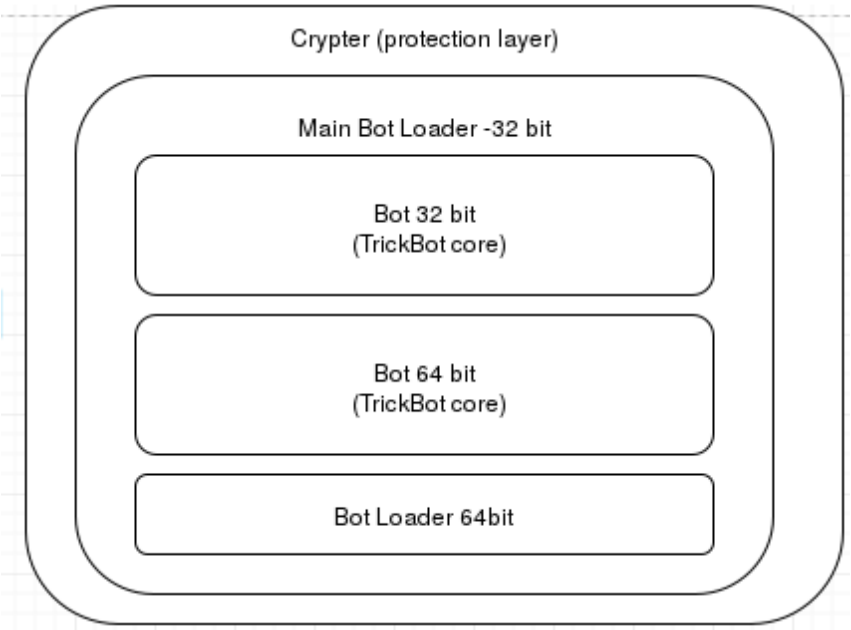


Image courtesy of Malwarebytes

Persistence and propagation

- TrickBot maintains access via the creation of a scheduled task
- Further spreading/lateral movement:
  - EternalBlue exploit
  - DLLs
  - PowerShell Empire
  - Vulnerable network shares

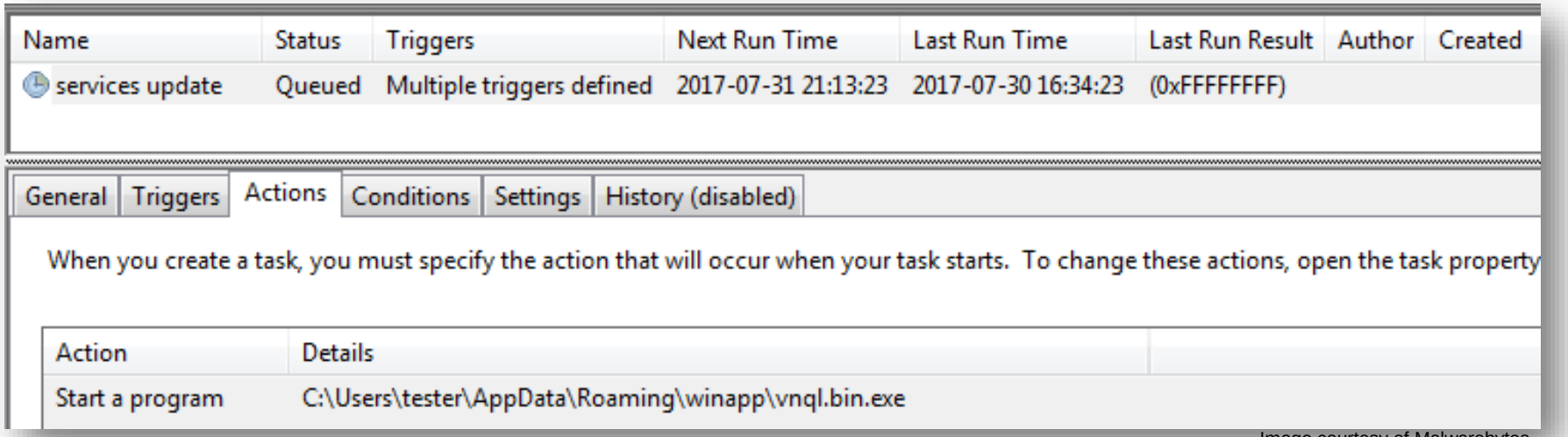
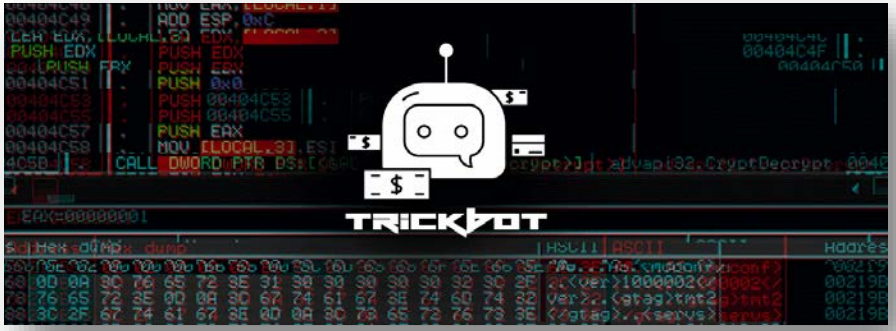


