Towards Reproducible Ransomware Analysis

CSET 2023

Shozab Hussain, Musa Waseem, Turyal Neeshat, Rja Batool, Omer Ahmed, Fareed Zaffar

LUMS

Ashish Gehani, Andy Poggio, Maneesh Yadav

SRI

Previous Work

UNVEIL (Kharaz et al., 2016)

- Identifies ransomware crypto and screenlocker binaries.
- Cuckoo Sandbox system with kernel instrumentation for capturing file I/O calls.
- Instrumented file I/O calls used to compare entropy of read and write requests from same file offset.
- Ransomware file operation sequences were found to be repetitive (open, read, write, close etc.) and distinct for different ransomware families.
- Identification of 13,637 ransomware samples out of 148,223 malware samples (3,156 labelled ransomware samples were used as ground truth).

RanSAP (Manabu et al., 2021)

- Open dataset of “low-level” disk write traces of 7 ransomware samples (from VirusTotal), 5 benign samples across several machine configurations (HDD, SDD, OS version etc.).
- Paper provides detailed descriptions of experimental setup.
- Demonstrated that ransomware can be adversarial to analysis,
- E.g., Darkside sample detecting and shutting down Minispy
- Standard ML classifiers demonstrated promising binary classification (ransomware or not) performance in seconds of activity.

  - Timestamp (s)
  - Timestamp (ms)
  - Logical Block Address (LBA) of a written sector
  - Size of a block accessed by a sample
  - Normalized Shannon entropy of a written sector

Peeler (Ahmed et al., 2021)

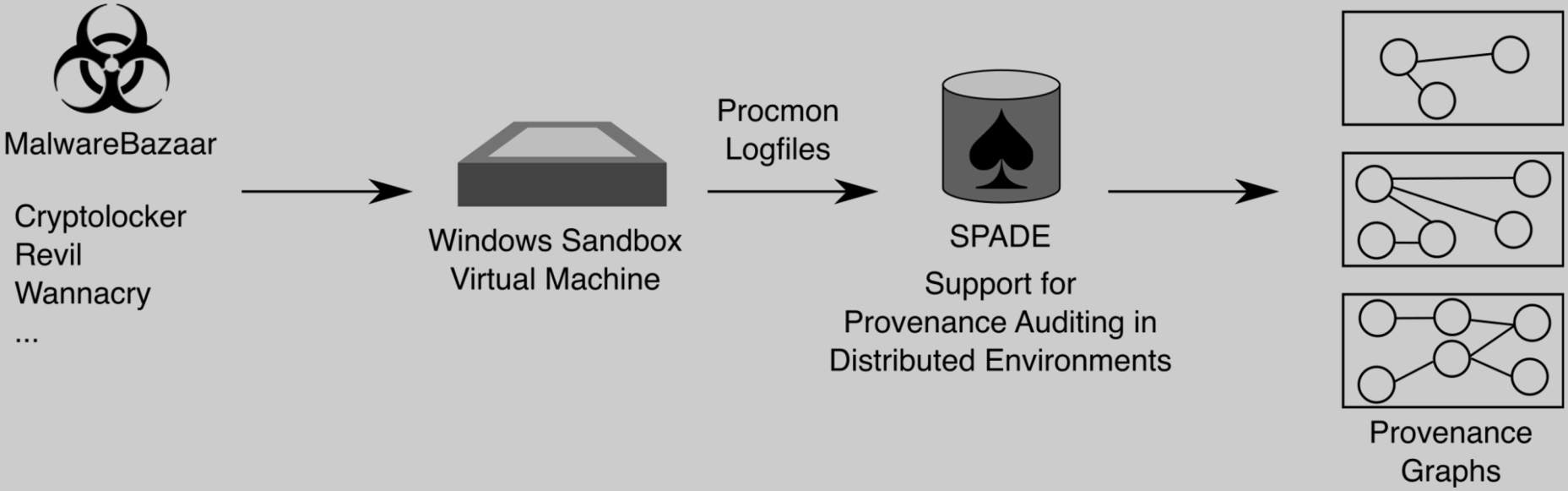
- ~28k samples were collected (primarily VirusTotal) representing 43 ransomware families and subjected to monitoring using the Peeler system.
- Benign processes that would resemble both crypto- and screenlocker-ransomware were also used as negative ground truth.
- Traces of kernel level file events were classified with a method that combined both pattern matching rules and machine learning methods.
- Compelling results: 70% of ransomware samples could be detected within 115ms of execution.

