TECHNICAL ANALYSIS OF CUBA RANSOMWARE
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Summary of Findings</td>
</tr>
<tr>
<td>5</td>
<td>Attack Overview</td>
</tr>
<tr>
<td>5</td>
<td>Impacted Countries</td>
</tr>
<tr>
<td>6</td>
<td>Technical Analysis</td>
</tr>
<tr>
<td>6</td>
<td>Lateral Movement</td>
</tr>
<tr>
<td>7</td>
<td>Ransomware Analysis</td>
</tr>
<tr>
<td>7</td>
<td>Packed Sample</td>
</tr>
<tr>
<td>7</td>
<td>Unpacked Sample</td>
</tr>
<tr>
<td>10</td>
<td>Recent Sample</td>
</tr>
<tr>
<td>10</td>
<td>Conclusion</td>
</tr>
<tr>
<td>11</td>
<td>IOCs</td>
</tr>
<tr>
<td>11</td>
<td>Email Addresses</td>
</tr>
<tr>
<td>11</td>
<td>Domain</td>
</tr>
<tr>
<td>11</td>
<td>Script for Lateral Movement and Deployment</td>
</tr>
<tr>
<td>11</td>
<td>Cuba Ransomware</td>
</tr>
<tr>
<td>12</td>
<td>Process / Services Kill List</td>
</tr>
<tr>
<td>12</td>
<td>MITRE ATT&amp;CK Techniques</td>
</tr>
<tr>
<td>14</td>
<td>YARA Rules</td>
</tr>
<tr>
<td>14</td>
<td>Cuba Dec 2019</td>
</tr>
<tr>
<td>15</td>
<td>Cuba Variant May 2020</td>
</tr>
<tr>
<td>17</td>
<td>Cuba Variant Dec 2020</td>
</tr>
<tr>
<td>18</td>
<td>Cuba Ransomware March 2021</td>
</tr>
<tr>
<td>20</td>
<td>Cuba Ransomware March 2021 Unpacked</td>
</tr>
<tr>
<td>23</td>
<td>About McAfee</td>
</tr>
<tr>
<td>23</td>
<td>McAfee ATR</td>
</tr>
<tr>
<td>23</td>
<td>Additional Resources</td>
</tr>
</tbody>
</table>
INTRODUCTION

Cuba ransomware is an older ransomware that has been active for the past few years. The actors behind it recently switched to leaking the stolen data to increase its impact and revenue, much like we have seen recently with other major ransomware campaigns.

In our analysis, we observed that the attackers had access to the network before the infection and were able to collect specific information in order to orchestrate the attack and have the greatest impact. The attackers operate using a set of PowerShell scripts that enables them to move laterally. The ransom note mentions that the data was exfiltrated before being encrypted. In similar attacks we have observed the use of a Cobalt Strike payload, although we have not found clear evidence of a relationship with Cuba ransomware.

We observed Cuba ransomware targeting financial institutions, industry, technology, and logistics organizations.

For active protection, more details can be found on our website: https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.cuba-ransomware.html

The following report provides an overview analysis of the capabilities of Cuba ransomware and an explanation of how it works. The data included in this report is related to a Cuba ransomware sample from late 2020. We have also updated the findings with a recent sample.
SUMMARY OF FINDINGS

- Cuba ransomware has targeted several companies in north and south America as well as in Europe.
- The attackers used a set of obfuscated PowerShell scripts to move laterally and deploy their attack.
- They used an online website to publish the stolen data.

- The malware is obfuscated and comes with several evasion techniques.
- The actors have sold some of the stolen data.
- The ransomware uses multiple argument options and has the possibility to discover shared resources using the NetShareEnum API.
ATTACK OVERVIEW
The current infection vectors are currently unknown. Once the network is breached, the attackers deploy a set of PowerShell scripts to move laterally and deploy the next stages.

The attackers recently leaked the stolen data online at this address: http://cuba4mp6ximo2zlo[.]onion.

The following screenshot shows the website.

It is interesting to note that the actors sold some specific stolen data rather than just leaked it. Below is an example for data stolen from the company AFTS.

