chuks.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:	687.00 KB (703488 bytes)
Compile time:	1993-02-19 13:17:11
MD5:	afbc621540758fe11333b3cd28b2d2f9
SHA1:	97f50c46925908de3cb5202604ce0e4cc6ee5dc3
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-08-01 20:12:09

URL(s) file hosting

http://eliasjadraque.eu/chuks.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-07-25 05:14:27	37/68	

Import library

mscoree.dll

9 Behaviors detected by system signatures

Attempts to remove evidence of file being downloaded from the Internet

- file: C:\Users\Seven01\AppData\Local\Temp\chuks.exe:Zone.Identifier

Installs itself for autorun at Windows startup

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

Creates a copy of itself

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

Anomalous binary characteristics

- anomaly: Timestamp on binary predates the release date of the OS version it requires by at least a year
- anomaly: Unprintable characters found in section name

Creates RWX memory

A process created a hidden window

- Process: chuks.exe -> cmd.exe
- Process: chuks.exe -> explorer.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/

Looks up the external IP address

- domain: checkip.dyndns.org

1 HTTP Request(s) detected

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