Image courtesy of Malwarebytes

TrickBot functionality overview

- Data exfiltration
  - Banking/Financial information
  - System/Network reconnaissance
  - Credential and user info harvesting
- Network propagation
- Remote control (C2)
- Dropper (Rig Expliot Kit, Ryuk)
- Persistence (scheduled task or registry key)
- Code injection
- Anti-detection/analysis
- SIM-swapping

"TrickBot was developed in 2016 as a banking malware, however, since then it has developed into something essentially different – a flexible, universal, module-based crimeware solution" – Sentinel Labs



Common TrickBot Modules

- Data exfiltration
  - TrickBot often leverages open redirections and server side injects to steal banking credentials.
    - What is an open redirect?
      - When a user-submitted link directs a web app/server to redirect the user to a malicious webpage instead.
      - https://legit_web_site.com/redirect.php?go=http://malicious_web_site.com/steal_credentials/
  - TrickBot has many modules to steal banking info
    - Dinj – File contains banking information; Uses server side web injections
    - Dpost – Most of the data exfiltrated by TrickBot is sent to the dpost IP address.
    - LoaderDll/InjectDll – Monitors for banking website activity; Leverages web injects to steal financial data.
    - Sinj – Retains information on targeted online banks; Utilizes redirection attacks (fake web injections) to exfiltrate financial data

Common TrickBot Modules (continued)

- System/Network Reconnaissance
  - Mailsearcher – Compares all files on the disk against a list of file extensions.
  - NetworkDll – Collects system information and maps networks
  - Systeminfo – Provides hackers with basic system information for reconnaissance purposes

- Credential harvesting
  - DomainDll – Uses LDAP to harvest credentials and configuration data from domain controller by accessing shared SYSVOL files.
  - ModuleDll/ImportDll – Harvests browser data – cookies and browser configs.
  - OutlookDll – Harvests saved MS Outlook credentials by querying registry keys
  - Pwgrab – Steals credentials, autofill data, history, and other information from browsers as well as several software applications
  - SqulDll – Forces WDigest authentication; Utilizes Mimikatz to scrape credentials from LSASS.exe. The worming modules use these credentials.

- Network Propogation
  - WormDll and ShareDll – Worming module that uses Server Message Block (SMB) and Lightweight Directory Access Protocol (LDAP) for lateral movement.
  - TabDll – Leverages EternalRomance exploit (CVE-2017-0147) to spread via SMBv1.

Wizard Spider

- Wizard Spider
  - Operators of TrickBot
  - Carry out wire fraud
  - Alleged to be affiliated with Russian cybercrime rings
  - Affiliated with Grim Spider, Lunar Spider and Mummy Spider
  - Some members were part of the group that operated Dyre (Dyreza)
    - Dyreza ceased operating in November 2015 after Russian law enforcement raided the entertainment company believed to be behind it
    - No Dyreza activity for a little over a year
    - October, 2016 - TrickBot identified in the wild for the first time with noted similarities to Dyreza; The operation was immediately successful and grew
- Secure Works identifies the same group as GOLD BLACKBURN

