Agenda

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

Slides Key:

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

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

Image courtesy of ZDNet
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
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
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

![Scheduled Task Image](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 Exploit 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.


- 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
  • Mailseacher – 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

- 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:

```
Emotet → TrickBot → Ryuk
```

- 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

**EMOTET ATTACK FLOW**

1. Attacker sends malicious mail with Word attachment.
2. Victim opens email and attachment.
3. Victim clicks away protected view and macro warnings.
4. Macro downloads Emotet from compromised website.
5. Emotet drops TrickBot.
6. 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 encrypted, victim might pay huge ransom.

Image courtesy of Swiss Government Computer Emergency Response Team.

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM

TLP: WHITE, ID# 202001091000

11
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 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 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]

## Indicators of Compromise

### Hashes

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4be3286c57630fb81e079c1aa3bf3203</td>
<td>dcd0e73b264427269c262d6dc070570ce76c56faaf5ccfceb0ae79b4e32130d</td>
</tr>
<tr>
<td>fe2d9595a96046e441e43f72deac8cb0</td>
<td>06690d06c356d91673510e083b5d61e1de2ae2efb15b77e88b103887d527fbd2</td>
</tr>
<tr>
<td>5a137c1cd4a55c06531bdbeaf15c894</td>
<td>2c8c58a6a929cd4e2b65c3982d57a255054764c9486d8a107272516787e5e44</td>
</tr>
<tr>
<td>8bf6ee817974c965f38484c0570718971</td>
<td>c19ed0c6256b88a076bb8b2da5c5e215eearc42ca835371d010a4ce64e90c8</td>
</tr>
<tr>
<td>9d166a822439a47eb2fada1ae8b23638</td>
<td>4d36a7c86bd93718c711c3c3f66f7445f41c5e193422b2a8dc38855558aa9c</td>
</tr>
<tr>
<td>6e714a44051f74ee2f8f570ea1a6b2b9</td>
<td>f1f15bc285256f1958a74419fd596952b3a166dd6174bd6835e2af76fac637e</td>
</tr>
<tr>
<td>44964db9c3ad8bea0dd43340c4b0a3a</td>
<td>be9d88f31e9d9aa5c2d22a1399e92d6ab41678d2b0c19fa2937cd40bccc158</td>
</tr>
<tr>
<td>45160aa23d640f8d1bcb263c179f849f</td>
<td>10e9308a297d64e32159c9383142cfd3b9c533c5cb5a7e0b7a7f4ec1b3ef7</td>
</tr>
<tr>
<td>e8fcaee05cfe7b2b109db17fe69c292758</td>
<td>67a3ddd64c18ab5b0f673638af4ab678d0974e952692a237a5eb5e7cc47cf7</td>
</tr>
<tr>
<td>c4acef13223d66b6f7a924d9af4ad6</td>
<td>473fdebe2b568751d762ffed5035c67ea8f6e1a2251b84f80279b95</td>
</tr>
<tr>
<td>440d284b8c4b85f806b113507dc55004</td>
<td>c7a3123a5c799c7e82f9d26c800a6c643134bca486ce11319a9a8f6a83945c</td>
</tr>
<tr>
<td>61350def0338e2bc6756bccc11416c9f6c</td>
<td>f095c73074424b572e0c234b66c67d23e32e04d53018606b66cd5e15c15415a6f</td>
</tr>
<tr>
<td>4be3286c57630f81e079c1aa3bf3203</td>
<td>8f31c2f384f7cea7fe93f2c793233ce10104a0a9a3a438e5efb7e5a575277c</td>
</tr>
<tr>
<td>fe2d9595a96046e441e43f72deac8cb0</td>
<td>c8577ae514d60239b8a13739685f85b1a661fefa37b6b51183ac239a2cb6d06</td>
</tr>
<tr>
<td>5a137c1dd4a55c06531bdbeaf15c894</td>
<td>79b772476c8d5dc09b9bb615408a33cfc70e0b4c9a268c25932c1f4fdcb940ff</td>
</tr>
<tr>
<td>8bf6ee817974c965f38484c0570718971</td>
<td>ae56db400ec47a773d91d689ac3a3d328a1604242c0146d76110d79892529243</td>
</tr>
<tr>
<td>9d166a822439a47eb2fada1ae8b23638</td>
<td>f70b800e6145186c7f746753636959e08ef8a084395ca25d1cf07f4d6a11795</td>
</tr>
<tr>
<td>1bc7517f20b7b3e9d67c776f5e1bd7f</td>
<td>eca44266bbaaeb69286b0edeb2e2f9ce6a063307044990c7d660c03058fbaa5</td>
</tr>
<tr>
<td>68e762001faa31193081279ccfb01c19</td>
<td>2f38a85818f2e4a97995027349798e81f588634b280d11e217b1387ae1c9b1a5</td>
</tr>
<tr>
<td>ef39133c67207f7cc685dccc59b0f5e</td>
<td>855282e675d0e6bbc4d3a3d501268f53cb35c8cc66fe7648a662530f303e3a9</td>
</tr>
<tr>
<td>3f8e65b06cb4b869fb7c4486ff0403</td>
<td>2d5b33a32e4df1169b09c06fe13f9e893cb108cc9163f322001a2d3b3a876519</td>
</tr>
<tr>
<td>998718d01e49f4ac30210092d17e7f4dc4</td>
<td>2d5deb9639c39f62da59687e75f277f4d71db18272add942a9352a8920eb2</td>
</tr>
<tr>
<td>2bd1d2bf8f10f32998c4a23a41286073</td>
<td>33a36a0172595eef4d4a682ffef173662b3092be7f1bdef4e5f4dcd365513564</td>
</tr>
<tr>
<td>2440448d00f0a2edfa321a2784c32775</td>
<td>357208a511d7d0277e467719036d801c91ae6b66a9988a5092db9b6af99603b8</td>
</tr>
<tr>
<td>5e6e795e64b3ea622799ac64d51ffbab</td>
<td>45aeda204fa240e37b87d8c183343aa617b7ae8f4d2bedebf4ecbf7e3385e3be</td>
</tr>
</tbody>
</table>
# Indicators of Compromise

