Threat Thursday: Ficker Infostealer Malware

blogs.blackberry.com/en/2021/08/threat-thursday-ficker-infostealer-malware

The BlackBerry Research & Intelligence Team

Ficker is a malicious information-stealer that is sold and distributed on underground Russian online forums by a threat actor using the alias @ficker. This Malware-as-a-Service (MaaS) was first uncovered in the wild in mid-2020.

Ficker has been previously distributed via Trojanized web links and compromised websites. For example, it could direct victims to pages purportedly offering free downloads of legitimate paid services like Spotify and YouTube Premium. It has also recently been deployed via the known malware downloader, Hancitor.

Notably written in Rust, Ficker has several targets for its information stealing, including web browsers, credit card information, crypto-wallets, FTP clients and other applications. Along with anti-analysis checks, the malware can also deploy further functionality and download additional malware once a system is successfully compromised.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	Medium
Risk	Medium

Ficker offers several paid packages, with different levels of subscription fees to use their malicious program. Once the malware subscription is purchased, the malware author provides a web-based panel to the buyer to collect and examine information stolen from victims, as well as the executable of the information stealer itself.

Figure 1: Ficker is named after its creator/promoter

The creator of the malware is frequently active on the forums related to the malware, as seen in the image below:

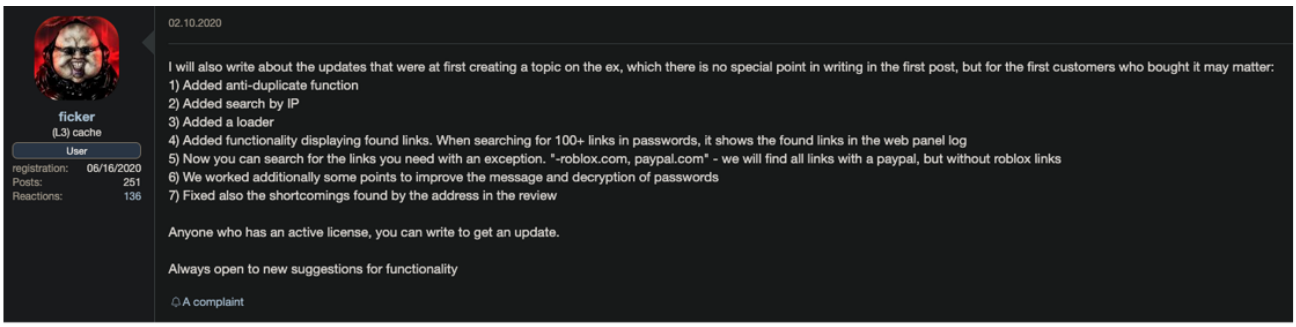

Figure 2: Translated "update log" from malware author

Since its introduction last year, Ficker has been deployed in a wide variety of ways. This is likely due to multiple threat actors using the malware differently in smaller individual campaigns.

In its early days, Ficker victims had mostly downloaded and executed the threat accidentally after visiting compromised websites or inadvertently clicking on malicious web links. Threat actors will often create fake ads for legitimate and popular services to lure unsuspecting users into visiting or clicking on Trojanized material.

For example, Ficker has previously been hosted on lure pages masquerading as a "Microsoft® Store" webpage, to entice users to download malicious applications while lulling them into a false sense of security.

Hancitor

In recent months, Ficker has been deployed and dropped by the known malware family Hancitor. Hancitor's attack chain often begins with the threat actor sending out fake DocuSign malspam emails, which results in a victim unknowingly downloading a Trojanized Microsoft® Word document, thinking they are getting a real DocuSign doc.

Once the fake DocuSign document is opened and its malicious macro code is allowed to run, Hancitor will often reach out to its command and control (C2) infrastructure to receive a malicious URL containing a sample of Ficker to download, as seen below:

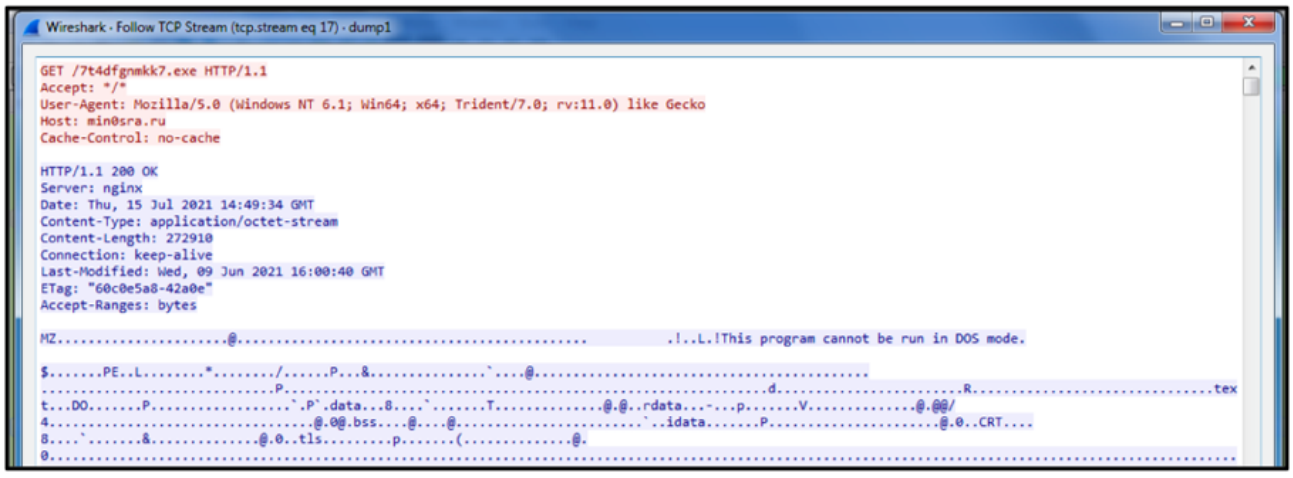

Figure 3: Example of Hancitor downloading Ficker infostealer

Depending on the commands the Hancitor C2 sends, Ficker is often injected into an instance of svchost.exe on a victim's machine, as seen below. It does this to further avoid detection and hide the activity of this malicious executable.

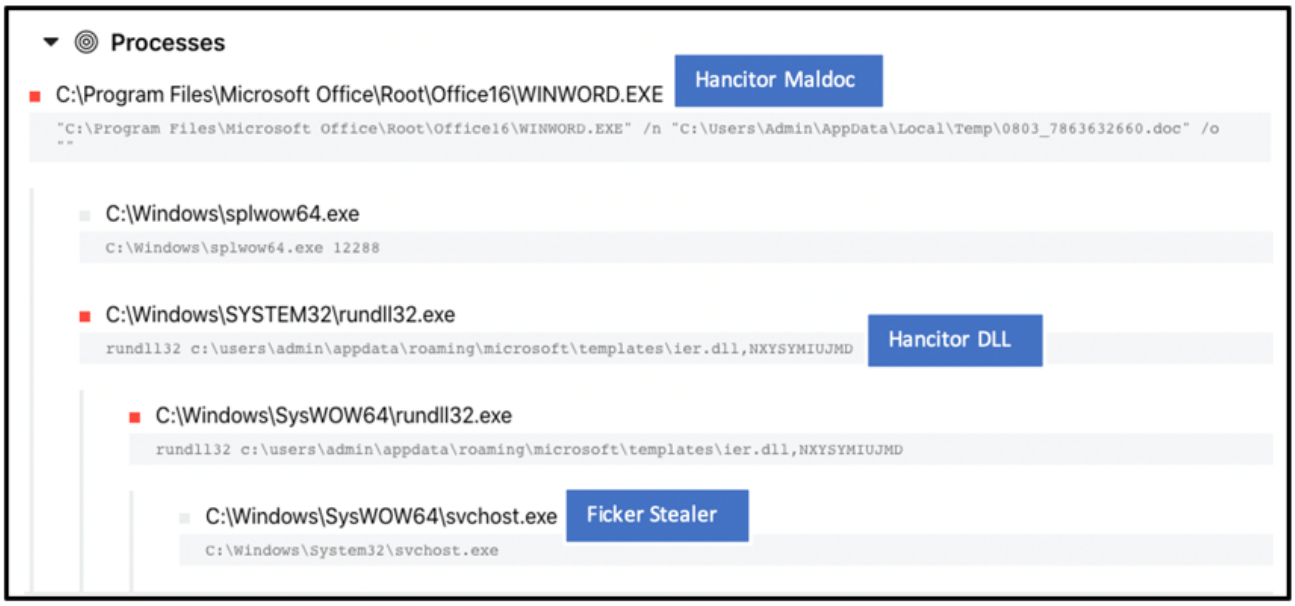

Figure 4: Process Flow of Ficker via Hancitor initial infection

Anti-Analysis and Initial Checks

When analyzing the file statically, we found that Ficker is heavily obfuscated. It also contains multiple anti-analysis checks, which are meant to thwart analysis and prevent the malware from executing in virtualized environments.

