Forensic Case Study

Chin Rivas

18-01-2022

Context

- Critical cyber-incident at a GAST afiliate agency
- The targeted employee was working from home.
- Nextcloud server set up in the affiliate’s network

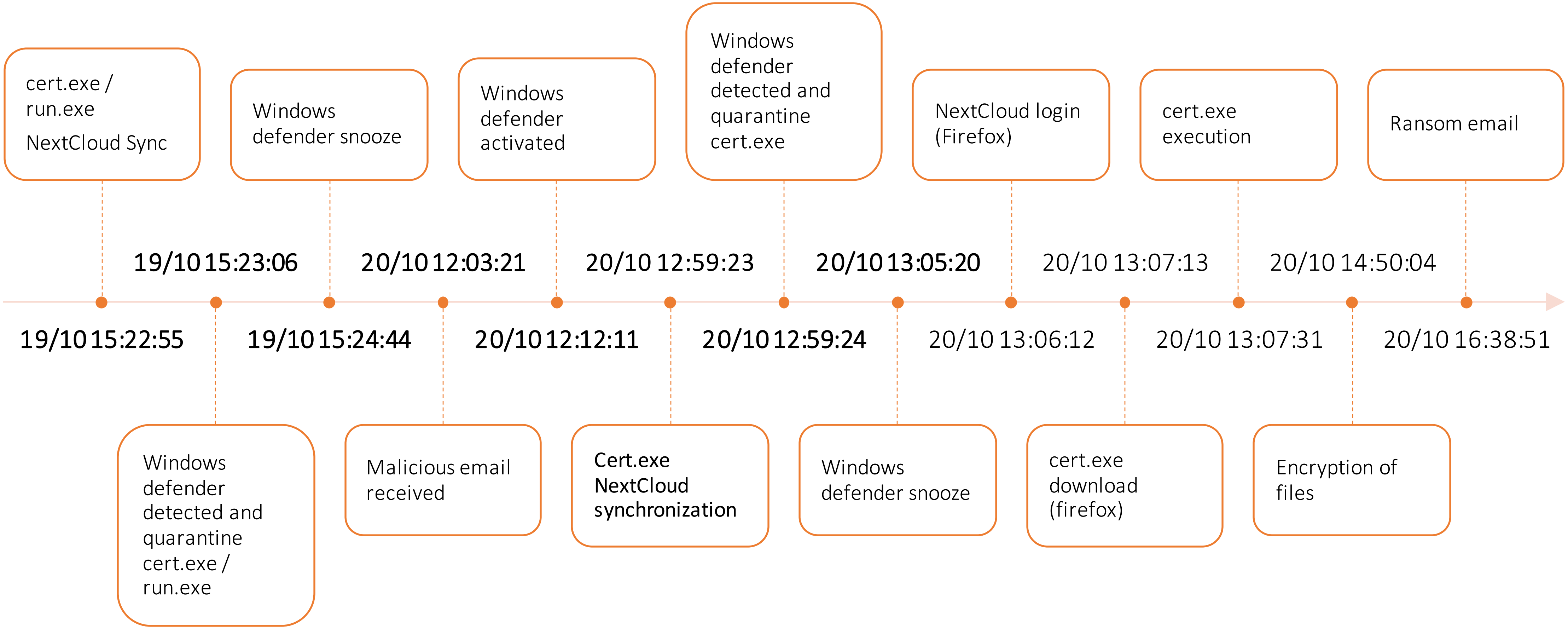
Information

- Confidential documents were obtained and then encrypted by a hacker group.
- 2021-10-20 at 16:39 - Employee received anonymous message.
- 2021-10-20 at 16:40 - Technician arrived at the workstation.
- 2021-10-20 at 16:48 – Adquisition of evidence started.
- Hard drive image of worstation is provided by the technician.

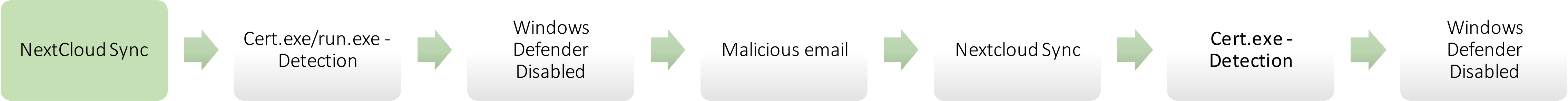
Workstation information

- Username : vagrant
- User full name: Victoria Timmers
- Account created: 2021-03-17 at 16:53:21
- Last Login: 2021-10-17 at 18:43:43

Timeline

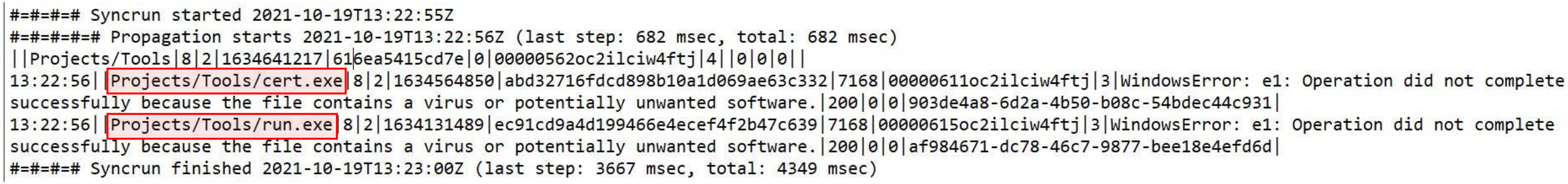


19/10 15:22:55	cert.exe / run.exe NextCloud Sync
19/10 15:23:06	Windows defender detected and quarantine cert.exe / run.exe
19/10 15:24:44	Windows defender snooze
20/10 12:03:21	Malicious email received
20/10 12:12:11	Windows defender activated
20/10 12:59:23	Cert.exe NextCloud synchronization
20/10 12:59:24	Windows defender detected and quarantine cert.exe
20/10 13:05:20	Windows defender snooze
20/10 13:06:12	NextCloud login (Firefox)
20/10 13:07:13	cert.exe download (firefox)
20/10 13:07:31	cert.exe execution
20/10 14:50:04	Encryption of files
20/10 16:38:51	Ransom email



NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → **Cert.exe - Detection** → Windows Defender Disabled

NextCloud Logs

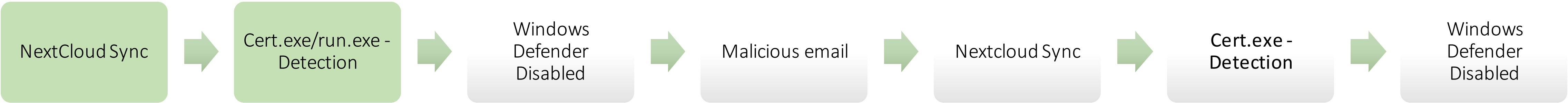


```
#=#=#=# Syncrun started 2021-10-19T13:22:55Z
#=#=#=#=# Propagation starts 2021-10-19T13:22:56Z (last step: 682 msec, total: 682 msec)
||Projects/Tools|8|2|1634641217|616ea5415cd7e|0|00000562oc2ilciw4ftj|4||0|0|0||
13:22:56||Projects/Tools/cert.exe|8|2|1634564850|abd32716fdcd898b10a1d069ae63c332|7168|00000611oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|903de4a8-6d2a-4b50-b08c-54bdec44c931|
13:22:56||Projects/Tools/run.exe|8|2|1634131489|ec91cd9a4d199466e4ecef4f2b47c639|7168|00000615oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|af984671-dc78-46c7-9877-bee18e4efd6d|
#=#=#=# Syncrun finished 2021-10-19T13:23:00Z (last step: 3667 msec, total: 4349 msec)
```

