



بسم الله الرحمن الرحيم





All That for a Coinminer

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

۴	 مقدمه
۵	 دسترسی اولیه
۵	 اجرا
۶	 فرار از شناسایی
۶	 ماندگاری
۶	 دسترسی به اعتبارنامه
۸	 کشف
۹	 حرکت جانبی
۹	 فرماندهی و کنترل
۹	 تأثیر
۱۰	 IOCs
۱۱	 Detections





مقدمه

یک تهدیدگر با استفاده از RDP، رمز عبور یک Local Administrator را با روش Brute Force پیدا کرد و سپس با استفاده از Mimikatz توانست credential ها را دامپ کند. آن‌ها نه تنها LogonPasswords را دامپ کردند، بلکه تمام تیکت‌های Kerberos را نیز استخراج کردند. تهدیدگر از Advanced IP Scanner برای اسکن محیط قبل از اتصال RDP به سیستم‌های متعدد، از جمله یک کنترل‌کننده دامنه، استفاده کرد. پس از یک ساعت حرکت در محیط، آن‌ها XMRig را روی سیستم compromise شده قبل از خروج از سیستم، مستقر کردند. تهدیدگر در مجموع حدود ۲ ساعت در شبکه فعال بود.





دسترسی اولیه

تهدیدگر با استفاده از RDP از یک آدرس 92.118.13[.]103 که هیچ تلاش ورود قبلی نداشت، وارد شد. حساب کاربری روز قبل با استفاده از یک آدرس IP مبدأ 54.38.67[.]132 ایجاد شده بود، که در تلاش برای پیدا کردن رمز عبور یک مدیر محلی با روش Brute Force بود. تهدیدگر از یک ایستگاه کاری به نام winstation استفاده کرد. در طول نفوذ، تهدیدگران همچنین از 5.122.15[.]138 برای ورود به یکی از سیستم‌ها استفاده کردند.

اجرا

تهدیدگر فایل svshost.exe را به C:\naz\naz کپی کرده و سپس آن را اجرا کرد. این فایل اجرایی (PE)، فایل‌های "XMRig CPU mine.exe" و HideAll.bat را در C:\Windows\PolicyDefinitions ایجاد کرده و سپس هر دو را اجرا می‌کند.

```
commandLine      C:\Windows\system32\cmd.exe /c "\"C:\Windows\PolicyDefinitions\HideAll.bat\" \"
company          Microsoft Corporation
currentDirectory C:\naz\naz\
description       Windows Command Processor
hashes           SHA1=8DCA9749CD48D286950E7A9FA1088C937CBCCAD4, MD5=D7AB69FAD18D4A643D84A271DFC0DBDF, SHA
                 ASH=272245E2988E1E430500B852C4FB5E18
image            C:\Windows\System32\cmd.exe
integrityLevel   High
originalFileName Cmd.Exe
parentCommandLine \"C:\naz\naz\svshost.exe\"
```





فرار از شناسایی

فایل اجرایی که XMRig را نصب می‌کند (svshost.exe) همچنین دارای یک اسکریپت (HideAll.bat) درون خود است که در زمان اجرا فراخوانی می‌شود. این محتویات آن batch file است. این اسکریپت در مسیر C:\Windows\PolicyDefinitions\کپی و اجرا می‌شود که باعث می‌شود فایل‌های مشخص شده مخفی شوند.

ماندگاری

قبل از اینکه تهدیدگر ارتباط را قطع کند، رمز عبور کاربر را تغییر داد.

