zzzz.exe

Is DLL ✗ | Packer ✓ | Anti Debug ✗ | Anti VM ✗ | Signed ✗ | XOR ✗

MalFamily: Formbook **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	610.50 KB (625152 bytes)
Compile time:	2017-11-15 13:56:27
MD5:	877c0e368b45d48370691cb0f3cacac9
SHA1:	af9de51b2917a5eae59fc1d98fc969b9392be37a
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2017-11-15 19:27:03

URL(s) file hosting

http://aboukangaz.com/ece/zzzz.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2017-11-15 16:37:58	20/67	

Import library

mscoree.dll

11 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: ET TROJAN Formbook 0.3 Checkin

- signature: Traffico Anomalo: Traffico verso host malevolo, GET HTTP Content "db" (Soc-Rule)

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\khabargyenose.exe

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\yaryarannolotdedf
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\yaryarannolotdedf.txt | cmd
- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\kalsheshyanDepicheloki
- data: cmd /c type C:\Users\Seven01\AppData\Local\Temp\kalsheshyanDepicheloki.txt | cmd
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\khabargyenose.exe
- file: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\khabargyenose.exe

Executed a process and injected code into it, probably while unpacking

- Injection: khabargyenose.exe(2864) -> khabargyenose.exe(2104)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 8.00, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x00097c00, virtual_size: 0x00097bf4

Performs some HTTP requests

- url: http://www.primeit.world/hx160/?id=godrTjAtsUSRSJc+ueF6I9/U2rPZ1p1/Kt3vG9QgAnid2uBAP72MoJcrjZvDWdZL9Ps9ALBB&M694u=elX0MnF0D8F
- url: http://www.belezaformen.com/hx160/?id=e2bmhQojAVKO+4bErZz1cSqI8d7AGQdMvrAJBu1Z1IdBPeYYecxY9ai6TpFY36JXNLCu5H94&M694u=elX0MnF0D8F
- url: http://www.munkypizzrecords.company/hx160/?id=nxK2qaX/L98KhrZXNzQtrw3BtMOYPGL/KIoGCiDLdJRW0j1RDCZhBkdcbHI0yAcfnJZjhHh8&M694u=elX0MnF0D8F
- url: http://www.airbnbmn.com/hx160/?id=23az8uLnYOam1PNgEUZP0Q4Admy+4T+e0zOSMJ922ck1sjqOCQEITg2elEVJNHJSQLr9wbam&M694u=elX0MnF0D8F
- url: http://www.febradyz.info/hx160/?id=2636bvxg0ELWTGu+mQ4IiPLjDyA9rPsceT7lu//fL6LjpU3xvFAUFvV7p79TpUpePFp5Wpzv&M694u=elX0MnF0D8F
- url: http://www.tnttraveler.com/hx160/
- url: http://www.febradyz.info/hx160/
- url: http://www.tnttraveler.com/hx160/?id=VSAChz4Xz0FTjbMwpVUtQq7eekKvCKx5vTBSVsXO3+2eN0oXmvyC9w9iUkdeSC8aNz6Fpfwp&M694u=elX0MnF0D8F

HTTP traffic contains suspicious features which may be indicative of malware related traffic

- get_no_useragent: HTTP traffic contains a GET request with no user-agent header
- suspicious_request: http://www.primeit.world/hx160/?id=godrTjAtsUSRSJc+ueF6I9/U2rPZ1p1/Kt3vG9QgAnid2uBAP72MoJcrjZvDWdZL9Ps9ALBB&M694u=elX0MnF0D8F
- suspicious_request: http://www.belezaformen.com/hx160/?id=e2bmhQojAVKO+4bErZz1cSqI8d7AGQdMvrAJBu1Z1IdBPeYYecxY9ai6TpFY36JXNLCu5H94&M694u=elX0MnF0D8F
- suspicious_request: http://www.munkypizzrecords.company/hx160/?id=nxK2qaX/L98KhrZXNzQtrw3BtMOYPGL/KIoGCiDLdJRW0j1RDCZhBkdcbHI0yAcfnJZjhHh8&M694u=elX0MnF0D8F
- suspicious_request:

http://www.airbnbmn.com/hx160/?id=23az8uLnYOam1PNgEUZP0Q4Admy+4T+e0zOSMJ922ck1sjqOCQEITg2elEVJNHJSQLr9wbam&M694u=elX0MnF0D8F
 - suspicious_request: http://www.febradyz.info/hx160/?id=2636bvxg0ELWTGu+mQ4IiPLjDyA9rPsceT7lu//fL6LjpU3xvFAUFvV7p79TpUpePFp5Wpzv&M694u=elX0MnF0D8F
 - suspicious_request: http://www.tnttraveler.com/hx160/
 - suspicious_request: http://www.febradyz.info/hx160/
 - suspicious_request: http://www.tnttraveler.com/hx160/?id=VSAChz4Xz0FTjbMwpVUtQq7eekKvCKx5vTBSVsXO3+2eN0oXmvyC9w9iUkdeSC8aNz6Fpfwp&M694u=elX0MnF0D8F

Drops a binary and executes it

 - binary: C:\Users\Seven01\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\khabargyenose.exe

A process created a hidden window

 - Process: zzzz.exe -> "cmd"
 - Process: khabargyenose.exe -> "cmd"
 - Process: khabargyenose.exe -> "cmd"

Network activity detected but not expressed in API logs

Creates RWX memory

10 HTTP Request(s) detected

http://www.primeit.world/hx160/?id=godrTjAtsUSRSJc+ueF6I9/U2rPZ1p1/Kt3vG9QgAnid2uBAP72MoJcrjZvDWdZL9Ps9ALBB&M694u=elX0MnF0D8F

Hostname: www.primeit.world

IP Address: 81.169.145.86

Port: 80

Count: 1

http://www.belezaformen.com/hx160/?id=e2bmhQojAVKO+4bErZz1cSqI8d7AGQdMvrAJBu1Z1IdBPeYYecxY9ai6TpFY36JXNLCu5H94&M694u=elX0MnF0D8F

Hostname: www.belezaformen.com

IP Address: 104.31.88.56

Port: 80

Count: 1

http://www.munkypizzrecords.company/hx160/?id=nxK2qaX/L98KhrZXNzQtrw3BtMOYPGL/KIoGCiDLdJRW0j1RDCZhBkdcbHI0yAcfnJZjhHh8&M694u=elX0MnF0D8F

Hostname: www.munkypizzrecords.company

IP Address: 199.34.228.41

Port: 80

Count: 1

http://www.airbnbmn.com/hx160/?id=23az8uLnYOam1PNgEUZP0Q4Admy+4T+e0zOSMJ922ck1sjqOCQEITg2elEVJNHJSQLr9wbam&M694u=elX0MnF0D8F
Hostname: www.airbnbmn.com
IP Address: 97.46.1.85
Port: 80
Count: 1

http://www.febradyz.info/hx160/?id=2636bvxg0ELWTGu+mQ4liPLjDyA9rPsceT7lu//fL6LjpU3xvFAUFvV7p79TpUpePFp5Wpzv&M694u=elX0MnF0D8F
Hostname: www.febradyz.info
IP Address: 5.206.225.211
Port: 80
Count: 1

http://www.tnttraveler.com/hx160/
Hostname: www.tnttraveler.com
IP Address:
Port: 80
Count: 1

http://www.tnttraveler.com/hx160/
Hostname: www.tnttraveler.com
IP Address:
Port: 80
Count: 1

http://www.febradyz.info/hx160/
Hostname: www.febradyz.info
IP Address: 5.206.225.211
Port: 80
Count: 1

http://www.febradyz.info/hx160/
Hostname: www.febradyz.info
IP Address: 5.206.225.211
Port: 80
Count: 1

http://www.tnttraveler.com/hx160/?id=VSAChz4Xz0FTjbMwpVUtQq7eekKvCKx5vTBSVsXO3+2eN0oXmvyC9w9iUkdeSC8aNz6Fpfwp&M694u=elX0MnF0D8F
Hostname: www.tnttraveler.com
IP Address:
Port: 80
Count: 1