Nextcloud_sync.log

cert.exe and run.exe

October 19 at 15:22:55



NextCloud Sync

Cert.exe/run.exe - Detection

Windows Defender Disabled

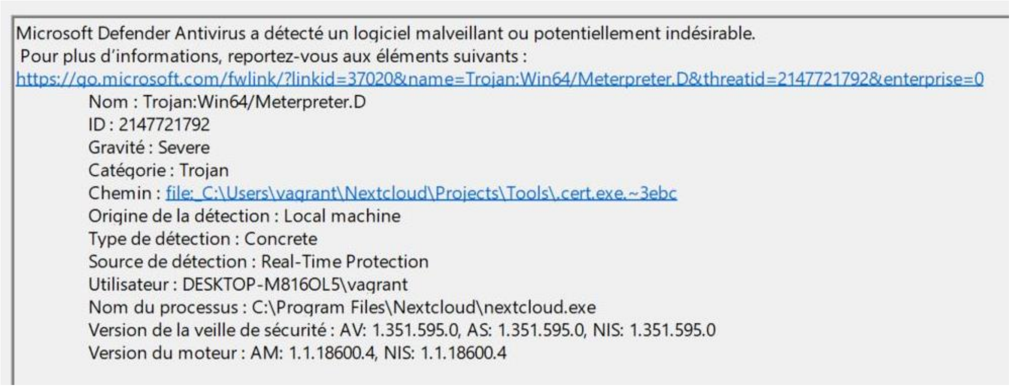
Malicious email

Nextcloud Sync

Cert.exe - Detection

Windows Defender Disabled

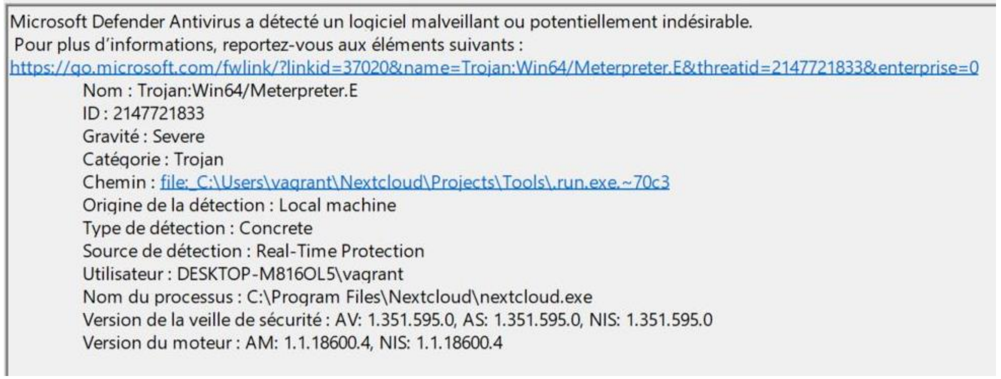
Event Logs (Windows Defender logs)



```
Microsoft Defender Antivirus a détecté un logiciel malveillant ou potentiellement indésirable.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
        Nom : Trojan:Win64/Meterpreter.D
        ID : 2147721792
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~3ebc
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : DESKTOP-M816OL5\vagrant
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Version de la veille de sécurité : AV: 1.351.595.0, AS: 1.351.595.0, NIS: 1.351.595.0
        Version du moteur : AM: 1.1.18600.4, NIS: 1.1.18600.4
```

cert.exe detection

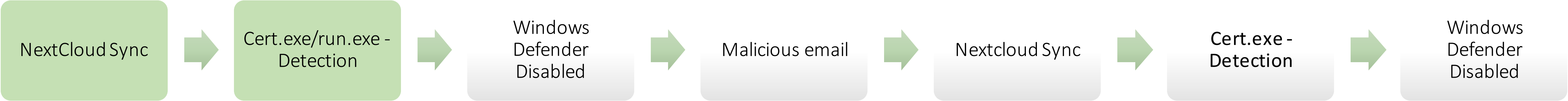
October 19 at 15:23:06



```
Microsoft Defender Antivirus a détecté un logiciel malveillant ou potentiellement indésirable.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.E&threatid=2147721833&enterprise=0
        Nom : Trojan:Win64/Meterpreter.E
        ID : 2147721833
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.run.exe.~70c3
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : DESKTOP-M816OL5\vagrant
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Version de la veille de sécurité : AV: 1.351.595.0, AS: 1.351.595.0, NIS: 1.351.595.0
        Version du moteur : AM: 1.1.18600.4, NIS: 1.1.18600.4
```

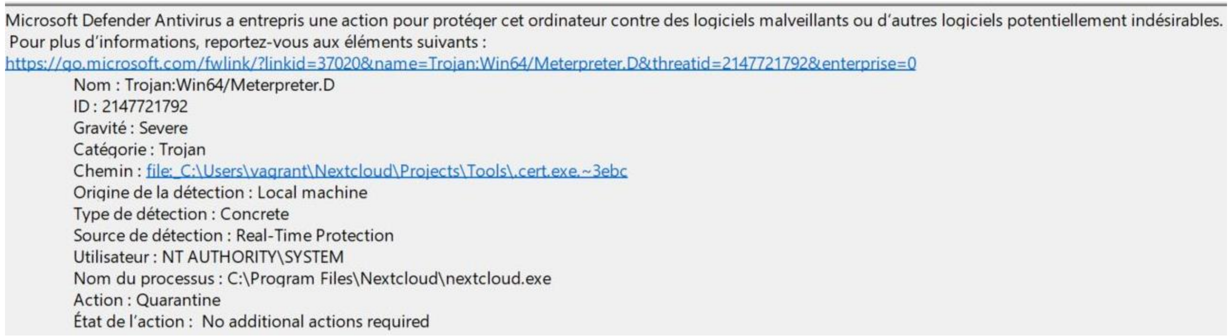
run.exe detection

October 19 at 15:23:11



NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → Cert.exe - Detection → Windows Defender Disabled

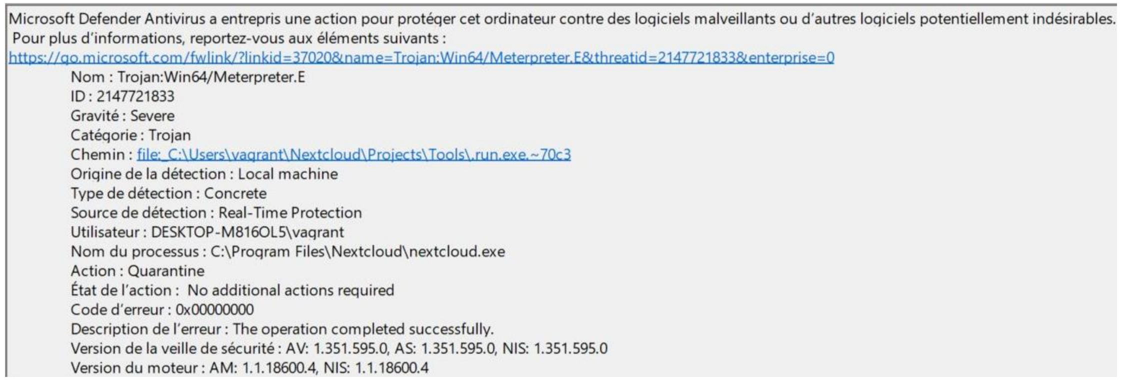
Event Logs (Windows Defender logs)



```
Microsoft Defender Antivirus a entrepris une action pour protéger cet ordinateur contre des logiciels malveillants ou d'autres logiciels potentiellement indésirables.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
        Nom : Trojan:Win64/Meterpreter.D
        ID : 2147721792
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~3ebc
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : NT AUTHORITY\SYSTEM
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Action : Quarantine
        État de l'action :  No additional actions required
```