Image courtesy of ThreatPost

TrickBot vs. Healthcare

- TrickBot – multi-stage attacks
  - Malware can drop TrickBot
    - Emotet
  - TrickBot can drop other malware
    - Ransomware
  - Dwell time means you shouldn't assume all attacks are single-step
- Ransomware, which ravages the healthcare community, is often dropped
- A frequent combination:

Image courtesy of Dark Reading

- Emotet: Initial compromise; Often delivered via spam/phishing or RDP exploitation; Delivers TrickBot
- TrickBot: Payload of Emotet; Used to conduct reconnaissance; Delivers Ryuk
- Ryuk executes it's ransomware functionality
- TrickBot is also commonly used to deploy Mimikatz

TrickBot Defense/Infection Prevention

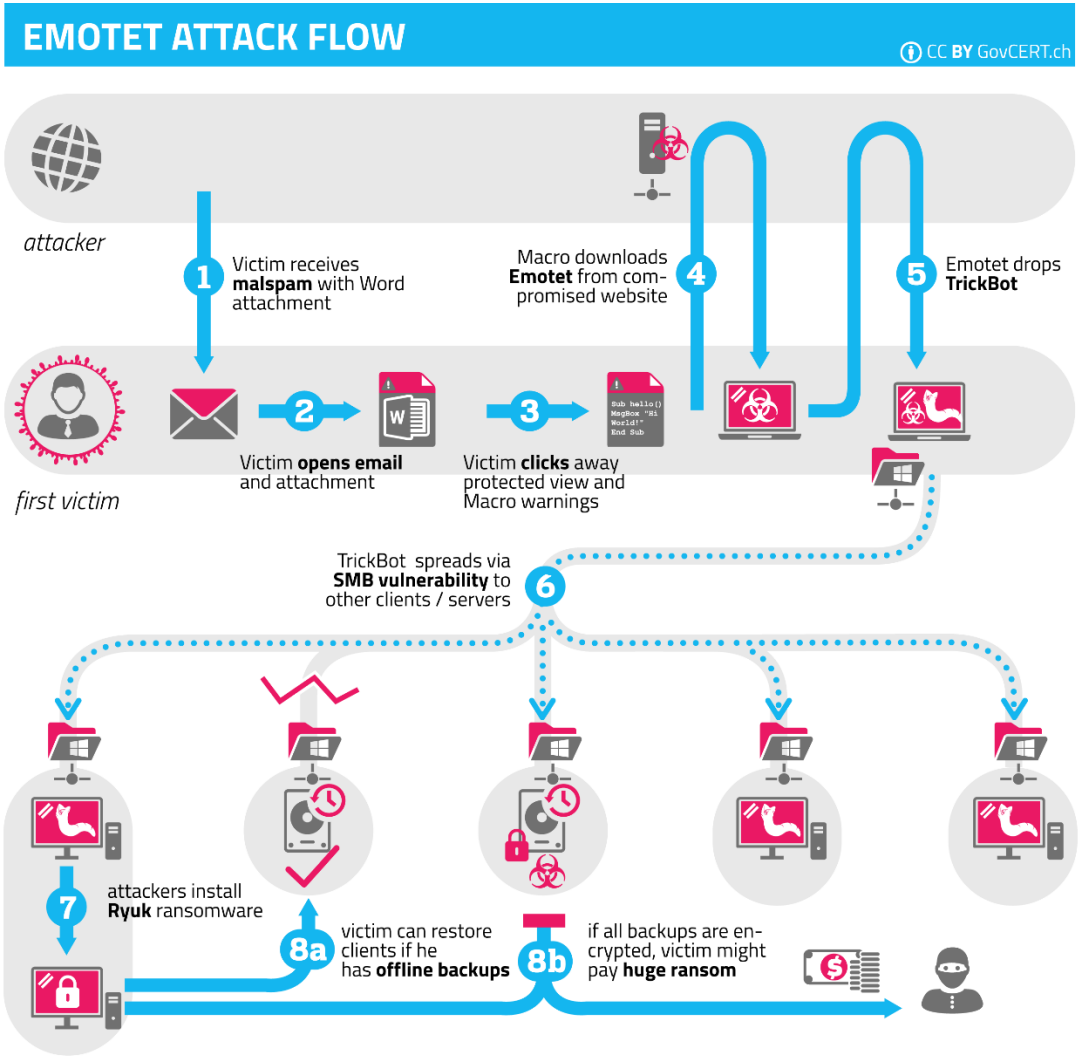


Image courtesy of Swiss Government Computer Emergency Response Team

TrickBot Defense/Infection Prevention

- Provide social engineering and phishing training to employees. **[10.S.A], [1.M.D]**
- Develop and maintain policy on suspicious e-mails for end users; Ensure suspicious e-mails are reported **[10.S.A], [10.M.A]**
- Ensure emails originating from outside the organization are automatically marked before received **[1.S.A], [1.M.A]**
- Apply applicable patches and updates immediately after testing; Develop and maintain patching program if necessary. **[7.S.A], [7.M.D]**
- Implement Intrusion Detection System (IDS). **[6.S.C], [6.M.C], [6.L.C]**
- Implement spam filters at the email gateways. **[1.S.A], [1.M.A]**
- Block suspicious IP addresses at the firewall. **[6.S.A], [6.M.A], [6.L.E]**