IMPACTED COUNTRIES
The following picture shows an overview of the countries that have been impacted according to our telemetry.
**TECHNICAL ANALYSIS**

**LATERAL MOVEMENT**

Several files, including deployment scripts, were discovered in the environment. The following batch files were created to deploy an obfuscated PowerShell script that loads into memory and installs the ransomware.

<table>
<thead>
<tr>
<th>File type</th>
<th>DOS batch file, ASCII text, with CRLF line terminators</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>151.bat</td>
</tr>
<tr>
<td>File size</td>
<td>175</td>
</tr>
<tr>
<td>Hash</td>
<td>Sha256</td>
</tr>
<tr>
<td>Value</td>
<td>54627975c0be0fe0075d6da1a53af9403f047d9e367389e48ae0d25c2a7154bc</td>
</tr>
</tbody>
</table>

The extract below shows the contents of this batch file. It is used to run a custom PowerShell script with the name 151.ps1 then autodeletes itself.

```bash
@echo off
c:\windows\syswow64\windowspowershell\v1.0\powershell.exe -windowstyle hidden -executionpolicy bypass -file c:\windows\temp\151.ps1
Timeout /t 15
del %0
exit
```

The number 151 for naming the script is related to the campaign number.

The remote C2 is at the address kurvalarva[.]com and is known as being malicious. The downloaded payload is the Cuba ransomware.
REPORT

RANSOMWARE ANALYSIS

In the version we analyzed, the ransomware comes packed and obfuscated. It uses the 360-antivirus icon and metadata to trick the user. In a more recent sample, the ransomware is using the OpenVPN metadata.

At the end of the encryption process the ransomware will display a fake message to prompt restarting of the system.

In every folder, the sample will write the following ransom note:

The sample uses multiple layers of obfuscation to avoid analysis and detection. Once unpacked, however, it is possible to analyze it.

PACKED SAMPLE

<table>
<thead>
<tr>
<th>File type</th>
<th>PE32 executable (GUI) Intel 80386, for MS Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>COM.exe</td>
</tr>
<tr>
<td>File size</td>
<td>3012952</td>
</tr>
<tr>
<td>Hash SHA256</td>
<td>c4b1f4e1ac9a28cc9e50195b29d6e8bd54527abc7f4d16899f9f8315c852af4</td>
</tr>
<tr>
<td>Compile time</td>
<td>1983-03-01 22:41:12</td>
</tr>
<tr>
<td>Sections</td>
<td>4 (0 suspicious)</td>
</tr>
<tr>
<td>Directories</td>
<td>import, resource, security</td>
</tr>
<tr>
<td>Detected</td>
<td>sign, antidbg</td>
</tr>
<tr>
<td>Import Hash</td>
<td>255ee022176f062a24b690a8edeb70334</td>
</tr>
</tbody>
</table>

UNPACKED SAMPLE

<table>
<thead>
<tr>
<th>File type</th>
<th>PE32 executable (GUI) Intel 80386, for MS Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>400000.COM.exe</td>
</tr>
<tr>
<td>File size</td>
<td>72544</td>
</tr>
<tr>
<td>Hash SHA256</td>
<td>944ee8789cc929d2efda5790669e5266fe80910cabbf050cb3e57dc62de2040</td>
</tr>
<tr>
<td>Compile time</td>
<td>2020-09-03 00:05:36</td>
</tr>
<tr>
<td>Sections</td>
<td>5 (0 suspicious)</td>
</tr>
<tr>
<td>Directories</td>
<td>import, resource, debug, tls, relocation</td>
</tr>
<tr>
<td>Detected</td>
<td>packer, mutex, antidbg</td>
</tr>
<tr>
<td>Import Hash</td>
<td>e9fcbf3a37836d5b16c8427ecb7ba2a7</td>
</tr>
</tbody>
</table>

It uses the extension “.cuba” and the file marker in the encrypted file is “FIDEL.CA,” as shown below:
In the unpacked sample, we can see that the compilation timestamp is dated “2020-09-03.”

The ransomware has special options that can be used, allowing the threat actor to have flexibility in the attack. The sample will also check the installed languages (looking, for example, for the Russian language).

The switches “/min” and “/max” can be used by an operator to encrypt files with a size between two values to make it faster and more impactful.