cert.exe quarantine

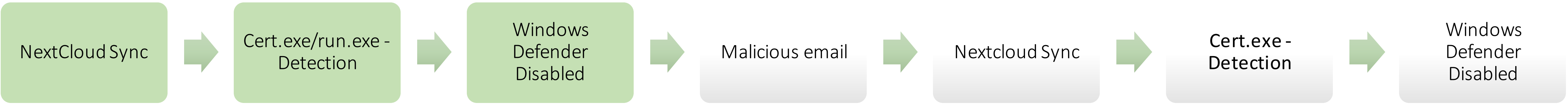
October 19 at 15:23:54



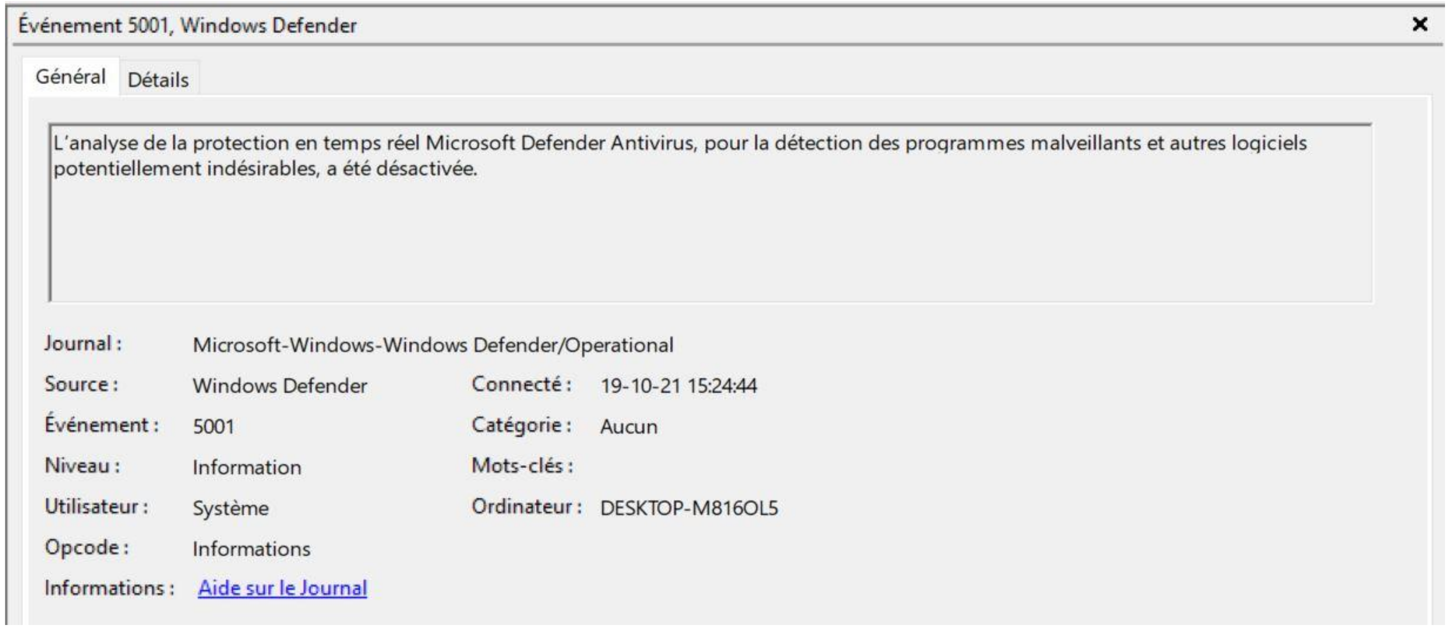
```
Microsoft Defender Antivirus a entrepris une action pour protéger cet ordinateur contre des logiciels malveillants ou d'autres logiciels potentiellement indésirables.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.E&threatid=2147721833&enterprise=0
        Nom : Trojan:Win64/Meterpreter.E
        ID : 2147721833
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.run.exe.~70c3
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : DESKTOP-M816OL5\vagrant
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Action : Quarantine
        État de l'action :  No additional actions required
        Code d'erreur : 0x00000000
        Description de l'erreur : The operation completed successfully.
        Version de la veille de sécurité : AV: 1.351.595.0, AS: 1.351.595.0, NIS: 1.351.595.0
        Version du moteur : AM: 1.1.18600.4, NIS: 1.1.18600.4
```

run.exe quarantine

October 19 at 15:24:16


NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → **Cert.exe - Detection** → Windows Defender Disabled

Event Logs (Windows Defender logs)

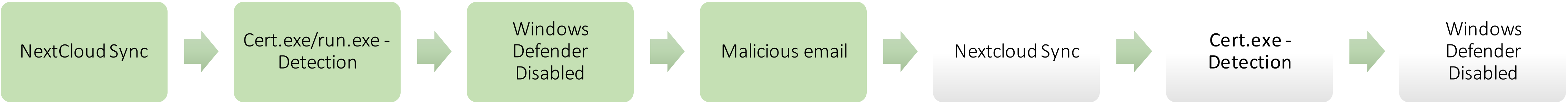

Événement 5001, Windows Defender

L'analyse de la protection en temps réel Microsoft Defender Antivirus, pour la détection des programmes malveillants et autres logiciels potentiellement indésirables, a été désactivée.

Journal :	Microsoft-Windows-Windows Defender/Operational		
Source :	Windows Defender	Connecté :	19-10-21 15:24:44
Événement :	5001	Catégorie :	Aucun
Niveau :	Information	Mots-clés :	
Utilisateur :	Système	Ordinateur :	DESKTOP-M816OL5
Opcode :	Informations		
Informations :	Aide sur le Journal		

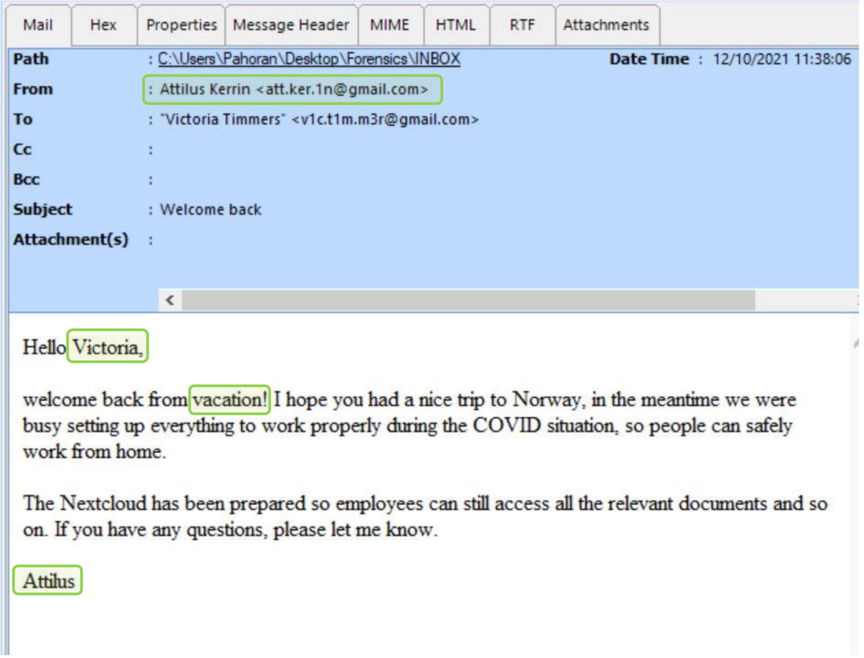
Windows Defender Disabled

October 19 at 15:24:44



NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → Cert.exe - Detection → Windows Defender Disabled

Attilus Kerrin normal email



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : C:\Users\Pahoran\Desktop\Forensics\INBOX **Date Time** : 12/10/2021 11:38:06
From : Attilus Kerrin <att.ker.1n@gmail.com>
To : "Victoria Timmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : Welcome back
Attachment(s) :

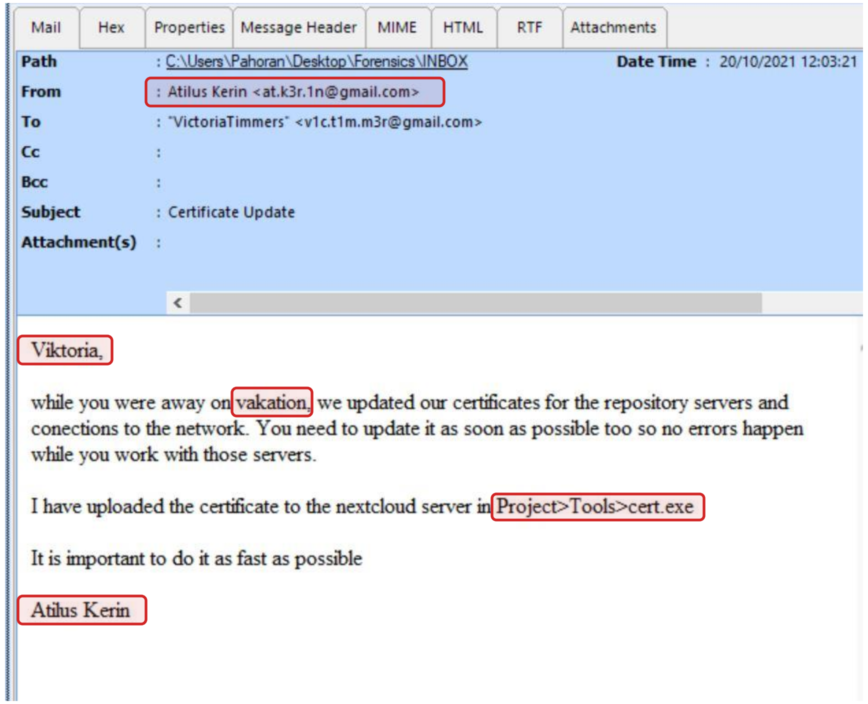
Hello Victoria,

welcome back from vacation! I hope you had a nice trip to Norway, in the meantime we were busy setting up everything to work properly during the COVID situation, so people can safely work from home.

