


TLP:WHITE



利用 ProxyShell 漏洞的 勒索病毒 LockFile 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 09 月

一、事件簡介

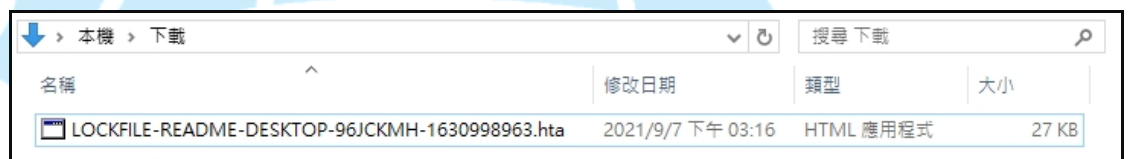
1. ProxyShell 是由臺灣安全研究員 Orange Tsai 所發現，它是三個不同安全漏洞的集合(CVE-2021-34473、CVE-2021-34523 與 CVE-2021-31207)，可用於控制 Microsoft Exchange 電子郵件伺服器。各種攻擊者正在積極利用該漏洞來破壞 Microsoft Exchange 伺服器，以植入 Web Shell 和勒索軟體。
2. ProxyShell 是 Orange Tsai 發現的三個攻擊鏈的一部分(ProxyLogon、ProxyOracle 與 ProxyShell)，而目前利用 ProxyShell 漏洞的勒索軟體有 Conti 與 Lockfile。
3. 根據 The Record by Recorded Future 報導近 2,000 台 Microsoft Exchange 電子郵件伺服器在 2021/8/20~2021/8/21 兩天內遭到駭客攻擊，並且在所有者沒有為 ProxyShell 的漏洞安裝修補程式後被後門感染。安全公司 Huntress Labs 檢測到這些攻擊是在 2021/8 月初在線上發布概念驗證漏洞利用代碼之後發生的，並於 2021/8/9~2021/8/13 那週開始掃描易受攻擊的系統。
4. 在 ProxyShell 概念驗證代碼發布兩天後，ISC SANS 於 8 月 8 日進行了一次掃描，發現總共 100,000 個系統中的 30,400 多台 Exchange 伺服器尚未修補漏洞，並且仍然容易受到攻擊。之後攻擊愈演愈烈，甚至一個名為 LockFile 的新勒索軟體也開始使用 ProxyShell 漏洞作為進入公司網路的一種方式。
5. 新的勒索軟體家族 LockFile 於 2021 年 7 月出現。它是通過利用 Microsoft Exchange 伺服器中統稱為 ProxyShell 的一系列漏洞進行散播的。這些漏洞的修補程式自 2021 年 4 月和 5 月就已經可用，但是許多組織還沒有修補他們的伺服器。自 2021 年 7 月以來，新型勒索軟體 LockFile 一直威脅著全球企業的受害者。其成功的關鍵是一些新技巧

(例如:間歇性加密)，這些技巧使反勒索軟體解決方案更難檢測到它。

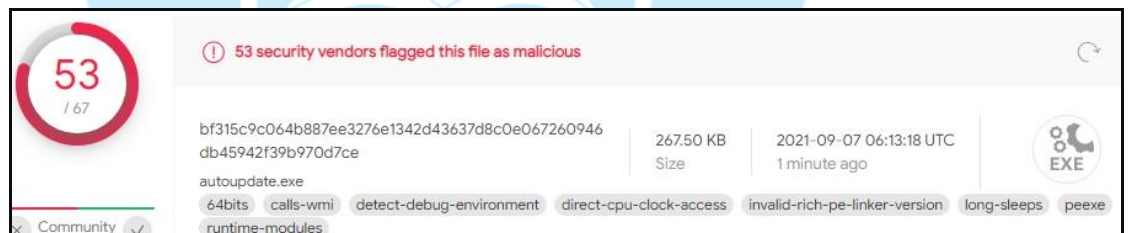
- 為了瞭解勒索軟體 LockFile 的攻擊行為，本中心取得該類型勒索軟體的樣本後進行檢測。

二、事件檢測

- 首先在 Win 10 系統上執行勒索軟體 Lockfile 樣本 autoupdate.exe (MD5: 52e1fed4c521294c5de95bba958909c1)後，產生 LOCKFILE 開頭的 hta 檔案，最後 autoupdate.exe 會消失不見，推測有內建自我刪除功能。



