

OUTPUT:

Cuckoo:

The screenshot shows the Cuckoo dashboard interface. On the left, there's a sidebar with various icons. The main area is divided into two main sections: "Insights" and "Cuckoo".

Insights:

- Cuckoo Installation:**

Version	2.0.6
Available	2.0.7

A new version has been released! [Update now](#)
- Usage statistics:**

reported	34
completed	0
total	36
running	0
pending	0
- From the press:**
 - Cuckoo Sandbox 2.0.7** - June 19, 2019, "Stability and security"
 - IQY malspam campaign** - October 15, 2018, "Analysis of a malspam campaign leveraging .IQY (Excel Web Query) files containing DDE to achieve code execution."
 - Hooking VBScript execution in Cuckoo**

Cuckoo:

SUBMIT A FILE FOR ANALYSIS

Submit URLs/hashes

Drag your file into the left field or click the icon to select a file.

System info

FREE DISK SPACE: 44.5 GB / 164.7 GB

CPU LOAD: 7% (8 cores)

Information:

The screenshot shows the Cuckoo summary page for a file named "File 267.exe".

Summary:

File 267.exe

Download | Resubmit sample

Size	384.0KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	f3f48c57c38bff2ddd220f20569e1ee6
SHA1	0421127f1bcc91a6ab2a570a47f8159101b751a
SHA256	b1cad1540ecb290088252635f8e130022eed7486eb128c0ca3d676945d60a9fc
SHA512	Show SHA512
CRC32	A995CBB5
ssdeep	None
PDB Path	c:\users\user\documents\visual studio 2005\projects\emetim\release\Emetim.pdb
Yara	None matched

Signatures

Queries for the computername (1 event)					
Time & API	Arguments	Status	Return	Repeated	
GetComputerNameW Aug. 4, 2020, 1:36 p.m.	computer_name: CUCKOO1	1	1	0	
This executable has a PDB path (1 event)					
pdb_path	c:\users\user\documents\visual studio 2005\projects\emetim\release\Emetim.pdb				
Allocates read-write-execute memory (usually to unpack itself) (2 events)					
Time & API	Arguments	Status	Return	Repeated	
NtAllocateVirtualMemory Aug. 4, 2020, 1:36 p.m.	process_identifier: 2900 region_size: 65536 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x003c0000 allocation_type: 4096 (MEM_COMMIT) process_handle: 0xffffffff	1	0	0	
NtAllocateVirtualMemory Aug. 4, 2020, 1:36 p.m.	process_identifier: 1984 region_size: 65536 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x01c60000 allocation_type: 4096 (MEM_COMMIT) process_handle: 0xffffffff	1	0	0	

Moves the original executable to a new location (1 event)

Time & API	Arguments	Status	Return	Repeated				
MoveFileWithProgressW Aug. 4, 2020, 1:36 p.m.	newfilepath_r: C:\Windows\SysWOW64\engineafter.exe flags: 3 oldfilepath_r: C:\Users\cuckoo\AppData\Local\Temp\267.exe newfilepath: C:\Windows\SysWOW64\engineafter.exe oldfilepath: C:\Users\cuckoo\AppData\Local\Temp\267.exe	1	1	0				
Communicates with host for which no DNS query was performed (34 events)								
Installs itself for autorun at Windows startup (1 event)								
service_name	engineafter	service_path	C:\Users\cuckoo\AppData\Local\Temp\C:\Windows\SysWOW64\engineafter.exe"					
Attempts to remove evidence of file being downloaded from the Internet (1 event)								
Connects to IP addresses that are no longer responding to requests (legitimate services will remain up-and-running usually) (50 out of 78 events)								

Screenshots



Name	Response	Post-Analysis Lookup	IP Address	Status	Action
time.windows.com			113.52.135.33	Active	Moloch
1.56.168.192.in-addr.arpa	PTR → iandi-cuckoo.local		138.197.140.163	Active	Moloch