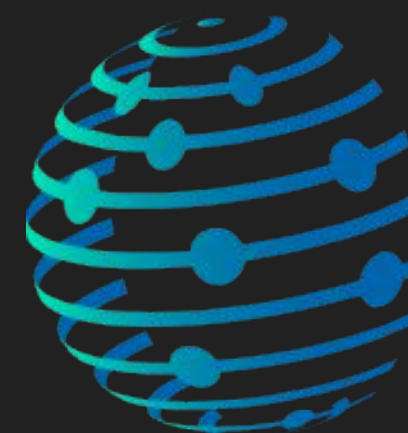


NioGuard



Security Lab



VB2020
localhost

Stealthy WastedLocker: eluding behavior blockers, but not only



Alexander Adamov, Ph.D.
Founder of NioGuard Security Lab
Teaching at NURE 🇺🇦 and BTH 🇸🇪

WastedLocker overview

- Operated by the *Evil Corp* group
- Attacked at least 31 US-based corporations since May 2020 including *Garmin* on July 23, 2020
- The ransom varies from **\$500,000 to \$10 million** in Bitcoin
- **Defense Evasion** techniques that includes *Digital Signing*, *Alternate Data Streams*, and *Lazy Writing*



The image shows three tweets from the official Garmin Twitter account (@Garmin). The first tweet, dated July 23, 2020, at 11:01 AM, states: "We are currently experiencing an outage that affects Garmin Connect, and as a result, the Garmin Connect website and mobile app are down at this time. (1/2)". It has 1K replies, 1.2K retweets, and 1.4K likes. The second tweet, also dated July 23, 2020, at 11:01 AM, continues: "This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience. (2/2)". It has 430 replies, 295 retweets, and 737 likes. The third tweet, dated July 27, 2020, at 11:01 AM, reports: "We are happy to report that many of the systems and services affected by the recent outage, including Garmin Connect, are returning to operation. Some features still have temporary limitations while all of the data is being processed." It has 692 replies, 602 retweets, and 3.6K likes.

Garmin @Garmin · Jul 23
We are currently experiencing an outage that affects Garmin Connect, and as a result, the Garmin Connect website and mobile app are down at this time. (1/2)
1K 1.2K 1.4K