- autoupdate.exe 經 Virustotal 檢測其惡意比例為 53/67，有 11 家防毒軟體以 LOCKFILE 命名它。



Acronis (Static ML)	⚠ Suspicious	Ad-Aware	⚠ Trojan.GenericKD.37457318
AhnLab-V3	⚠ Ransomware/Win.LOCKFILE.C4607022	Alibaba	⚠ Ransom:Win32/LockFile.6eada94f
ALYac	⚠ Trojan.Ransom.Filecoder	Antiy-AVL	⚠ Trojan.Generic.ASMalwS.348497F
SecureAge APEX	⚠ Malicious	Arcabit	⚠ Trojan.Generic.D23B8DA6
Avast	⚠ Win64:MalwareX-gen [Trj]	AVG	⚠ Win64:MalwareX-gen [Trj]
Avira (no cloud)	⚠ HEUR/AGEN.1140227	BitDefender	⚠ Trojan.GenericKD.37457318
CAT-QuickHeal	⚠ Trojan.Win32	Comodo	⚠ Malware@#nndx3tcp74vo
CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (W)	Cylance	⚠ Unsafe

Cynet	ⓘ Malicious (score: 100)	Cyren	ⓘ W64/Trojan2.QYED
DrWeb	ⓘ Trojan.Encoder.34276	eGambit	ⓘ Unsafe.AI_Score_98%
Emnisoft	ⓘ Trojan.GenericKD.37457318 (B)	eScan	ⓘ Trojan.GenericKD.37457318
ESET-NOD32	ⓘ A Variant Of Win64/Filecoder.LockFile.A	FireEye	ⓘ Generic.mg.52e1fed4c521294c
Fortinet	ⓘ W64/Lockfile.D65F!tr.ransom	GData	ⓘ Trojan.GenericKD.37457318
Gridinsoft	ⓘ Ransom.Win64.Ransom.oa	Ikarus	ⓘ Trojan-Ransom.Lockfile
Jiangmin	ⓘ Trojan.GenericCrytor.gk	K7AntiVirus	ⓘ Trojan (005814c51)
K7GW	ⓘ Trojan (005814c51)	Kaspersky	ⓘ Trojan-Ransom.Win32.GenericCrytor.lig
Kingsoft	ⓘ Win32.Troj.Undef.(kcloud)	Lionic	ⓘ Trojan.Win32.GenericCrytor.jlc
Malwarebytes	ⓘ Ransom.LockFile	MAX	ⓘ Malware (ai Score=100)
MaxSecure	ⓘ Trojan.Malware.121028144.susgen	McAfee	ⓘ Ransom-lockfile.a
McAfee-GW-Edition	ⓘ BehavesLike.Win64.Dropper.dc	Microsoft	ⓘ Trojan:MSIL/Cryptor
NANO-Antivirus	ⓘ Trojan.Win64.GenericCrytor.izopdm	Palo Alto Networks	ⓘ Generic.ml
Panda	ⓘ Trj/CI.A	Sangfor Engine Zero	ⓘ Suspicious.Win32.Save.a
Sophos	ⓘ Mal/Generic-R = Troj/Ransom-GKF	Symantec	ⓘ Ransom.Lockfile
Tencent	ⓘ Win32.Trojan.Genericcryptor.Swur	TrendMicro	ⓘ Ransom.Win64.LOCKFILE.A
TrendMicro-HouseCall	ⓘ Ransom.Win64.LOCKFILE.A	VBA32	ⓘ Trojan.MSIL.Cryptor
ViRobot	ⓘ Trojan.Win64.S.Ransom.273920	Webroot	ⓘ W32.Ransom.Lockfile
Yandex	ⓘ Trojan.AgentCrytor!UtUSyk9Bytg	Baidu	✓ Undetected

3. 分析 autoupdate.exe 內容，得知它在 2021/8/21 完成 compiler，為很新的病毒樣本。

c:\users\ruby\downloads\autoupdate.exe	property	value
indicators (9/23)	signature	0x00004550
virustotal (53/67 - 07.09.2021)	machine	Amd64
dos-stub (!This program cannot be run in	sections	3
file-header (Aug. 2021)	compiler-stamp	0x611FECDD (Sat Aug 21 01:56:45 2021)
optional-header (suspicious)	pointer-symbol-table	0x00000000
directories (6)		