## IPs

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>103.198.130.148</td>
<td>49.156.45.139</td>
</tr>
<tr>
<td>103.58.144.249</td>
<td>5.172.33.237</td>
</tr>
<tr>
<td>115.186.139.104</td>
<td>5.172.34.138</td>
</tr>
<tr>
<td>138.186.22.2</td>
<td>82.146.94.150</td>
</tr>
<tr>
<td>168.194.80.70</td>
<td>82.146.94.86</td>
</tr>
<tr>
<td>176.121.213.31</td>
<td>84.42.159.138</td>
</tr>
<tr>
<td>177.104.69.130</td>
<td>95.104.2.225</td>
</tr>
<tr>
<td>177.231.253.158</td>
<td>96.9.69.131</td>
</tr>
<tr>
<td>177.87.233.4</td>
<td>190.138.249.45</td>
</tr>
<tr>
<td>184.160.113.13</td>
<td>200.119.236.86</td>
</tr>
<tr>
<td>185.158.175.95</td>
<td>36.66.107.162</td>
</tr>
<tr>
<td>185.27.219.173</td>
<td>221.179.156.39</td>
</tr>
<tr>
<td>185.47.136.111</td>
<td>80.51.120.132</td>
</tr>
<tr>
<td>185.8.0.182</td>
<td>203.92.62.46</td>
</tr>
<tr>
<td>186.208.102.185</td>
<td>84.42.159.138</td>
</tr>
<tr>
<td>186.208.106.234</td>
<td>190.138.249.45</td>
</tr>
<tr>
<td>186.208.111.188</td>
<td></td>
</tr>
<tr>
<td>188.255.156.67</td>
<td></td>
</tr>
<tr>
<td>188.255.249.27</td>
<td></td>
</tr>
<tr>
<td>190.2.235.246</td>
<td></td>
</tr>
<tr>
<td>196.11.84.62</td>
<td></td>
</tr>
<tr>
<td>200.116.206.58</td>
<td></td>
</tr>
<tr>
<td>217.31.110.43</td>
<td></td>
</tr>
<tr>
<td>36.66.107.162</td>
<td></td>
</tr>
<tr>
<td>37.61.239.216</td>
<td></td>
</tr>
</tbody>
</table>