- Implement whitelisting technology on appropriate assets to ensure that only authorized software is allowed to execute. **[2.S.A], [2.M.A], [2.L.E]**
- Implement access control based on the principal of least privilege. **[3.S.A], [3.M.A], [3.L.C]**
- Implement and maintain anti-malware solution. **[2.S.A], [2.M.A], [2.L.D]**
- Conduct system hardening to ensure proper configurations. **[7.S.A], [7.M.D]**
- Disable the use of SMBv1 (and all other vulnerable services and protocols) and require at least SMBv2. **[7.S.A], [7.M.D]**
- **Yara Rules**: https://malpedia.caad.fkie.fraunhofer.de/details/win.TrickBot

Indicators of Compromise

Hashes
4be3286c57630fb81e079c1aa3bf3203
fe2d9595a96046e441e43f72deac8cb0
5a137c1dd4a55c06531bdbfeaf15c894
8bf6ee81794c965f38484c0570718971
9d166a822439a47eb2dfad1aeb823638
6e714a44051f74ee2f8f570ea1a6b2b9
44964db9c3ad8bea0d0d43340c4b0a3a
45160aa23d640f8d1bcb263c179f84f9
e8fcae05cfb72b109db17fe69c292758
c4acef1322b335d6b6f7a924d9af4ad6
440d284b8c4b85f806b113507dc55004
6135d0ef033e82c6756cbc11416c9f6c
4be3286c57630fb81e079c1aa3bf3203
fe2d9595a96046e441e43f72deac8cb0
5a137c1dd4a55c06531bdbfeaf15c894
8bf6ee81794c965f38484c0570718971
9d166a822439a47eb2dfad1aeb823638
1bc7517f20b7b3e9d67c776f5e1bf7df
68e762001faa31193081279ccfb01c19
ef393133f39f20f7cc685d0cc59b0f5e
3f8fe650b06cb4b869fb7c4486ff0403
998718d01e49f4ac30210092d17ef4dc
2bd1db2f8f10f32998c4a23a41286073
2440448d00f0a2edfa321a2784c32775
5e6795e64b3ea622799acad4d51ffbab

