(ENCRYPTION) TIME FLIES WHEN YOU'RE HAVING FUN: THE CASE OF THE EXOTIC BLACKCAT RANSOMWARE

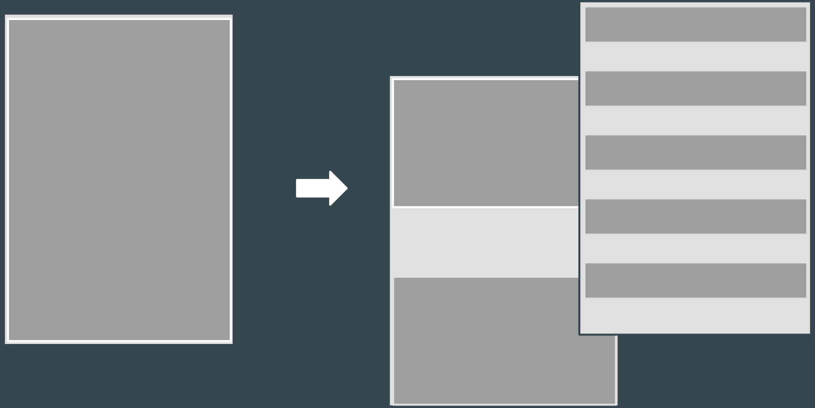
•••

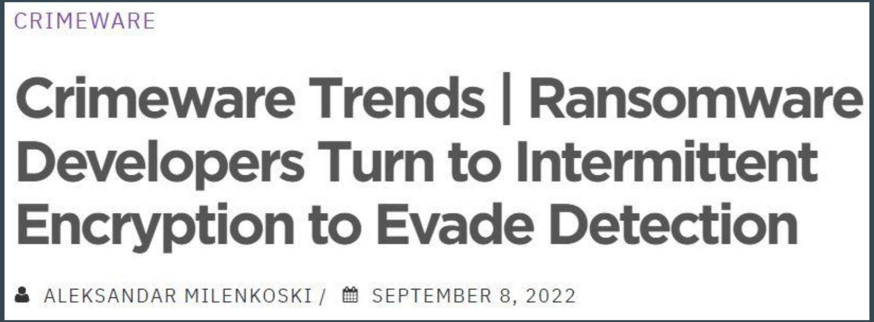
Aleksandar Milenkoski

VB Conference 2022

Ransomware Design (And Why It Is Changing)

What Is Changing?

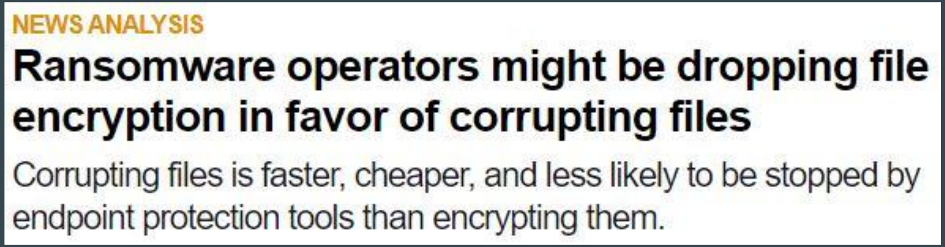




CRIMEWARE

Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection

ALEKSANDAR MILENKOSKI / SEPTEMBER 8, 2022



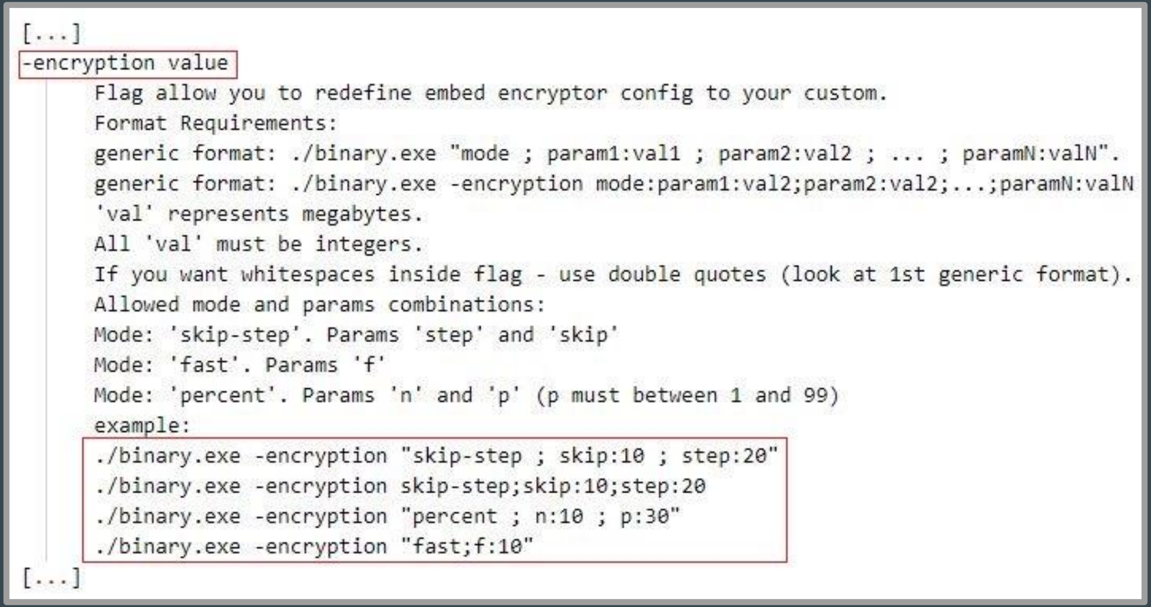
NEWS ANALYSIS

Ransomware operators might be dropping file encryption in favor of corrupting files

Corrupting files is faster, cheaper, and less likely to be stopped by endpoint protection tools than encrypting them.

Why Is It Changing?