## Hashes

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4859cb4bc26d257e2720dacb777895b2541f72a8848dfa554665e1b04e1a9f7a</td>
</tr>
<tr>
<td>566e1ee0d6ab08685f722c041c635894d0169f30accf5325d5f0413717c1beab</td>
</tr>
<tr>
<td>600b00554ff77da736f199efa7338cabc92307d32dc527f096e00ec718039778</td>
</tr>
<tr>
<td>767fab90d7e27102d3208766bba0f5956073c36fc31b93b854c2afbdcc25b6c15</td>
</tr>
<tr>
<td>ad1a5597477817161619ea4b0dbd92186260947f808ced5e18f60990b229795</td>
</tr>
<tr>
<td>c3c4acdb0f7164a8c3095df6fa5932d5d8617254856576372b86238c092dac80</td>
</tr>
<tr>
<td>ef87f15fb3383455cbb8d6c5c1c795235d06c334499025ab8c5091c33a722f1c</td>
</tr>
<tr>
<td>fdf5bae149683eff434f734295693723dd83b3769b63e5317e137c4ac4aff6ae</td>
</tr>
</tbody>
</table>
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

• Let’s Learn: Introducing New TrickBot LDAP "DomainGrabber" Module

• Let’s Learn: TrickBot Implements Network Collector Module Leveraging CMD, WMI & LDAP

• 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://blog.fraudwatchinternational.com/malware/TrickBot-malware-works
References

• TrickBot comes up with new tricks: attacking Outlook and browsing data

• What’s new in TrickBot? Deobfuscating elements

• The 2019 Resurgence of Smokeloader

• TrickBot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire

• TrickBot Shows Off New Trick: Password Grabber Module

• TrickBot spread by Necurs botnet, adds Nordic countries to its targets

• Little TrickBot Growing Up: New Campaign
  • [https://f5.com/labs/articles/threat-intelligence/malware/little-TrickBot-growing-up-new-campaign-24412](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

• GitHub: TrickBot config files
  • https://github.com/JR0driquezB/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
- Tricks of the Trade: A Deeper Look Into TrickBot’s Machinations
- New Version of “TrickBot” Adds Worm Propagation Module
- TrickBot Gang Evolves, Incorporates Account Checking Into Hybrid Attack Model
- Deep Analysis of TrickBot New Module pwgrab
- 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
- TrickBot Banking Trojan - DOC00039217.doc
- The TrickBot and MikroTik connection
• 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

• 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
• 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
• F5 Networks: The TrickBot Evolution
• Detricking TrickBot Loader
• “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

• 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

• 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

• 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

• 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

• 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

• Let's Learn: Introducing New TrickBot LDAP "DomainGrabber" Module

• Let's Learn: TrickBot Implements Network Collector Module Leveraging CMD, WMI & LDAP

• TrickBot spread by Necurs botnet, adds Nordic countries to 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

• GitHub: malware_configs
  • https://github.com/JR0driquezB/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

• What Is an Open Redirection Vulnerability and How to Prevent it?
  • https://dzone.com/articles/what-is-an-open-redirection-vulnerability-and-how
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.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

**About Us**

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

**Products**

**Sector & Victim Notifications**

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

**White Papers**

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.

**Threat Briefings & Webinar**

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