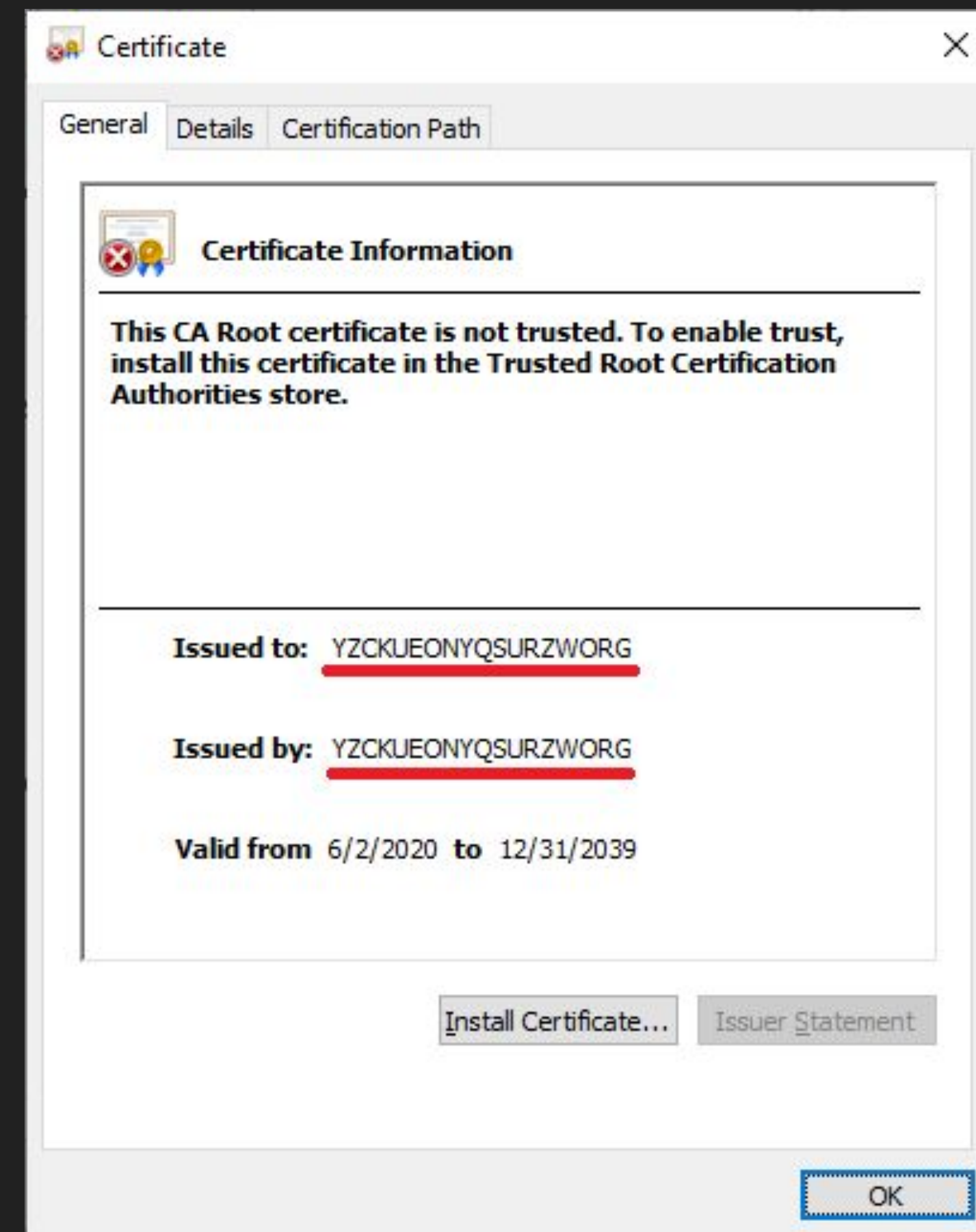
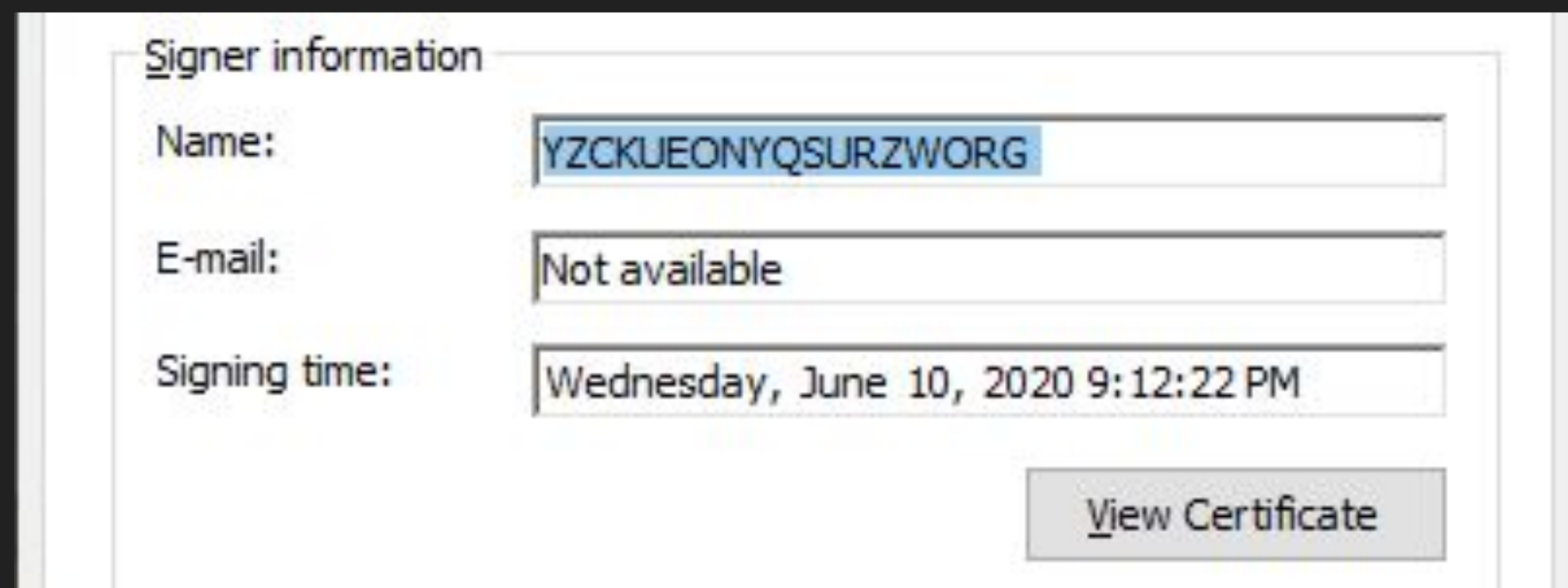
Garmin @Garmin · Jul 23
This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience. (2/2)
430 295 737