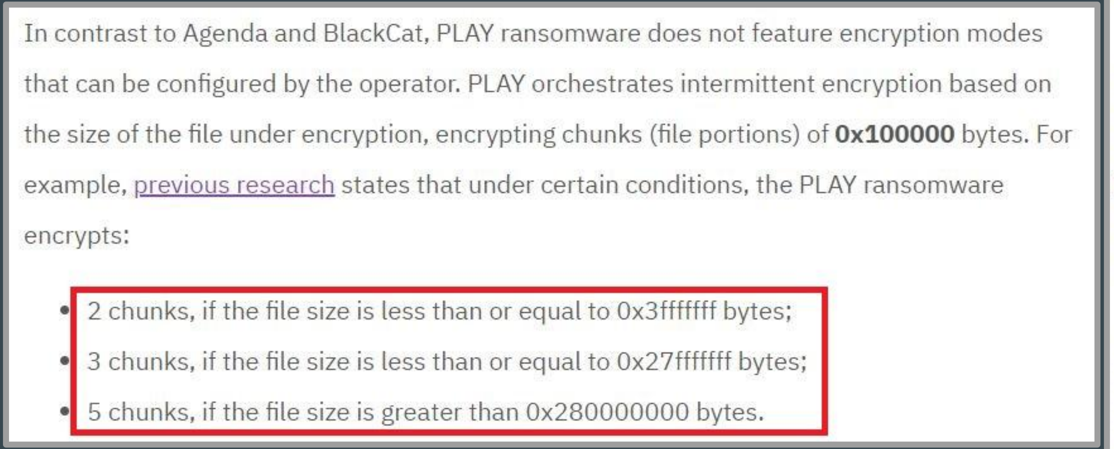
Agenda Ransomware



```
[...]
-encryption value
      Flag allow you to redefine embed encryptor config to your custom.
      Format Requirements:
      generic format: ./binary.exe "mode ; param1:val1 ; param2:val2 ; ... ; paramN:valN".
      generic format: ./binary.exe -encryption mode:param1:val2;param2:val2;...;paramN:valN
      'val' represents megabytes.
      All 'val' must be integers.
      If you want whitespaces inside flag - use double quotes (look at 1st generic format).
      Allowed mode and params combinations:
      Mode: 'skip-step'. Params 'step' and 'skip'
      Mode: 'fast'. Params 'f'
      Mode: 'percent'. Params 'n' and 'p' (p must between 1 and 99)
      example:
      ./binary.exe -encryption "skip-step ; skip:10 ; step:20"
      ./binary.exe -encryption skip-step;skip:10;step:20
      ./binary.exe -encryption "percent ; n:10 ; p:30"
      ./binary.exe -encryption "fast;f:10"
[...]
```

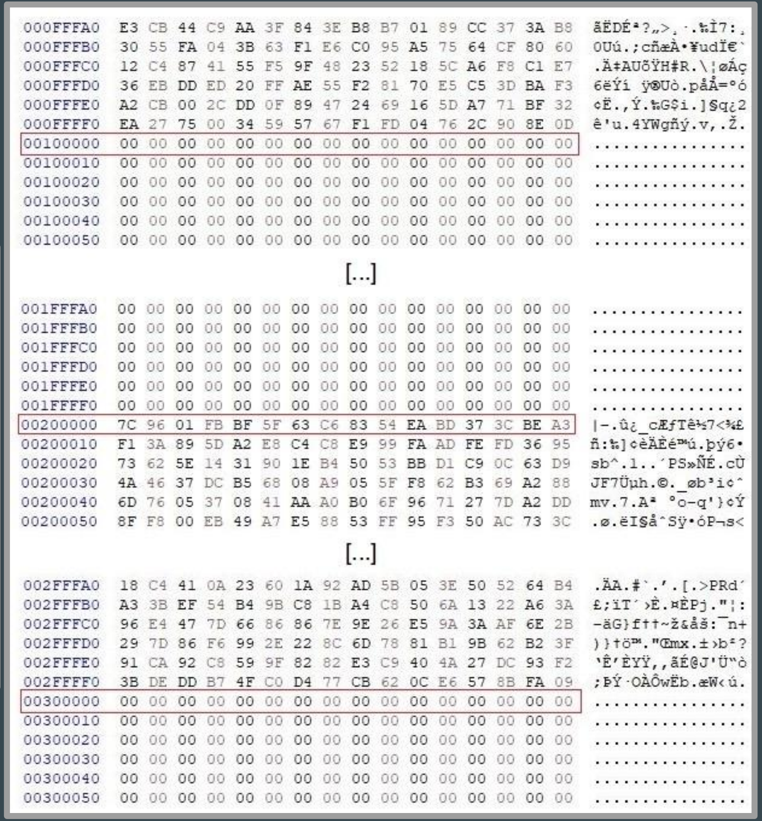
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

PLAY Ransomware



In contrast to Agenda and BlackCat, PLAY ransomware does not feature encryption modes that can be configured by the operator. PLAY orchestrates intermittent encryption based on the size of the file under encryption, encrypting chunks (file portions) of **0x100000** bytes. For example, previous research states that under certain conditions, the PLAY ransomware encrypts:

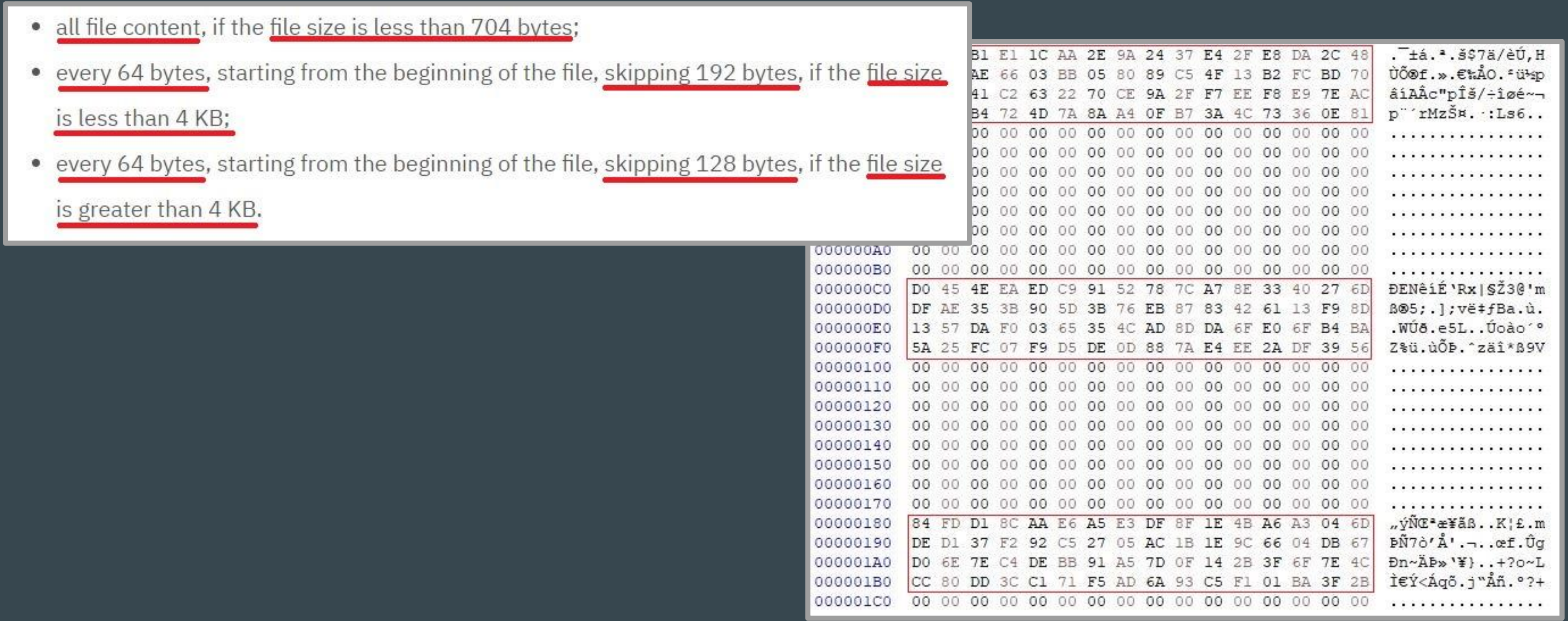
- 2 chunks, if the file size is less than or equal to 0x3fffffff bytes;
- 3 chunks, if the file size is less than or equal to 0x27fffffff bytes;
- 5 chunks, if the file size is greater than 0x280000000 bytes.



```
000FFFA0  E3 CB 44 C9 AA 3F 84 3E B8 B7 01 89 CC 37 3A B8  ãËDÉª?„>¸·.‰Ì7:¸
000FFFB0  30 55 FA 04 3B 63 F1 E6 C0 95 A5 75 64 CF 80 60  0Uú.;cñæÀ•¥udÏ€`
000FFFC0  12 C4 87 41 55 F5 9F 48 23 52 18 5C A6 F8 C1 E7  .Ä‡AUõŸH#R.\¦øÁç
000FFFD0  36 EB DD ED 20 FF AE 55 F2 81 70 E5 C5 3D BA F3  6ëÝí ÿ®Uò.påÅ=ºó
000FFFE0  A2 CB 00 2C DD 0F 89 47 24 69 16 5D A7 71 BF 32  ¢Ë.,Ý.‰G$i.]§q¿2
000FFFF0  EA 27 75 00 34 59 57 67 F1 FD 04 76 2C 90 8E 0D  ê'u.4YWgñý.v,.Ž.
00100000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00100010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00100020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00100030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00100040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00100050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

                              [...]

001FFFA0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001FFFB0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001FFFC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001FFFD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001FFFE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
001FFFF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00200000  7C 96 01 FB BF 5F 63 C6 83 54 EA BD 37 3C BE A3  |–.û¿_cÆƒTê½7<¾£
00200010  F1 3A 89 5D A2 E8 C4 C8 E9 99 FA AD FE FD 36 95  ñ:‰]¢èÄÈé™ú.þý6•
00200020  73 62 5E 14 31 90 1E B4 50 53 BB D1 C9 0C 63 D9  sb^.1..´PS»ÑÉ.cÙ
00200030  4A 46 37 DC B5 68 08 A9 05 5F F8 62 B3 69 A2 88  JF7Üµh.©._øb³i¢ˆ
00200040  6D 76 05 37 08 41 AA A0 B0 6F 96 71 27 7D A2 DD  mv.7.Aª °o–q'}¢Ý
00200050  8F F8 00 EB 49 A7 E5 88 53 FF 95 F3 50 AC 73 3C  .ø.ëI§åˆSÿ•óP¬s<

                              [...]

002FFFA0  18 C4 41 0A 23 60 1A 92 AD 5B 05 3E 50 52 64 B4  .ÄA.#`.’.[.>PRd´
002FFFB0  A3 3B EF 54 B4 9B C8 1B A4 C8 50 6A 13 22 A6 3A  £;ïT´›È.¤ÈPj."¦:
002FFFC0  96 E4 47 7D 66 86 86 7E 9E 26 E5 9A 3A AF 6E 2B  –äG}f††~ž&åš:¯n+
002FFFD0  29 7D 86 F6 99 2E 22 8C 6D 78 81 B1 9B 62 B2 3F  )}†ö™."Œmx.±›b²?
002FFFE0  91 CA 92 C8 59 9F 82 82 E3 C9 40 4A 27 DC 93 F2  ‘Ê’ÈYŸ‚‚ãÉ@J'Ü“ò
002FFFF0  3B DE DD B7 4F C0 D4 77 CB 62 0C E6 57 8B FA 09  ;ÞÝ·OÀÔwËb.æW‹ú.
00300000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00300010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00300020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00300030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00300040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00300050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

BlackBasta Ransomware

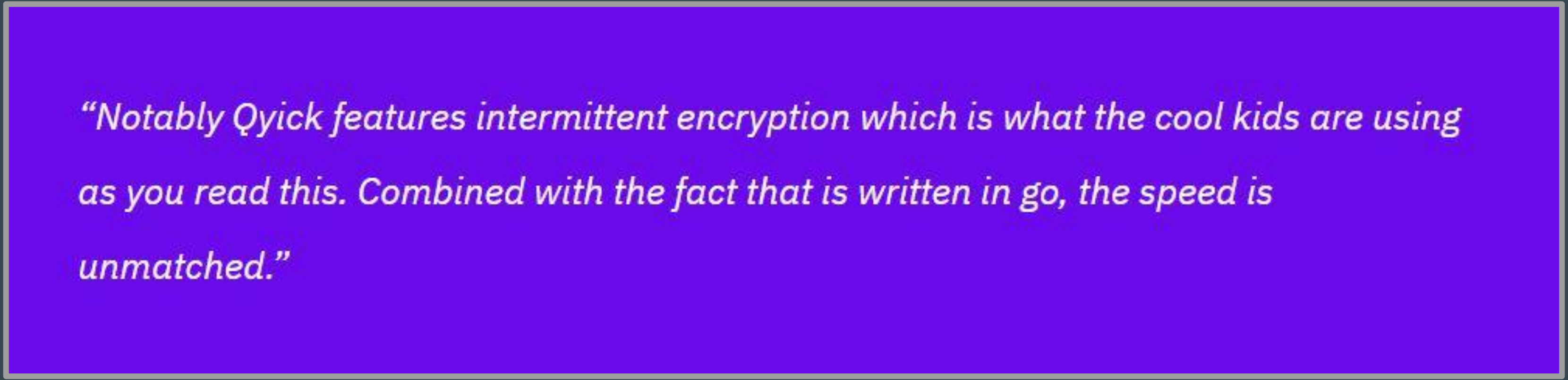


- all file content, if the file size is less than 704 bytes;
- every 64 bytes, starting from the beginning of the file, skipping 192 bytes, if the file size is less than 4 KB;
- every 64 bytes, starting from the beginning of the file, skipping 128 bytes, if the file size is greater than 4 KB.