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

دسترسی به اعتبارنامه

از Mimikatz برای دامپ کردن اعتبارنامه‌ها از حافظه و همچنین استخراج تیکت‌های Kerberos با استفاده از دستور زیر استفاده شد:

```
mimikatz.exe", "log" "privilege::debug" "sekurlsa::logonpasswords" "sekurlsa::tickets /export" "exit"
```

```
commandLine  "C:\Users\gentilkiwi\Desktop\mimikatz_trunk\x64\mimikatz.exe" "log" "privilege::debug" "sekurlsa::logonpasswords" "sekurlsa::tickets /export" "exit"
company      gentilkiwi (Benjamin DELPY)
currentDirectory  C:\Users\gentilkiwi\Desktop\mimikatz_trunk\x64\
description   mimikatz for Windows
fileVersion   2.2.0.0
hashes        SHA1=E8DA948F182FFB7EE87DBF150BCE569BCE648B8D, MD5=62057628295220AB08CEAA5C7A1F2592, SHA256=5EA61A39FFD3F7B295A50BB84F1D7DFF63BF7B72E0C072EA15F0AC8E434012F4, IMPH
              ASH=7C9E07271759937A59A888B722B4DCD8
image         C:\Users\gentilkiwi\Desktop\mimikatz_trunk\x64\mimikatz.exe
integrityLevel  High
logonGuid      [REDACTED]
logonId        [REDACTED]
originalFileName  mimikatz.exe
parentCommandLine "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c 'C:\Windows\System32\cmd.exe /c C:\Users\gentilkiwi\Desktop\mimikatz_trunk\x64\launch.vbs'"
```





تهدیدگران از یک اسکریپت vbs به نام launch برای اجرای mimikatz استفاده کردند. این محتوای فایل launch.vbs است.

```
set shell=CreateObject("Shell.Application")
```

```
shell.ShellExecute "mimikatz.exe", ""log"" "privilege::debug"" "sekurlsa::logonpasswords""  
"sekurlsa::tickets /export"" "exit""", "", "runas", 0
```

```
set shell=nothing
```

از آنجایی که پارامتر log استفاده شد، خروجی در فایل mimikatz.log ذخیره شد.

mimikatz.log - Notepad

File Edit Format View Help

Using 'mimikatz.log' for logfile : OK

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

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

تیکت‌های Kerberos به دلیل استفاده تهدیدگر از `sekurlsa::tickets /export` روی دیسک ذخیره شدند.

```
image      C:\Users\...\Desktop\mimikatz_trunk\x64\mimikatz.exe  
processGuid {008cde44-0208-6004-4386-000000001100}  
processId  9848  
targetFilename C:\Users\...\Desktop\mimikatz_trunk\x64\[...]  
@krbtgt-... .kirbi
```





کشف

از Advanced IP Scanner برای اسکن محیط استفاده شد.

```
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=E9C693271FDCE1DD3B9C186214335507312161A3, MD5=0695E43202C3752967C92E04  
                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 چندین بار باز شد. احتمالاً این کار به منظور مشاهده کاربران وارد شده و/یا فرآیندها استفاده شده است.