4. Autoupdate.exe 執行後會呼叫 cmd.exe 來執行 WMIC.exe，對於檔名含有特定用字的應用程序會中斷執行。之後會執行數個 mshta.exe 的腳本程序，最後會執行 cmd.exe 來刪除自己本身。

Process	Description	Command
autoupdate.exe (3320)		"C:\Users\AMY\Downloads\autoupdate.exe"
conhost.exe (164)	Console Window Host	"C:\Windows\system32\conhost.exe 0xffffffff -ForceV1"
cmd.exe (5380)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%vmwp%'" call terminate
WMIC.exe (2008)	WMI Commandline Utility	wmic process where "name like '%vmwp%'" call terminate
cmd.exe (3712)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%virtualbox%'" call terminate
WMIC.exe (1468)	WMI Commandline Utility	wmic process where "name like '%virtualbox%'" call terminate
cmd.exe (320)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%vbox%'" call terminate
WMIC.exe (376)	WMI Commandline Utility	wmic process where "name like '%vbox%'" call terminate
cmd.exe (3208)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%sqlservr%'" call terminate
WMIC.exe (5072)	WMI Commandline Utility	wmic process where "name like '%sqlservr%'" call terminate
cmd.exe (3936)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%mysqld%'" call terminate
WMIC.exe (3980)	WMI Commandline Utility	wmic process where "name like '%mysqld%'" call terminate
cmd.exe (4772)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%omtsrec%'" call terminate
WMIC.exe (5444)	WMI Commandline Utility	wmic process where "name like '%omtsrec%'" call terminate
cmd.exe (3880)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%oracle%'" call terminate
WMIC.exe (4756)	WMI Commandline Utility	wmic process where "name like '%oracle%'" call terminate
cmd.exe (3552)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%tnslsnr%'" call terminate
WMIC.exe (5264)	WMI Commandline Utility	wmic process where "name like '%tnslsnr%'" call terminate
cmd.exe (900)	Windows 命令處理程式	C:\Windows\system32\cmd.exe /c wmic process where "name like '%vmware%'" call terminate
WMIC.exe (3280)	WMI Commandline Utility	wmic process where "name like '%vmware%'" call terminate
mshta.exe (4032)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5368)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5580)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5996)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5316)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5900)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (3000)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (3104)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (380)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
mshta.exe (5340)	Microsoft (R) HTML 主應用程式	mshta "C:\Users\Public\LOCKFILE-README.hta" [1E460B07-F1C3-4B2E-88BF-4E770A288AF5][1E460B07-F1C3-4B2E-88BF-4E770A288AF5]
cmd.exe (4556)	Windows 命令處理程式	cmd /c ping 127.0.0.1 -n 5 && del "C:\Users\AMY\Downloads\autoupdate.exe" && exit
conhost.exe (728)	Console Window Host	"C:\Windows\system32\conhost.exe 0xffffffff -ForceV1"
PING.EXE (3488)	TCP/IP Ping 命令	ping 127.0.0.1 -n 5