The malware author has also included checks so that the malware will not execute if it is running in selected countries, which is likely intended to protect the threat actors who tend to purchase such malware. Ficker achieves this by checking the keyboard layout of the victim's machine. If their keyboard layout is related to one of these nations, the malware will terminate:

Keyboard Layout	Country
ru-RU	Russia
be-BY	Belarus
Uz-UZ	Uzbekistan
hy-AM	Armenia
kk-KZ	Kazakhstan

az-AZ	Azerbaijan

To do this, Ficker will reach out to the web API at api[.]ipify[.]org. This is a public IP address web API used by the malware to gather the external IP address of the victim's device. The threat likely uses this as another anti-virtualized environment check, as the malware will not reach out to its C2 infrastructure if it doesn't get a successful response to this API call.

Once the victim's IP address is obtained, the malware will attempt to reach out to its C2 server. If a response is sent successfully, the malware will receive its configuration commands to perform its desired actions. If the malware cannot obtain such information from this API call, it will wait until an Internet connection is re-established before reaching out to its C2.

Stolen Data

Unlike traditional information stealers, Ficker does not write its stolen data to disk. Traditional infostealer families will often store a local copy of the data it intends to steal, and then exfiltrate it after a set period of time. Instead, Ficker loops through its instructions and sends its information directly to the operator of the malware.

The malware author has designed Ficker to have another unique feature: decrypting stolen data server-side rather than "victim-side." This is likely done to avoid detection, but it also gives Ficker's creator greater control over who is allowed to use their malware.

When sending stolen data, Ficker will initially encrypt it using an XOR rotation. During analysis, it appears that the same XOR key (0x0A) is used across all samples.

Depending on its commands, Ficker will attempt to exfiltrate the following information:

- Chromium web browsers
    - Saved login credentials
    - Cookies
    - Auto-compete history
- Mozilla-based web-browsers.
    - Saved login credentials
    - Cookies
    - Auto-complete history
- Credit card information
- Cryptocurrency wallets
- FileZilla FTP client
- WinScp FTP client
- Discord login

- Steam accounts
- Pidgin accounts
- Thunderbird accounts

The malware will also gather system information, as shown below:

```
MicrosoftEdge<0x00><0x00><0x00><0x00><0x00><0x00><0x00><0x00><0
Exe path: C:\\Windows\\SysWOW64\\svchost.exe
Compter's name: MRBKYMNO
Prodct name: Some("Windows 7 Professional")
Processor:Persocon Processor 2.5+
Resoltion 1280X720CPU cont 2RAM MB: 2047
GPU RDP Reflector Display DriverUTC 0:00
Time zone Coordinated Universal
TimeKeyboards: English (United States)
English (United States)
HWID: Some("17ebba21-ade9-4848-b865-5b9359ee593d")
Processes:"[System Process]"
"System"-4"smss.exe"-260
"csrss.exe"-336
"wininit.exe"-372
"csrss.exe"-380
"winlogon.exe"-420
"services.exe"-464
"lsass.exe"-480
"lsm.exe"-488
"svchost.exe"-584
"svchost.exe"-660
"spoolsv.exe"-1016
"svchost.exe"-1036
"taskhost.exe"-1120
"dwm.exe"-1212
"explorer.exe"-1256
"rndll32.exe"-2028
"WMIADAP.exe"-612
"rndll32.exe"-1496
"WmiPrvSE.exe"-1636
"svchost.exe"-1768
"sppsvc.exe"-1776
"dllhost.exe"-1088
"svchost.exe"-1468

Software:
Adobe AIR - 1.0.4990
Google Chrome - 89.0.4389.114
Microsoft Office Professional Pls 2010 - 14.0.4763.1000
```

Figure 5: Decoded system information sent by Ficker to its C2

The malware also has screen-grab abilities, which allow the malware's operator to remotely capture an image of the victim's screen. The malware also enables file-grabbing and additional downloading capabilities once connection to its C2 is established, as shown below. This enables further stages of exploitation on a victim's device.

