

## Reviewing the spam filters: Malspam pushing Gozi-ISFB

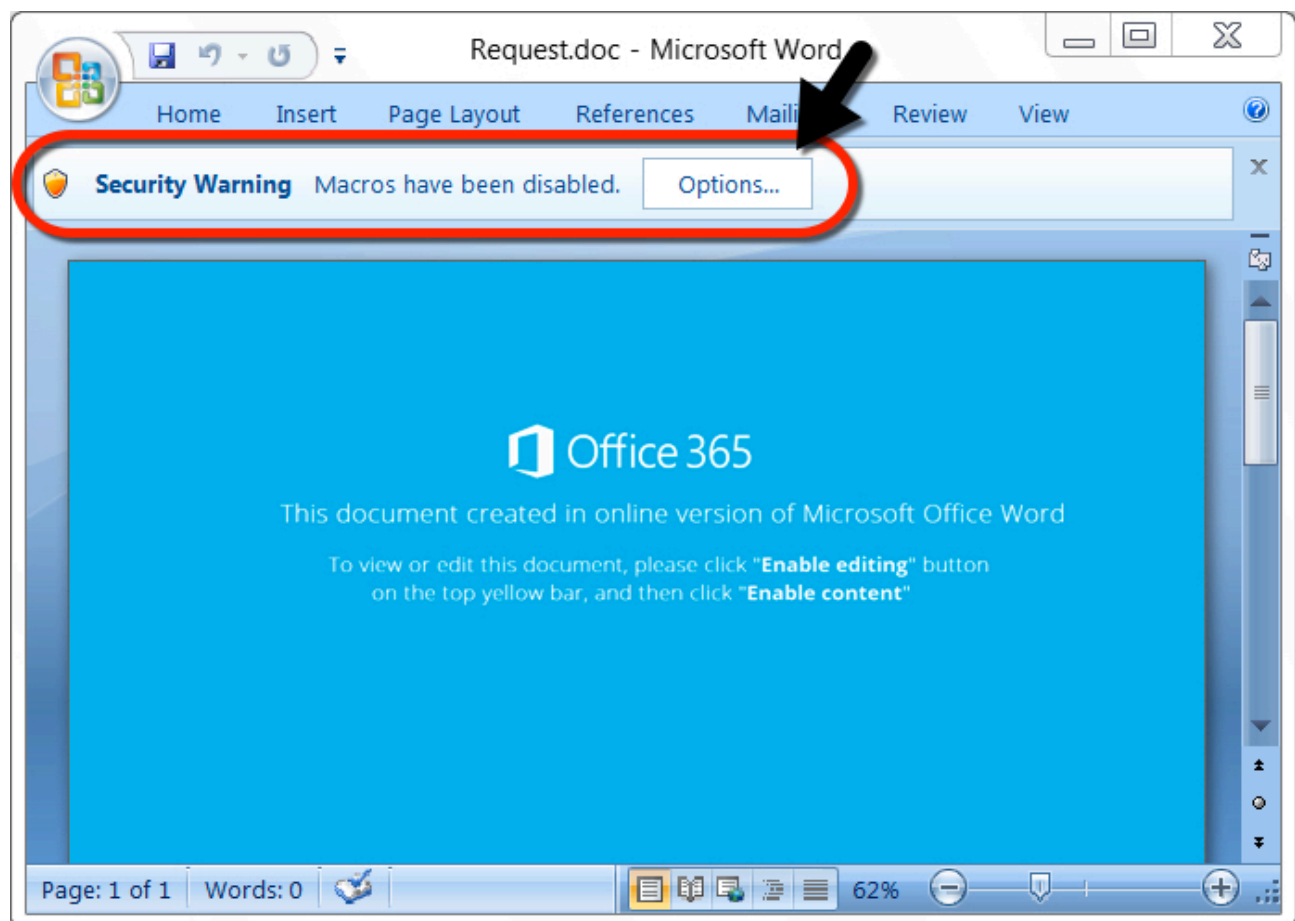
By SANS Internet Storm Center

Archived: 2026-04-05 17:34:13 UTC

### Introduction

Researchers should review their spam filters to see what malware is getting caught. Security professionals should be aware of current practices used by criminals pushing malware, even if it has little chance of infecting anyone in their organizations. Reviewing the spam filters keeps provides a clearer picture of our cyber-threat landscape.