The Nextcloud has been prepared so employees can still access all the relevant documents and so on. If you have any questions, please let me know.

Attilus

Attacker's malicious email



Mail | Hex | Properties | Message Header | MIME | HTML | RTF | Attachments

Path : C:\Users\Pahoran\Desktop\Forensics\INBOX **Date Time** : 20/10/2021 12:03:21
From : Atilus Kerin <at.k3r.1n@gmail.com>
To : "VictoriaTimmers" <v1c.t1m.m3r@gmail.com>
Cc :
Bcc :
Subject : Certificate Update
Attachment(s) :

Viktoria,

while you were away on vakation, we updated our certificates for the repository servers and conections to the network. You need to update it as soon as possible too so no errors happen while you work with those servers.

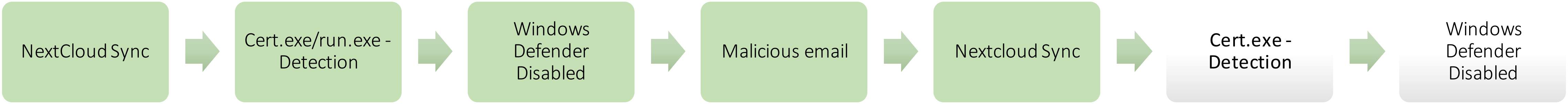
I have uploaded the certificate to the nextcloud server in Project>Tools>cert.exe

It is important to do it as fast as possible

Atilus Kerin

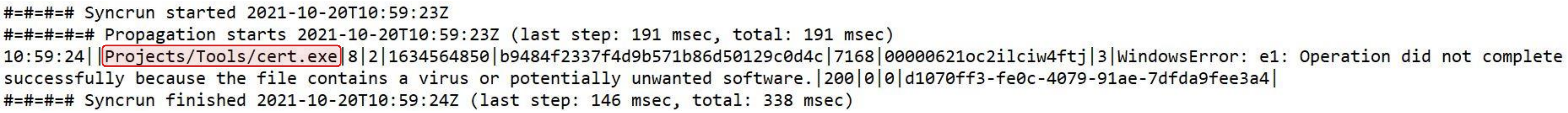
Malicious Email

October 20 at 12:03:21



NextCloud Sync
Cert.exe/run.exe - Detection
Windows Defender Disabled
Malicious email
Nextcloud Sync
Cert.exe - Detection
Windows Defender Disabled

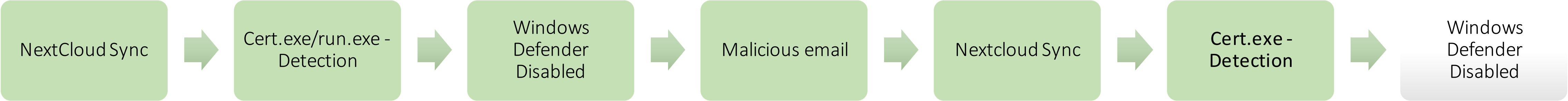
NextCloud Logs



```
#=#=#=# Syncrun started 2021-10-20T10:59:23Z
#=#=#=#=# Propagation starts 2021-10-20T10:59:23Z (last step: 191 msec, total: 191 msec)
10:59:24||Projects/Tools/cert.exe|8|2|1634564850|b9484f2337f4d9b571b86d50129c0d4c|7168|00000621oc2ilciw4ftj|3|WindowsError: e1: Operation did not complete
successfully because the file contains a virus or potentially unwanted software.|200|0|0|d1070ff3-fe0c-4079-91ae-7dfda9fee3a4|
#=#=#=# Syncrun finished 2021-10-20T10:59:24Z (last step: 146 msec, total: 338 msec)
```

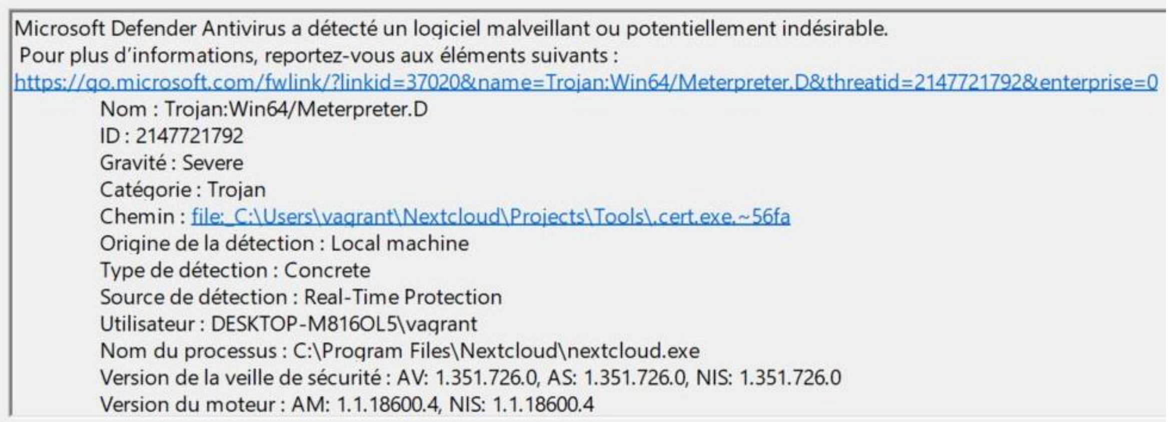
cert.exe

October 20 at 12:59:23



NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → **Cert.exe - Detection** → Windows Defender Disabled

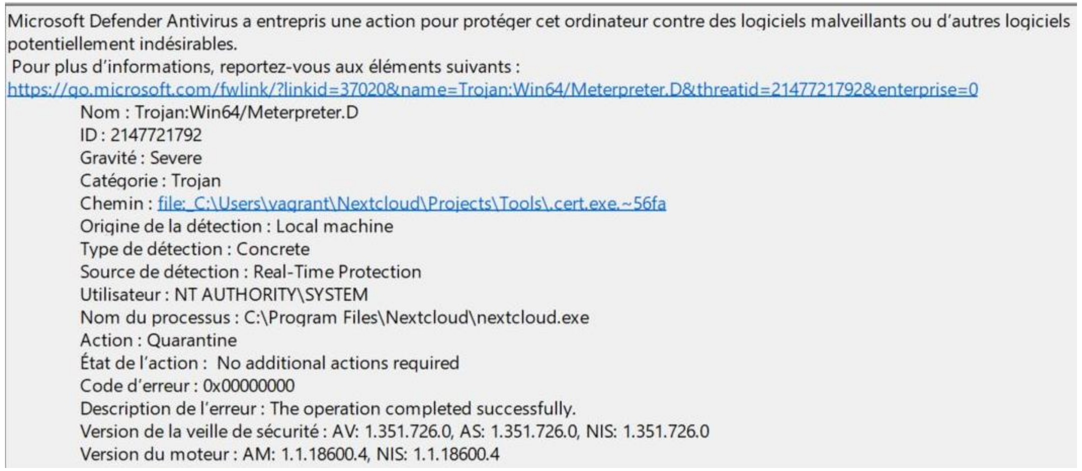
Event Logs (Windows Defender logs)



```
Microsoft Defender Antivirus a détecté un logiciel malveillant ou potentiellement indésirable.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
        Nom : Trojan:Win64/Meterpreter.D
        ID : 2147721792
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~56fa
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : DESKTOP-M816OL5\vagrant
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Version de la veille de sécurité : AV: 1.351.726.0, AS: 1.351.726.0, NIS: 1.351.726.0
        Version du moteur : AM: 1.1.18600.4, NIS: 1.1.18600.4
```