Motivation

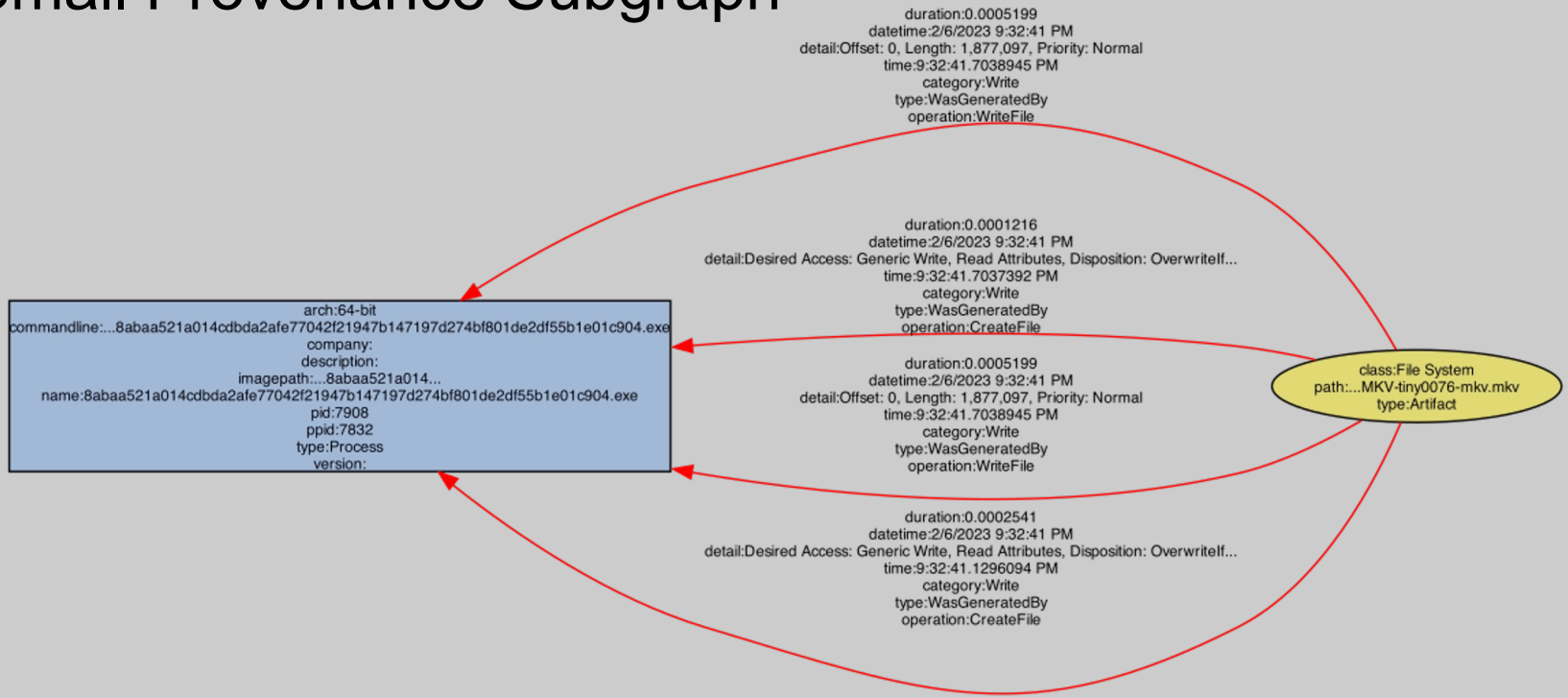
- Ransomware is a problem, look at the news on any given day.
- Malware detection/mitigation and backup methods do not appear to be entirely effective.
- There is research being done in the service of making this less of a problem.
- Assuming ransomware has successfully entered begun to encrypt the user's files, can this activity be detected before too much damage is done?
- Is there a path to apply this research to widely deployed defense? Is it possible to "stop" ransomware?

Pilot Machine Learning Study

- Setup a windows sandbox virtual machine for running ransomware binaries.
- Randomly tested binaries from Malware Bazaar to see if activity can be easily discerned manually, found 21.
- Used ProcMon was used to capture the activity of ransomware process, and then SPADE (Support for Provenance Auditing in Distributed Environments) to transform the log into a provenance graph.
- Quickgrail querying was used to extract the subgraph corresponding to the descendants of the PID (node) associated with the ransomware binary.
- File I/O events (edges) were extracted and converted into 1000 event “slices”. Slices from other PIDs were considered benign.
- Manually designed regexs show that slices could be classified as malicious/binary.
- https://github.com/REPROD-prov/REPROD-initialml


MalwareBazaar
Cryptolocker
Revil
Wannacry
...
Windows Sandbox
Virtual Machine
Procmon
Logfiles
SPADE
Support for
Provenance Auditing in
Distributed Environments
Provenance
Graphs

Small Provenance Subgraph



Malicious Slice Detection Across Samples

Regex	jigsaw	wannacry	cryptolocker	troldesh	dharma	globeimposter2	lockdown	netfilim	rapid	hive	phobos	REvil	sugar	thanos
benign1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
benign2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
benign3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
cryptolocker	0	0	256	0	0	0	4	0	0	0	0	0	0	0
cryptolocker2	0	0	256	0	0	0	4	0	0	0	0	0	0	0
dharma	0	0	0	0	15953	0	0	0	0	0	0	0	0	0
dharma2	0	0	0	0	1536	0	0	0	0	0	0	0	0	0
globeimposter2	0	0	0	0	0	57	0	0	0	0	0	0	0	0
globelmposter	0	0	0	0	0	60	0	0	0	0	0	0	0	0
hive	0	0	0	0	0	0	0	966	0	3260	0	2	0	0
hive2	0	0	0	0	0	0	0	57	0	466	0	1	0	0
jigsaw	1770	0	0	0	0	0	0	0	0	0	0	0	0	0
lockdown	0	0	0	0	0	0	41	0	0	0	0	0	0	0
nefilim2	0	0	0	0	0	0	0	13	0	0	0	0	0	0
netfilim	0	0	0	0	0	0	0	4486	0	0	0	0	0	0
phobos	0	0	0	15	0	0	0	0	0	0	3203	0	0	0
rapid	0	0	0	0	0	0	0	0	1420	0	0	0	0	0
rapid2	0	0	0	0	0	0	0	0	223	0	0	0	0	0
REvil	0	0	0	0	0	0	0	9	0	0	0	77	0	0
revil2	0	0	0	0	0	0	0	0	0	0	0	109	0	0
sugar	0	0	0	0	0	0	0	0	0	0	0	0	1194	0
sugar2	0	0	0	0	0	0	0	0	0	0	0	0	1263	0
thanos	0	0	0	0	0	0	0	0	0	0	0	0	0	74
thanos2	0	0	0	0	0	0	0	0	0	0	0	0	0	105
troldesh	0	0	0	1799	0	0	0	1094	0	0	0	0	0	0
wannacry	0	348	0	0	0	0	0	0	0	0	0	0	0	0
wannacry2	0	1811	0	0	0	0	0	0	0	0	0	0	0	0