In today's trip through the spam filters, I found two emails with malicious attachments. These attachments are Word documents with malicious macros designed to infect a vulnerable Windows host with Gozi-ISFB.



Shown above: Never a good sign when the document asks you to enable macros.

Unfortunately, I cannot share the emails. Both emails appear to contain legitimate correspondence. They each include a chain of previous messages, and I could not easily redact the information like I normally do with other examples of malicious spam.

Therefore, this diary will focus on the attachments, follow-up malware, and network traffic.

### What is Gozi-ISFB?

Gozi-ISFB is a variant of Ursnif, and today's traffic looked like an example shared by [@DynamicAnalysis](#) in a blog post on [malwarebreakdown.com](#).

I generated two infections using each of the Word documents. In today's activity, about 8 to 10 minutes after the initial infection, the infected Windows host downloaded follow-up malware. Here's what I saw:

- 1st Word document --> Gozi-ISFB --> Nymaim Trojan
- 2nd Word document --> Gozi-ISFB --> unknown malware

The first infection followed-up with the Nymaim Trojan, and I've documented Nymaim traffic back in [November](#) and [December](#) of 2017.

Filter: http.request or dns qry.name contains dtybgsb

Date/Time	Port	Host	Info
2018-01-17 03:35:12	80	ijqdjqrnwiduqujqieuzxc.com	GET /NU/sof.php?utma=baw HTTP/1.1
2018-01-17 03:35:12	80	ijqdjqrnwiduqujqieuzxc.com	GET /NU/baw.pfx HTTP/1.1
2018-01-17 03:35:16	80	ijqdjqrnwiduqujqieuzxc.com	GET /s.php?id=baw HTTP/1.1
2018-01-17 03:38:59	80	adistributedmean.net	POST /images/l8jbA1rj/VEcIQ4EhBV8F1oehM...
2018-01-17 03:38:59	80	adistributedmean.net	POST /images/EimMh_2F2kF/sI6GA7X99haLkF...
2018-01-17 03:38:59	80	adistributedmean.net	POST /images/vnQhqc6ty3Jwi9MhqFA/vmEf...
2018-01-17 03:38:59	80	adistributedmean.net	POST /images/Sc_2BvQNY/DqYTjKPR0HqtfgMp...
2018-01-17 03:41:54	80	adistributedmean.net	GET /images/o4hJpzkRi8S_2FA/CU4i1dBLiK2F...
2018-01-17 03:42:05	80	adistributedmean.net	POST /images/KLP0eHHf/ajp0jDLbrkinR1D00f...
2018-01-17 03:42:17	80	adistributedmean.net	POST /images/F_2FgDSTPvBY/D86k7_2BC0y/J...
2018-01-17 03:42:19	80	adistributedmean.net	POST /images/X9B_2Bwj0FjdHqSE_2F1Fq/KY_...
2018-01-17 03:44:48	80	fyibc.com	GET /images/oiEMYfI1K6I1RjLxGfgpu/V1Y0dl...
2018-01-17 03:44:49	80	fyibc.com	GET /vfv.bin HTTP/1.1
2018-01-17 03:44:49	80	fyibc.com	GET /nori3.bin HTTP/1.1
2018-01-17 03:44:49	80	fyibc.com	GET /nori6.bin HTTP/1.1
2018-01-17 03:44:58	53	8.8.4.4	Standard query 0x9ec4 A dtybgsb.com
2018-01-17 03:44:59	51451	10.1.17.101	Standard query response 0x9ec4 A 203.48
2018-01-17 03:44:59	80	zepter.com	POST /5lpomdt9j/index.php HTTP/1.1 (app...
2018-01-17 03:45:09	53	8.8.8.8	Standard query 0x4c28 A dtybgsb.com
2018-01-17 03:45:09	51452	10.1.17.101	Standard query response 0x4c28 A 151.20
2018-01-17 03:45:09	80	zepter.com	POST /5lpomdt9j/index.php HTTP/1.1 (app...
2018-01-17 03:45:20	53	8.8.4.4	Standard query 0xb2c4 A dtybgsb.com
2018-01-17 03:45:20	51454	10.1.17.101	Standard query response 0xb2c4 A 22.136
2018-01-17 03:45:20	80	carfax.com	POST / HTTP/1.1 (application/x-www-form...
2018-01-17 03:45:22	80	carfax.com	POST / HTTP/1.1 (application/x-www-form...
2018-01-17 03:45:22	53	8.8.8.8	Standard query 0xad34 A dtybgsb.com
2018-01-17 03:45:23	51455	10.1.17.101	Standard query response 0xad34 A 85.12

Shown above: Traffic from the 1st infection filtered in Wireshark.