```
               B1 E1 1C AA 2E 9A 24 37 E4 2F E8 DA 2C 48  .¯±á.ª.š$7ä/èÚ,H
               AE 66 03 BB 05 80 89 C5 4F 13 B2 FC BD 70  ÙÕ®f.».€‰ÅO.²ü½p
               41 C2 63 22 70 CE 9A 2F F7 EE F8 E9 7E AC  âíAÂc"pÎš/÷îøé~¬
               B4 72 4D 7A 8A A4 0F B7 3A 4C 73 36 0E 81  p¨´rMzŠ¤.·:Ls6..
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
               00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  D0 45 4E EA ED C9 91 52 78 7C A7 8E 33 40 27 6D  ÐENêíÉ'Rx|§Ž3@'m
000000D0  DF AE 35 3B 90 5D 3B 76 EB 87 83 42 61 13 F9 8D  ß®5;.];vë‡ƒBa.ù.
000000E0  13 57 DA F0 03 65 35 4C AD 8D DA 6F E0 6F B4 BA  .WÚð.e5L..Úoào´º
000000F0  5A 25 FC 07 F9 D5 DE 0D 88 7A E4 EE 2A DF 39 56  Z%ü.ùÕÞ.ˆzäî*ß9V
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  84 FD D1 8C AA E6 A5 E3 DF 8F 1E 4B A6 A3 04 6D  „ýÑŒªæ¥ãß..K¦£.m
00000190  DE D1 37 F2 92 C5 27 05 AC 1B 1E 9C 66 04 DB 67  ÞÑ7ò'Å'.¬..œf.Ûg
000001A0  D0 6E 7E C4 DE BB 91 A5 7D 0F 14 2B 3F 6F 7E 4C  Ðn~ÄÞ»'¥}..+?o~L
000001B0  CC 80 DD 3C C1 71 F5 AD 6A 93 C5 F1 01 BA 3F 2B  Ì€Ý<Áqõ.j"Åñ.º?+
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

Qyick Ransomware

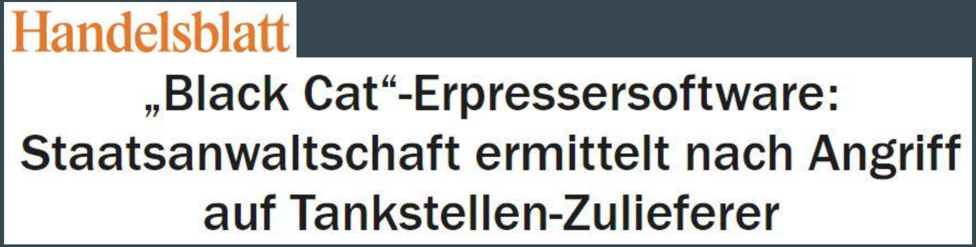


“Notably Qyick features intermittent encryption which is what the cool kids are using as you read this. Combined with the fact that is written in go, the speed is unmatched.”

https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

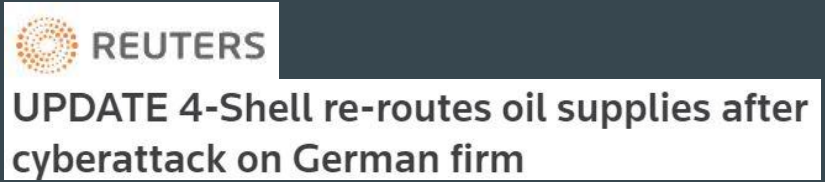
The Exotic BlackCat Ransomware

ALPHV/BlackCat: A Formidable Rust RaaS Threat



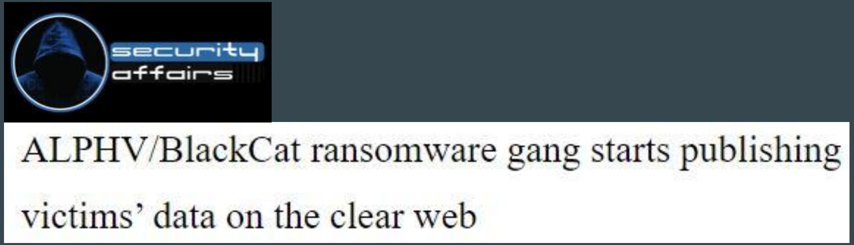
Handelsblatt

„Black Cat“-Erpressersoftware: Staatsanwaltschaft ermittelt nach Angriff auf Tankstellen-Zulieferer