Garmin @Garmin · Jul 27
We are happy to report that many of the systems and services affected by the recent outage, including Garmin Connect, are returning to operation. Some features still have temporary limitations while all of the data is being processed.
692 602 3.6K

Defense evasion: Digital signing

Self-signed certificate

- **Issued to:** YZCKUEONYQSURZWORG
- **Issued by:** YZCKUEONYQSURZWORG
- **Valid:** June 2, 2020 - 31 December, 2039
- **Signing time:** Wednesday, June 10, 2020



Defense evasion: Alternate Data Stream

WastedLocker drops its payload to <random word>:bin stream that is not visible in the File Explorer.

```
C:\Users\IEUser\AppData\Roaming>c:\streams64.exe Join
streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\IEUser\AppData\Roaming\Join:
    :bin:$DATA 1076112
```

ida64.exe	0.19	113,196 K	4,000 K	1492	The Interactive Disassembler	Hex-Rays SA
wastedlocker.exe		2,400 K	568 K	5156	Launchy	Code Jelly
Join:bin	Susp...	1,688 K	220 K	8704	Launchy	Code Jelly
ida64.exe	0.21	137,656 K	47,968 K	8520	The Interactive Disassembler	Hex-Rays SA
procexp64.exe			48,764 K	3312	Sysinternals Process Explorer	Sysinternals - www.sysinter...
MusNotification			7,216 K	3088	MusNotificationUx.exe	Microsoft Corporation

Command Line:
 C:\Users\IEUser\AppData\Roaming\Join:bin
 Path:
 C:\Users\IEUser\AppData\Roaming\Join:bin