Since I've covered Nymaim before, I'm far more interested in the second infection where I couldn't identify the follow-up malware.

### The second infection

The second infection follows the same patterns as the first. However, this time the follow-up malware is different. I saw encrypted traffic with no associated DNS requests or domains. Two of the IP addresses had interesting certificate data as shown in the images below.

Filter: `http.request or ssl.handshake.type == 1` Expression... Clear Apply Save

Date/Time	Src	port	Host	port	Info
2018-01-17 17:04:00			fortrunernaskdneazxd.com		GET /NA/sof.php?utma=kur HTTP/1.1
2018-01-17 17:04:06	84.54.187.24	80	fortrunernaskdneazxd.com		GET /NA/kur.pfx HTTP/1.1
2018-01-17 17:04:11	84.54.187.24	80	fortrunernaskdneazxd.com		GET /s.php?id=kur HTTP/1.1
2018-01-17 17:07:40	213.6.121.106	80	bithedistributedlicense.net		POST /images/l8jbA1rj/VEcIQ4EhBV8F1oehMM:
2018-01-17 17:07:40	213.6.121.106	80	bithedistributedlicense.net		POST /images/EimMh_2F2kF/sI6GA7X99haLkF/:
2018-01-17 17:07:40	213.6.121.106	80	bithedistributedlicense.net		POST /images/cK5yLiTXxhUYUIHVYQ/AftQi0C:
2018-01-17 17:10:21	213.6.121.106	80	bithedistributedlicense.net		POST /images/vYWoUnzrZi/Ik9Q_2FUgBbwIR2S:
2018-01-17 17:10:21	85.105.167.110	80	bithedistributedlicense.net		GET /images/KJllp_2FhQ20cM2LL_2BAa/wAGd:
2018-01-17 17:10:32	85.105.167.110	80	bithedistributedlicense.net		POST /images/v45Lmt8RLQN0Ec4C/FazUkoy64u:
2018-01-17 17:10:44	85.105.167.110	80	bithedistributedlicense.net		POST /images/Pj1NDBpQ2Dcywdfiuua/Qtul2j9:
2018-01-17 17:12:20	85.105.167.110	80	bithedistributedlicense.net		POST /images/nvp8r03Mioxm5gPswCpjh/QS4p7zH:
2018-01-17 17:12:21	184.168.187.1	80	fyicreative.ca		GET /dih.bin HTTP/1.1
2018-01-17 17:12:21	184.168.187.1	80	fyicreative.ca		GET /nori3.bin HTTP/1.1
2018-01-17 17:12:21	184.168.187.1	80	fyicreative.ca		GET /nori6.bin HTTP/1.1
2018-01-17 17:12:32	85.105.167.110	80	bithedistributedlicense.net		POST /images/uTbL0GBM1Bq/IdhJLyf9HSVeQa/:
2018-01-17 17:12:39	69.90.132.196	443			Client Hello
2018-01-17 17:12:41	69.90.132.196	443			Client Hello
2018-01-17 17:12:45	69.90.132.196	443			Client Hello
2018-01-17 17:12:51	69.90.132.196	443			Client Hello
2018-01-17 17:14:20	90.180.1.23	80	bithedistributedlicense.net		GET /images/FE7q_2Bi/2c_2F34SNeHQ8NsaJ7h:
2018-01-17 17:15:44	85.105.167.110	80	bithedistributedlicense.net		POST /images/497hDhXq0ePLZmEARd9/SJcKXm6:
2018-01-17 17:16:20	85.105.167.110	80	bithedistributedlicense.net		GET /images/m9qs4fkQJbCEk4yPQW7Z_2/BMo9L:
2018-01-17 17:16:31	85.105.167.110	80	bithedistributedlicense.net		POST /images/zpugKRxX62356Y/dF1pAvL50mgG:
2018-01-17 17:16:50	41.193.159.41	443			Client Hello
2018-01-17 17:20:25	41.193.159.41	443			Client Hello
2018-01-17 17:20:32	41.193.159.41	443			Client Hello

Shown above: Traffic from the 2nd infection filtered in Wireshark.