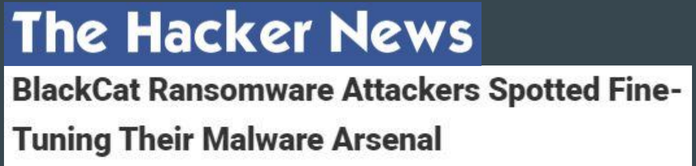
REUTERS

UPDATE 4-Shell re-routes oil supplies after cyberattack on German firm



security affairs

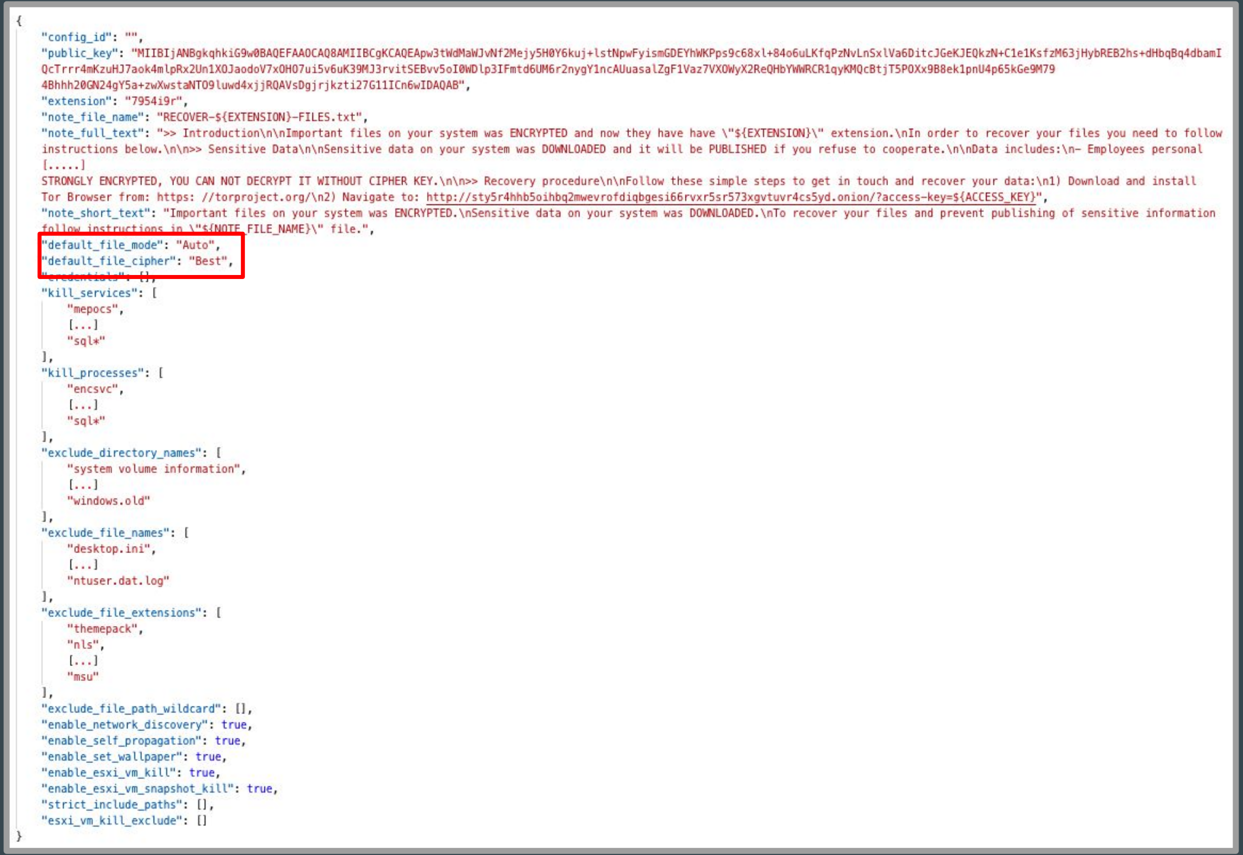
ALPHV/BlackCat ransomware gang starts publishing victims’ data on the clear web



The Hacker News

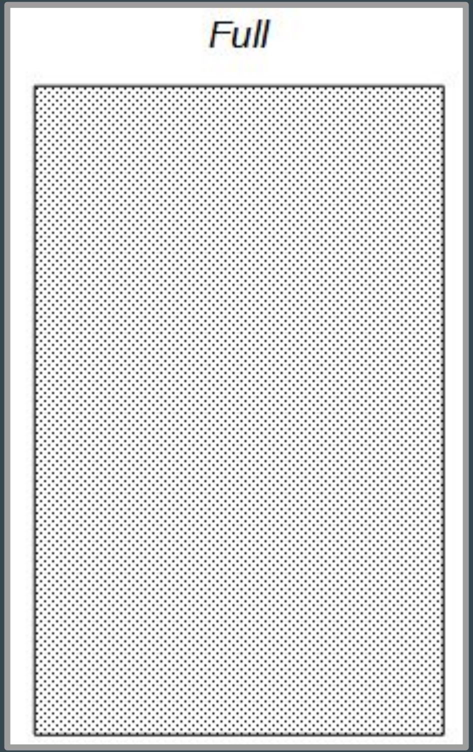
BlackCat Ransomware Attackers Spotted Fine-Tuning Their Malware Arsenal