Defense evasion: Lazy Writing

Regular flow

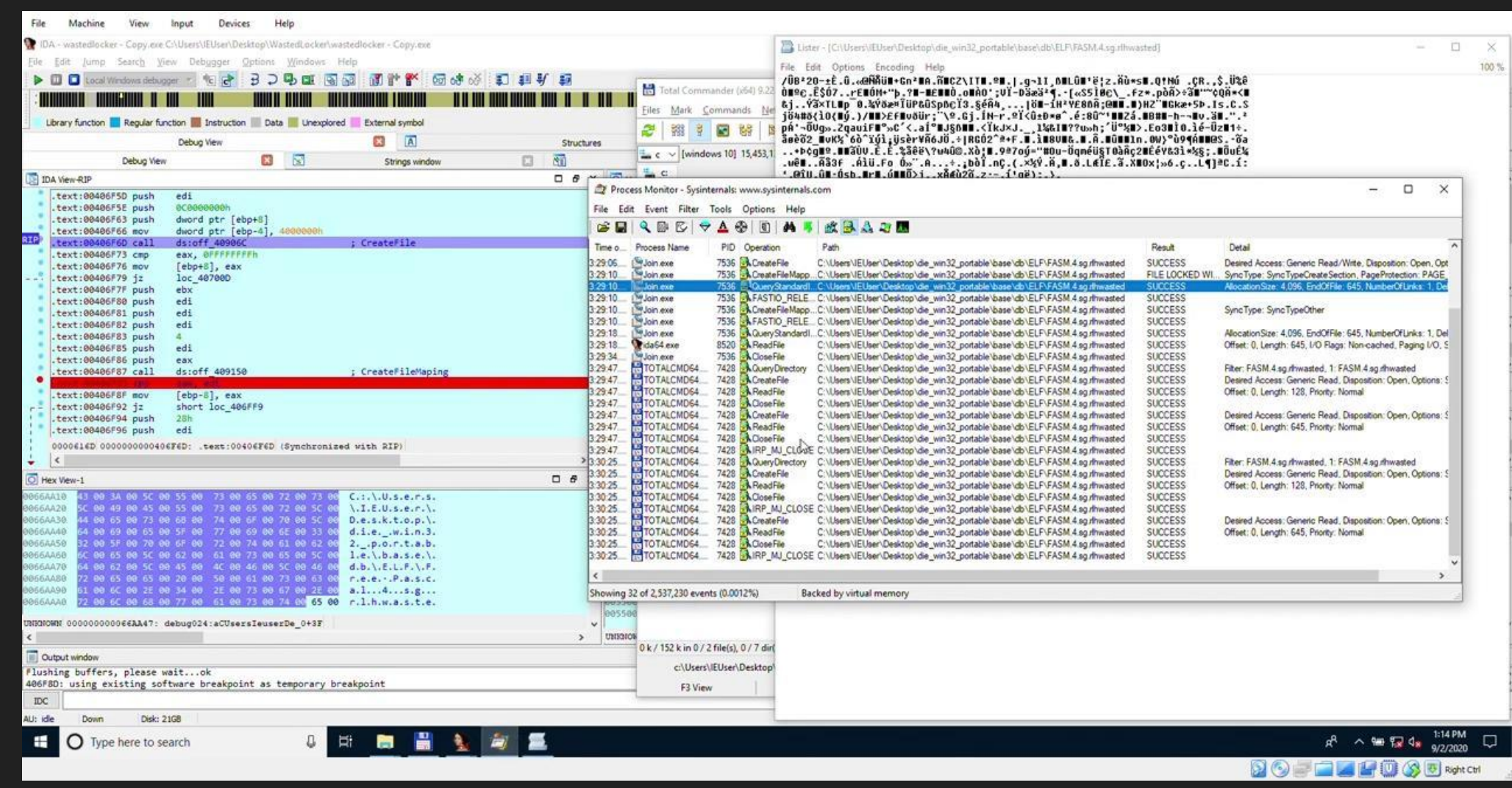
1. CreateFile() - open file
2. GetFileSize()
3. CreateFileMapping()
4. MapViewOfFile()
5. Modify mapped data
6. UnmapViewOfFile()
7. CloseHandle(file map)
8. **CloseHandle(file)**

WastedLocker way

1. CreateFile() - open file
2. GetFileSize()
3. CreateFileMapping()
4. MapViewOfFile()
5. **CloseHandle(file)**
6. Encrypt mapped data
7. UnmapViewOfFile()
8. CloseHandle(file map)

