robots.exe

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

MalFamily: Razy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	303.50 KB (310784 bytes)
Compile time:	2018-05-10 23:30:57
MD5:	a381684bf1f5f47a0f68d8c40d8d3b50
SHA1:	51e5270911de7d16b506ba4177bca63b9f6c9594
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-12 17:30:07

URL(s) file hosting

http://hygoscooter.com/robots.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-11 12:03:03	29/66	

Import library

mscoree.dll

11 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: Traffico Anomalo ? Start Traffico)

- 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\cvnmor.exe

Installs itself for autorun at Windows startup

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

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

- Injection: cvnmor.exe(2816) -> cvnmor.exe(3064)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.99, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0004a800, virtual_size: 0x0004a694

Performs some HTTP requests

- url: http://gallerdo.info/hx183/?_ZOx46=sB1YjzgkckPRmK78F88IV2RIV8W/BDuNxBZ7LJDFEZ3yoEotkOlz4/sEmo+baxyOPo4SIHFJ&GzuD=WBjTZrPPs
- url: http://ctnzd.info/hx183/?_ZOx46=14jLC9XZYfDQsiapzAItf4J39uLdcK7tW/al14RweCTk0SXHUvS6a1JtvgWRPcFpv3CGkgzG&GzuD=WBjTZrPPs
- url: http://ctnzd.info/hx183/
- url: http://industrialriggers.net/hx183/?_ZOx46=5MRPrDbid7UVrJb5Ydp4h3Noh/BxZWJ4zjzgqd7qUPB9fgfDwikOhDy+OC9x0dnAkpjU1e9D&GzuD=WBjTZrPPs
- url: http://industrialriggers.net/hx183/
- url: http://carven-korea.com/hx183/?_ZOx46=qvHXpOJ8SiWWUut4TfKsiukzH/LsfdO41SgjUeRXkLz1Lb45VYbeBujGdDUJ0yWMkPRwekOR&GzuD=WBjTZrPPs
- url: http://carven-korea.com/hx183/
- url: http://dongganshanxi.com/hx183/?_ZOx46=/FPnsUJEKnT2OoI9UY6WjmN/jRcKXQkx/lZWkReFGOCR9ygdLEgOIy/T2ohkejJdu3xlr7c1&GzuD=WBjTZrPPs
- url: http://dongganshanxi.com/hx183/
- url: http://blockchainassetsforum.com/hx183/?_ZOx46=m5yoJihL04w4DJWXqQPGAouIhMmO5qOIxEbSvl57CgPQ4vNQu12HpQDd/XZezD1MA37XrTs7&GzuD=WBjTZrPPs
- url: http://blockchainassetsforum.com/hx183/

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://gallerdo.info/hx183/?_ZOx46=sB1YjzgkckPRmK78F88IV2RIV8W/BDuNxBZ7LJDFEZ3yoEotkOlz4/sEmo+baxyOPo4SIHFJ&GzuD=WBjTZrPPs
- suspicious_request: http://ctnzd.info/hx183/?_ZOx46=14jLC9XZYfDQsiapzAItf4J39uLdcK7tW/al14RweCTk0SXHUvS6a1JtvgWRPcFpv3CGkgzG&GzuD=WBjTZrPPs
- suspicious_request: http://ctnzd.info/hx183/
- suspicious_request: http://industrialriggers.net/hx183/?_ZOx46=5MRPrDbid7UVrJb5Ydp4h3Noh/BxZWJ4zjzgqd7qUPB9fgfDwikOhDy+OC9x0dnAkpjU1e9D&GzuD=WBjTZrPPs
- suspicious_request: http://industrialriggers.net/hx183/

- suspicious_request: http://carven-korea.com/hx183/?_ZOx46=qvHXpOJ8SiWWUut4TfKsiukzH/LsfdO41SgjUeRXkLz1Lb45VYbeBujGdDUJ0yWMkPRwekOR&GzuD=WBjTZrPPs
- suspicious_request: http://carven-korea.com/hx183/
- suspicious_request: http://dongganshanxi.com/hx183/?_ZOx46=/FPnsUJEKnT2OoI9UY6WjmN/jRcKXQkx/lZWkReFGOCR9ygdLEgOIy/T2ohkejJdu3xlr7c1&GzuD=WBjTZrPPs
- suspicious_request: http://dongganshanxi.com/hx183/
- suspicious_request: http://blockchainassetsforum.com/hx183/?_ZOx46=m5yoJihL04w4DJWXqQPGAouIhMmO5qOIxEbSvl57CgPQ4vNQu12HpQDd/XZezD1MA37XrTs7&GzuD=WBjTZrPPs
- suspicious_request: http://blockchainassetsforum.com/hx183/