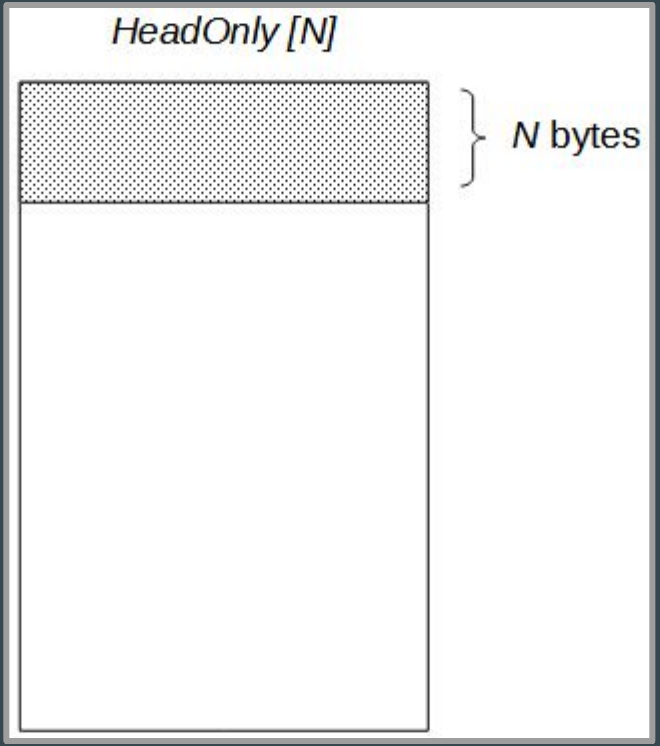
Large Configuration Space

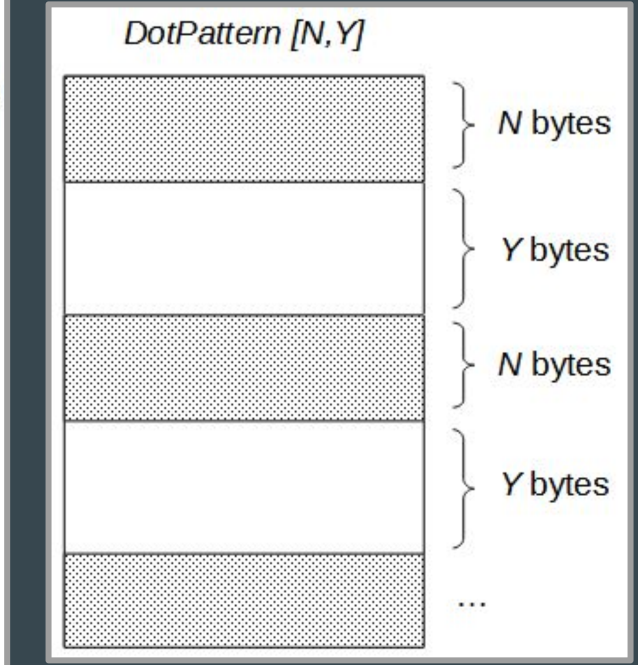


```
{
    "config_id": "",
    "public_key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApw3tWdMaWJvNf2Mejy5H0Y6kuj+lstNpwFyismGDEYhWKPps9c68xl+84o6uLKfqPzNvLnSxlVa6DitcJGeKJEQkzN+C1e1KsfzM63jHybREB2hs+dHbqBq4dbamI
    QcTrrr4mKzuHJ7aok4mlpRx2Un1XOJaodoV7xOHO7ui5v6uK39MJ3rvitSEBvv5oI0WDlp3IFmtd6UM6r2nygY1ncAUuasalZgF1Vaz7VXOWyX2ReQHbYWWRCR1qyKMQcBtjT5POXx9B8ek1pnU4p65kGe9M79
    4Bhhh20GN24gY5a+zwXwstaNTO9luwd4xjjRQAVsDgjrjkzti27G11ICn6wIDAQAB",
    "extension": "7954i9r",
    "note_file_name": "RECOVER-${EXTENSION}-FILES.txt",
    "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now they have have \"${EXTENSION}\" extension.\nIn order to recover your files you need to follow
    instructions below.\n\n>> Sensitive Data\n\nSensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.\n\nData includes:\n- Employees personal
    [.....]
    STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.\n\n>> Recovery procedure\n\nFollow these simple steps to get in touch and recover your data:\n1) Download and install
    Tor Browser from: https: //torproject.org/\n2) Navigate to: http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=${ACCESS_KEY}",
    "note_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your system was DOWNLOADED.\nTo recover your files and prevent publishing of sensitive information
    follow instructions in \"${NOTE_FILE_NAME}\" file.",
    "default_file_mode": "Auto",
    "default_file_cipher": "Best",
    "credentials": [],
    "kill_services": [
        "mepocs",
        [...]
        "sql*"
    ],
    "kill_processes": [
        "encsvc",
        [...]
        "sql*"
    ],
    "exclude_directory_names": [
        "system volume information",
        [...]
        "windows.old"
    ],
    "exclude_file_names": [
        "desktop.ini",
        [...]
        "ntuser.dat.log"
    ],
    "exclude_file_extensions": [
        "themepack",
        "nls",
        [...]
        "msu"
    ],
    "exclude_file_path_wildcard": [],
    "enable_network_discovery": true,
    "enable_self_propagation": true,
    "enable_set_wallpaper": true,
    "enable_esxi_vm_kill": true,
    "enable_esxi_vm_snapshot_kill": true,
    "strict_include_paths": [],
    "esxi_vm_kill_exclude": []
}
```