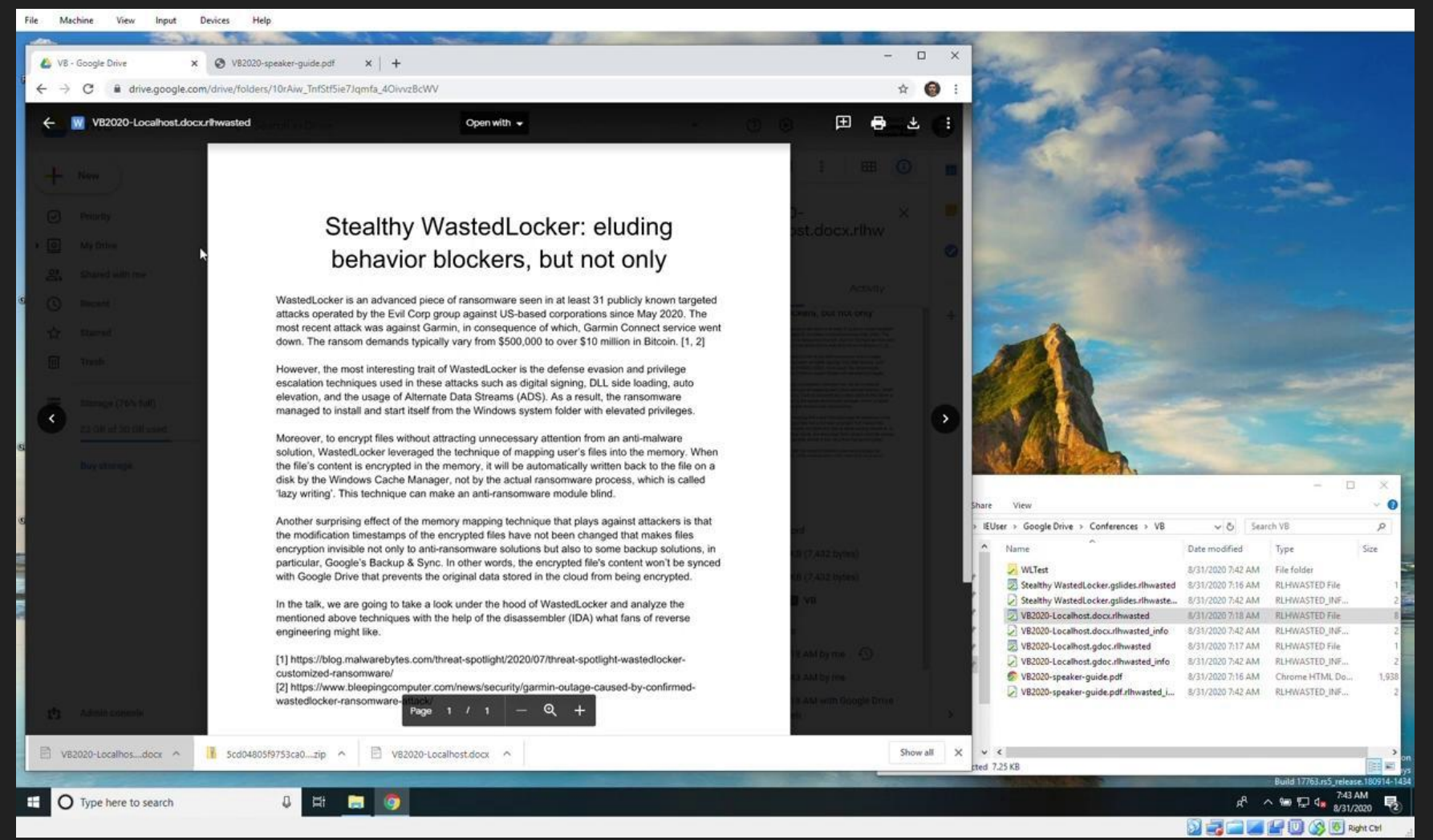
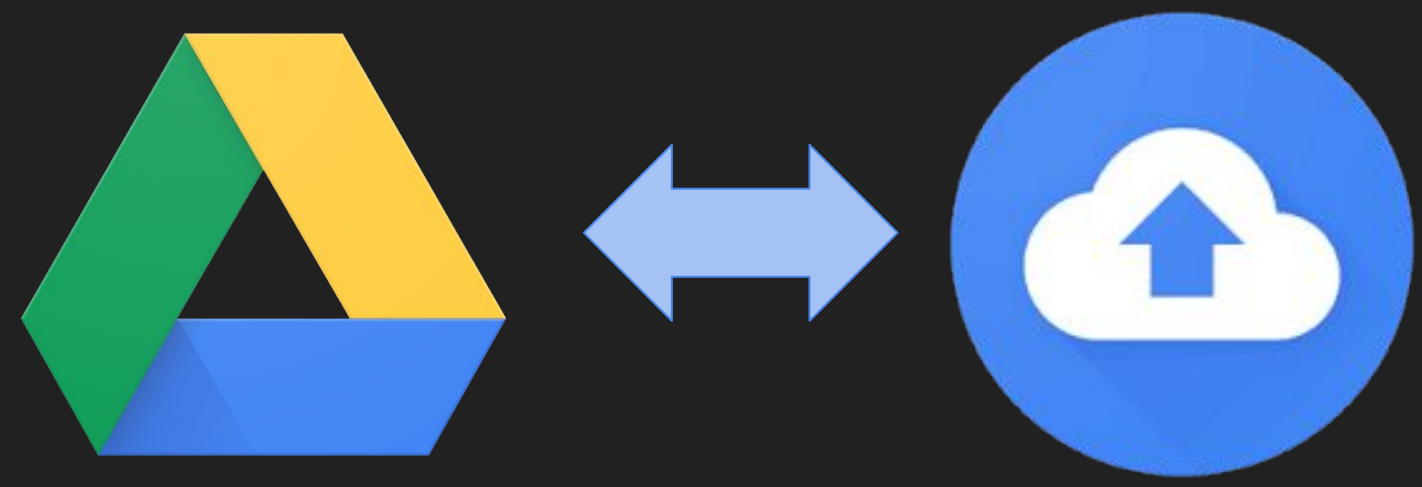