After the end of the attack, or by using the option “/dm”, it will terminate the execution of the process and delete itself using “cmd.exe /c del”.

/dm
/min
/max
/net
/scan
The switch “/net” will get the ARP table using the function GetIpNetTable and search the machine’s network shares with the function NetShareEnum. Using GetIpNetTable can recover the last connections to the victim machine, allowing those IP addresses to be used to attack more targets.

Prior to encrypting files, it will terminate the following services and processes:

- MSSQLSERVER
- MSDTC
- SQLBrowser
- SqlServr.exe
- terminate_process
- SqlWriter.exe
- terminate_process
- Msdtc.exe
- terminate_process
- SqlBrowser.exe
- terminate_process
- avMvmp.exe
- terminate_process
- avMsp.exe
- terminate_process
- avMms.exe
- terminate_process

The malware also has the capability to encrypt shared resources.

```plaintext
mov    edx, offset aMysql ; "MySQL"
call   close_and_terminate
mov    edx, offset aMysql80 ; "MySQL80"
call   close_and_terminate
mov    edx, offset aMssqlserver ; "MSSQLSERVER"
call   close_and_terminate
mov    edx, offset aSqlwriter ; "SQLWriter"
call   close_and_terminate
mov    edx, offset aMsdtc ; "MSDTC"
call   close_and_terminate
mov    edx, offset aSqlbrowser ; "SQLBrowser"
call   close_and_terminate
mov    ecx, offset aSqlservrExe ; "sqlservr.exe"
call   terminate_process
mov    ecx, offset aSqlwriterExe ; "sqlwriter.exe"
call   terminate_process
mov    ecx, offset aMsdtcExe ; "msdtc.exe"
call   terminate_process
mov    ecx, offset aSqlbrowserExe ; "sqlbrowser.exe"
call   terminate_process
mov    ecx, offset aVmwpExe ; "vmwp.exe"
call   terminate_process
mov    ecx, offset aVmspExe ; "vmsp.exe"
call   terminate_process
mov    ecx, offset aVmsmsExe ; "vmsms.exe"
call   terminate_process
```
RECENT SAMPLE

In a recent sample, the actors behind Cuba ransomware updated some of its functions. In this variant the ransomware is using SeDebugPrivilege to elevate privileges. Additionally, they updated the list of services and processes to terminate.

```c
HANDLE hpl; // ptr
struct _TOKEN_PRIVILEGES NewState; // [esp+8H] [ebp-1CH]
struct _LUID Luid; // [esp+18H] [ebp-CH]

hpl = GetCurrentProcess();
if ( LookupPrivilegeValueW(0, "SeDebugPrivilege", &Luid ) )
{
    NewState.Privileges[0].Luid = Luid;
    NewState.PrivilegeCount = 1;
    NewState.Privileges[0].Attributes = 2;
    if ( AdjustTokenPrivileges(hpl, 0, &NewState, 0, 0, 0 )
    GetLastError();
}
#endif

// Additional updated functions
```

The other function remains the same in the new variant.

CONCLUSION

Cuba ransomware has recently impacted several organizations. In this short report we briefly detailed the threat actors’ capabilities and provided an overview of the ransomware. It is interesting to note that the website for leaking stolen data was put online some months ago and follows the same trends as other ransomware actors.

The use of arguments demonstrates that the ransomware has been developed to be modular and practical for the authors to gain access, discover, and encrypt data more easily.

While this brief threat report shows some aspects of the Cuba ransomware, it also provides an overview of the operating methods used by the attackers.

McAfee® Advanced Threat Research Team is actively monitoring this threat for future releases.
Technical Analysis of Cuba Ransomware

**(IOCS)**

**Email Addresses**
- under_amur@protonmail[.]ch
- helpadmin2@cock[.]li
- helpadmin2@protonmail[.]com
- iracomp2@protonmail[.]ch
- fedelsupportagent@cock.li
- admin@cuba-supp.com
- cuba_support@exploit.im