Hashes
dcd0e73b264427269c262d6dc070570ce76c56faaf5ccfcebc0ae79b4e32130d
06690d06c356d91673510e083b5d6e1d1ae2bef1b5b77e88b10388d7527fbde2
2c8c58a6ac929cd4e2b65c3982d57a255504764c4986d8a107272516787e5e44
c19ed0c625bc88aa076bb8b2da5c52e215eeac42caf835371d010a4ce64e90c8
4d36a7c86db693718ec71c33fc66f7444f541c5e193422b2a8dc38855558aa9c
f1f15bc285256f1958da74419fd596952b3a166dd6174bd6835e2af76fac637e
be9d8f31e9dfaab5c2d22a1399e92d6ab41678d2b0c1c9fa2937c6d40bcc1158
10e93082a97d64e3215c9338142cfbd3bc95c533c5cb5aa7e0b7a7f4ec1b3ef7
67a3dedd64c18a8b50f673638af4ab678d0974e952692a237a57eb5e7cc47cf7
473fdeb2b568751d762ffe64287ed5035c6e7ea8fa6e1aba22518f480827ab95
c7a3123a5cff9c78e2fd926c6800a6c6431c8bca486ce11319a9a8f6fa83945c
f095c730442b5d72e0c234bc66c7d23e32e04d53018606b6cdc5e13c51451a6f
8f31c2f384cf7aecd7cef93f2c793233ce10104a09a3a438e5efb7e5a575277c
c8577ae514d60239b81a37396f85fb1ab661efae37b6b511e83ac239a2cbbd06
79b772476c8d5dc09bbbc615408a33cfc70eb0c49a268c25932c1f4fdcb940ff
ae5d6b400ec4ca773d19d689ca3a3d328a1604242c0146d76110d79892529243
f70b800fe6145186c7f4763536959eeb8efa804395cca25d1cf07f4d46a11795
eca44266bbaeb69286b0edbbe2f9cea6ca0633077044990c7d660c03058fbaa5
2f38a85818f2e4a97995027349798e81f588634b280d11e217b1387ae1cb91a5
85528e675dd0ebbc4dca36d501268f5fc3b35c8cc6fe7648aa62530f032ec3a9
2d5b33a32e4df1169b09c06fe13f98e93cb108cc9163f322001a2db3b8a76519
2d5deb963cf9cef62da59687e75f27ffd4d71db18272add942a93952a8920eb2
33a36a0172595eedf4a682ffe173662b3092bfe71fbdfdf4e5f4dcd365513564
357208a511d7d0277e467719036d801c91ae6b66a9988a5092db9b6af99603b8
45aeda204fa240e37b87d8c183343aa617ba7e8fd42bedbfc4ebcf7e3385e3be

Indicators of Compromise

IPs
103.198.130.148
103.58.144.249
115.186.139.104
138.186.22.2
168.194.80.70
176.121.213.31
177.104.69.130
177.231.253.158
177.87.233.4
184.160.113.13
185.158.175.95
185.27.219.173
185.47.136.111
185.8.0.182
186.208.102.185
186.208.106.234
186.208.111.188
188.255.156.67
188.255.249.27
190.2.235.246
196.11.84.62
200.116.206.58
217.31.110.43
36.66.107.162
37.61.239.216

IPs
49.156.45.139
5.172.33.237
5.172.34.138
82.146.94.150
82.146.94.86
84.42.159.138
95.104.2.225
96.9.69.131
190.138.249.45
200.119.236.86
36.66.107.162
221.179.156.39
80.51.120.132
203.92.62.46
84.42.159.138
190.138.249.45

Hashes
4859cb4bc26d257e2720dacb777895b2541f72a8848dfa554665e1b04e1a9f7a
566e1ee0d6ab08685f722c041c635894d0169f30accf5325d5f0413717c1beab
600b00554ff77da736f199efa7338cabc92307d32dc527f096e00ec718039778
767fab90d7e27102d3208766baa0f5956073c36fc31b93b854c2afbdc25b6c15
ad1a5597477817161619ea4b0dbdf92186260947f808ced5e18f60990b229795
c3c4acdb0f7164a8c3095df6fa5932d5d8617254856576372b86238c092dac80
ef87f15fb3383455cbd86bb5c1c792535d06c334499025ab8c5091c33a722f1c
fdf5bae149683eff434f734295693723dd83b3769b63e5317e137c4ac4aff6ae

NOTE: There exists a very large quantity of IOCs associated with TrickBot. This presentation contains only a small sample. Furthermore, due to the aggressive and constant development of the tool, new IOCs are frequently released. Therefore, we strongly advice any organization that wishes to adequately protect itself from TrickBot continually maintain situational awareness regarding the latest releases.