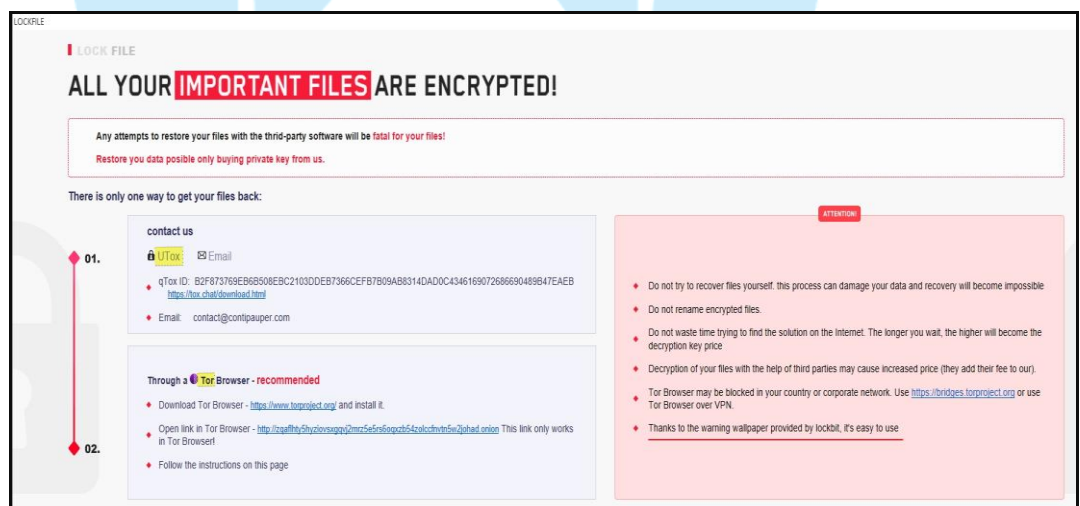
5. Autoupdate.exe 執行後，桌面會出現

LOCKFILE-README-DESKTOP-96JCKMH-1630998963.hta 的畫面

(LOCKFILE-README-[hostname]-[id].hta)。駭客告訴受害者可以透過

Utox 或 Tor 的管道與他們聯絡，也感謝 lockbit 提供易用的警告模板。

此 HTA Ransom note 是一個 HTML 的應用程式，與一般常見的 TXT 格式的 Ransom note 不同。此 Ransom note 與 LockBit 2.0 勒索軟體使用的 Ransom note 非常相似。



6. 在 Ransom note 中 LockFile 要求受害者聯繫特定的電子郵件地址，所使

用網域名「contipauper.com」是在 2021/8/16 被建立。

contact us

🔒 UTox ✉ Email

♦ qTox ID: B2F873769EB6B508EBC2103DDEB7366CEFB7B09AB8314DAD0C4346169072686690489B47EAEB
<https://tox.chat/download.html>

♦ Email: contact@contipauper.com

Domain Information

Name: CONTIPAUPER.COM

Registry Domain ID: 2634168640_DOMAIN_COM-VRSN

Domain Status:
[clientTransferProhibited](#)

Nameservers:
NS1.DNSOWL.COM
NS2.DNSOWL.COM
NS3.DNSOWL.COM

Dates

Registry Expiration: 2022-08-16 15:32:29 UTC

Created: 2021-08-16 15:32:29 UTC

7. 使用 Tor 瀏覽器開啟駭客所提供網址後，看到與 Ransom note 相同內容的網頁。

LOCKFILE

🔍 zqaflthyShyzlovsxgqj2mrz5e5rs6oqzb54zoccfmtn5w2johad.onion

LOCK FILE

ALL YOUR IMPORTANT FILES ARE ENCRYPTED!

Any attempts to restore your files with the third-party software will be fatal for your files!
Restore your data possible only buying private key from us.

There is only one way to get your files back:

01. contact us

🔒 UTox ✉ Email

♦ qTox ID: B2F873769EB6B508EBC2103DDEB7366CEFB7B09AB8314DAD0C4346169072686690489B47EAEB
<https://tox.org/>

♦ Email: contact@contipauper.com

02. Through a Tor Browser - recommended

♦ Download Tor Browser - <https://www.torproject.org/> and install it.

♦ Open link in Tor Browser - <http://zqaflthyShyzlovsxgqj2mrz5e5rs6oqzb54zoccfmtn5w2johad.onion>
This link only works in Tor Browser!

♦ Follow the instructions on this page

ATTENTION!

- Do not try to recover files yourself. this process can damage your data and recovery will become impossible
- Do not rename encrypted files.
- Do not waste time trying to find the solution on the Internet. The longer you wait, the higher will become the decryption key price
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our).
- Tor Browser may be blocked in your country or corporate network. Use <https://bridges.torproject.org> or use Tor Browser over VPN.
- Thanks to the warning wallpaper provided by lockbit, it's easy to use

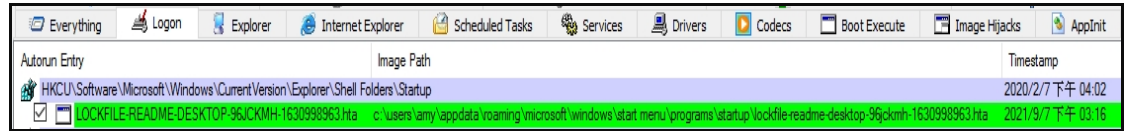
8. Autoupdate.exe 執行後會呼叫 mshta.exe 執行放在 public 資料夾內的 LOCKFILE-README.hta。

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Command Line	VirusTotal
mshta.exe		14,892 K	2,948 K	5316	Microsoft (R) HTML 主應用程式	Microsoft Corporation	mshta "C:\Users\Public\LOCKFILE-README.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}	0/74