```
commandLine    "\"C:\\Windows\\system32\\taskmgr.exe\" /4"  
company        Microsoft Corporation  
currentDirectory C:\\Windows\\system32\\  
description     Task Manager  
[REDACTED]  
hashes          SHA1=5A16BD59C698B992C73BD6064C1B198005D52  
                ASH=6B6920B078F3E37056561018E7E726DB  
image           C:\\Windows\\System32\\Taskmgr.exe  
integrityLevel  High  
[REDACTED]  
originalFileName Taskmgr.exe  
parentCommandLine C:\\Windows\\Explorer.EXE
```

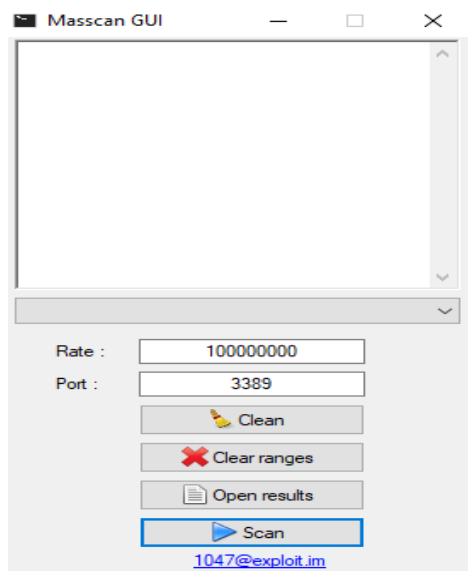




از Net Accounts برای بررسی User Policy ها استفاده شد.

`net accounts`

ابزارهای masscan و رابط کاربری گرافیکی آن رها شدند اما اجرا نشدند.



حرکت جانبی

برای حرکت جانبی به ماشین‌های متعدد در محیط که شامل کنترل‌کننده‌های دامنه، ماشین‌های پشتیبان و غیره می‌شد، از RDP استفاده شد.

فرماندهی و کنترل

برای دسترسی به محیط و همچنین حرکت درون محیط از RDP استفاده شد.

تأثیر

XMRig روی سیستم در حال اجرا بود و از مقداری CPU استفاده می‌کرد، اما نه به اندازه‌ای که مشکلی ایجاد کند. ما معمولاً نقاط پایانی ماینینگ را مسدود می‌کنیم، که ممکن است تأثیر این نفوذ را کاهش داده باشد. XMRig تلاش‌های اتصالی به 104.140.201[.]42 و 104.142.244[.]186 انجام داد.





تهدیدگران به مدت ۷۳۸ روز از کیف پول مونرو مرتبط استفاده می کنند و در مجموع حدود ۵,۱۵۹ دلار به دست آورده اند.

83baxCJTxdH8a5RY41u67WEh3n2CKeJP2cZb4z4tUWk383kipGRwTcFLtyDqfFtnBF3T4ostVt6P2VD4UzikB3N8CH6iB

0.13039036

XMR Pending

33.09584834

XMR Paid

Pay 0.13039036 XMR Now (for 0.001 XMR fee)

0.4000

Set Threshold

Close Payment History

Payment Sent	Amount (XMR)	Transaction
3 Days Ago	0.39954046	4bdea7963779872e813e241ech6aa53ed7dfcc4fd65d7cdd00a6b4d864237a
13 Days Ago	0.40112066	7af9e5043bc7ed61293bec0d548fd182c10a0392a12d9c4d832196939afec0cdf
24 Days Ago	0.103568	2defba90f006fd628801bed2009c2083eda29b1db97c2118054551ac6427aa15
26 Days Ago	0.40085663	c02e417912b9ebdc53c18d09b289c70ed6af0d8e26dfd99812f38190eaebed23
35 Days Ago	0.40029956	405e9df1e4b8758e751b6f7ef65b2e5ad1218b35fc2adb3955235ea7d72de58
44 Days Ago	0.40056559	667db5386bf7e7c0078c35b2f2096cfc18d1fb87582d2673c3875b59c1dbd6
52 Days Ago	3.37036429	6178be5655e20c3af2ae65b6552dfbcefb94cf21e17ec287e5b6f870ba6839fb

آیا مأموریت تهدیدگران استخراج مونرو بود؟ یا این یک مأموریت شناسایی بود؟ احتمالاً هر دو؟

IOCs

MISP <https://misppriv.circl.lu/events/view/81975> & OTX

<https://otx.alienvault.com/pulse/60062031b621e8e94a93ff36>

Network

۹۲.۱۱۸.۱۳.۱۰۳

۵۴.۳۸.۶۷.۱۳۲

۵.۱۲۲.۱۵.۱۳۸

۱۰۴.۱۴۰.۲۰۱.۴۲

۱۰۴.۱۴۲.۲۴۴.۱۸۶

File

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

Detections

Network

[۱:۲۰۲۴۷۹۲:۴]ET POLICY Cryptocurrency Miner Checkin

[۱:۲۸۲۶۹۳۰:۳]ETPRO POLICY XMR CoinMiner Usage

[۱:۲۸۴۱۰۷۹:۱]ETPRO TROJAN CoinMiner Known Malicious Stratum Authline (2020-02-18 2<





Sigma

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_mimikatz_command_line.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_alert_mimikatz_keywords.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_attrib_hiding_files.yml

Custom created Sigma rule

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

Yara

*/

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 occurred in hwloc %s inside process '%s', while" fullword ascii

\$s2 = "__kernel void find_shares(__global const uint64_t* hashes,uint64_t target,uint32_t start_nonce,__global uint32_t* shares)" fullword ascii

\$s3 = "ISystem.Resources.ResourceReader, mscorlib, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.R" ascii

\$s4 = "svshost.exe" fullword wide

\$s5 = "Could not read dumped cpuid file %s, ignoring cpuidump." fullword ascii

\$s6 = "%PROGRAMFILES%\\NVIDIA Corporation\\NVSMI\\nvml.dll" fullword ascii

\$s7 = "void blake2b_512_process_single_block(ulong *h,const ulong* m,uint blockTemplateSize)" fullword ascii

\$s8 = "* the input XML was generated by hwloc %s inside process '%s'." fullword ascii

\$s9 = "blake2b_512_process_single_block(hash,m,blockTemplateSize);" fullword ascii

\$s10 = "F:\\Apps\\cSharp\\myMinerup\\myM\\myM\\obj\\Debug\\svshost.pdb" fullword ascii

\$s11 = "|attrib +h svshost.exe" fullword ascii

\$s12 = "Found non-x86 dumped cpuid summary in %s: %s" fullword ascii

\$s13 = "GetCurrentProcessorNumberExProc || (GetCurrentProcessorNumberProc && nr_processor_groups == 1)" fullword ascii

\$s14 = "__kernel void blake2b_initial_hash(__global void *out,__global const void* blockTemplate,uint blockTemplateSize,uint start_nonce" ascii

\$s15 = "* hwloc %s received invalid information from the operating system." fullword ascii