Reference Materials

References

- Deep Analysis of the Online Banking Botnet TrickBot
  - http://blog.fortinet.com/2016/12/06/deep-analysis-of-the-online-banking-botnet-TrickBot
- Quick Test Drive of TrickBot (It now has a Monero module)
  - http://www.malware-traffic-analysis.net/2018/02/01/
- Quick Analysis of a TrickBot Sample with NSA's Ghidra SRE Framework
  - http://www.peppermalware.com/2019/03/quick-analysis-of-TrickBot-sample-with.html
- TrickBot's bag of tricks
  - http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/TrickBots-bag-of-tricks.html
- Let's Learn: TrickBot Socks5 Backconnect Module In Detail
  - http://www.vkremez.com/2017/11/lets-learn-TrickBot-socks5-backconnect.html
- Let's Learn: Introducing New TrickBot LDAP "DomainGrabber" Module
  - http://www.vkremez.com/2017/12/lets-learn-introducing-new-TrickBot.html
- Let's Learn: TrickBot Implements Network Collector Module Leveraging CMD, WMI & LDAP
  - http://www.vkremez.com/2018/04/lets-learn-TrickBot-implements-network.html
- How Does the TrickBot Malware Work?
  - https://blog.fraudwatchinternational.com/malware/TrickBot-malware-works
- Introducing TrickBot, Dyreza's successor
  - https://blog.malwarebytes.com/threat-analysis/2016/10/trick-bot-dyrezas-successor/
- TrickBot comes up with new tricks: attacking Outlook and browsing data
  - https://www.bleepingcomputer.com/news/security/TrickBot-comes-up-with-new-tricks-attacking-outlook-and-browsing-data/

References

- TrickBot comes up with new tricks: attacking Outlook and browsing data
  - https://blog.malwarebytes.com/threat-analysis/2017/08/TrickBot-comes-with-new-tricks-attacking-outlook-and-browsing-data/
- What's new in TrickBot? Deobfuscating elements
  - https://blog.malwarebytes.com/threat-analysis/malware-threat-analysis/2018/11/whats-new-TrickBot-deobfuscating-elements/
- The 2019 Resurgence of Smokeloader
  - https://blog.talosintelligence.com/2018/07/smoking-guns-smoke-loader-learned-new.html
- TrickBot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire
  - https://blog.trendmicro.com/trendlabs-security-intelligence/TrickBot-adds-remote-application-credential-grabbing-capabilities-to-its-repertoire/
- TrickBot Shows Off New Trick: Password Grabber Module
  - https://blog.trendmicro.com/trendlabs-security-intelligence/TrickBot-shows-off-new-trick-password-grabber-module
- TrickBot spread by Necurs botnet, adds Nordic countries to its targets
  - https://www.forcepoint.com/fr/blog/security-labs/TrickBot-spread-necurs-botnet-adds-nordic-countries-its-targets
- Little TrickBot Growing Up: New Campaign
  - https://f5.com/labs/articles/threat-intelligence/malware/little-TrickBot-growing-up-new-campaign-24412

References

- TrickBot Expands Global Targets Beyond Banks and Payment Processors to CRMs
  - https://f5.com/labs/articles/threat-intelligence/malware/TrickBot-expands-global-targets-beyond-banks-and-payment-processors-to-crms
- GitHub: TrickBot config files
  - https://github.com/JR0driguezB/malware_configs/tree/master/TrickBot
- Inquest: Memory Analysis of TrickBot
  - https://inquest.net/blog/2019/08/26/TrickBot-Memory-Analysis
- Vipre: TrickBot's Tricks
  - https://labs.vipre.com/TrickBots-tricks/
- Reverse engineering malware: TrickBot (part 1 - packer)
  - https://malware.news/t/reverse-engineering-malware-TrickBot-part-1-packer/15759
- Reverse engineering malware: TrickBot (part 2 - loader)
  - https://malware.news/t/reverse-engineering-malware-TrickBot-part-2-loader/15758
- Reverse engineering malware: TrickBot (part 3 - core)
  - https://malware.news/t/reverse-engineering-malware-TrickBot-part-3-core/15757
- TrickBot Takes to Latin America, Continues to Expand Its Global Reach
  - https://securityintelligence.com/TrickBot-takes-to-latin-america-continues-to-expand-its-global-reach/