cert.exe detected

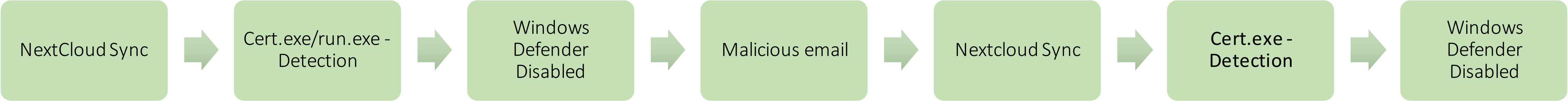
October 20 at 12:59:24



```
Microsoft Defender Antivirus a entrepris une action pour protéger cet ordinateur contre des logiciels malveillants ou d'autres logiciels
potentiellement indésirables.
 Pour plus d'informations, reportez-vous aux éléments suivants :
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win64/Meterpreter.D&threatid=2147721792&enterprise=0
        Nom : Trojan:Win64/Meterpreter.D
        ID : 2147721792
        Gravité : Severe
        Catégorie : Trojan
        Chemin : file:_C:\Users\vagrant\Nextcloud\Projects\Tools\.cert.exe.~56fa
        Origine de la détection : Local machine
        Type de détection : Concrete
        Source de détection : Real-Time Protection
        Utilisateur : NT AUTHORITY\SYSTEM
        Nom du processus : C:\Program Files\Nextcloud\nextcloud.exe
        Action : Quarantine
        État de l'action :  No additional actions required
        Code d'erreur : 0x00000000
        Description de l'erreur : The operation completed successfully.
        Version de la veille de sécurité : AV: 1.351.726.0, AS: 1.351.726.0, NIS: 1.351.726.0
        Version du moteur : AM: 1.1.18600.4, NIS: 1.1.18600.4
```

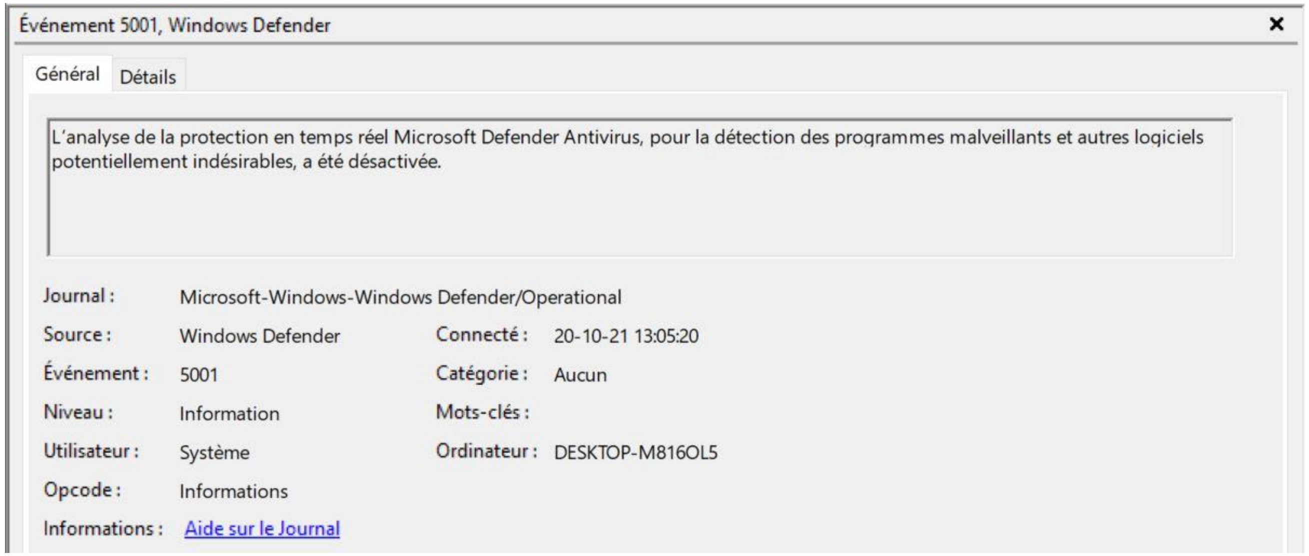
Cert.exe quarantine

October 20 at 12:59:49



NextCloud Sync → Cert.exe/run.exe - Detection → Windows Defender Disabled → Malicious email → Nextcloud Sync → **Cert.exe - Detection** → Windows Defender Disabled

Event Logs (Windows Defender logs)



Événement 5001, Windows Defender

L'analyse de la protection en temps réel Microsoft Defender Antivirus, pour la détection des programmes malveillants et autres logiciels potentiellement indésirables, a été désactivée.

Journal : Microsoft-Windows-Windows Defender/Operational

Source : Windows Defender
Connecté : 20-10-21 13:05:20

Événement : 5001
Catégorie : Aucun

Niveau : Information
Mots-clés :

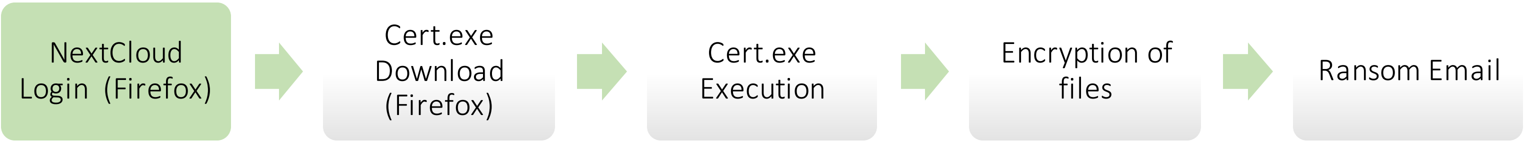
Utilisateur : Système
Ordinateur : DESKTOP-M816OL5

Opcode : Informations

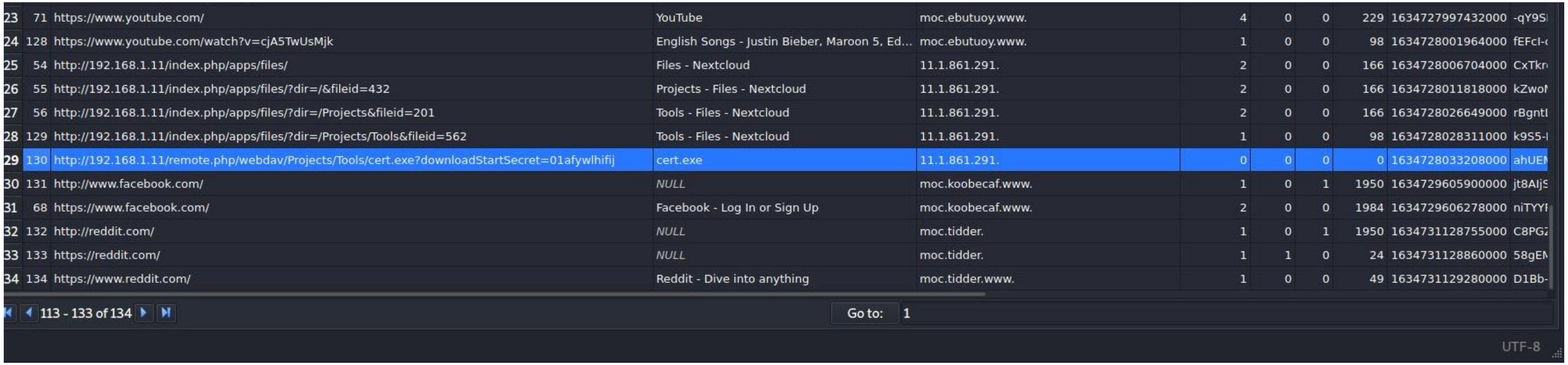
Informations : Aide sur le Journal

Windows Defender Disabled

October 10 at 13:05:20



Web Browser Forensics (Firefox)



