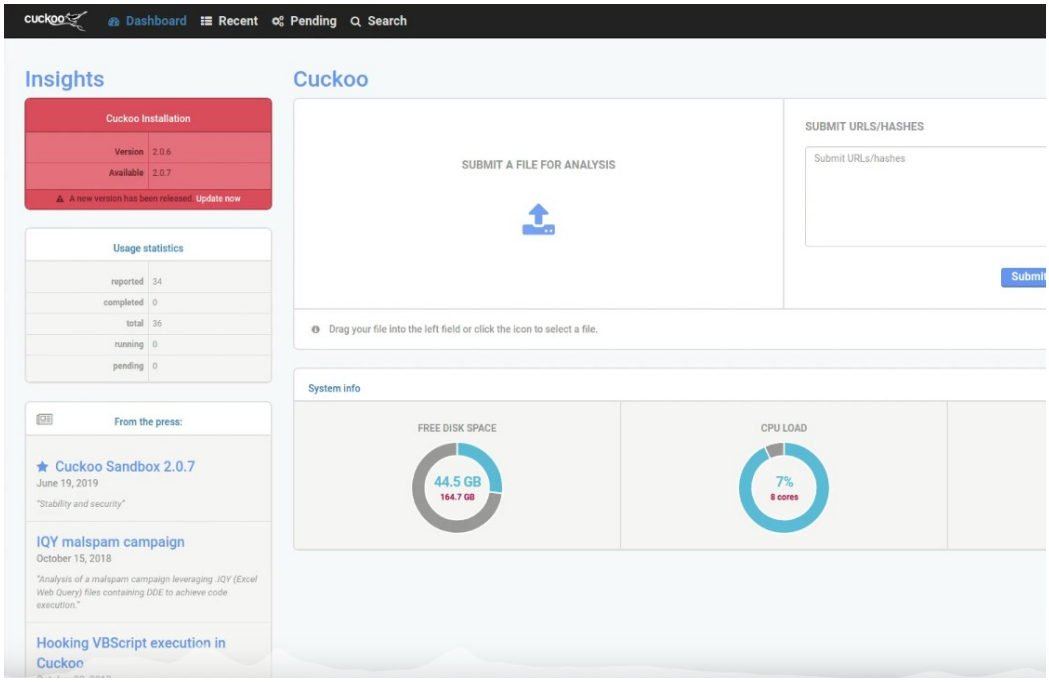
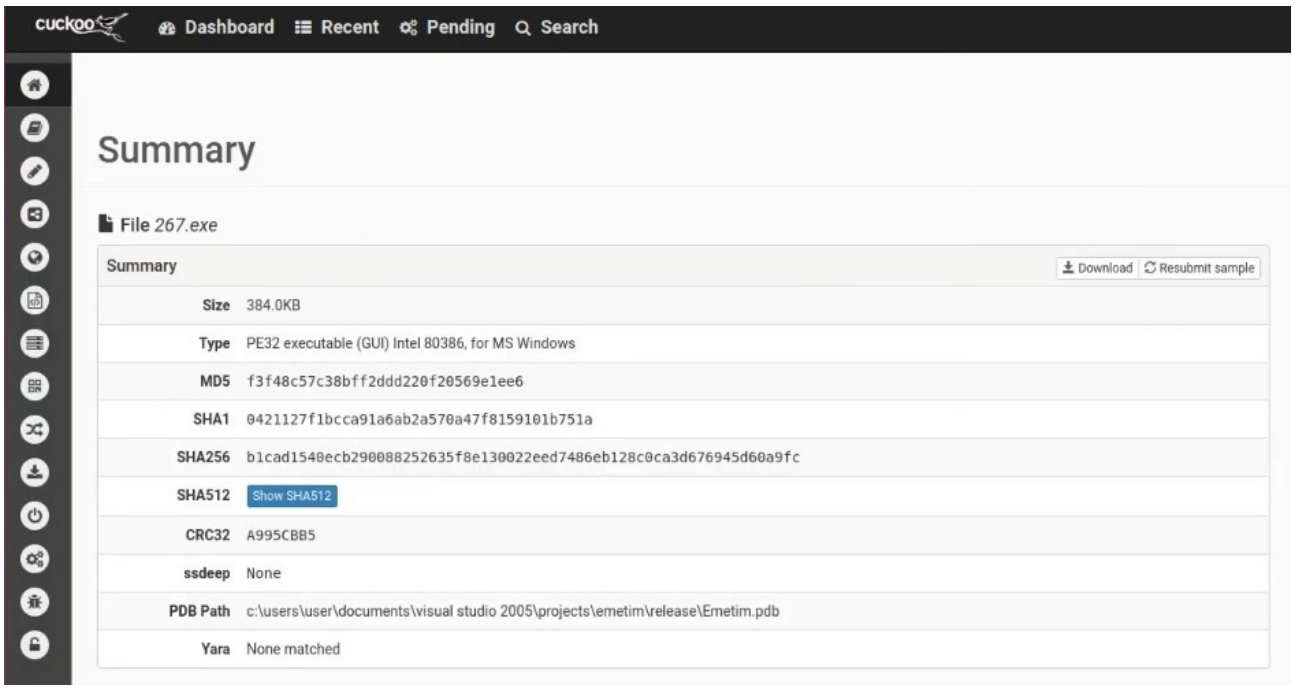
OUTPUT:

Cuckoo:



Information:



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)

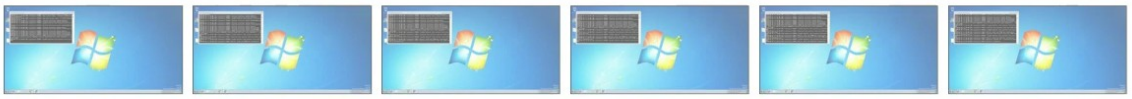
Installs itself for autorun at Windows startup (1 event)

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
time.windows.com		
1.56.168.192.in-addr.arpa	PTR → iandi-cuckoo.local	

IP Address	Status	Action
113.52.135.33	Active	Moloch
138.197.140.163	Active	Moloch