Broad Conclusions From Pilot Study

- Fairly easy to differentiate between compression and encryption.
- Malicious file operation sequences can be picked out by eye, and regexes can be designed to pick out malicious activity with specificity.
- This is promising for machine learning approaches.

Ransomware Execution PROvenance Dataset (REPROD)

Primary REPROD Components

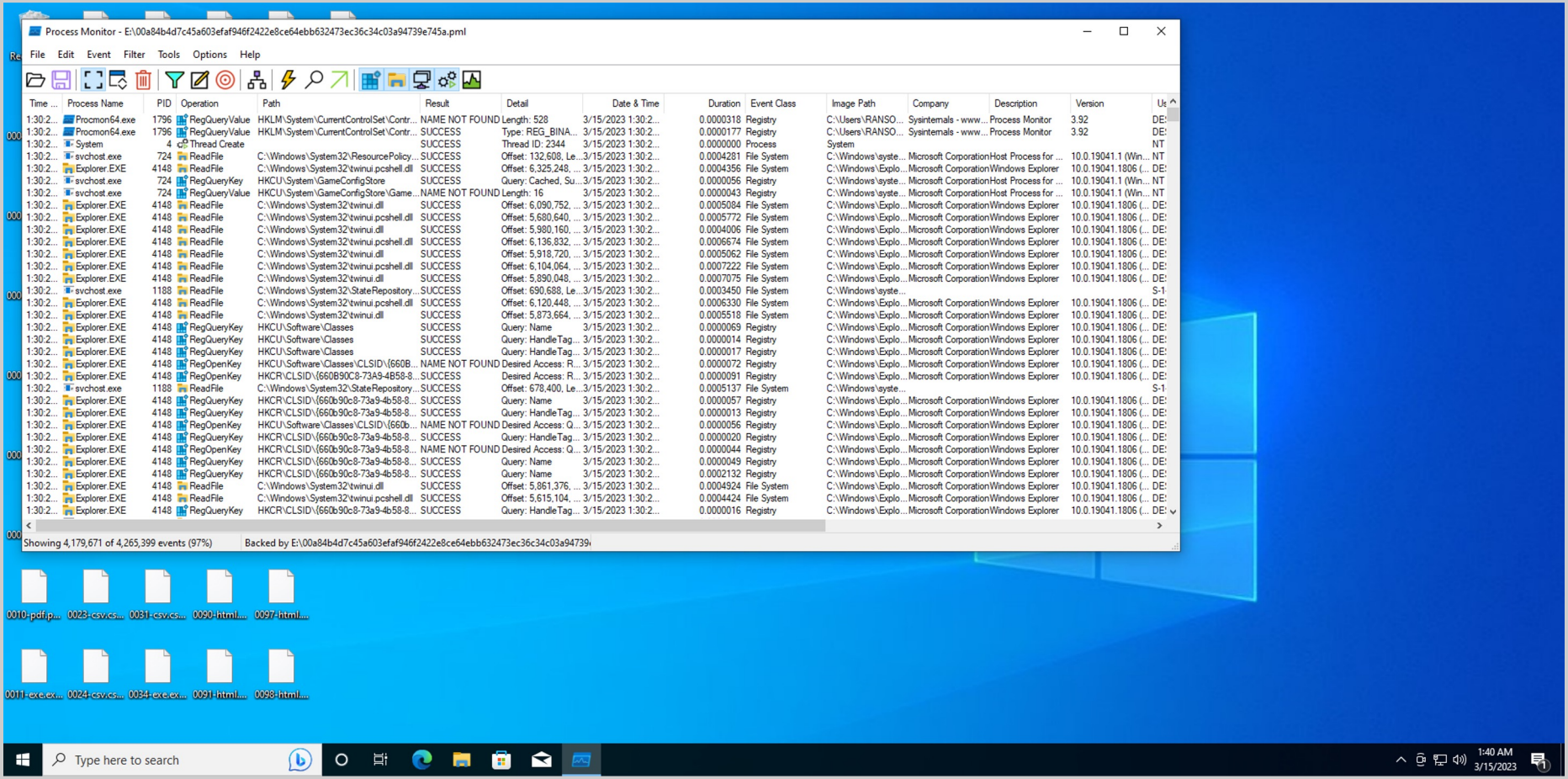
- Assembly of off-the-shelf components to automatically download ransomware-labelled binaries from Malware Bazaar (free, no registration at the time of writing), run inside a Windows sandbox virtual machine with ProcMon log collection.
- Primary Components include:
  - Python - Virtual machine scripting
  - Virtualbox - Virtual machine running
  - ProcMon - WIndows activity logging
  - SPADE - Conversion of ProcMon log files to Open Provenance Model graph (graphviz “dot” format).
  - NapierOne - Virtual machine population, honeypot files.
  - DensityScout - Measuring “density” (entropy) for selected files
- https://github.com/REPROD-prov/REPROD-workflow