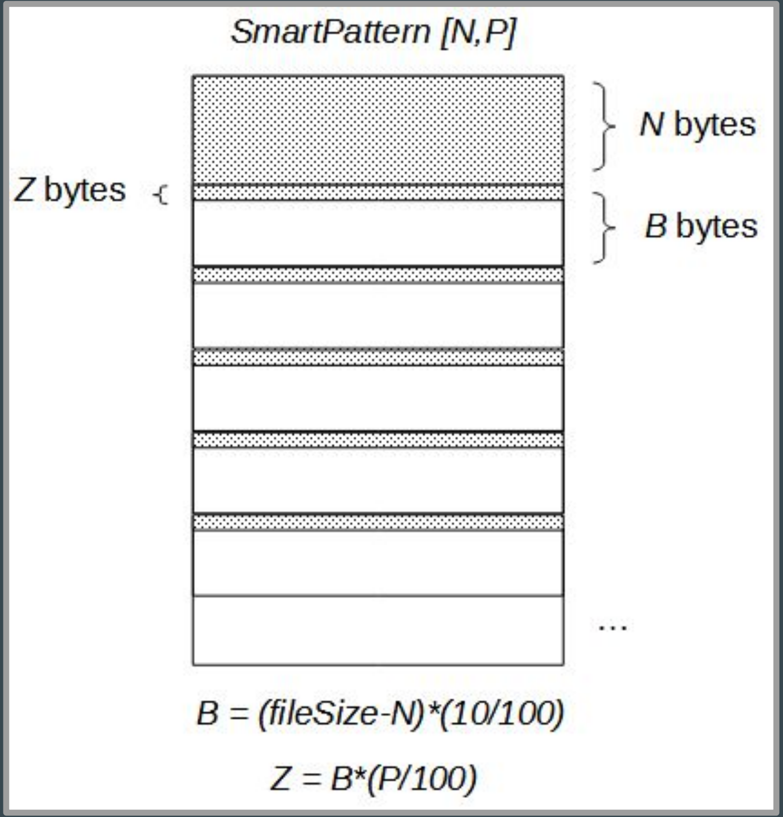
Intricate Encryption Modes

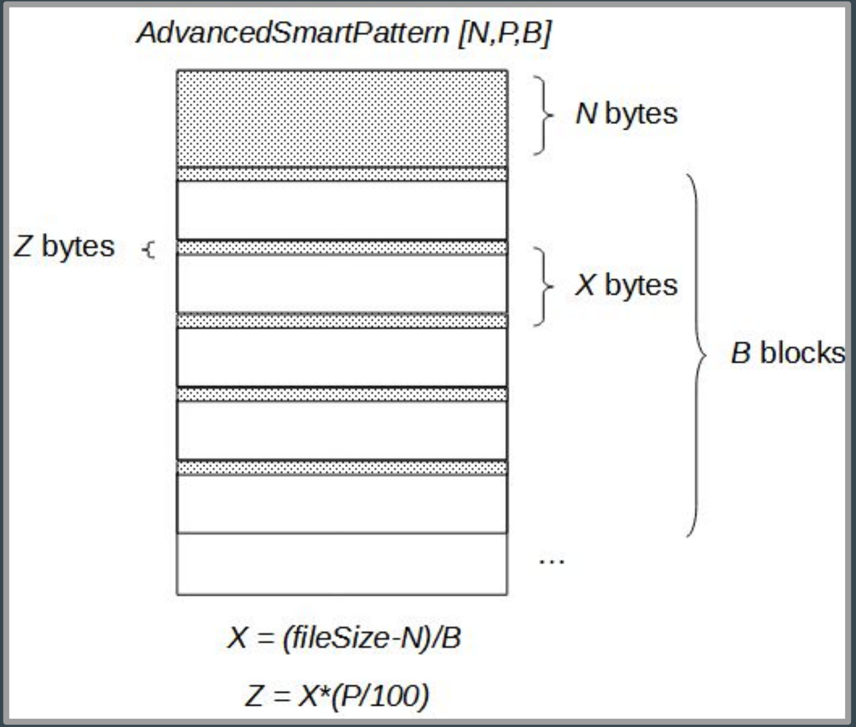




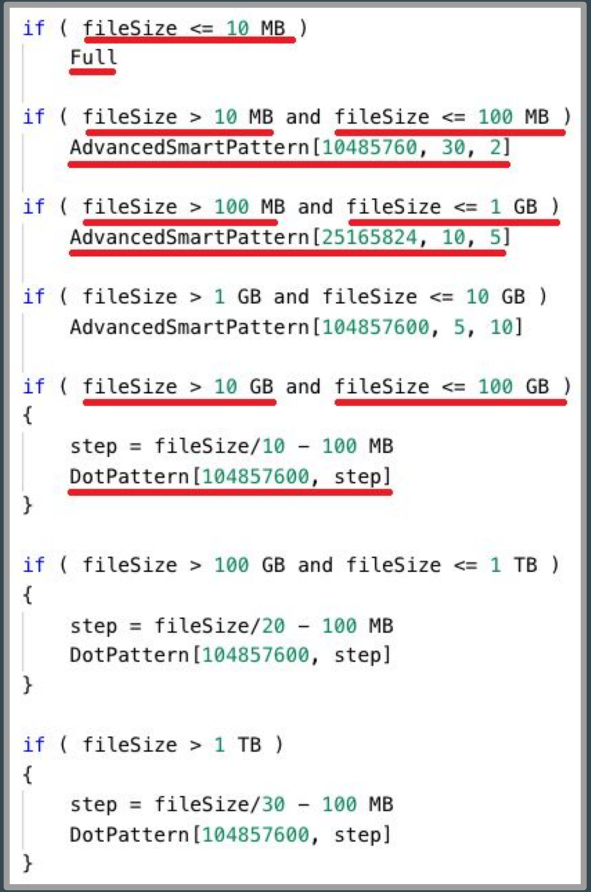


Intricate Encryption Modes (cont.)

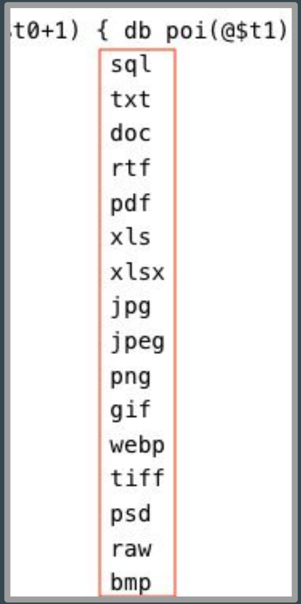




Intricate Encryption Modes (cont.)



```
if ( fileSize <= 10 MB )
    Full

if ( fileSize > 10 MB and fileSize <= 100 MB )
    AdvancedSmartPattern[10485760, 30, 2]

if ( fileSize > 100 MB and fileSize <= 1 GB )
    AdvancedSmartPattern[25165824, 10, 5]

if ( fileSize > 1 GB and fileSize <= 10 GB )
    AdvancedSmartPattern[104857600, 5, 10]

if ( fileSize > 10 GB and fileSize <= 100 GB )
{
    step = fileSize/10 - 100 MB
    DotPattern[104857600, step]
}

if ( fileSize > 100 GB and fileSize <= 1 TB )
{
    step = fileSize/20 - 100 MB
    DotPattern[104857600, step]
}

if ( fileSize > 1 TB )
{
    step = fileSize/30 - 100 MB
    DotPattern[104857600, step]
}
```



```
t0+1) { db poi(@$t1)
        sql
        txt
        doc
        rtf
        pdf
        xls
        xlsx
        jpg
        jpeg
        png
        gif
        webp
        tiff
        psd
        raw
        bmp
```

Encryption Configuration Space: Measurement

Data Throughput
(MB/sec.)

Wallclock Processing Time
(sec.)

Unencrypted Content
(%)

50 MB

500 MB

5 GB

50 GB

Encryption Configuration Space: Impact - Highlights

AES-NI vs. ChaCha20
Encryption mode: *Full*

5 GB	+51.56 MB/sec.	-5.24 sec.
50 GB	+53.76 MB/sec.	-18.42 sec.

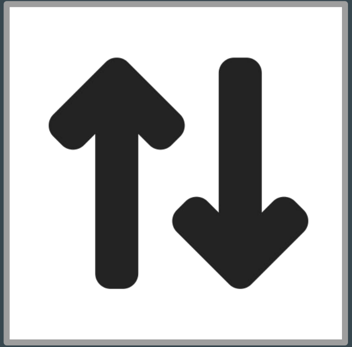
Encryption Configuration Space: Impact - Highlights

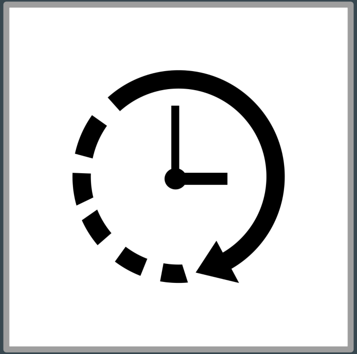
Auto vs. *Full*

📄	⚙	⇅	🕒
500 MB	86.68 %	-178.51 MB/sec.	-0.82 sec.
50 GB	98.05 %	-250.37 MB/sec.	-117.44 sec.