23	71	https://www.youtube.com/	YouTube	moc.ebutuoy.www.	4	0	0	229	1634727997432000	-qY9S
24	128	https://www.youtube.com/watch?v=cjA5TwUsMjk	English Songs - Justin Bieber, Maroon 5, Ed...	moc.ebutuoy.www.	1	0	0	98	1634728001964000	fEFcl-
25	54	http://192.168.1.11/index.php/apps/files/	Files - Nextcloud	11.1.861.291.	2	0	0	166	1634728006704000	CxTkr
26	55	http://192.168.1.11/index.php/apps/files/?dir=/&fileid=432	Projects - Files - Nextcloud	11.1.861.291.	2	0	0	166	1634728011818000	kZwo
27	56	http://192.168.1.11/index.php/apps/files/?dir=/Projects&fileid=201	Tools - Files - Nextcloud	11.1.861.291.	2	0	0	166	1634728026649000	rBgntl
28	129	http://192.168.1.11/index.php/apps/files/?dir=/Projects/Tools&fileid=562	Tools - Files - Nextcloud	11.1.861.291.	1	0	0	98	1634728028311000	k9S5-l
29	130	http://192.168.1.11/remote.php/webdav/Projects/Tools/cert.exe?downloadStartSecret=01afywlhifij	cert.exe	11.1.861.291.	0	0	0	0	1634728033208000	ahUE
30	131	http://www.facebook.com/	*NULL*	moc.koobecaf.www.	1	0	1	1950	1634729605900000	jt8AljS
31	68	https://www.facebook.com/	Facebook - Log In or Sign Up	moc.koobecaf.www.	2	0	0	1984	1634729606278000	niTYY
32	132	http://reddit.com/	*NULL*	moc.tidder.	1	0	1	1950	1634731128755000	C8PG
33	133	https://reddit.com/	*NULL*	moc.tidder.	1	1	0	24	1634731128860000	58gE
34	134	https://www.reddit.com/	Reddit - Dive into anything	moc.tidder.www.	1	0	0	49	1634731129280000	D1Bb-

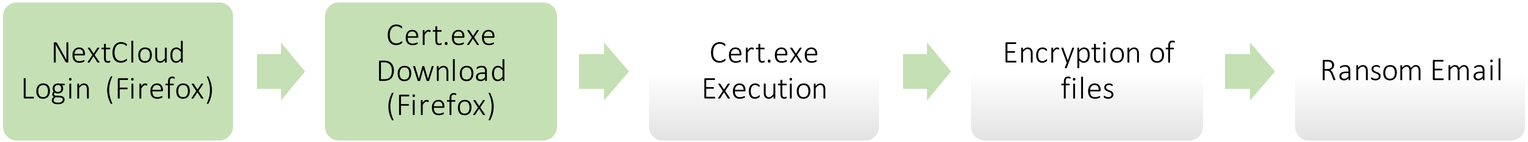
113 - 133 of 134

Go to: 1

UTF-8

NextCloud log in

October 20 at 13:06:12


NextCloud Login (Firefox)

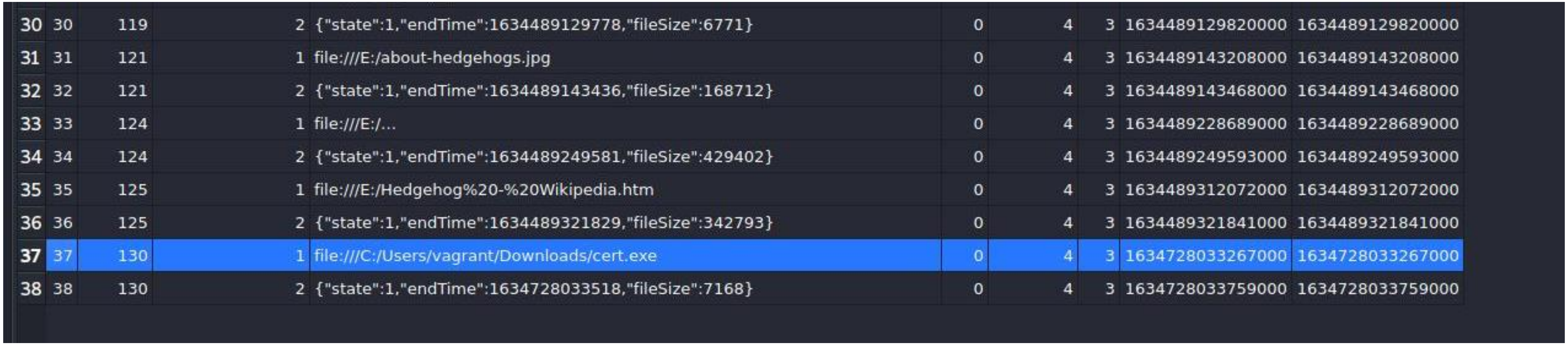
Cert.exe Download (Firefox)

Cert.exe Execution

Encryption of files

Ransom Email

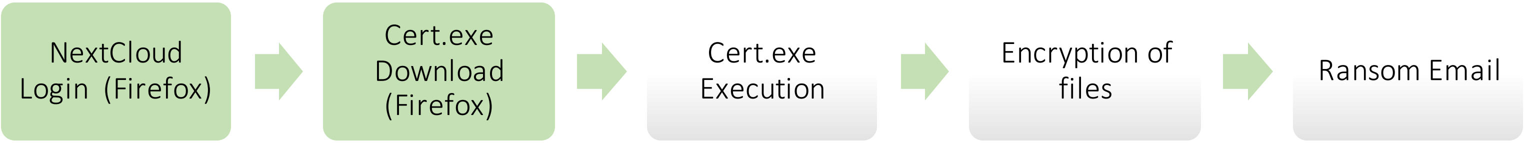
Web Browser Forensics (Firefox)



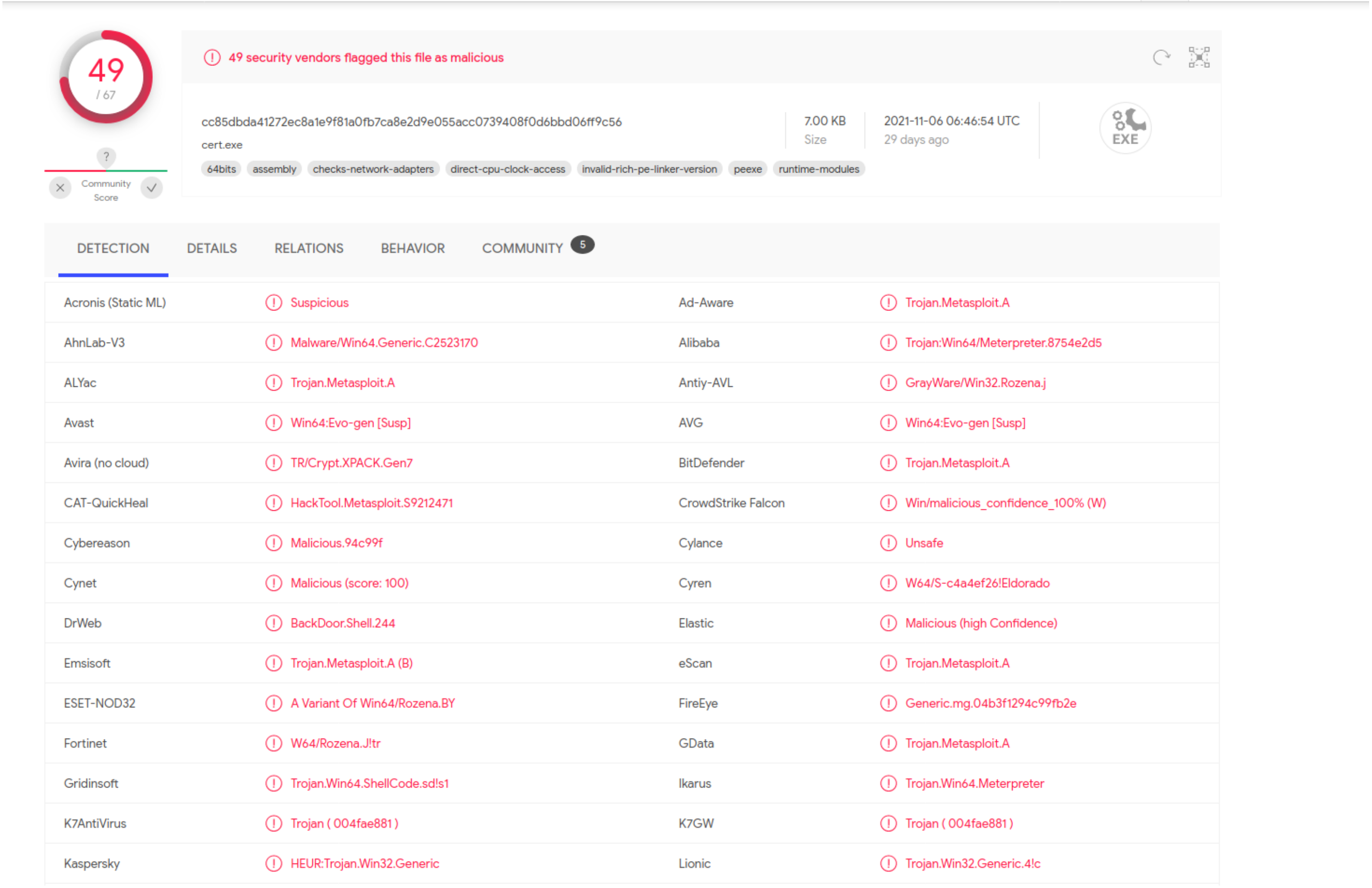
30	30	119	2	{"state":1,"endTime":1634489129778,"fileSize":6771}	0	4	3	1634489129820000	1634489129820000
31	31	121	1	file:///E:/about-hedgehogs.jpg	0	4	3	1634489143208000	1634489143208000
32	32	121	2	{"state":1,"endTime":1634489143436,"fileSize":168712}	0	4	3	1634489143468000	1634489143468000
33	33	124	1	file:///E:/...	0	4	3	1634489228689000	1634489228689000
34	34	124	2	{"state":1,"endTime":1634489249581,"fileSize":429402}	0	4	3	1634489249593000	1634489249593000
35	35	125	1	file:///E:/Hedgehog%20-%20Wikipedia.htm	0	4	3	1634489312072000	1634489312072000
36	36	125	2	{"state":1,"endTime":1634489321829,"fileSize":342793}	0	4	3	1634489321841000	1634489321841000
37	37	130	1	file:///C:/Users/vagrant/Downloads/cert.exe	0	4	3	1634728033267000	1634728033267000
38	38	130	2	{"state":1,"endTime":1634728033518,"fileSize":7168}	0	4	3	1634728033759000	1634728033759000

