project.exe

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

MalFamily: Malicious **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	266.00 KB (272384 bytes)
Compile time:	2018-01-09 09:08:30
MD5:	7e0a5b6f8b6425ad20fd2f8d212cd4d0
SHA1:	673ec3f07c47c317404dfd69a80ac68f26213d6d
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-02-07 01:24:02

URL(s) file hosting

http://gg.usdipc.com/project.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-02-03 07:43:50	47/66	

Import library

mscoree.dll

21 Behaviors detected by system signatures

Collects information to fingerprint the system

Attempts to restart the guest VM

Installs itself for autorun at Windows startup

- key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\cns
- data: C:\Users\Seven01\AppData\Roaming\cns\cns.exe

Creates a hidden or system file

- file: C:\Users\Seven01\AppData\Roaming\cns\cns.exe
- file: C:\Users\Seven01\AppData\Roaming\ScreenShot

Retrieves Windows ProductID, probably to fingerprint the sandbox

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

Creates a copy of itself

- copy: C:\Users\Seven01\AppData\Roaming\cns\cns.exe

Attempts to disable System Restore

Attempts to disable UAC

Installs an hook procedure to monitor for mouse events

Deletes its original binary from disk

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Roaming\cns\cns.exe:Zone.Identifier

Sniffs keystrokes

- SetWindowsHookExW: Process: project.exe(2536)

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

- Injection: project.exe(2360) -> project.exe(2536)

A process attempted to delay the analysis task.

- Process: project.exe tried to sleep 315 seconds, actually delayed analysis time by 0 seconds

Drops a binary and executes it

- binary: C:\Users\Seven01\AppData\Local\Temp\C54.exe

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://checkip.dyndns.org/

Performs some HTTP requests

- url: http://checkip.dyndns.org/

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.98, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0003d000, virtual_size: 0x0003ce74

Looks up the external IP address

- domain: checkip.dyndns.org

Creates RWX memory

1 HTTP Request(s) detected

http://checkip.dyndns.org/
Hostname: checkip.dyndns.org
IP Address: 216.146.43.71
Port: 80
Count: 1