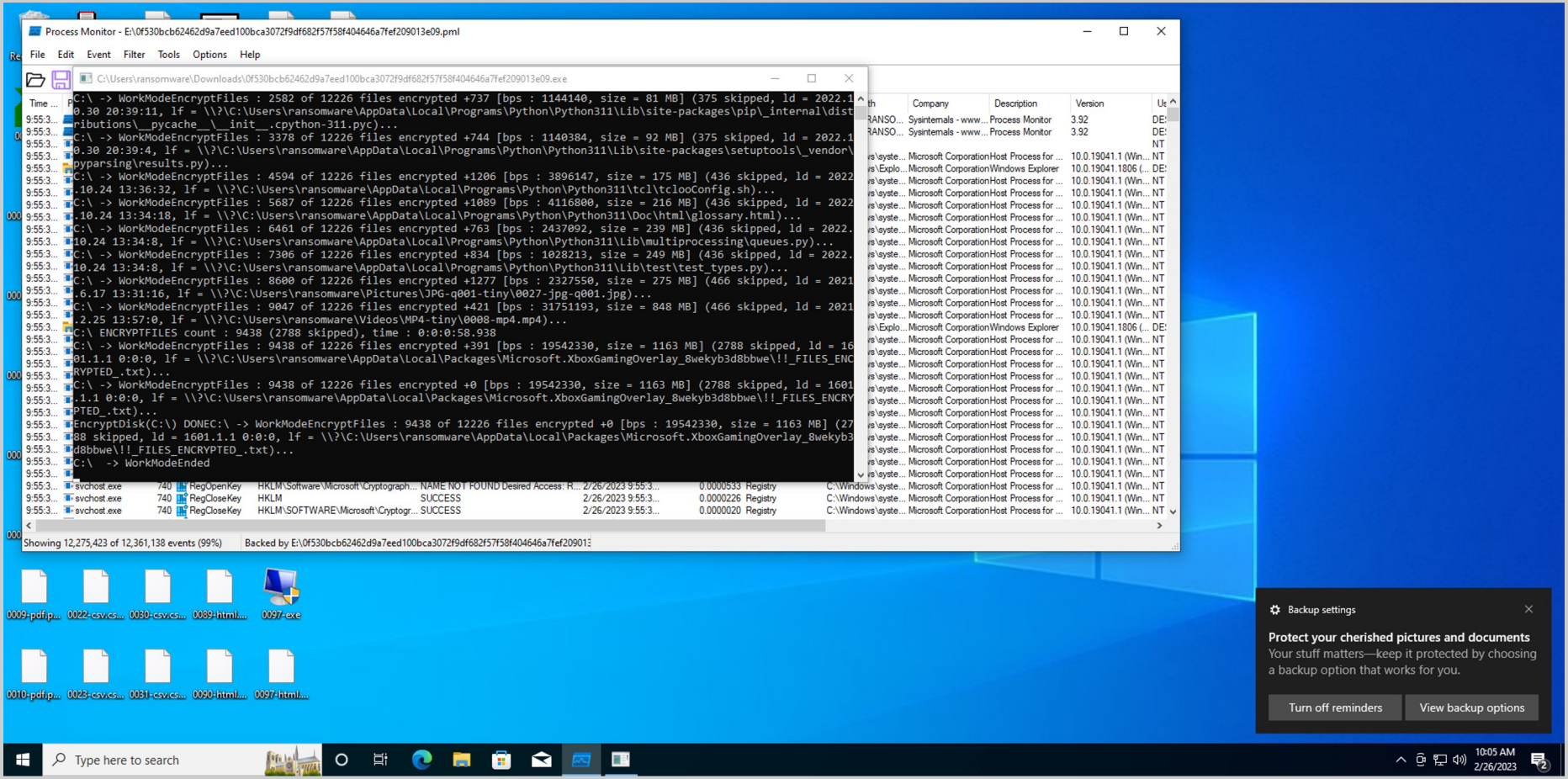
REPROD Dataset Statistics

- Number of binaries: 1,298 (all ransomware tagged binaries on Malware Bazaar)
- Ideal executions: 861 (run results in a readable ProcMon log file)
- Imperfect Timing: 316 evidence of ransomware activity (screenshot) but could not extract readable ProcMon log file
- Instrumentation Limitation: 72 unusable log that are consistent with a ProcMon termination bug, 49 cases inaccessible log with no apparent evidence of ransomware activity.
- Graphviz DOT files are provided for all 861 ideal executions. Tukey five number summaries of:
  - Node count distribution: (24, 467, 1042, 13477, 349000)
  - Edge count distribution: (54, 6192, 23125, 216729, 7766739)
- 405 ProcMon PML files are provided, 98 logs where both density changes of honeypot files and anomalous screen activity was observed, 181 logs where only density changes were seen, and 117 logs where only anomalous screen activity occurred.
- https://doi.org/10.5281/zenodo.7933806