Download of cert.exe

October 20 at 13:07:13



cert.exe Analysis



49 / 67

Community Score

49 security vendors flagged this file as malicious

cc85dbda41272ec8a1e9f81a0fb7ca8e2d9e055acc0739408f0d6bbd06ff9c56

cert.exe

64bits assembly checks-network-adapters direct-cpu-clock-access invalid-rich-pe-linker-version peexe runtime-modules

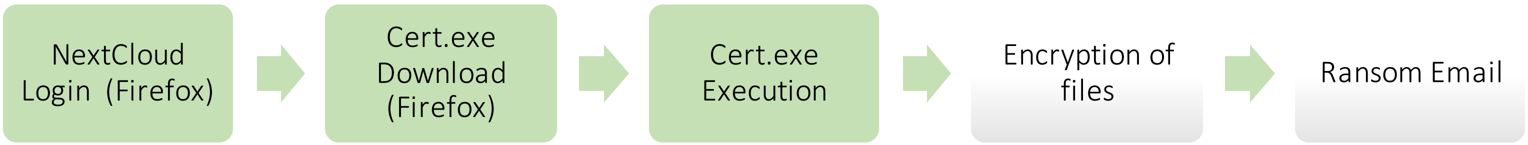
7.00 KB
Size

2021-11-06 06:46:54 UTC
29 days ago

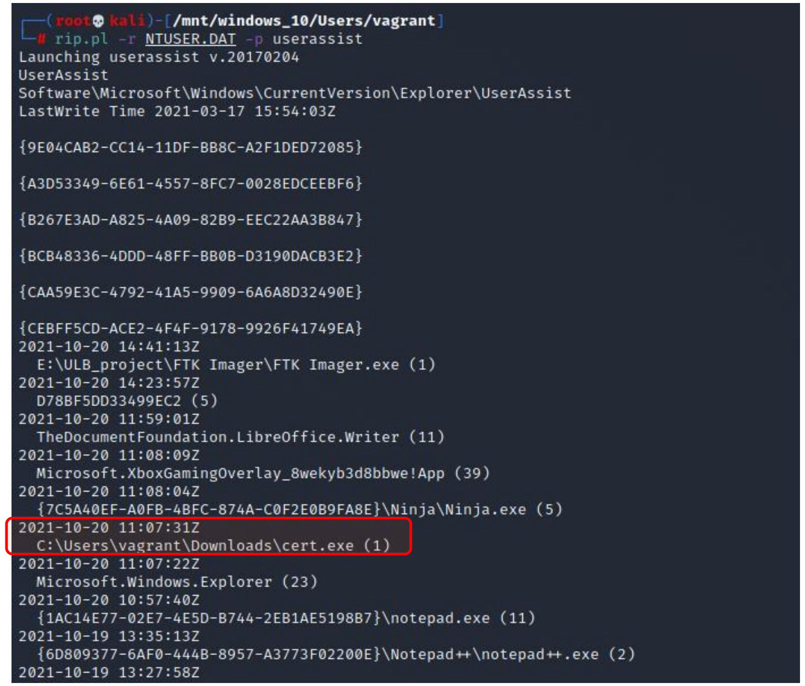
EXE

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.Metasploit.A
AhnLab-V3	Malware/Win64.Generic.C2523170	Alibaba	Trojan:Win64/Meterpreter.8754e2d5
ALYac	Trojan.Metasploit.A	Antiy-AVL	GrayWare/Win32.Rozena.j
Avast	Win64:Evo-gen [Susp]	AVG	Win64:Evo-gen [Susp]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
CAT-QuickHeal	HackTool.Metasploit.S9212471	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.94c99f	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W64/S-c4a4ef26!Eldorado
DrWeb	BackDoor.Shell.244	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Metasploit.A (B)	eScan	Trojan.Metasploit.A
ESET-NOD32	A Variant Of Win64/Rozena.BY	FireEye	Generic.mg.04b3f1294c99fb2e
Fortinet	W64/Rozena.J!tr	GData	Trojan.Metasploit.A
Gridinsoft	Trojan.Win64.ShellCode.sd!s1	Ikarus	Trojan.Win64.Meterpreter
K7AntiVirus	Trojan (004fae881)	K7GW	Trojan (004fae881)
Kaspersky	HEUR:Trojan.Win32.Generic	Lionic	Trojan.Win32.Generic.4!c

https://www.virustotal.com



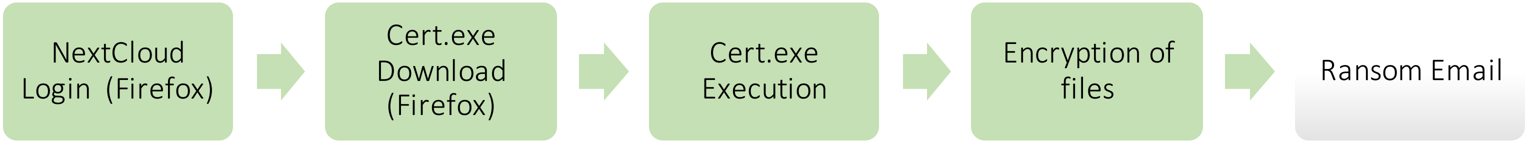
UserAssist Registry Key



```
┌──(root💀kali)-[/mnt/windows_10/Users/vagrant]
└─# rip.pl -r NTUSER.DAT -p userassist
Launching userassist v.20170204
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2021-03-17 15:54:03Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2021-10-20 14:41:13Z
  E:\ULB_project\FTK Imager\FTK Imager.exe (1)
2021-10-20 14:23:57Z
  D78BF5DD33499EC2 (5)
2021-10-20 11:59:01Z
  TheDocumentFoundation.LibreOffice.Writer (11)
2021-10-20 11:08:09Z
  Microsoft.XboxGamingOverlay_8wekyb3d8bbwe!App (39)
2021-10-20 11:08:04Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Ninja\Ninja.exe (5)
2021-10-20 11:07:31Z
  C:\Users\vagrant\Downloads\cert.exe (1)
2021-10-20 11:07:22Z
  Microsoft.Windows.Explorer (23)
2021-10-20 10:57:40Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (11)
2021-10-19 13:35:13Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Notepad++\notepad++.exe (2)
2021-10-19 13:27:58Z
```