**Domain**
- kurvalarva[.]com

**Script for Lateral Movement and Deployment**

```
54627975c0beefe0075d6da1a53af9403f047d9e367389e48ae0d25ca7154bc
51f825ef9ff3e0bb80b7076ef19b837e927efe9da1232c2104c8ac8d51bdd
9882c2f5a95d780626470f6c0d3609c7590eb552065f81ab41ffe074ea47892
54627975c0beefe0075d6da1a53af9403f047d9e367389e48ae0d25ca7154bc
1f825ef9ff3e0bb80b7076ef19b837e927efe9da1232c2104c8ac8d51bdd
9882c2f5a95d780626470f6c0d3609c7590eb552065f81ab41ffe074ea47892
```

Cuba Ransomware

```
c4bf4e1ac9a28cc9e50195b292d8d54527abcf7f4d16899f9f8315c8524adfd4
944ee6879cc9292efda5790669e52666fe80910cabf1055cbb3e57dc6262de040
78ce13d98287f8b60cf5f8247bac07379d0c88b8e8b1a6996c29163f4e4b659
3352a85645cfcc247bc4765b177f5f97df0db220103d44228ec545b43d30e
672fb249e520f4496e72021f887f8886f6c5604317d8af3f0800d49aa157b1e
942a8bcb34a65f6df6a65224d5825d7d3be369ecda1356a660acbd39453d30
907f42a79192a016154f1127fbb1e676676f769d6947b亟7145acc4a66eb
28140850cf794ffef2755673ca646d680fc8b8a69453d0310e4a397f0e04e64
271ef3c1022829f0b15f2471d05a28d478eabaf0a9e1742bede36f36b3672ad
6396ea2f49a3d3a6f2eb2e510ac371ic23bd67dab5eb4ee6ba49f5df9df
b4da4bdcbd14e0412bab453e28a4fba86f16ac898387db391043ebe6297e9fa1
7a1f7344d9167f0272b9480336e0a50d533147b8be2e71c3261ea30a32d73f3ecb
206593d266ef8bfc5d159b5ec16a298890e88bae6a232c2104c8ac8d51bdd
9882c2f5a95d780626470f6c0d3609c7590eb552065f81ab41ffe074ea47892
54627975c0beefe0075d6da1a53af9403f047d9e367389e48ae0d25ca7154bc
1f825ef9ff3e0bb80b7076ef19b837e927efe9da1232c2104c8ac8d51bdd
9882c2f5a95d780626470f6c0d3609c7590eb552065f81ab41ffe074ea47892
```
**PROCESS / SERVICES KILL LIST**

MySQL, MySQL80, SQLSERVERAGENT, MSSQSERVER, SQLWriter, SQLTELEMETRY, MSDTC, SQLBrowser, sqlagent.exe, sqlservr.exe, sqlwriter.exe, sqlceip.exe, msdtc.exe, sqlbrowser.exe, vmcompute, vmmms, vmwp.exe, vmsp.exe, outlook.exe, MSEXchangeUMCR, MSEXchangeUM, MSEXchangeTransportLogSearch, MSEXchangeTransport, MSEXchangeThrottling, MSEXchargeSubmission, MSEXchargeServiceHost, MSEXchargeRFC, MSEXchargeRep1, MSEXchangePOP3BE, MSEXchangePop3, MSEXchangeNotificationsBroker, MSEXchangeMailboxReplication, MSEXchangeMailboxAssistant, MSEXchangeIS, MSEXchangeIMAP4BE, MSEXchangeIMap4, MSEXchangeHMRcovery, MSEXchangeM, MSEXchangeFrontEndTransport, MSEXchangeFastSearch, MSEXchangeEdgeSync, MSEXchangeDiagnostics, MSEXchargeDelivery, MSEXchangeDagMgmt, MSEXchangeCompliance, MSEXchangeAntispamUpdate