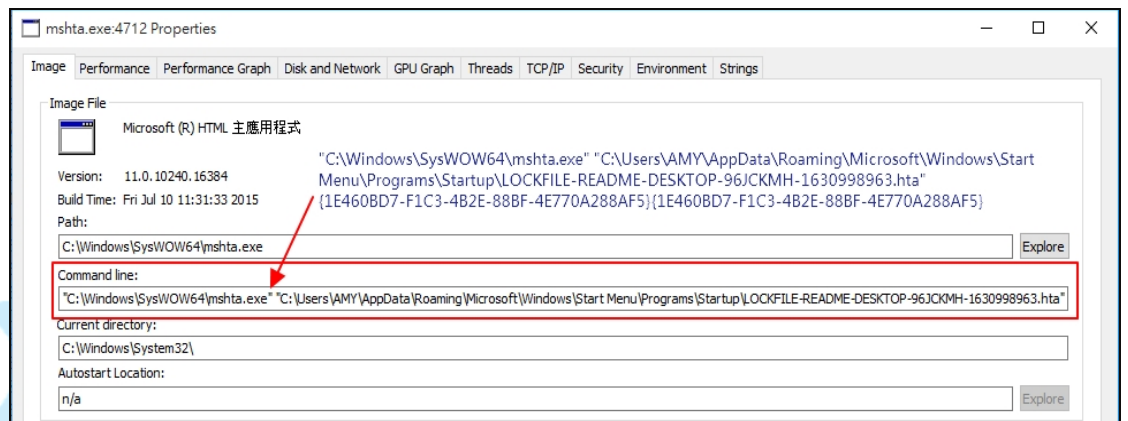
9. Autoupdate.exe 執行後會修改登錄檔，將

LOCKFILE-README-[hostname]-[id].hta 設定為每次開機啟動。

(修改登錄檔後如下圖)



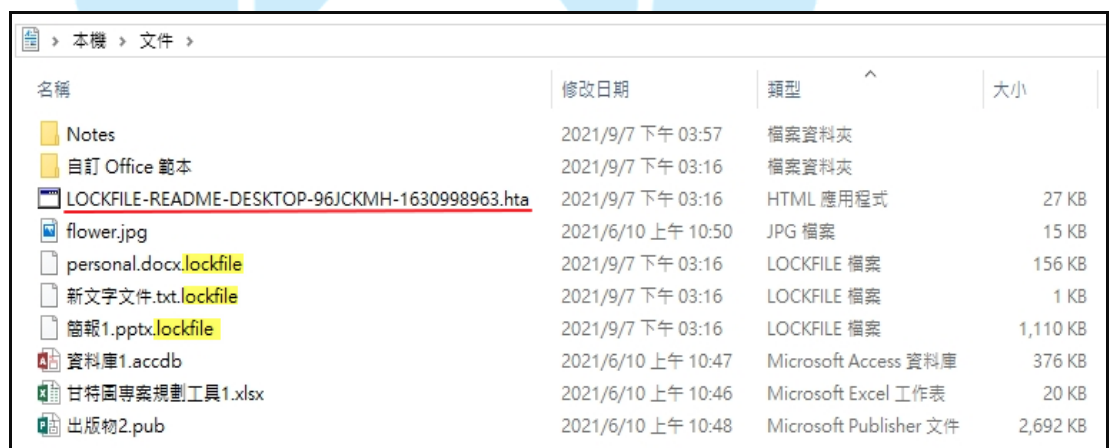
(重開機後啟動 mshta.exe 程式來執行 hta 腳本如下圖)