Demo: WastedLocker's Lazy Writing



The screenshot displays a Windows desktop environment. In the foreground, the IDA Pro debugger is open, showing the assembly code for a process named 'wastedlocker - Copy.exe'. The code includes instructions like 'push', 'mov', 'call', and 'jz', with a highlighted instruction: `call ds:off_4096C ; CreateFile`. Below the assembly view, the hex dump shows the corresponding machine code. In the background, the Process Monitor (ProcMon) is running, displaying a list of file operations. The operations include 'CreateFile', 'FASTIO_RELE', and 'ReadFile', with details such as 'Process Name', 'PID', 'Operation', 'Path', 'Result', and 'Detail'. The operations are performed on files in the path `C:\Users\IEUser\Desktop\ide_win32_portable\base\idb\ELF-FASM.4.sg#fhwasted`. The ProcMon window shows a 'FILE LOCKED' error for one of the operations.

WastedLocker's "Lazy Writing" can trick not only anti-ransomware guards



The screenshot shows a Windows 10 desktop environment. A web browser window is open, displaying a document titled "Stealthy WastedLocker: eluding behavior blockers, but not only". The document text includes:

Stealthy WastedLocker: eluding behavior blockers, but not only

WastedLocker is an advanced piece of ransomware seen in at least 31 publicly known targeted attacks operated by the Evil Corp group against US-based corporations since May 2020. The most recent attack was against Garmin, in consequence of which, Garmin Connect service went down. The ransom demands typically vary from \$500,000 to over \$10 million in Bitcoin. [1, 2]

However, the most interesting trait of WastedLocker is the defense evasion and privilege escalation techniques used in these attacks such as digital signing, DLL side loading, auto elevation, and the usage of Alternate Data Streams (ADS). As a result, the ransomware managed to install and start itself from the Windows system folder with elevated privileges.

Moreover, to encrypt files without attracting unnecessary attention from an anti-malware solution, WastedLocker leveraged the technique of mapping user's files into the memory. When the file's content is encrypted in the memory, it will be automatically written back to the file on a disk by the Windows Cache Manager, not by the actual ransomware process, which is called 'lazy writing'. This technique can make an anti-ransomware module blind.

Another surprising effect of the memory mapping technique that plays against attackers is that the modification timestamps of the encrypted files have not been changed that makes files encryption invisible not only to anti-ransomware solutions but also to some backup solutions, in particular, Google's Backup & Sync. In other words, the encrypted file's content won't be synced with Google Drive that prevents the original data stored in the cloud from being encrypted.

In the talk, we are going to take a look under the hood of WastedLocker and analyze the mentioned above techniques with the help of the disassembler (IDA) what fans of reverse engineering might like.

[1] <https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/>
[2] <https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware/>

A file explorer window is open in the bottom right corner, showing a folder named "VB" with several files. The files list includes:

Name	Date modified	Type	Size
WLTTest	8/31/2020 7:42 AM	File folder	
Stealthy WastedLocker.gldes.rhwasted	8/31/2020 7:16 AM	RLHWASTED File	1
Stealthy WastedLocker.gldes.rhwasted...	8/31/2020 7:42 AM	RLHWASTED_INF...	2
VB2020-Localhost.docx.rhwasted	8/31/2020 7:18 AM	RLHWASTED File	1
VB2020-Localhost.docx.rhwasted_info	8/31/2020 7:42 AM	RLHWASTED_INF...	2
VB2020-Localhost.gdoc.rhwasted	8/31/2020 7:17 AM	RLHWASTED File	1
VB2020-Localhost.gdoc.rhwasted_info	8/31/2020 7:42 AM	RLHWASTED_INF...	2
VB2020-speaker-guide.pdf	8/31/2020 7:16 AM	Chrome HTML Do...	1,938
VB2020-speaker-guide.pdf.rhwasted_...	8/31/2020 7:42 AM	RLHWASTED_INF...	2

Outcomes

1. Syncing files in real-time with a cloud storage is not a good idea.
2. Make daily/weekly backups of your data.
3. @user: Install an anti-malware solution.
4. @vendor: Test your anti-ransomware modules against these techniques before it meets a new breed of ransomware.



ada@nioguard.com



@Alex_Ad