**MITRE ATT&CK TECHNIQUES**

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Observable</th>
<th>IOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter: PowerShell (T1059.001)</td>
<td>Cuba team is using PowerShell payload to drop Cuba ransomware</td>
<td>f739977004981fbe4a54bc68be18ea79 68a9962f49b8cd956108edcc44e07c bdeb5acc7b569c783f81499f400b2745</td>
</tr>
<tr>
<td>Execution</td>
<td>System Services: Service Execution (T1569.002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution</td>
<td>Shared Modules (T1129)</td>
<td>Cuba ransomware links function at runtime</td>
<td>Functions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“GetModuleHandle”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“GetProcAddress”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“GetModuleHandleEx”</td>
</tr>
<tr>
<td>Execution</td>
<td>Command and Scripting Interpreter (T1059)</td>
<td>Cuba ransomware accepts command line arguments</td>
<td>Functions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“GetCommandLine”</td>
</tr>
<tr>
<td>Persistence</td>
<td>Create or Modify System Process: Windows Service (T1543.003)</td>
<td>Cuba ransomware can modify services</td>
<td>Functions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“OpenService”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“ChangeServiceConfig”</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Access Token Manipulation (T1134)</td>
<td>Cuba ransomware can adjust access privileges</td>
<td>Functions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“SeDebugPrivilege”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“AdjustTokenPrivileges”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“LookupPrivilegeValue”</td>
</tr>
<tr>
<td>Tactic</td>
<td>Technique</td>
<td>Observable</td>
<td>IOCs</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>File and Directory Permissions Modification (T1222)</td>
<td>Cuba ransomware will set file attributes</td>
<td>Functions: &quot;SetFileAttributes&quot;</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>Obfuscated files or Information (T1027)</td>
<td>Cuba ransomware is using xor algorithm to encode data</td>
<td></td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>Virtualization/Sandbox Evasion: System Checks</td>
<td>Cuba ransomware executes anti-vm instructions</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>File and Directory Discovery (T1083)</td>
<td>Cuba ransomware enumerates files</td>
<td></td>
</tr>
<tr>
<td>Discovery</td>
<td>Process Discovery (T1057)</td>
<td>Cuba ransomware enumerates process modules</td>
<td>Functions: &quot;K32EnumProcesses&quot;</td>
</tr>
<tr>
<td>Discovery</td>
<td>System Information Discovery (T1082)</td>
<td>Cuba ransomware can get keyboard layout, enumerates disks, etc.</td>
<td>Functions: &quot;GetKeyboardLayoutList&quot; &quot;FindFirstVolume&quot; &quot;FindNextVolume&quot;</td>
</tr>
<tr>
<td>Discovery</td>
<td>System Service Discovery (T1007)</td>
<td>Cuba ransomware can query service status</td>
<td>Functions: &quot;QueryServiceStatusEx&quot;</td>
</tr>
<tr>
<td>Collection</td>
<td>Input Capture: Keylogging (T1056.001)</td>
<td>Cuba ransomware logs keystrokes via polling</td>
<td>Functions: &quot;GetKeyState&quot; &quot;VkKeyScan&quot;</td>
</tr>
<tr>
<td>Impact</td>
<td>Service Stop (T1489)</td>
<td>Cuba ransomware can stop services</td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>Data encrypted for Impact (T1486)</td>
<td>Cuba ransomware encrypts data</td>
<td></td>
</tr>
</tbody>
</table>
REPORT

YARA RULES

CUBA DEC 2019

rule RANSOM_Cuba_Dec2019 {
    meta:
    description = "Rule to detect Cuba Ransomware 2019 version"
    author = "McAfee ATR"
    date = "2021-02-23"
    rule_version = "v1"
    hash = "bda4bddcbd140e4012bab453e28a4fba86f16ac8983d7db391043eab627e9fa1"
    malware_type = "Ransom"

    strings:
    $s1 = "VirtualProtect" fullword ascii
    $s2 = "GetStartupInfoA" fullword ascii
    $s3 = "GetModuleHandleA" fullword ascii
    $s4 = "ListDrop" fullword ascii
    $s5 = "WinExec" fullword ascii

    $pattern1 = {BF90C5BC9827B183908CB29090103240409A1DCE40BE90004D68704433AC0B6BF294087400D878C2940C5C17940B00903AC3064062400D9B8940B80DBF88CB90902ABFBF-C951C9505C472C6908E41904F}
    $pattern2 = {000CADDD1B48CCB34848CCB34848CCB34827D3B38480CCB348348CCB34827D3B94813CCB348B7ECCB7484DCCB34848CCB24809CCB3482AD3A0484ACCC348B7ECC-B9484ACC3481CEF82484ECCB348}
    $pattern3 = {F2FB58C3A06EA22ED5FB2BD44D066B68626B187B123740FB2FC36B107EEF2A2463D6FB406B6BF33A36B76FB01D66BFBOCC02BFBA70FD36B682E2CA20A6B6B286B-6BA06B2B}
REPORT