References

- TrickBot's Cryptocurrency Hunger: Tricking the Bitcoin Out of Wallets
  - https://securityintelligence.com/TrickBots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/
- Tricks of the Trade: A Deeper Look Into TrickBot's Machinations
  - https://securityintelligence.com/tricks-of-the-trade-a-deeper-look-into-TrickBots-machinations/
- New Version of "TrickBot" Adds Worm Propagation Module
  - https://www.flashpoint-intel.com/blog/new-version-TrickBot-adds-worm-propagation-module/
- TrickBot Gang Evolves, Incorporates Account Checking Into Hybrid Attack Model
  - https://www.flashpoint-intel.com/blog/TrickBot-account-checking-hybrid-attack-model/
- Deep Analysis of TrickBot New Module pwgrab
  - https://www.fortinet.com/blog/threat-research/deep-analysis-of-TrickBot-new-module-pwgrab.html
- Severe Ransomware Attacks Against Swiss SMEs
  - https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes
- TrickBot - An analysis of data collected from the botnet
  - https://www.govcert.ch/blog/37/TrickBot-an-analysis-of-data-collected-from-the-botnet
- TrickBot Banking Trojan - DOC00039217.doc
  - https://www.ringzerolabs.com/2017/07/TrickBot-banking-trojan-doc00039217doc.html
- The TrickBot and MikroTik connection
  - https://www.secdata.com/the-TrickBot-and-mikrotik/

References

- TrickBot Modifications Target U.S. Mobile Users
  - https://www.secureworks.com/blog/TrickBot-modifications-target-us-mobile-users
- INNOVACIÓN EN PROCESOS - ORGANIZATIVOS INFORME DE MALWARE -Evolución de TrickBot (Report in Spanish, but MD5 hashes on page 4)
  - https://www.securityartwork.es/wp-content/uploads/2017/06/Informe_Evoluci%C3%B3n_TrickBot.pdf
- Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez
  - https://www.slideshare.net/proidea_conferences/inside-cybercrime-groups-harvesting-active-directory-for-fun-and-profit-vitali-kremez
- Sneaky Monkey - TrickBot – Analysis
  - https://www.sneakymonkey.net/2019/05/22/TrickBot-analysis/
- Sneaky Monkey - TrickBot – Analysis Part II
  - https://www.sneakymonkey.net/2019/10/29/TrickBot-analysis-part-ii/
- Evolving TrickBot Adds Detection Evasion and Screen-Locking Features
  - https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/evolving-TrickBot-adds-detection-evasion-and-screen-locking-features
- Tale of the Two Payloads – TrickBot and Nitol
  - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tale-of-the-two-payloads-TrickBot-and-nitol/

References

- Random RE: TrickBot & UACME
  - https://sysopfb.github.io/malware/2018/04/16/TrickBot-uacme.html
- Targeted TrickBot activity drops 'PowerBrace' backdoor
  - https://technical.nttsecurity.com/post/102fnog/targeted-TrickBot-activity-drops-powerbrace-backdoor
- Palo Alto Unit 42 - Wireshark Tutorial: Examining TrickBot Infections
  - https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-TrickBot-infections/
- Netscout - TrickBot Banker Insights
  - https://www.arbornetworks.com/blog/asert/TrickBot-banker-insights/
- TrickBot banking trojan using EFLAGS as an anti-hook technique
  - https://www.blueliv.com/research/TrickBot-banking-trojan-using-eflags-as-an-anti-hook-technique/
- F5 Networks: The TrickBot Evolution
  - https://www.botconf.eu/wp-content/uploads/2016/11/2016-LT09-TrickBot-Adams.pdf
- Detricking TrickBot Loader
  - https://www.cert.pl/en/news/single/detricking-TrickBot-loader/
- “Sin”-ful SPIDERS: WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web
  - https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web

References

- Latest TrickBot Variant has New Tricks Up Its Sleeve
  - https://www.cyberbit.com/blog/endpoint-security/latest-TrickBot-variant-has-new-tricks-up-its-sleeve/
- Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk
  - https://www.cybereason.com/blog/triple-threat-emotet-deploys-TrickBot-to-steal-data-spread-ryuk-ransomware
- TrickBot: We Missed you, Dyre
  - https://www.fidelissecurity.com/threatgeek/2016/10/TrickBot-we-missed-you-dyre
- A Nasty Trick: From Credential Theft Malware to Business Disruption
  - https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html
- TrickBot Banking Trojan Adapts with New Module
  - https://www.webroot.com/blog/2018/03/21/TrickBot-banking-trojan-adapts-new-module/
- TrickBot Adds ‘Cookie Grabber’ Information Stealing Module
  - https://cofense.com/TrickBot-adds-cookie-grabber-information-stealing-module/
- How Does the TrickBot Malware Work?
  - https://fraudwatchinternational.com/malware/TrickBot-malware-works/
- TrickBot Malware Goes After Remote Desktop Credentials
  - https://threatpost.com/TrickBot-remote-desktop/141879/