```
$s16 = "__local exec_t* execution_plan=__local  
exec_t*)(execution_plan_buf+(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER  
_HASH*si" ascii
```

```
$s17 = "__kernel void execute_vm(__global void* vm_states,__global void* rounding,__global  
void* scratchpads,__global const void* dataset" ascii
```

```
$s18 = "__kernel void execute_vm(__global void* vm_states,__global void* rounding,__global  
void* scratchpads,__global const void* dataset" ascii
```

```
$s19 = "__local exec_t* execution_plan=__local  
exec_t*)(execution_plan_buf+(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER  
_HASH*si" ascii
```

```
$s20 = "__kernel void blake2b_initial_hash(__gl
```

```
obal void *out,__global const void* blockTemplate,uint blockTemplateSize,uint start_nonce"  
ascii
```

condition:

```
uint16(0) == 0x5a4d and filesize < 19000KB and
```

^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_Isadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx  
SAM Accounts (0x%08x)" fullword wide
```





\$x2 = "ERROR kuhl_m_Isadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx user (%s)" fullword wide

\$x3 = "ERROR kuhl_m_Isadump_Isa ; kull_m_process_getVeryBasicModuleInformationsForName (0x%08x)" fullword wide

\$x4 = "ERROR kuhl_m_Isadump_getComputerAndSyskey ; kull_m_registry_RegOpenKeyEx LSA KO" fullword wide

\$x5 = "ERROR kuhl_m_Isadump_dcsync ; kull_m_rpc_drsrc_ProcessGetNCChangesReply" fullword wide

\$x6 = "ERROR kuhl_m_Isadump_trust ; kull_m_process_getVeryBasicModuleInformationsForName (0x%08x)" fullword wide

\$x7 = "ERROR kuhl_m_Isadump_getUsersAndSamKey ; kuhl_m_Isadump_getSamKey KO" fullword wide

\$x8 = "ERROR kuhl_m_Isadump_Isa_getHandle ; OpenProcess (0x%08x)" fullword wide

\$x9 = "ERROR kuhl_m_Isadump_netsync ; I_NetServerTrustPasswordsGet (0x%08x)" fullword wide

\$x10 = "ERROR kuhl_m_dpapi_chrome ; Input 'Login Data' file needed (/in: \"%localappdata%\\Google\\Chrome\\User Data\\Default\\Login Da" wide

\$x11 = "ERROR kuhl_m_kernel_processProtect ; Argument /process:program.exe or /pid:processid needed" fullword wide

\$x12 = "ERROR kuhl_m_Isadump_getHash ; Unknow SAM_HASH revision (%hu)" fullword wide

\$x13 = "ERROR kuhl_m_Isadump_sam ; kull_m_registry_RegOpenKeyEx (SAM) (0x%08x)" fullword wide

\$x14 = "ERROR kull_m_rpc_drsrc_ProcessGetNCChangesReply_decrypt ; Checksums don't match (C:0x%08x - R:0x%08x)" fullword wide

\$x15 = "ERROR kuhl_m_Isadump_enumdomains_users ; /user or /rid is needed" fullword wide

\$x16 = "ERROR kuhl_m_Isadump_changentlm ; Argument /oldpassword: or /oldntlm: is needed" fullword wide