$pattern4 = {40908BC00BF909000C909859C64090CB54B255A870900DB2C09B2901490901AF35BE3490C307BF8476CB40901B0AD840BFA32590FB409078053D0040F814853}

$pattern5 = {6B6BE03967E0397FE01943017332589458ABC7570A1769474BAAA4666893899BEA9430D72101E0317BE0791E02369B0AE0E9BE0269B682357E2E656594494D1636B}

condition:
filesize <= 750KB and
4 of ($s\ast$) and
4 of ($pattern\ast$)

CUBA VARIANT MAY 2020

rule RANSOM_Cuba_variant_May2020 {
meta:

description = “Rule to detect Cuba Ransomware variant from May 2020”

author = “McAfee ATR”

date = “2021-02-23”

rule_version = “v1”

hash = “7a17f34d916f7f0272b9480336fb05d33147b8be2e71c3261ea30a32d73fecb”

malware_type = “Ransom”

strings:
$s1 = “Good day. All your files are encrypted. For decryption contact us.” fullword ascii

$s2 = “CryptGenRandom” fullword ascii
$s3 = "VirtualAlloc" fullword ascii
$s4 = (002100210460041005100200066006F007200200040065006300720079007000740069006F006E0E0021002102E007400780074)

// !!FAQ for Decryption!! .txt

$s1 = {C1C109334D8C8D3C01C1C70D337D94897D9C8D0439C1C01233C28B55988945A08d0413c1C00733458803D0c1c2093355848D1c02c1c3D335d0895d08d3c1A8D897DB-
8C1C312335D9885DB88B5DB403D8C1C30733DE8B75B4895D0895DC08d3c33C1C70933F9897D8C97DC48D0C3BC1C10D33C8894D}

$s2 = {B08D4DFB33C03BF977078D4DBC3BD1730B4E3F3BF977253BD672218B5DB48B75B88D55BC03D0408A0C16320A880C1383F84072ED8B75C8B5DACEB3E0F1045B-
C0F100E660FEFC80F10)

$s3 = {837E283872E0FB646078846640FB646068A6660FB6460584660FB64604884660FB6460384660FB6460284660FB646018466A0FB6068466B8D462C5056E81E01}

$s4 = {342A3464349434C43402355A35A235D4350A366536B536F236A337CD37F2371A384A389938D43804392A395A39A9390A3914A323A6E35E3A3E323B5C}

$s5 = {512085F673372133B15FC294600732985F67725720583FA1D731E0FB682AC28460039411875128B0495802946005F5B890133C05E8BE55DC30BD6750B5F89}

condition:
filesize <= 600KB and
3 of ($s*) and
4 of ($pattern*)
CUBA VARIANT DEC 2020

rule RANSOM_Cuba_variant_Dec2020 {
meta:

description = "Rule to detect Cuba Ransomware variant from December 2020"
author = "McAfee ATR"
date = "2021-02-23"
rule_version = "v1"
hash = "33352a38454cfc247bc7465bf177f5f97d7fd0bd220103d4422c8ec45b4d3d0e"
malware_type = "Ransom"

strings:
$s1 = "Good day. All your files are encrypted. For decryption contact us." fullword ascii
$s2 = "SeDebugPrivilege" fullword ascii
$s3 = "md5WithRSAEncryption" fullword ascii
$s4 = "CryptGenRandom" fullword ascii
$s5 = "CryptAcquireContextW" fullword ascii
$s6 = "FindFirstFileExW" fullword ascii

// Main function
$main1 = { 55 8b ec 83 ec 44 a1 0c 70 42 00 33 c5 89 45 fc 8b 45 10 56 33 f6 66 39 30 74 03 50 eb 05 68 08 be 41 00 e8 17 ea ff ff 8d 45 bc 50 6a 10 68 ff 15 c8 71 41 00 85 c0 7e 0c 80 7c b5 bc 19 74 0a 46 3b f0 7c f4 e8 11 ff ff ff 8b 4d fc 33 c0 33 cd 5e e8 34 74 00 00 c9 c2 10 00 }
$main2 = {558bec83ec44a1????????33c58945fc8b4510633f666393074??50eb???68????????e8????????e8????????8d45bc506a7????????8c07e??807cb5bc1974????3463bf07????8b4d3c33c033cd5e8????????e9e21??70}
**REPORT**

