dngab.exe

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

MalFamily: Nanocore **MalScore: 100**

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File size:	284.50 KB (291328 bytes)
Compile time:	2018-06-09 23:07:11
MD5:	49d00de33e1560bf9c0c07afbd50fb34
SHA1:	8aacc0a59aec8f756de138b4b6bdfa2248c6b384
Import hash:	f34d5f2d4577ed6d9ceec516c1f5a744
Submitted:	2018-06-11 21:24:05

URL(s) file hosting

http://denmarkheating.net/chillers/ocxa/dngab.exe

Antivirus Report

Report date	Detection Ratio	Permalink
2018-06-11 06:46:11	24/67	

Import library

mscoree.dll

15 Behaviors detected by system signatures

Collects information to fingerprint the system

Creates a copy of itself

- copy: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe

Exhibits behavior characteristic of Nanocore RAT

Installs itself for autorun at Windows startup

- key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\UPNP Subsystem
- data: C:\Program Files (x86)\UPNP Subsystem\upnpss.exe
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job
- file: C:\Windows\Tasks\Adobe Flash Player Updater.job

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

- Spam: services.exe (484) called API GetSystemTimeAsFileTime 3908438 times

Attempts to remove evidence of file being downloaded from the Internet

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

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

- Injection: dngab.exe(2572) -> dngab.exe(2748)

The binary likely contains encrypted or compressed data.

- section: name: .text, entropy: 7.96, characteristics: IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ, raw_size: 0x0003ce00, virtual_size: 0x0003cde4

Performs some HTTP requests

- url: http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

A process created a hidden window

- Process: dngab.exe -> "schtasks.exe" /create /f /tn "UPNP Subsystem" /xml "C:\Users\Seven01\AppData\Local\Temp\tmp1EF.tmp"
- Process: dngab.exe -> "schtasks.exe" /create /f /tn "UPNP Subsystem Task" /xml "C:\Users\Seven01\AppData\Local\Temp\tmp15B6.tmp"

Reads data out of its own binary image

- self_read: process: dngab.exe, pid: 2748, offset: 0x00000000, length: 0x00001000
- self_read: process: dngab.exe, pid: 2748, offset: 0x00000080, length: 0x00000200

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

- ioc: v2.0.50727
- ioc: inetsim.org0

A process attempted to delay the analysis task.

- Process: dngab.exe tried to sleep 661 seconds, actually delayed analysis time by 0 seconds

Creates RWX memory

Attempts to connect to a dead IP:Port (4 unique times)

- IP: 192.168.56.1:3752
- IP: 192.168.56.1:443
- IP: 192.168.56.1:80
- IP: 185.208.211.11:3752 (Netherlands)

1 HTTP Request(s) detected

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
Hostname: www.download.windowsupdate.com
IP Address: 93.184.221.240
Port: 80
Count: 1

3 Host(s) detected

IP Address	Hostname	Reverse DNS
8.8.8.8		google-public-dns-a.google.com.
8.8.4.4		google-public-dns-b.google.com.
185.208.211.11		

2 Countr(y|ies) detected

Hosts	Country
2	United States
1	Netherlands