- https://doi.org/10.5281/zenodo.7933806

Anomalous Screenshots


Process Monitor - E:\00a84b4d7c45a603efaf946f2422e8ce64ebb632473ec36c34c03a94739e745a.pml
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail Date & Time Duration Event Class Image Path Company Description Version
1:30:2... Procmon64.exe 1796 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 528 3/15/2023 1:30:2... 0.0000318 Registry C:\Users\RANSO... Sysinternals - www... Process Monitor 3.92
1:30:2... Procmon64.exe 1796 RegQueryValue HKLM\System\CurrentControlSet\Contr... SUCCESS Type: REG_BINA... 3/15/2023 1:30:2... 0.0000177 Registry C:\Users\RANSO... Sysinternals - www... Process Monitor 3.92
1:30:2... System 4 Thread Create SUCCESS Thread ID: 2344 3/15/2023 1:30:2... 0.0000000 Process System
1:30:2... svchost.exe 724 ReadFile C:\Windows\System32\ResourcePolicy... SUCCESS Offset: 132,608, Le... 3/15/2023 1:30:2... 0.0004281 File System C:\Windows\syste... Microsoft Corporation Host Process for ... 10.0.19041.1 (Win...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 6,325,248, ... 3/15/2023 1:30:2... 0.0004356 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... svchost.exe 724 RegQueryKey HKCU\System\GameConfigStore SUCCESS Query: Cached, Su... 3/15/2023 1:30:2... 0.0000056 Registry C:\Windows\syste... Microsoft Corporation Host Process for ... 10.0.19041.1 (Win...
1:30:2... svchost.exe 724 RegQueryValue HKCU\System\GameConfigStore\Game... NAME NOT FOUND Length: 16 3/15/2023 1:30:2... 0.0000043 Registry C:\Windows\syste... Microsoft Corporation Host Process for ... 10.0.19041.1 (Win...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 6,090,752, ... 3/15/2023 1:30:2... 0.0005084 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 5,680,640, ... 3/15/2023 1:30:2... 0.0005772 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,980,160, ... 3/15/2023 1:30:2... 0.0004006 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 6,136,832, ... 3/15/2023 1:30:2... 0.0006674 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,918,720, ... 3/15/2023 1:30:2... 0.0005062 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 6,104,064, ... 3/15/2023 1:30:2... 0.0007222 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,890,048, ... 3/15/2023 1:30:2... 0.0007075 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... svchost.exe 1188 ReadFile C:\Windows\System32\StateRepository... SUCCESS Offset: 690,688, Le... 3/15/2023 1:30:2... 0.0003450 File System C:\Windows\syste... S-1
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 6,120,448, ... 3/15/2023 1:30:2... 0.0006330 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,873,664, ... 3/15/2023 1:30:2... 0.0005518 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name 3/15/2023 1:30:2... 0.0000069 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag... 3/15/2023 1:30:2... 0.0000014 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCU\Software\Classes SUCCESS Query: HandleTag... 3/15/2023 1:30:2... 0.0000017 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegOpenKey HKCU\Software\Classes\CLSID\{660B... NAME NOT FOUND Desired Access: R... 3/15/2023 1:30:2... 0.0000072 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegOpenKey HKCR\CLSID\{660B90C8-73A9-4B58-8... SUCCESS Desired Access: R... 3/15/2023 1:30:2... 0.0000091 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... svchost.exe 1188 ReadFile C:\Windows\System32\StateRepository... SUCCESS Offset: 678,400, Le... 3/15/2023 1:30:2... 0.0005137 File System C:\Windows\syste... S-1
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: Name 3/15/2023 1:30:2... 0.0000057 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: HandleTag... 3/15/2023 1:30:2... 0.0000013 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegOpenKey HKCU\Software\Classes\CLSID\{660b... NAME NOT FOUND Desired Access: Q... 3/15/2023 1:30:2... 0.0000056 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: HandleTag... 3/15/2023 1:30:2... 0.0000020 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegOpenKey HKCR\CLSID\{660b90c8-73a9-4b58-8... NAME NOT FOUND Desired Access: Q... 3/15/2023 1:30:2... 0.0000044 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: Name 3/15/2023 1:30:2... 0.0000049 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: Name 3/15/2023 1:30:2... 0.0002132 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.dll SUCCESS Offset: 5,861,376, ... 3/15/2023 1:30:2... 0.0004924 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 ReadFile C:\Windows\System32\twinui.pcshell.dll SUCCESS Offset: 5,615,104, ... 3/15/2023 1:30:2... 0.0004424 File System C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
1:30:2... Explorer.EXE 4148 RegQueryKey HKCR\CLSID\{660b90c8-73a9-4b58-8... SUCCESS Query: HandleTag... 3/15/2023 1:30:2... 0.0000016 Registry C:\Windows\Explo... Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
Showing 4,179,671 of 4,265,399 events (97%)
Backed by E:\00a84b4d7c45a603efaf946f2422e8ce64ebb632473ec36c34c03a94739
0010-pdf.p... 0023-csv.cs... 0031-csv.cs... 0090-html.... 0097-html....
0011-exe.ex... 0024-csv.cs... 0034-exe.ex... 0091-html.... 0098-html....
Type here to search
1:40 AM
3/15/2023