\$main3 = {558bec83ec44a1????????33c58945fc8b45105633f6663930[2-6]50[2-6]e8????????e8????????8d45bc506a??????????85c0[2-6]807cb5bc19[2-6]463bf0[2-6]}

\$main4 = { 55 8B EC 83 EC 44 A1 ?? ?? ?? ?? 33 C5 89 45 ?? 8B 45 ?? 56 33 F6 66 39 30 74 ?? 50 EB ?? 68 08 BE 41 00 E8 ?? ?? ?? ?? 8D 45 ?? 50 6A 10

condition:

\$main3 = {558bec83ec44a1????????33c58945fc8b45105633f6663930[2-6]50[2-6]e8????????e8????????8d45bc506a??????????85c0[2-6]807cb5bc19[2-6]463bf0[2-6]}

\$main4 = { 55 8B EC 83 EC 44 A1 ?? ?? ?? ?? 33 C5 89 45 ?? 8B 45 ?? 56 33 F6 66 39 30 74 ?? 50 EB ?? 68 08 BE 41 00 E8 ?? ?? ?? ?? 8D 45 ?? 50 6A 10

**CUBA RANSOMWARE MARCH 2021**

**rule RANSOM _ Cuba _ March2021**

```
{ }
```

**meta:**

description = “Rule to detect Cuba ransomware March 2021 version”

author = “McAfee ATR”

date = “2021-03-31”

hash = “2af30ca88d11eb0c1a4bd4f0aa0ce685”
strings:
$s1 = "VirtualAlloc" wide ascii
$s2 = "GetSystemDirectoryW" wide ascii
$s3 = "ShellExecuteEx" wide ascii
$s4 = "SHEmptyRecycleBinA" wide ascii
$s5 = "CommandLineToArgvW" wide ascii

$fnc1 = { 55 8b ec 83 ec 18 c7 45 fc 40 00 00 00 c7 45 f4 00 00 00 00 a1 40 c1 44 00 89 45 e8 c7 45 f8 ff ff ff 8b 0d 7c a7 44 00 89 0d a0 c1 44 00 ff 75 fc 68 01 30 00 00 83 2c 24 01 ff 75 e8 ff 75 f4 ff 35 a0 c1 44 00 59 ff d1 89 45 ec 8b 55 ec 89 15 84 c1 44 00 a1 40 c1 44 00 a3 44 c1 44 00 8b 0d 84 c1 44 00 81 c1 c0 51 02 00 89 0d 50 c1 44 00 8b ec 8b 45 ec 8b e5 5d c3 }

$fnc2 = {558bec83ec18c7????????????a1????????8945e8c7?????????8b??????????89???????????ff75fc68????????832c2401ff75e8ff75f4ff??????????9ff-d18945ec8b5ec89??????????a1????????8b?????????81??????????89????????78b45ec8be55dc3}

$fnc3 = { 55 8B EC 83 EC 18 C7 45 ?? 40 00 00 00 C7 45 ?? 00 00 00 A1 ?? ?? ?? ?? 89 45 ?? C7 45 ?? FF FF FF FF 8B OD ?? ?? ?? ?? 89 OD ?? ?? ?? FF 75 ?? 68 01 30 00 00 83 2C 24 01 FF 75 ?? FF 75 ?? FF FF 35 ?? ?? ?? ?? 59 FF D1 89 45 ?? 8B 55 ?? 89 15 ?? ?? ?? ?? A1 ?? ?? ?? ?? A3 ?? ?? ?? ?? 8B OD ?? ?? ?? ?? 81 C1 C0 S1 02 00 89 OD ?? ?? ?? ?? 8B 45 ?? 8B E5 5D C3 }

condition:
filesize => 350KB and filesize <= 500KB and
4 of ($s*) and
1 of ($fnc*)
}
rule RANSOM_Cuba_Unpacked_March2021
{

meta:
description = "Rule to detect Cuba ransomware unpacked"
author = "McAfee ATR"
date = "2021-03-31"
hash = "aef29cad14fd64de387c274476887c94"
malware_type = "Ransom"

strings:
$s1 = "Good day" wide ascii
$s2 = "AppPolicyGetProcessTerminationMethod" wide ascii
$s3 = "GetOEMCP" wide ascii
$s4 = "GetCommandLineA" wide ascii
$s5 = "GetProcAddress" wide ascii