Encryption Configuration Space: Impact

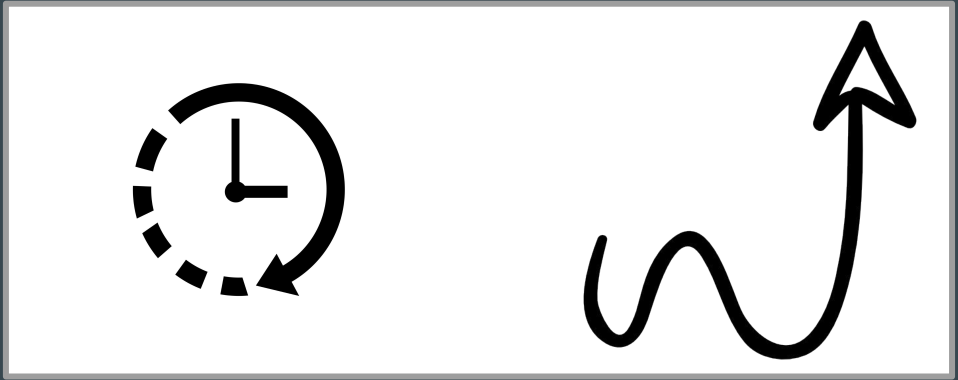
The configuration space is ***impactful***





Where are we? Where are we going?

Where Are We?



Threat actors know where they want to go

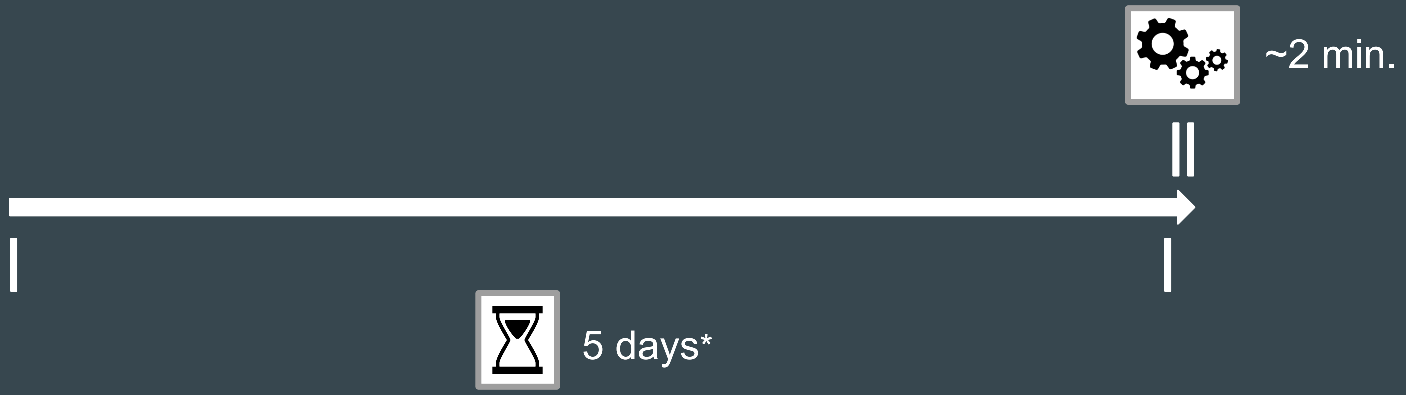
Do we?

Where Are We Going?

Infection prevention remains an absolute priority

Where Are We Going?

Infection prevention remains an absolute priority



~2 min.

5 days*

**Mandiant M-Trends Report 2022*

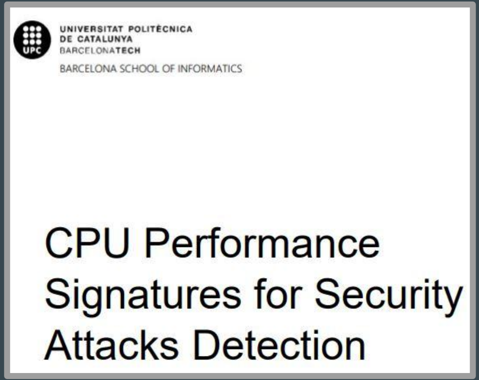
Where Are We Going... If Prevention Has Failed?

Detection engineering

How good are our file I/O-based detections?

Should we develop new?

What about CPU/memory performance signatures?



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

BARCELONA SCHOOL OF INFORMATICS

CPU Performance Signatures for Security Attacks Detection

Where Are We Going... If Prevention Has Failed?

Response

Do we need **new response logic**?

Evidence gathering

Verdict and response

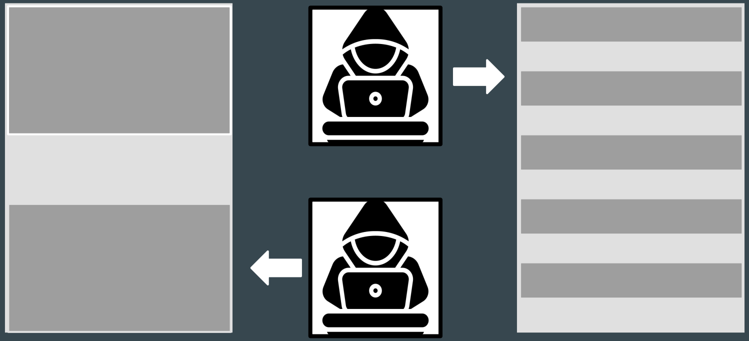
~~Evidence gathering~~

Verdict and response

Where Are We Going… If Prevention Has Failed?

Threat Intelligence

Can we increase attribution confidence?



Can we better understand and estimate the malware market dynamics?

Thank you!

Aleksandar Milenkoski

@milenkowski

www.linkedin.com/in/aleksmilenkoski/