References

- TrickBot, today's top trojan, adds feature to aid SIM swapping attacks
  - https://www.zdnet.com/article/TrickBot-todays-top-trojan-adds-feature-to-aid-sim-swapping-attacks/
- TrickBot or Treat – Knocking on the Door and Trying to Enter
  - https://www.fortinet.com/blog/threat-research/TrickBot-or-treat-threat-analysis.html
- Stealthy TrickBot Malware Has Compromised 250 Million Email Accounts And Is Still Going Strong
  - https://www.forbes.com/sites/leemathews/2019/07/14/stealthy-TrickBot-malware-has-compromised-250-million-email-accounts-and-is-still-going-strong/#6d1ea4b34884
- MS-ISAC Releases Security Primer on TrickBot Malware
  - https://www.us-cert.gov/ncas/current-activity/2019/03/14/MS-ISAC-Releases-Security-Primer-TrickBot-Malware
- Trojan.TrickBot
  - https://blog.malwarebytes.com/detections/trojan-TrickBot/
- Security Primer – TrickBot
  - https://www.cisecurity.org/white-papers/security-primer-TrickBot/
- TrickBot Trojan Getting Ready to Steal OpenSSH and OpenVPN Keys
  - https://www.bleepingcomputer.com/news/security/TrickBot-trojan-getting-ready-to-steal-openssh-and-openvpn-keys/
- Deep Analysis of the Online Banking Botnet TrickBot
  - http://blog.fortinet.com/2016/12/06/deep-analysis-of-the-online-banking-botnet-TrickBot

References

- 2018-02-01 - QUICK TEST DRIVE OF TrickBot (IT NOW HAS A MONERO MODULE)
  - http://www.malware-traffic-analysis.net/2018/02/01/
- Quick Analysis of a TrickBot Sample with NSA's Ghidra SRE Framework
  - http://www.peppermalware.com/2019/03/quick-analysis-of-TrickBot-sample-with.html
- TrickBot's bag of tricks
  - http://www.pwc.co.uk/issues/cyber-security-data-privacy/research/TrickBots-bag-of-tricks.html
- Let's Learn: TrickBot Socks5 Backconnect Module In Detail
  - http://www.vkremez.com/2017/11/lets-learn-TrickBot-socks5-backconnect.html
- Let's Learn: Introducing New TrickBot LDAP "DomainGrabber" Module
  - http://www.vkremez.com/2017/12/lets-learn-introducing-new-TrickBot.html
- Let's Learn: TrickBot Implements Network Collector Module Leveraging CMD, WMI & LDAP
  - http://www.vkremez.com/2018/04/lets-learn-TrickBot-implements-network.html
- TrickBot spread by Necurs botnet, adds Nordic countries to its targets
  - https://blogs.forcepoint.com/security-labs/TrickBot-spread-necurs-botnet-adds-nordic-countries-its-targets
- Little TrickBot Growing Up: New Campaign
  - https://f5.com/labs/articles/threat-intelligence/malware/little-TrickBot-growing-up-new-campaign-24412

References

- TrickBot Expands Global Targets Beyond Banks and Payment Processors to CRMs
  - https://f5.com/labs/articles/threat-intelligence/malware/TrickBot-expands-global-targets-beyond-banks-and-payment-processors-to-crms
- GitHub: malware_configs
  - https://github.com/JR0driguezB/malware_configs/tree/master/TrickBot
- TrickBot — a concise treatise
  - https://medium.com/@vishal_29486/TrickBot-a-concise-treatise-d7e4cc97f737
- TrickBot banking trojan using EFLAGS as an anti-hook technique
  - https://www.blueliv.com/research/TrickBot-banking-trojan-using-eflags-as-an-anti-hook-technique/
- What Is an Open Redirection Vulnerability and How to Prevent it?
  - https://dzone.com/articles/what-is-an-open-redirection-vulnerability-and-how

Questions

Questions

Upcoming Briefs

- Botnet Threats to the healthcare industry
- Zeppelin Ransomware

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV