newimage.exe

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

MalScore: 100

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	301.50 KB (308736 bytes)
Compile time:	2018-05-29 16:22:57
MD5:	0375083a5f17035e28f9f227b3f0101a
SHA1:	41bb0a8d5bb4ef8f3b4b35659b13bfdce7c5e1f4
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-30 13:15:02

URL(s) file hosting

http://urganchsh28-m.uz//wp-content/newimage.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-30 05:04:07	19/66	

Import library

mscoree.dll

13 Behaviors detected by system signatures

Created network traffic indicative of malicious activity

- signature: Traffico Anomalo ? Start Traffico)

Attempts to repeatedly call a single API many times in order to delay analysis time

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 1447435 times

Queries information on disks, possibly for anti-virtualization

Deletes its original binary from disk

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

- Injection: newimage.exe(2492) -> newimage.exe(2696)

Anomalous .NET characteristics

- anomalous_version: Assembly version is set to 0

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: 0x0004a634

Performs some HTTP requests

- url: http://www.hemalipaterl.com/hx339/?EZA4Ip=9jFyNYSrDMNtqSEW/2TkfGJn6jimqhmWwTUUsAWCTca92+CooD+vfW5+km/oknhNV0WjTF4b&GzrXY=Azr8389
- url: http://www.uprolhodagua.com/hx339/?EZA4Ip=0qrSVDOFJibhi91kJiG2wNzJjx+pmEYezsObMlsdZE2hEsCKyXp9XBvMaTaLjvHeD6ByQeUP&GzrXY=Azr8389
- url: http://www.uprolhodagua.com/hx339/
- url: http://www.graciousmepaper.com/hx339/?EZA4Ip=Y0zJQ+FHbZCHFUVZDz55NwFf7oSbOYAK5lj4QEfr+8VLUeEK2nJhm1pTQI1lq4OuXm8nxmtR&GzrXY=Azr8389
- url: http://www.graciousmepaper.com/hx339/
- url: http://www.slidedokumen.com/hx339/?EZA4Ip=XrlD2heP0en6F+e7mkMMlna9Qy49z93rYktwywLLvCFka9tGPsaz+3W2gtFW4MfsWaFsAi2T&GzrXY=Azr8389
- url: http://www.slidedokumen.com/hx339/

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.hemalipaterl.com/hx339/?EZA4Ip=9jFyNYSrDMNtqSEW/2TkfGJn6jimqhmWwTUUsAWCTca92+CooD+vfW5+km/oknhNV0WjTF4b&GzrXY=Azr8389
- suspicious_request: http://www.uprolhodagua.com/hx339/?EZA4Ip=0qrSVDOFJibhi91kJiG2wNzJjx+pmEYezsObMlsdZE2hEsCKyXp9XBvMaTaLjvHeD6ByQeUP&GzrXY=Azr8389
- suspicious_request: http://www.uprolhodagua.com/hx339/
- suspicious_request: http://www.graciousmepaper.com/hx339/?EZA4Ip=Y0zJQ+FHbZCHFUVZDz55NwFf7oSbOYAK5lj4QEfr+8VLUeEK2nJhm1pTQI1lq4OuXm8nxmtR&GzrXY=Azr8389
- suspicious_request: http://www.graciousmepaper.com/hx339/
- suspicious_request: http://www.slidedokumen.com/hx339/?EZA4Ip=XrlD2heP0en6F+e7mkMMlna9Qy49z93rYktwywLLvCFka9tGPsaz+3W2gtFW4MfsWaFsAi2T&GzrXY=Azr8389
- suspicious_request: http://www.slidedokumen.com/hx339/

A process created a hidden window

- Process: cmstp.exe -> C:\Windows\SysWOW64\cmd.exe

Network activity detected but not expressed in API logs

A process attempted to delay the analysis task.

- Process: sppsvc.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

10 HTTP Request(s) detected

http://www.hemalipaterl.com/hx339/?EZA4Ip=9jFyNYSrDMNtqSEW/2TkfGJn6jimqhmWwTUUsAWCTca92+CooD+vfW5+km/oknhNV0WjTF4b&GzrXY=Azr8389
Hostname: www.hemalipaterl.com
IP Address: 199.188.206.251
Port: 80
Count: 1

http://www.uprolhodagua.com/hx339/?EZA4Ip=0qrSVDOFJibhi91kJiG2wNzJjx+pmEYezsObMlsdZE2hEsCKyXp9XBvMaTaLjvHeD6ByQeUP&GzrXY=Azr8389
Hostname: www.uprolhodagua.com
IP Address: 98.124.204.16
Port: 80
Count: 1

http://www.uprolhodagua.com/hx339/
Hostname: www.uprolhodagua.com
IP Address: 98.124.204.16
Port: 80
Count: 1

http://www.uprolhodagua.com/hx339/
Hostname: www.uprolhodagua.com
IP Address: 98.124.204.16
Port: 80
Count: 1

http://www.graciousmepaper.com/hx339/?EZA4Ip=Y0zJQ+FHbZCHFUVZDz55NwFf7oSbOYAK5lj4QEfr+8VLUeEK2nJhm1pTQI1Iq4OuXm8nxmtR&GzrXY=Azr8389
Hostname: www.graciousmepaper.com
IP Address: 203.170.80.250
Port: 80
Count: 1

http://www.graciousmepaper.com/hx339/
Hostname: www.graciousmepaper.com
IP Address: 203.170.80.250
Port: 80
Count: 1

http://www.graciousmepaper.com/hx339/
Hostname: www.graciousmepaper.com
IP Address: 203.170.80.250
Port: 80
Count: 1

http://www.slidedokumen.com/hx339/?EZA4Ip=XrlD2heP0en6F+e7mkMMlna9Qy49z93rYktwywLLvCFka9tGPsaz+3W2gtFW4MfsWaFsAi2T&GzrXY=Azr8389
Hostname: www.slidedokumen.com
IP Address:
Port: 80
Count: 1

http://www.slidedokumen.com/hx339/
Hostname: www.slidedokumen.com
IP Address:
Port: 80
Count: 1

http://www.slidedokumen.com/hx339/
Hostname: www.slidedokumen.com
IP Address:
Port: 80
Count: 1