$main1 = { 55 8b ec 81 ec 78 06 00 00 a1 0c a0 42 00 33 c5 89 45 fc 56 8b 75 10 b9 b8 aa 42 00 6a 05 68 18 f0 41 00 e8 b8 04 00 00 66 c7 05 d0 aa
42 00 00 00 0f 57 c0 c6 05 d2 aa 42 00 00 06 0f 13 05 d8 aa 42 00 c7 05 e0 aa 42 00 ff ff ff ff ff c7 05 e4 aa 42 00 ff ff ff ff ff 7f 85 f6 0f 84 57 01 00
00 66 83 3e 00 0f 84 4d 01 00 00 8d 85 e0 f9 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 50 56 ff 15 c4 a1 41 00 8b 8d e0 f9 ff ff ff ff ff 89 85 f9 ff ff 85 c9
0f 84 21 01 00 00 57 8b 38 33 f6 66 83 3f 2f 74 31 8b d7 84 02 66 8b 02 83 c2 02 66 85 c0 0f 75 f5 2b 6b 9b aa 42 00 d1 fa 52 57 e8 20 04 00 00
8b 8d e0 f9 ff ff ff ff ff ff ff 00 00 00 8b 85 88 f9 ff ff ff f3 f1 0f 8d dc 00 00 00 00 33 ff ff ff ff ff ff ff ff ff ff f1 f7 0c 8b 04 b0 66 83 38 2f
74 03 8b f8 46 68 24 f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 0c c6 05 d2 aa 42 00 01 e9 8e 00 00 00 00 68 2c f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 1a
85 ff 74 7a 57 e8 98 bd 00 00 00 83 c4 04 a3 d5 aa 42 00 00 89 15 dc 00 00 00 00 68 48 44 f0 41 00 53 ff 15 5c a0 41 00 85 c0 75 1a 85 ff 74 50 57 e8 6e
bd 00 00 83 c4 04 a3 e0 aa 42 00 00 89 15 4a 42 00 eb 3a 8b 3d 5c a0 41 00 68 44 f0 41 00 53 ff d7 85 c0 75 09 c6 05 d0 aa 42 00 01 eb 1f 68 50 f0}
REPORT

Technical Analysis of Cuba Ransomware

REPORT

$main2 = {558bec81ec7806????a1????????33c58945fc56b7510b9??????????75a77e68????????????????????85f60f84????????66833e70f084????????8d85e0f9ffffff85056ff?????????8b8de0f9ffe88b85e0f9ffe85056f0af7f?????

775758b3833f66833f2f74728bd78d720266828b32026685c07522bd6b9?????????d1fa527e8????????8b8de0f9ffe88b85e0f9ffe85056f0af7f??????????????????????????????????????????53660f1f44

-7788b1cb03f463b1f1d728b04b06683382f74728bf84668???????????5ff????????785c0757c6??????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????????}
condition:

filesize >= 150KB and filesize <= 250KB and

4 of ($s*$) and

1 of ($main*$)

}
ABOUT MCAFEE
McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies’ products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

MCAFEE ATR
The McAfee® Advanced Threat Research Operational Intelligence team operates globally around the clock, keeping watch of the latest cyber campaigns and actively tracking the most impactful cyber threats. Several McAfee products and reports, such as MVISION Insights and APG ATLAS, are fueled with the team’s intelligence work. In addition to providing the latest Threat Intelligence to our customers, the team also performs unique quality checks and enriches the incoming data from all of McAfee’s sensors in a way that allows customers to hit the ground running and focus on the threats that matter.

Subscribe to receive our Threat Information.

ADDITIONAL RESOURCES