Process Monitor - E:\0f530bcb62462d9a7eed100bca3072f9df682f57f58f404646a7fef209013e09.pml
File Edit Event Filter Tools Options Help
C:\Users\ransomware\Downloads\0f530bcb62462d9a7eed100bca3072f9df682f57f58f404646a7fef209013e09.exe
C:\ -> WorkModeEncryptFiles : 2582 of 12226 files encrypted +737 [bps : 1144140, size = 81 MB] (375 skipped, ld = 2022.1
0.30 20:39:11, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\Lib\site-packages\pip_internal\dist
ributions__pycache____init__.cpython-311.pyc)...
C:\ -> WorkModeEncryptFiles : 3378 of 12226 files encrypted +744 [bps : 1140384, size = 92 MB] (375 skipped, ld = 2022.1
0.30 20:39:4, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\Lib\site-packages\setuptools_vendor\
pyparsing\results.py)...
C:\ -> WorkModeEncryptFiles : 4594 of 12226 files encrypted +1206 [bps : 3896147, size = 175 MB] (436 skipped, ld = 2022
.10.24 13:36:32, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\tcl\tclooConfig.sh)...
C:\ -> WorkModeEncryptFiles : 5687 of 12226 files encrypted +1089 [bps : 4116800, size = 216 MB] (436 skipped, ld = 2022
.10.24 13:34:18, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\Doc\html\glossary.html)...
C:\ -> WorkModeEncryptFiles : 6461 of 12226 files encrypted +763 [bps : 2437092, size = 239 MB] (436 skipped, ld = 2022.
10.24 13:34:8, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\Lib\multiprocessing\queues.py)...
C:\ -> WorkModeEncryptFiles : 7306 of 12226 files encrypted +834 [bps : 1028213, size = 249 MB] (436 skipped, ld = 2022.
10.24 13:34:8, lf = \\?\C:\Users\ransomware\AppData\Local\Programs\Python\Python311\Lib\test\test_types.py)...
C:\ -> WorkModeEncryptFiles : 8600 of 12226 files encrypted +1277 [bps : 2327550, size = 275 MB] (466 skipped, ld = 2021
.6.17 13:31:16, lf = \\?\C:\Users\ransomware\Pictures\JPG-q001-tiny\0027-jpg-q001.jpg)...
C:\ -> WorkModeEncryptFiles : 9047 of 12226 files encrypted +421 [bps : 31751193, size = 848 MB] (466 skipped, ld = 2021
.2.25 13:57:0, lf = \\?\C:\Users\ransomware\Videos\MP4-tiny\0008-mp4.mp4)...
C:\ ENCRYPTFILES count : 9438 (2788 skipped), time : 0:0:0:58.938
C:\ -> WorkModeEncryptFiles : 9438 of 12226 files encrypted +391 [bps : 19542330, size = 1163 MB] (2788 skipped, ld = 16
01.1.1 0:0:0, lf = \\?\C:\Users\ransomware\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\!!_FILES_ENC
RYPTED_.txt)...
C:\ -> WorkModeEncryptFiles : 9438 of 12226 files encrypted +0 [bps : 19542330, size = 1163 MB] (2788 skipped, ld = 1601
.1.1 0:0:0, lf = \\?\C:\Users\ransomware\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe\!!_FILES_ENCRY
PTED_.txt)...
EncryptDisk(C:\) DONEC:\ -> WorkModeEncryptFiles : 9438 of 12226 files encrypted +0 [bps : 19542330, size = 1163 MB] (27
88 skipped, ld = 1601.1.1 0:0:0, lf = \\?\C:\Users\ransomware\AppData\Local\Packages\Microsoft.XboxGamingOverlay_8wekyb3
d8bbwe\!!_FILES_ENCRYPTED_.txt)...
C:\ -> WorkModeEnded
Company Description Version
Sysinternals - www... Process Monitor 3.92
Microsoft Corporation Host Process for ... 10.0.19041.1 (Win...
Microsoft Corporation Windows Explorer 10.0.19041.1806 (...
svchost.exe 740 RegOpenKey HKLM\Software\Microsoft\Cryptograph... NAME NOT FOUND Desired Access: R... 2/26/2023 9:55:3... 0.0000533 Registry
svchost.exe 740 RegCloseKey HKLM SUCCESS 2/26/2023 9:55:3... 0.0000226 Registry
svchost.exe 740 RegCloseKey HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS 2/26/2023 9:55:3... 0.0000020 Registry
Showing 12,275,423 of 12,361,138 events (99%)
Backed by E:\0f530bcb62462d9a7eed100bca3072f9df682f57f58f404646a7fef209013
0009-pdf.p...
0022-csv.cs...
0030-csv.cs...
0089-html....
0097-exe
0010-pdf.p...
0023-csv.cs...
0031-csv.cs...
0090-html....
0097-html....
Backup settings
Protect your cherished pictures and documents
Your stuff matters—keep it protected by choosing a backup option that works for you.
Turn off reminders
View backup options
Type here to search
10:05 AM
2/26/2023

LockBit

LOCKBIT2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

Any attempts to restore your files with the thrid-party software will be fatal for your files!
To recovery your data and not to allow data leakage, it is possible only through purchase of a private key from us

There is only one way to get your files back:

Through a standard browser

Brave (supports Tor links) FireFox Chrome Edge Opera

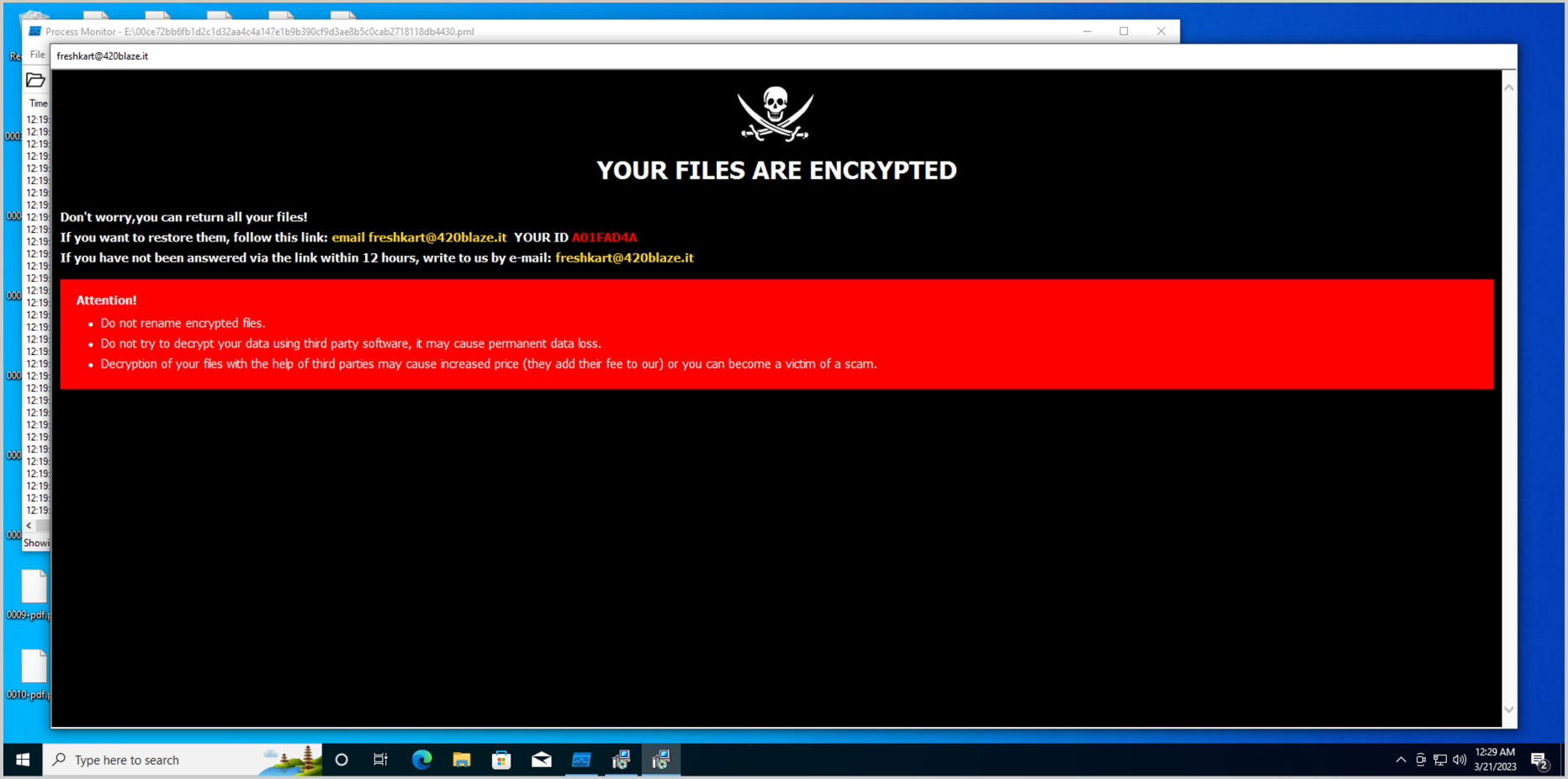
- Open link - https://decoding.at/

Through a Tor Browser - recommended

- Download Tor Browser - https://www.torproject.org/ and install it.
- Open one of links in Tor browser and follow instructions on these pages:
  http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion/
  or mirror
  http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion/
  These links work only in the Tor browser!
- Follow the instructions on this page

ATTENTION!

- https://decoding.at may be blocked. We recommend using a Tor browser (or Brave) to access the TOR site
- Do not rename encrypted files.
- Do not try to decrypt using third party software, it may cause permanent data loss.
- 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.
- Tor Browser user manual https://tb-manual.torproject.org/about
- All your **stolen important data** will be loaded into our blog if you do not pay ransom.
- Our blog http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion or https://bigblog.at where you can see data of the companies which refused to pay ransom.


Process Monitor - E:\00ce72bb6fb1d2c1d32aa4c4a147e1b9b390cf9d3ae8b5c0cab2718118db4430.pml
File
Time
freshkart@420blaze.it
YOUR FILES ARE ENCRYPTED
Don't worry,you can return all your files!
If you want to restore them, follow this link: email freshkart@420blaze.it YOUR ID A01FAD4A
If you have not been answered via the link within 12 hours, write to us by e-mail: freshkart@420blaze.it
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
Type here to search
12:29 AM
3/21/2023

Loki locker

All your files have been encrypted by Loki locker!

14d,23:50:9 LEFT TO LOSE ALL OF YOUR FILES

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email **Unlockpls.dr01@protonmail.com**

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
After payment we will send you the decryption tool.
You have to 48 hours(2 Days) To contact or paying us After that, you have to Pay **Double**.
In case of no answer in 24 hours (1 Day) write to this email **Unlockpls.dr01@yahoo.com**
Your unique ID is : **A01FAD4A**

You only have LIMITED time to get back your files!