10. 檢視主機被加密情形，發現該勒索軟體只對特定檔案格式進行加密，

例如:.docx、.txt、.pptx。該勒索軟體不會攻擊 JPG 圖像文件，比如

照片。被加密的檔案會延伸出副檔名為 lockfile。



名稱	修改日期	類型	大小
AnyDesk	2021/9/7 下午 03:16	檔案資料夾	
Common Files	2021/9/7 下午 03:16	檔案資料夾	
EEEE.adb	2020/12/10 上午 10:03	ADB 檔案	0 KB
NTUSER.DAT	2009/7/14 下午 01:32	DAT 檔案	758 KB
GGG.hdb	2020/12/10 上午 10:20	HDB 檔案	0 KB
LOCKFILE-README-DESKTOP-96JCKMH-1630998963.hta	2021/9/7 下午 03:16	HTML 應用程式	27 KB
dfsdfs.itdb	2020/12/10 上午 11:30	ITDB 檔案	0 KB
Tulips.jpg	2009/7/14 下午 01:32	JPG 檔案	607 KB
dsfsdf.json	2020/12/10 上午 11:31	JSON 檔案	0 KB
GGGHHJ.json	2020/12/10 上午 10:44	JSON 檔案	0 KB
FF.kdb	2020/12/10 上午 10:04	KDB 檔案	0 KB
Chrysanthemum.lib	2009/7/14 下午 01:32	LIB 檔案	859 KB
Koala.lib	2009/7/14 下午 01:32	LIB 檔案	763 KB
hkhklh.4dl.lockfile	2021/9/7 下午 03:16	LOCKFILE 檔案	582 KB
hydrangeas.his.lockfile	2021/9/7 下午 03:16	LOCKFILE 檔案	582 KB
penguins.4dd.lockfile	2021/9/7 下午 03:16	LOCKFILE 檔案	761 KB
Hydaaaaa.accdc	2009/7/14 下午 01:32	Microsoft Access Sig...	763 KB
Lighthouse	2009/7/14 下午 01:32	Microsoft Access Sto...	549 KB
Hyd.accdb	2009/7/14 下午 01:32	Microsoft Access 資...	758 KB
CCCCC.opt	2020/12/10 上午 10:03	OPT 檔案	0 KB
BBBBBB.rod	2020/12/10 上午 10:02	ROD 檔案	0 KB
DDDDDDDD.sis	2020/12/10 上午 10:03	SIS 檔案	0 KB
AAAAA.sql	2020/12/10 上午 10:02	SQL 檔案	0 KB
Desert.sys	2009/7/14 下午 01:32	系統檔案	827 KB
py.exe	2017/10/3 下午 05:27	應用程式	869 KB
twain_32.dll	2019/12/7 下午 05:10	應用程式擴充	64 KB

11. LockFile 勒索軟體會對文件檔每隔 16 bytes 進行加密(間歇性加密)，這意味著文件檔保持部分可讀。間歇性加密會扭曲統計分析，並且會混淆一些保護技術。

間歇性加密有助於勒索軟體逃避某些勒索軟體保護解決方案的檢測，因為加密文件在統計上看起來與未加密的原始文件非常相似。使用 DarkSide 和 LockFile 加密相同的文件檔，之後比較 LockFile 加密後的檔案與 Darkside 加密後的檔案，會發現 LockFile 加密後的檔案與原始檔案相似(因為採用間歇性加密)，而 Darkside 加密後的檔案則與原始檔案完全不同(因為整個檔案進行加密)。這間歇性加密技巧將成功對抗勒索病毒保護軟體，而該保護軟體通過統計分析執行內容檢查以檢測加密。

personal.docx

Address	Hex	ASCII
0620h	00 00 00 00 00 00 00 00
0630h	00 00 00 00 00 00 00 00
0640h	00 00 00 00 00 00 00 00
0650h	00 00 00 00 00 00 00 00
0660h	00 00 00 00 00 00 00 00
0670h	00 00 00 00 00 00 00 00
0680h	00 00 00 00 00 00 00 00
0690h	00 00 00 00 00 00 00 00
06A0h	00 00 00 00 00 00 00 00
06B0h	00 00 00 AC 92 4D 4B 03 31 10 86 EF 82 FF 21 CC	...MK.1.ti,y!i
06C0h	BD 3B DB 2A 22 D2 DD 5E 44 E8 4D 64 FD 01 43 32	4;U*OY^DeMdy.C2

06B0h未加密
06C0h加密前

personal.docx.lockfile

LockFile加密結果如下

Address	Hex	ASCII
0620h	4D 70 FB 51 81 F5 FF 5F 47 D0 B3 E6 CD CB EB 58	MpûQ.ðý_GD'æiEeX
0630h	00 00 00 00 00 00 00 00
0640h	4D 70 FB 51 81 F5 FF 5F 47 D0 B3 E6 CD CB EB 58	MpûQ.ðý_GD'æiEeX
0650h	00 00 00 00 00 00 00 00
0660h	4D 70 FB 51 81 F5 FF 5F 47 D0 B3 E6 CD CB EB 58	MpûQ.ðý_GD'æiEeX
0670h	00 00 00 00 00 00 00 00
0680h	4D 70 FB 51 81 F5 FF 5F 47 D0 B3 E6 CD CB EB 58	MpûQ.ðý_GD'æiEeX
0690h	00 00 00 00 00 00 00 00
06A0h	4D 70 FB 51 81 F5 FF 5F 47 D0 B3 E6 CD CB EB 58	MpûQ.ðý_GD'æiEeX
06B0h	00 00 00 AC 92 4D 4B 03 31 10 86 EF 82 FF 21 CC	...MK.1.ti,y!i
06C0h	74 C6 7E 91 E2 21 4B 54 D0 6B 3F 0E E6 2A B1 76	tE~'â!KTDk?.æ*±v