\$x17 = "livessp.dll" fullword wide /* reversed goodware string 'lld.pssevil/* '

\$x18 = "ERROR kuhl_m_Isadump_enumdomains_users ; SamLookupNamesInDomain: %08x" fullword wide

\$x19 = "ERROR kuhl_m_Isadump_getComputerAndSyskey ; kuhl_m_Isadump_getSyskey KO" fullword wide





```
$x20 = "ERROR kuhl_m_lsadump_getKeyFromGUID ; kuhl_m_lsadump_LsaRetrievePrivateData: 0x%08x" fullword wide
```

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)" fullword  
ascii
```

```
$s2 = "Usage: masscan [Options] -p{Target-Ports} {Target-IP-Ranges}" fullword ascii
```

```
$s3 = "GetProcessAffinityMask() returned error %u" fullword ascii
```

```
$s4 = "Via: HTTP/1.1 ir14.fp.bf1.yahoo.com (YahooTrafficServer/1.2.0.13 [c s f ])" fullword ascii
```

```
$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" fullword ascii
$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 DFI
R Report"
reference = "https://thedfirreport.com"/
date = "2021-01-18"
hash1 = "a8b2e85b3e0f5de4b82a92b3ca56d2d889a30383a3f9283ae48aec879edd0376"
strings:
$s1 = "* The error occurred in hwloc %s inside process `%s', while" fullword ascii
    $s2 = "__kernel void find_shares(__global const uint64_t* hashes,uint64_t
target,uint32_t start_nonce,__global uint32_t* shares)" fullword ascii
    $s3 = "Could not read dumped cpuid file %s, ignoring cpuidump." fullword ascii
```





```
$s4 = "%PROGRAMFILES%\\NVIDIA Corporation\\NVSMI\\nvml.dll" fullword ascii

$s5 = "void blake2b_512_process_single_block(ulong *h,const ulong* m,uint
blockTemplateSize)" fullword ascii

$s6 = "* the input XML was generated by hwloc %s inside process `%s'." fullword ascii

$s7 = "blake2b_512_process_single_block(hash,m,blockTemplateSize);" fullword ascii

$s8 = "Found non-x86 dumped cpuid summary in %s: %s" fullword ascii

$s9 = "GetCurrentProcessorNumberExProc || (GetCurrentProcessorNumberProc &&
nr_processor_groups == 1)" fullword ascii

$s10 = "__kernel void blake2b_initial_hash(__global void *out,__global const void*
blockTemplate,uint blockTemplateSize,uint start_nonce" ascii

$s11 = "** hwloc %s received invalid information from the operating system." fullword ascii

$s12 = "__local exec_t* execution_plan=(__local
exec_t*)(execution_plan_buf+(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER
_HASH*si" ascii

$s13 = "__kernel void execute_vm(__global void* vm_states,__global void* rounding,__global
void* scratchpads,__global const void* datase" ascii

$s14 = "__kernel void execute_vm(__global void* vm_states,__global void* rounding,__global
void* scratchpads,__global const void* datase" ascii

$s15 = "__local exec_t* execution_plan=(__local
exec_t*)(execution_plan_buf+(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER
_HASH*si" ascii

$s16 = "__kernel void blake2b_initial_hash(__global void *out,__global const void*
blockTemplate,uint blockTemplateSize,uint start_nonce" ascii

$s17 = "nvml.dll" fullword ascii

$s18 = "__kernel void Groestl(__global ulong *states,__global uint *BranchBuf,__global uint
*output,ulong Target,uint Threads)" fullword ascii

$s19 = "__kernel void Blake(__global ulong *states,__global uint *BranchBuf,__global uint
*output,ulong Target,uint Threads)" fullword ascii

$s20 = "__kernel void JH(__global ulong *states,__global uint *BranchBuf,__global uint
*output,ulong Target,uint Threads)" fullword ascii
```

condition:





```
uint16(0) == 0x5a4d and filesize < 19000KB and  
)pe.imphash() == "5c21c3e071f2116dcdb008ad5fc936d4" or 8 of them(  
{
```

MITRE

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

منبع:

<https://thedfirreport.com/2021/01/18/all-that-for-a-coinminer/>