Drops a binary and executes it

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

A process created a hidden window

- Process: robots.exe -> "cmd"
- Process: cvnmor.exe -> "cmd"

Network activity detected but not expressed in API logs

Creates RWX memory

16 HTTP Request(s) detected

http://gallerdo.info/hx183/?_ZOx46=sB1YjzgkckPRmK78F88IV2RIV8W/BDuNxBZ7LJDFEZ3yoEotkOlz4/sEmo+baxyOPo4SIHFJ&GzuD=WBjTZrPPs

Hostname: gallerdo.info

IP Address: 192.64.116.236

Port: 80

Count: 1

http://ctnzd.info/hx183/?_ZOx46=14jLC9XZYfDQsiapzAItf4J39uLdcK7tW/al14RweCTk0SXHUvS6a1JtvgWRPcFpv3CGkgzG&GzuD=WBjTZrPPs

Hostname: ctnzd.info

IP Address:

Port: 80

Count: 1

http://ctnzd.info/hx183/

Hostname: ctnzd.info

IP Address:

Port: 80

Count: 1

http://ctnzd.info/hx183/
Hostname: ctnzd.info
IP Address:
Port: 80
Count: 1

http://industrialriggers.net/hx183/?_ZOx46=5MRPrDbid7UVrJb5Ydp4h3Noh/BxZWJ4zjzgqd7qUPB9fgfDwikOhDy+OC9x0dnAkpjU1e9D&GzuD=WBjTZrPPs
Hostname: industrialriggers.net
IP Address: 205.178.189.131
Port: 80
Count: 1

http://industrialriggers.net/hx183/
Hostname: industrialriggers.net
IP Address: 205.178.189.131
Port: 80
Count: 1

http://industrialriggers.net/hx183/
Hostname: industrialriggers.net
IP Address: 205.178.189.131
Port: 80
Count: 1

http://carven-korea.com/hx183/?_ZOx46=qvHXpOJ8SiWWUut4TfKsiukzH/LsfdO41SgjUeRXkLz1Lb45VYbeBujGdDUJ0yWMkPRwekOR&GzuD=WBjTZrPPs
Hostname: carven-korea.com
IP Address: 112.175.31.180
Port: 80
Count: 1

http://carven-korea.com/hx183/
Hostname: carven-korea.com
IP Address: 112.175.31.180
Port: 80
Count: 1

http://carven-korea.com/hx183/
Hostname: carven-korea.com
IP Address: 112.175.31.180
Port: 80
Count: 1

http://dongganshanxi.com/hx183/?_ZOx46=/FPnsUJEKnT2OoI9UY6WjmN/jRcKXQkx/lZWkReFGOCR9ygdLEgOly/T2ohkejJdu3xlr7c1&GzuD=WBjTZrPPs
Hostname: dongganshanxi.com
IP Address:
Port: 80
Count: 1

http://dongganshanxi.com/hx183/
Hostname: dongganshanxi.com
IP Address:
Port: 80
Count: 1

http://dongganshanxi.com/hx183/
Hostname: dongganshanxi.com
IP Address:
Port: 80
Count: 1

http://blockchainassetsforum.com/hx183/?_ZOx46=m5yoJihL04w4DJWXqQPGAouIhMmO5qOIxEbSvl57CgPQ4vNQu12HpQDd/XZezD1MA37XrTs7&GzuD=WBjTZrPPs
Hostname: blockchainassetsforum.com
IP Address: 192.64.119.52
Port: 80
Count: 1

http://blockchainassetsforum.com/hx183/
Hostname: blockchainassetsforum.com
IP Address: 192.64.119.52
Port: 80
Count: 1

http://blockchainassetsforum.com/hx183/
Hostname: blockchainassetsforum.com
IP Address: 192.64.119.52
Port: 80
Count: 1