Date/Time	Src	port	Dst	port	Info
2018-01-17 17:12:39	10.1.17.102	49198	69.90.132.196	443	49198->https [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2018-01-17 17:12:39	69.90.132.196	443	10.1.17.102	49198	https->49198 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
2018-01-17 17:12:39	10.1.17.102	49198	69.90.132.196	443	49198->https [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-01-17 17:12:39	10.1.17.102	49198	69.90.132.196	443	Client Hello
2018-01-17 17:12:39	69.90.132.196	443	10.1.17.102	49198	https->49198 [ACK] Seq=1 Ack=134 Win=15744 Len=0
2018-01-17 17:12:39	69.90.132.196	443	10.1.17.102	49198	Server Hello, Certificate, Server Hello Done
2018-01-17 17:12:39	10.1.17.102	49198	69.90.132.196	443	49198->https [ACK] Seq=134 Ack=1096 Win=64512 Len=0
2018-01-17 17:12:39	10.1.17.102	49198	69.90.132.196	443	Client Key Exchange. Change Cipher Spec. Encr

```

    Signature (sha256withRSAEncryption)
    issuer: rdnSequence (0)
      rdnSequence: 5 items (id-at-commonName=parore-gtistio.erioustabon.aarp,id-at-organizatio
        RDNSSequence item: 1 item (id-at-countryName=SG)
        RDNSSequence item: 1 item (id-at-localityName=Singapore)
        RDNSSequence item: 1 item (id-at-organizationName=Armasn Ultd.)
        RDNSSequence item: 1 item (id-at-organizationalUnitName=aseg2tsnt Areramnad)
        RDNSSequence item: 1 item (id-at-commonName=parore-gtistio.erioustabon.aarp)
    validity
    subject: rdnSequence (0)
  
```

Shown above: One example of certificate data from the encrypted post-infection traffic.

Date/Time	Src	port	Dst	port	Info
2018-01-17 17:16:50	10.1.17.102	49222	41.193.159.41	443	49222-https [SYN] Seq=0 Win=8192 Len=0 MSS=14
2018-01-17 17:16:50	41.193.159.41	443	10.1.17.102	49222	https-49222 [SYN, ACK] Seq=0 Ack=1 Win=40960
2018-01-17 17:16:50	10.1.17.102	49222	41.193.159.41	443	49222-https [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-01-17 17:16:50	10.1.17.102	49222	41.193.159.41	443	Client Hello
2018-01-17 17:16:50	41.193.159.41	443	10.1.17.102	49222	https-49222 [ACK] Seq=1 Ack=134 Win=40827 Len=0
2018-01-17 17:16:51	41.193.159.41	443	10.1.17.102	49222	Server Hello, Certificate, Server Hello Done
2018-01-17 17:16:51	10.1.17.102	49222	41.193.159.41	443	49222-https [ACK] Seq=134 Ack=1108 Win=64512
2018-01-17 17:16:51	10.1.17.102	49222	41.193.159.41	443	Client Key Exchange. Change Cipher Spec. Encr

```

    issuer: rdnSequence (0)
      rdnSequence: 6 items (id-at-commonName=sineixwhim.onthediantl.pet,id-at-organizationalUn
        ⊕ RDNSequence item: 1 item (id-at-countryName=CA)
        ⊕ RDNSequence item: 1 item (id-at-stateOrProvinceName=Sason Dwinc)
        ⊕ RDNSequence item: 1 item (id-at-localityName=Ottawa)
        ⊕ RDNSequence item: 1 item (id-at-organizationName=Stonvit Thide EURL)
        ⊕ RDNSequence item: 1 item (id-at-organizationalUnitName=uleye)
        ⊕ RDNSequence item: 1 item (id-at-commonName=sineixwhim.onthediantl.pet)
    validity
  
```

Shown above: Another example of certificate data from the encrypted post-infection traffic.

Based on the network traffic and post-infection artifacts, I could not identify the follow-up malware. The follow-up malware is a malicious DLL named **winmm.dll** that's loaded by a legitimate Windows system file named **presentationsettings.exe**. Both were found in a newly-created directory under the infected user's **AppData\Roaming** folder. See the indicators section below for details.