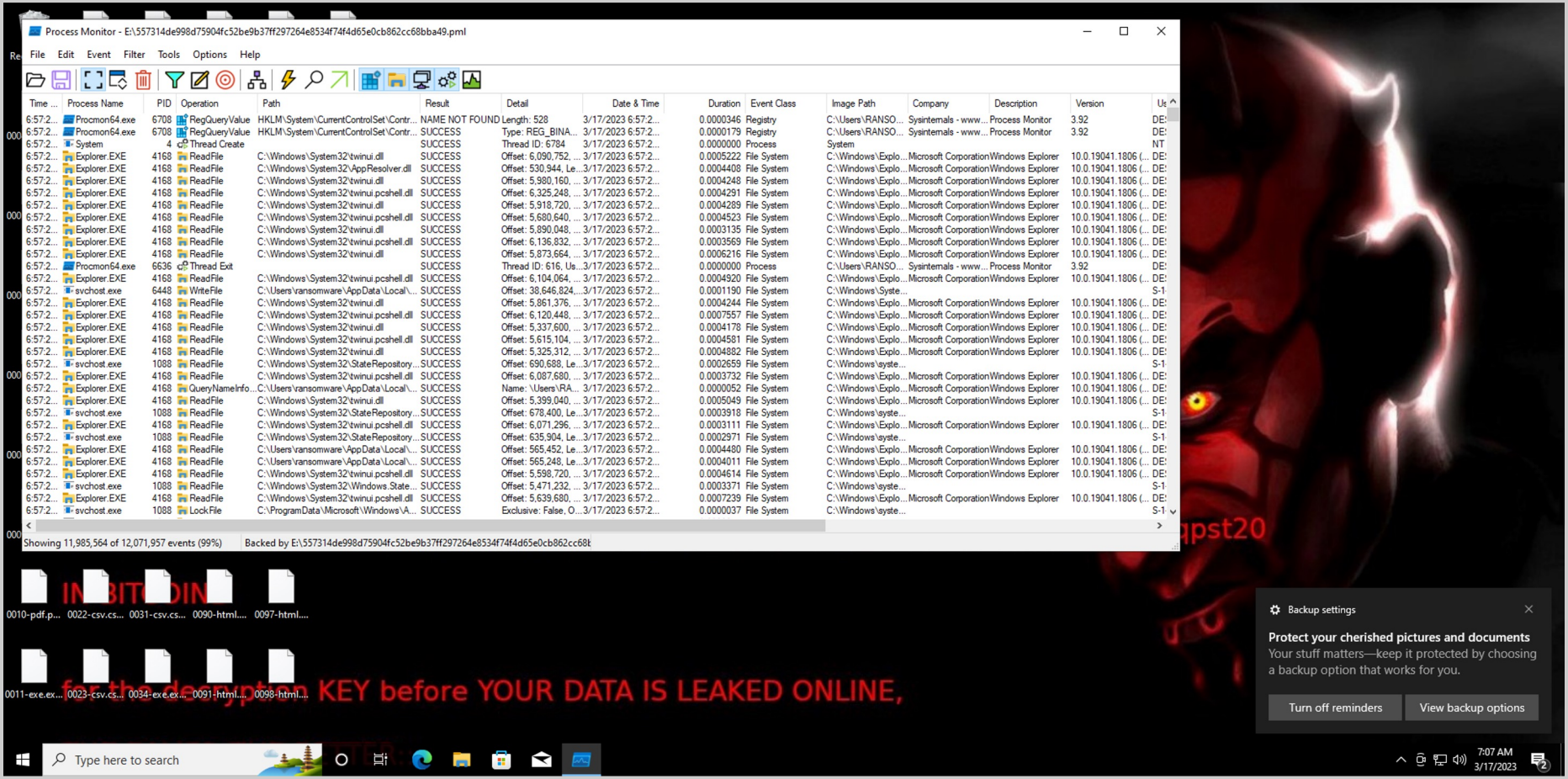
- If timer runs out and you dont pay us , all of files will be DELETED and you hard disk will be seriously DAMAGED.
- You will lose some of your data on day 2 in the timer.
- You can buy more time for pay. Just email us.
- THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)

What is our decryption guarantee?

- Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

Attention!

- **DO NOT** pay any money before decrypting the test files.
- **DO NOT** trust any intermediary. they wont help you and you may be victim of scam. just email us , we help you in any steps.
- **DO NOT** reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.


Process Monitor - E:\557314de998d75904fc52be9b37ff297264e8534f74f4d65e0cb862cc68bba49.pml
File Edit Event Filter Tools Options Help
Showing 11,985,564 of 12,071,957 events (99%)
Backed by E:\557314de998d75904fc52be9b37ff297264e8534f74f4d65e0cb862cc68b
0010-pdf.p... 0022-csv.cs... 0031-csv.cs... 0090-html.... 0097-html....
0011-exe.ex... 0023-csv.cs... 0034-exe.ex... 0091-html.... 0098-html....
for the decryption KEY before YOUR DATA IS LEAKED ONLINE,
Backup settings
Protect your cherished pictures and documents
Your stuff matters—keep it protected by choosing a backup option that works for you.
Turn off reminders
View backup options
Type here to search
7:07 AM
3/17/2023

Final Thoughts

- We would have liked something like REPROD when we started our pilot study, we hope it will be useful for others.
- Timescales of file access vary considerably across ransomware samples.
- Estimating the distribution of benign activity (large variance) is very difficult, this seems to be essential to a successful outcome where machine learning will be used in production.
- A considerable of amount of ransomware seems to trigger without much effort, but there is a lot apparent variance in activity. Lots of disk activity is not necessarily associated with locking.
- Assume an ideal future where low level methods can detect malicious crypto activity reliably against a benign background, how will adversaries respond ? We can envision fairly obvious counters including diluting crypto activity in space (“scattershot encryption”) or time. Perhaps we should ask what research directions are most likely lead to a “successful” outcome against ransomware.

Acknowledgements

Anirban Roy

Robert Halley

Carolyn Talcott

Pat Lincoln

ONR