06B0h未加密
06C0h加密後

personal.docx.4ae7466e

Darkside加密結果如下全加密

Address	Hex	ASCII
0620h	E2 8E BC 8D 78 7B D2 64 72 EA B0 69 53 FE 0B 48	ãZ4.x{ôdrê°iSp.H
0630h	22 42 50 99 84 83 AA 38 BA 0D 77 1D 76 9B D6 4B	"BFP™..f*8°.w.v>ôK
0640h	03 83 00 1F 75 E5 75 F2 F6 4E 87 C2 6A A6 37 C8	.f..uâuðòN+Ãj;7E
0650h	D9 AE 5A 19 4B 10 65 51 16 4B EA A3 84 47 37 E5	Ù0Z.K.eQ.KêL„G7â
0660h	37 AD 5A 54 72 DB 4A 46 9E 1A 51 71 E9 12 0B 89	7-ZTrÛJFž.Qqé..%
0670h	99 7F 59 C7 08 09 CD 71 43 9B E9 03 9C 5F C6 BB	™.YÇ..îqC>é.æ_Ex
0680h	AA 01 DA 81 3B 39 A9 57 E9 34 25 16 8D FD E2 2B	*.Ú.;9GWé4%..ýâ+
0690h	7D 8E 0E CA E2 EF BF DA 97 16 61 30 F9 6D A8 A7	}Ž.Êâi;Û-.a0ùm's
06A0h	F3 6A 70 04 2D C7 C1 A1 0D 2E 1C BC 7C F2 FC 03	ôjp.-ÇÃ;...% ôü.
06B0h	3D 20 57 DB 8B EB A8 1F 82 B8 B6 0C 83 95 E8 6F	= WÜ<ë'..,q.f*èc
06C0h	08 68 E9 7F 7B 92 B6 50 3D 01 9C 5F 63 F6 C2 43	.hé.{'QP=.æ_cûâC
06D0h	BE C9 30 FB A8 34 17 39 A3 F7 76 96 EA B4 A6 17	%E0û~4.9E÷-v-ê'.
06E0h	FB 75 FC 29 53 AC 28 D0 24 EB 51 3B 02 33 95 C0	ûuû)S-(ð\$ëQ;.3.â
06F0h	59 CD 57 12 0B 1E 67 B5 AC 73 26 6C 81 9D 4D F0	YîW...gu-s&1..Mâ
0700h	9A B9 DF 4E 08 08 28 26 52 3E 1E 22 51 87 46 91	š'âN..(sR>."Q+F\
0710h	ED 94 5F C9 E7 32 24 FD 9A 3F EC D6 C5 4D 61 AA	i" Êç2\$ýš?iÔÂMa
0720h	23 D8 C9 35 11 51 BE 93 7B 64 D5 5C 2D B6 EB 33	#0E5.Q%{dÔ\~që3

12.被加密檔案與 LOCKFILE-README-[hostname]-[id].hta 經 ID

Ransomware 勒索軟體識別網站檢測為 LockFile 勒索軟體，目前該勒索軟體仍然在被分析中。

LockFile

? This ransomware is still under analysis.

Please refer to the appropriate topic for more information.
Samples of encrypted files and suspicious files may be needed for continued investigation.