### Indicators

Artifacts from the 1st infection:

SHA256 hash: [febb37762a92bedad337d0489ac482e356e2787533d65a757c3375fb147ff0a8](#)

- File size: 55,248 bytes
- File name: **Request.doc**
- File description: Word document with malicious macro

SHA256 hash: [14284152d53c119ad04c986a2a115485ae480d8012603679bf28ec27e3869929](#)

- File size: 1,101,824 bytes
- File location: C:\Users\[username]\AppData\Roaming\52a8081a.exe
- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Adsnsdmo\CRPPport.exe
- Associated Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Value name: adprvmgr
- Value type: REG\_SZ
- Value data: C:\Users\[username]\AppData\Roaming\Microsoft\Adsnsdmo\CRPPport.exe
- File description: Gozi-ISFB (an Ursnif variant)

SHA256 hash: [d254e82bdbfd16aa9f0037e2c536c3b9ddddd6ec559d26a5af005d3a1f8199d59](#)

- File size: 580,864 bytes
- File location: C:\Users\[username]\AppData\Local\molarity-24\molarity-12.exe

- Associated Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Value name: molarity-96
- Value type: REG\_SZ
- Value data: C:\Users\[username]\AppData\Local\molarity-24\molarity-12.exe -s0
- File description: Probable Nymaim Trojan

SHA256 hash: [f1c9544e8f1de92f60f13e29403fc459811b93a7a316d957cb30c1b4a61ba61d](#)

- File size: 656,896 bytes
- File location: C:\ProgramData\wedge-46\wedge-6.exe
- Associated Registry key: HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
- Value name: shell
- Value type: REG\_SZ
- Value data: C:\ProgramData\wedge-46\wedge-6.exe -46,explorer.exe
- File description: Probable Nymaim Trojan

SHA256 hash: [6e5faf4c3eb47a5218f173564fc1e5a8afc65a8126ff7f602e8dbfe98a2ba695](#)

- File size: 651,776 bytes
- File location: C:\Users\[username]\AppData\Roaming\aliasing-40\aliasing-2.exe
- File description: Probable Nymaim Trojan

Artifacts from the 2nd infection:

SHA256 hash: [044e86936bfc30cd0c07186b6e270650f896f6a42e9b8015abc184d161880090](#)

- File size: 55,012 bytes
- File name: ***NBS\_Request.doc***
- File description: Word document with malicious macro

SHA256 hash: [f8bdb65d54ccab04a506e84f14bdbbeef15f6266a7bd6e4e7dfde69de424dd10a](#)

- File size: 1,010,688 bytes
- File location: C:\Users\[username]\AppData\Roaming\6d9be056.exe
- File location: C:\Users\[username]\AppData\Roaming\Microsoft\Bitsxapi\efsuvoas.exe
- Associated Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Value name: dmusdBth
- Value type: REG\_SZ
- Value data: C:\Users\[username]\AppData\Roaming\Microsoft\Bitsxapi\efsuvoas.exe
- File description: Gozi-ISFB (an Ursnif variant)

SHA256 hash: [208b94fd66a6ce266c3195f87029a41a0622fff47f2a5112552cb087adbb1258](#) (not malware)

- File size: 176,640 bytes
- File location: C:\Users\[username]\AppData\Roaming\XPIALj1\PresentationSettings.exe
- Associated Registry key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- Value name: Ehlho
- Value type: REG\_SZ
- Value data: "C:\Users\[username]\AppData\Roaming\XPiALj1\PresentationSettings.exe"
- Start menu shortcut: C:\Users\[username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Ehlho
- File description: Legitimate system file that loads any DLL named **winmm.dll** in the same directory.

SHA256 hash: [018084df00799387be61c5f849af8fce093aab8f73420a2ece7b47d0f45fa07e](#)

- File size: 176,640 bytes
- File location: C:\Users\[username]\AppData\Roaming\XPiALj1\WINMM.dll
- File description: Malicious component called by PresentationSettings.exe
- File description: Malware DLL loaded by legitimate system file **PresentationSettings.exe** in the same directory

1st run infection traffic:

- 188.25.175.38 port 80 - **ijqdjqnwiduqujqieuzxc.com** - GET /NU/sof.php?utma=baw
- 188.25.175.38 port 80 - **ijqdjqnwiduqujqieuzxc.com** - GET /NU/baw.pfx
- 188.25.175.38 port 80 - **ijqdjqnwiduqujqieuzxc.com** - GET /s.php?id=baw
- 109.166.237.170 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 109.166.237.170 port 80 - **adistributedmean.net** - POST /images/[long string].bmp
- 212.98.131.181 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 212.98.131.181 port 80 - **adistributedmean.net** - POST /images/[long string].bmp
- 86.120.77.221 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 86.120.77.221 port 80 - **adistributedmean.net** - GET /images/[long string].jpeg
- 86.120.77.221 port 80 - **adistributedmean.net** - POST /images/[long string].bmp
- 80.80.165.93 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 80.80.165.93 port 80 - **adistributedmean.net** - POST /images/[long string].bmp
- 186.73.245.226 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 188.237.190.24 port 80 - **adistributedmean.net** - GET /images/[long string].gif
- 184.168.187.1 port 80 - **fyibc.com** - GET /vvv.bin
- 184.168.187.1 port 80 - **fyibc.com** - GET /nori3.bin
- 184.168.187.1 port 80 - **fyibc.com** - GET /nori6.bin
- DNS queries (using Google DNS) for **dybgsb.com**
- 86.120.168.154 port 80 - **zepter.com** - POST /5lpomdt9j/index.php
- 203.91.116.53 port 80 - **zepter.com** - POST /5lpomdt9j/index.php
- 155.133.93.30 port 80 - **zepter.com** - POST /5lpomdt9j/index.php
- 85.105.167.110 port 80 - **carfax.com** - POST /
- 85.105.167.110 port 80 - **zepter.com** - POST /
- NOTE: **carfax.com** and **zepter.com** are legitimate domains and not compromised. They just resolve to bad IP addresses for **dybgsb.com** due to the nature of this Nymaim infection.

2nd run infection traffic:

- 84.54.187.24 port 80 - **fortrunernaskdneazxd.com** - GET /NA/sof.php?utma=kur
- 84.54.187.24 port 80 - **fortrunernaskdneazxd.com** - GET /NA/kur.pfx
- 84.54.187.24 port 80 - **fortrunernaskdneazxd.com** - GET /s.php?id=kur
- 213.6.121.106 port 80 - **bithedistributedlicense.net** - POST /images/[long string].bmp
- 85.105.167.110 port 80 - **bithedistributedlicense.net** - POST /images/[long string].bmp
- 85.105.167.110 port 80 - **bithedistributedlicense.net** - GET /images/[long string].gif
- 90.180.1.23 port 80 - **bithedistributedlicense.net** - GET /images/[long string].gif
- 184.168.187.1 port 80 - **fyicreative.ca** - GET /dih.bin
- 184.168.187.1 port 80 - **fyicreative.ca** - GET /nori3.bin
- 184.168.187.1 port 80 - **fyicreative.ca** - GET /nori6.bin
- 41.193.159.41 port 443 - Encrypted traffic both with and without certificate data
- 69.90.132.196 port 443 - Encrypted traffic both with certificate data
- 69.75.114.66 port 443 - Encrypted traffic (no certificate data)
- 74.50.133.9 port 443 - Encrypted traffic (no certificate data)
- 41.193.159.41 port 444 - attempted TCP connections, but no response from the server
- 95.150.74.40 port 443 - attempted TCP connections, but no response from the server
- 179.108.87.11 port 443 - attempted TCP connections, but no response from the server
- 190.208.42.36 port 443 - attempted TCP connections, but no response from the server

Of note, during the first infection, I rebooted the infected Windows host 3 or 4 times, which might account for multiple copies of what I assume are Nymaim. If you review the pcaps, the reboots are indicated any place you see an HTTP request to **www.msftncsi.com**.

### ***Malicious domains***

Indicators are not a block list. If you feel the need to block web traffic based on this diary, I suggest the following domains:

- ijqjdjqnwiduqujqieuzxc.com
- adistributedmean.net
- fyibc.com
- fortrunernaskdneazxd.com
- bithedistributedlicense.net
- fyicreative.ca

### ***Final words***

Pcaps and malware for today's diary can be found [here](#).

Good spam filtering, proper Windows administration, and best security practices will ensure most people never see this malware. However, criminals are constantly tweaking their methods in an attempt to slip past our defenses. It pays to be aware of current malware indicators, so we're prepared if any ever make it into our network.

---

Brad Duncan

brad [at] malware-traffic-analysis.net

---

Source: <https://isc.sans.edu/forums/diary/Reviewing+the+spam+filters+Malspam+pushing+GoziISFB/23245>