maxninini.exe

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

MalFamily: Ispy **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	699.00 KB (715776 bytes)
Compile time:	2018-05-28 08:45:00
MD5:	687cad4427cf912d7207865942276fa4
SHA1:	c59b283a4216d7dd609a07373d867a0b681e57ce
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-05-29 15:39:05

URL(s) file hosting

https://emifile.com/intranets/maxni/maxninini.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-05-29 09:16:13	11/65	

Import library

mscoree.dll

12 Behaviors detected by system signatures

Collects information to fingerprint the system

Checks the CPU name from registry, possibly for anti-virtualization

Checks the version of Bios, possibly for anti-virtualization

Exhibits behavior characteristic of iSpy Keylogger

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

- Injection: maxninini.exe(2516) -> maxninini.exe(2668)

Looks up the external IP address

- domain: bot.whatismyipaddress.com

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.97, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0009da00, virtual_size: 0x0009d9d4

Performs some HTTP requests

- url: http://bot.whatismyipaddress.com/

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://bot.whatismyipaddress.com/

At least one IP Address, Domain, or File Name was found in a crypto call

- ioc: o.b7
- ioc: 5.8mO7

A process attempted to delay the analysis task.

- Process: maxninini.exe tried to sleep 430 seconds, actually delayed analysis time by 0 seconds
- Process: WmiPrvSE.exe tried to sleep 300 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

1 HTTP Request(s) detected

http://bot.whatismyipaddress.com/
Hostname: bot.whatismyipaddress.com
IP Address: 66.171.248.178
Port: 80
Count: 1