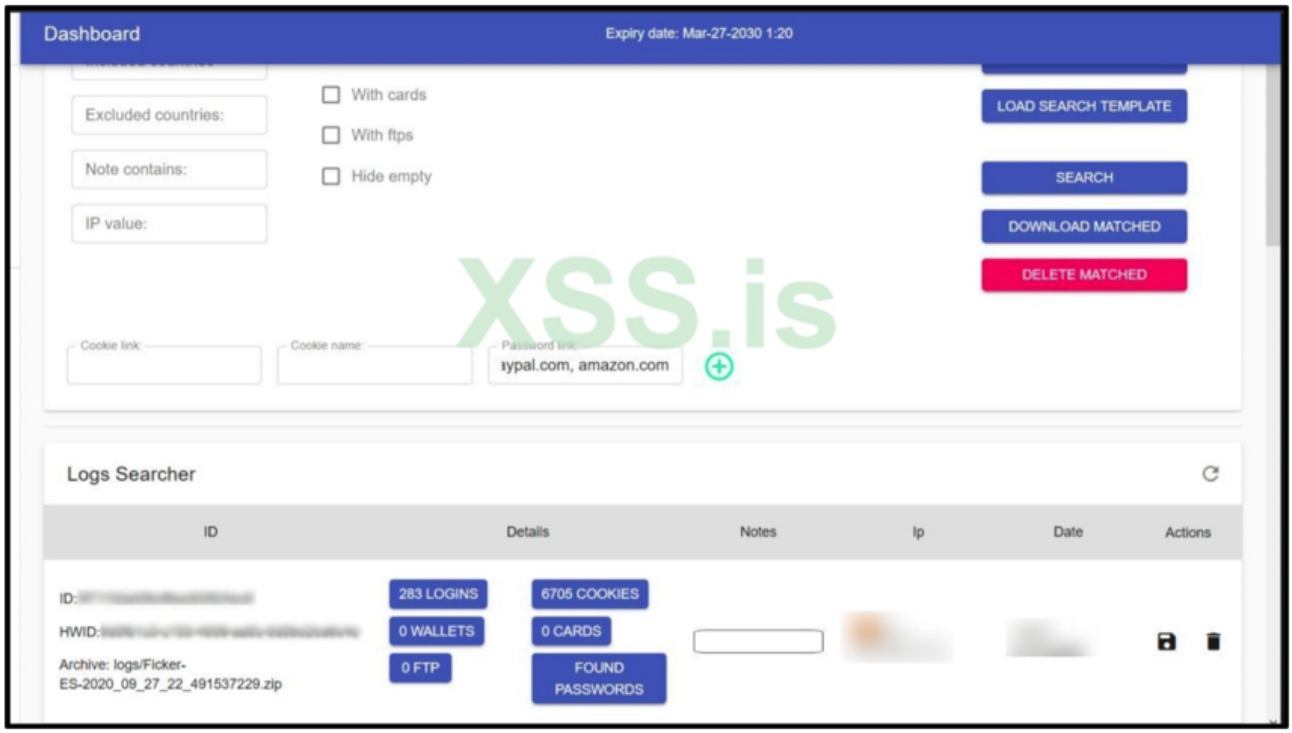

Figure 6: Example of Ficker dashboard

Once information is sent back to Ficker's C2, the malware operator can access and search for all exfiltrated data.

YARA Rule

The following YARA rule was authored by the BlackBerry Research & Intelligence Team to catch the threat described in this document:

```
import "pe"

rule Mal_Infostealer_Win32_Ficker_Stealer
{
  meta:
    description = "Yara rule to detect Ficker Stealer"
    author = "Blackberry Threat Research Team"
    date = "04-08-2021"

  strings:
    $x1 = "kindmessage"
    $x2 = "SomeNone"
    $x3 = ".Kind"

  condition:
    //PE File
    uint16(0) == 0x5A4D and

    // Must have the following sections in the following order
    pe.section_index(".text") == 0 and
    pe.section_index(".data") == 1 and
    pe.section_index(".rdata") == 2 and
    pe.section_index("/4") == 3 and
    pe.section_index(".bss") == 4 and
    pe.section_index(".idata") == 5 and
    pe.section_index(".CRT") == 6 and
    pe.section_index(".tls") == 7 and

    // Must be less than
    filesize < 300KB and

    //One of $x
    (2 of ($x*))

}
```

Indicators of Compromise (IoCs)

Operating System: **Windows**

Mutex

- serhershesrhsfesrf
- hrth
- o;jtfytyjftyjftyjftyj;ijo;
- ijlhlkwaftyjftyjftjftyh;joi;i
- ah;waeh;jftyjftyjfiftfdgaf
- hotyjftyj;afdh
- whftyjftyjftyjtfyjtfyjtfyj;ijo;h
- whoareyoutellmeandilltellwhoyou

Network Communication

Ficker Download IOC:

Domain	Created	Registrar
s0lom0n[.]ru/7hsjfd9w4refsd[.]exe		-
min0sra[.]ru/7t4dfgnmkk7[.]exe		-
falan4zadron[.]ru/7hsjfd9w4refsd.exe		-
4a5ikol[.]ru/7jkio8943wk[.]exe		-
pirocont70l[.]ru/7hjujnfds[.]exe		-

Ficker C2:

Domain	Created	Registrar
pospvisis[.]com	January 19, 2021	-
functionalrejh[.]com	September 22, 2020	-
asfasfvcxvdbs[.]com	July 7, 2021	-

BlackBerry Assistance

If you're battling Ficker malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you providing around-the-clock support, where required, as well as local assistance. Please contact us here:

https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back