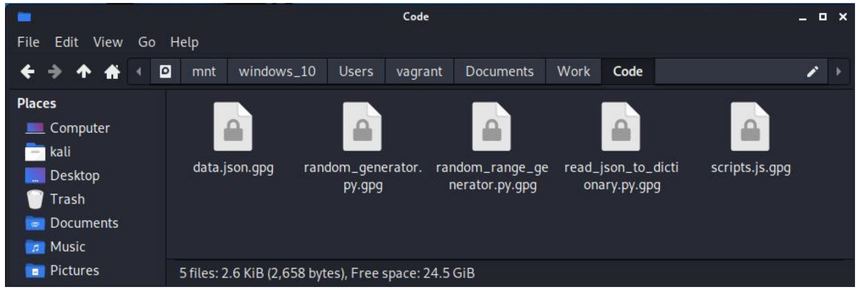
cert.exe Execution

October 20 at 13:07:31



NextCloud Login (Firefox) → Cert.exe Download (Firefox) → Cert.exe Execution → Encryption of files → Ransom Email

Encrypted files



data.json.gpg

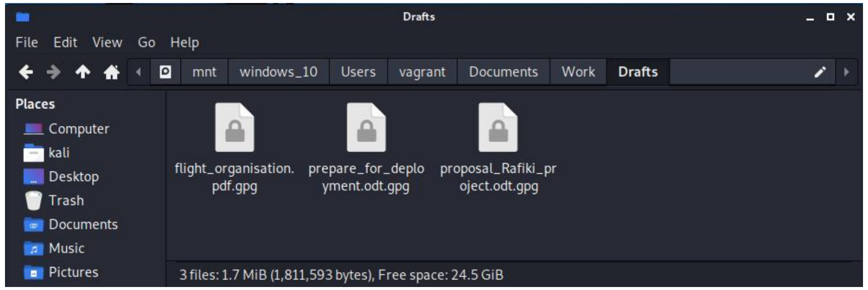
random_generator.py.gpg

random_range_generator.py.gpg

read_json_to_dictionary.py.gpg

scripts.js.gpg

5 files: 2.6 KiB (2,658 bytes), Free space: 24.5 GiB

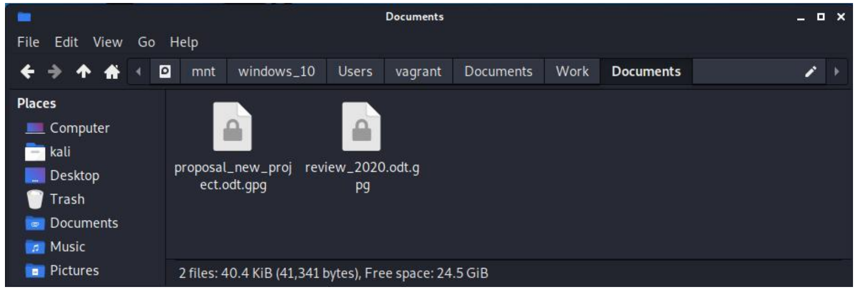


flight_organisation.pdf.gpg

prepare_for_deployment.odt.gpg

proposal_Rafiki_project.odt.gpg

3 files: 1.7 MiB (1,811,593 bytes), Free space: 24.5 GiB



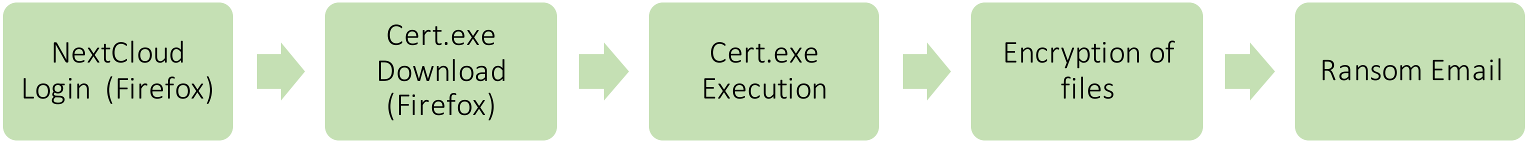
proposal_new_project.odt.gpg

review_2020.odt.gpg

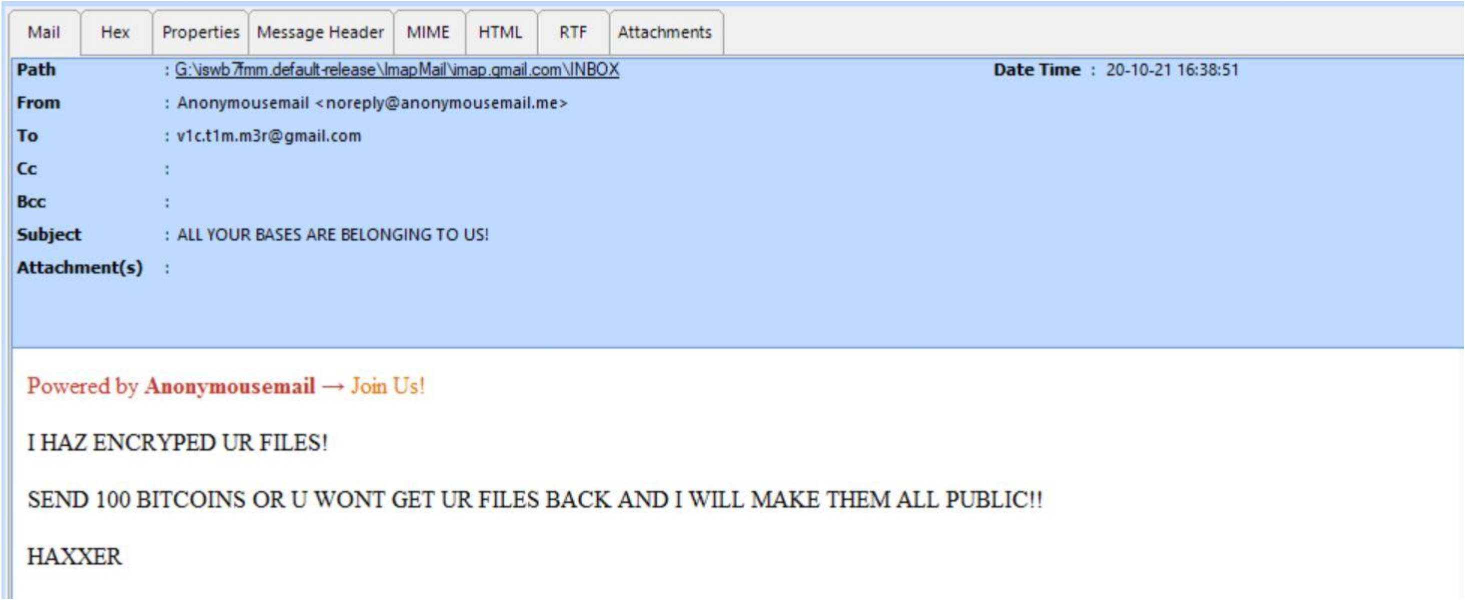
2 files: 40.4 KiB (41,341 bytes), Free space: 24.5 GiB

Encryption

October 20 at 14:50:04



Ransom email



Path : G:\iswb7fmm.default-release\ImapMail\imap.gmail.com\INBOX **Date Time** : 20-10-21 16:38:51

From : Anonymousemail <noreply@anonymousemail.me>

To : v1c.t1m.m3r@gmail.com

Cc :

Bcc :

Subject : ALL YOUR BASES ARE BELONGING TO US!

Attachment(s) :

Powered by **Anonymousemail** → Join Us!

I HAZ ENCRYPED UR FILES!

SEND 100 BITCOINS OR U WONT GET UR FILES BACK AND I WILL MAKE THEM ALL PUBLIC!!

HAXXER

October 20 at 16:38:51

What do we know about the Attacker?

- He has access to the Nextcloud server
- He has knowledge of the relationship between Victoria and Attilus Kerrin
- He knows Victoria Timmers email address

What do we know about the workstation's user?

- Disabled Windows Defender twice
- Received a malicious email from the attacker to get her to download the malware
- Log in and download the malware using the Firefox browser

Questions

- Was workstation’s user implicated in the incident?
- Was he acting responsibly and could not have prevented the incident ?
- Was he of good faith but negligent?
- Was he willfully committing sabotage?

Recommendations

- If possible, avoid giving users admin rights.
- Files uploaded to Nextcloud server should be scanned for malicious files.
- Configuration and storage of relevant Nextcloud server logs that can be used in the forensic investigation.
- Installing better email filters to minimize receiving malicious emails.

Questions?