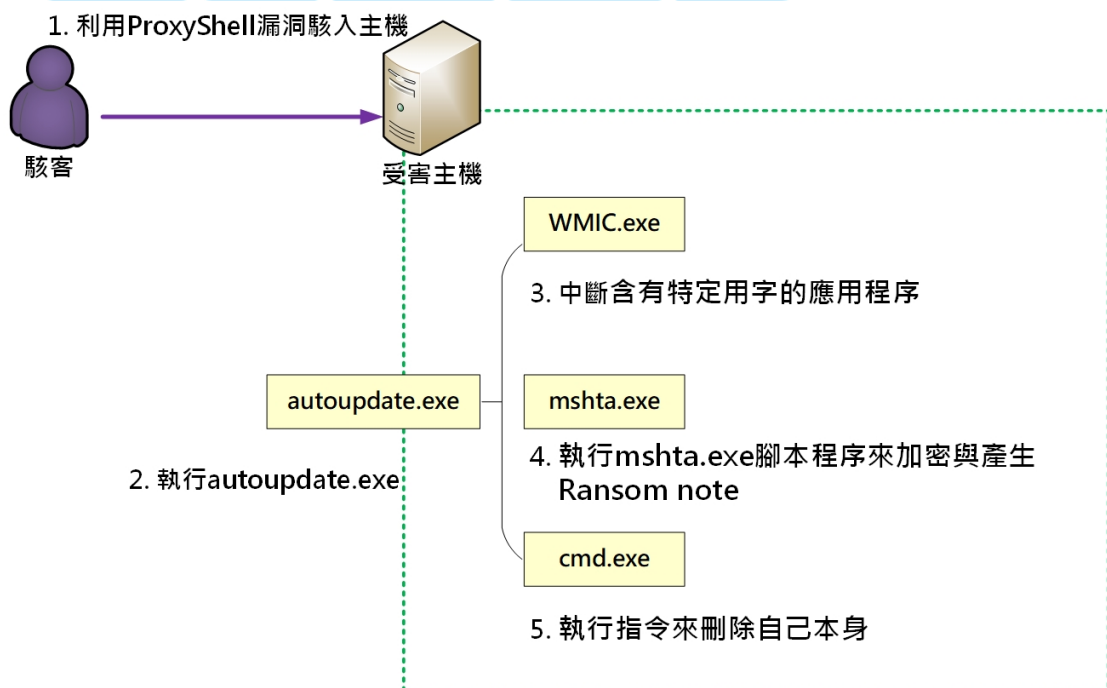
Identified by

- ransomnote_url: <http://zqaf1hty5hyziovsxcgvj2mrz5e5rs6oqxzb54zolccfnvt5w2johad.onion>
- sample_extension: .lockfile

Not enough information is public about LockFile. Please check back later.

🔔 Would you like to be notified if there is any development regarding this ransomware? [Click here.](#)

三、攻擊行為示意圖



1. 駭客利用 ProxyShell 漏洞駭入受害主機。
2. 在受害主機上執行 autoupdate.exe。
3. 呼叫 WMIC.exe 來中斷含有特定用字的應用程式。
4. 執行 mshta.exe 腳本程序來加密與產生 Ransom note。
5. 呼叫 cmd.exe 執行指令來刪除自己本身。

四、總結與建議

1. 勒索軟體 LockFile 為一種新型病毒，它與其他勒索軟體最大的差異在其使用間歇性加密來逃避檢測。
2. LockBit 2.0、DarkSide 和 BlackMatter 等其他勒索軟體使用了部分加密，僅加密檔案的開頭以加快程序，但 LockFile 的方法不同。它只加密檔案內的資料塊，而不是其完整內容。這做法加快了加密過程(資料損壞過程)，但也欺騙了依賴統計分析來檢測潛在未授權檔案加密的勒索軟體保護系統。
3. 它利用 Windows 管理界面 (WMI) 掃描並中斷與業務應用程序相關的重要程序。(包括 Hyper-V 虛擬機、Oracle VM Virtual Box 管理器、Oracle VM Virtual Box 服務、Microsoft SQL Server、MySQL 資料庫、Oracle MTS 恢復服務、Oracle RDBMS 內核、Oracle TNS 偵聽器和 VMware 虛擬機。)
4. 終止這些程序的目的是移除資料庫、虛擬機或這些應用程序放置的配置檔案上的任何系統鎖，以便勒索軟體可以加密它們。通過利用 WMI，程序將被系統本身終止，而不是由勒索軟體可執行檔案終止。這是另一種檢測規避技術，也旨在使事件響應複雜化。
5. 關於預防勒索軟體 LockFile 攻擊的資安防護措施，除了定期進行資料備份外，需修補 ProxyShell 漏洞，以防止它透過漏洞入侵主機。

五、相關參考資料

1. **ProxyShell vulnerabilities actively exploited to deliver web shells and ransomware**

<https://www.helpnetsecurity.com/2021/08/23/proxyshell-vulnerabilities-ex>

ploited/

2. Almost 2,000 Exchange servers hacked using ProxyShell exploit

<https://therecord.media/almost-2000-exchange-servers-hacked-using-proxyshell-exploit>

