# DarkBit Ransomware Targets Israel with Command-Line Options and Optimized Encryption Routines

blogs.blackberry.com/en/2023/02/darkbit-ransomware-targets-israel

The BlackBerry Research & Intelligence Team

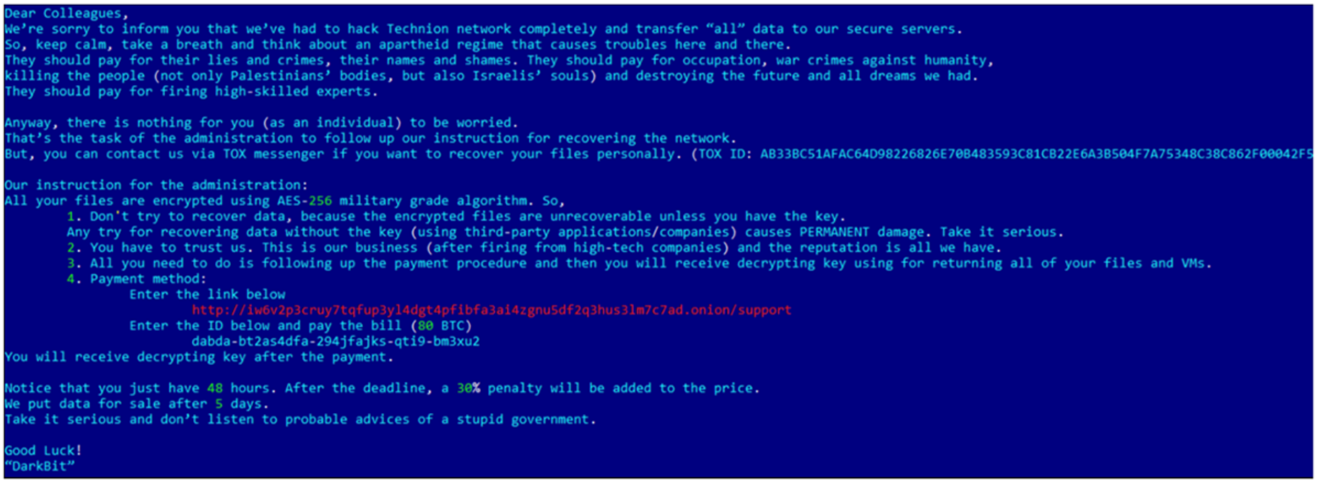
1. BlackBerry Blog
2. DarkBit Ransomware Targets Israel with Command-Line Options and Optimized Encryption Routines

## Summary

A new ransomware strain dubbed "DarkBit" has recently appeared on the threat landscape after targeting one of Israel's top research universities, Technion - Israel Institute of Technology (IIT).

The threat actor behind this Golang-compiled ransomware appears to have geopolitical motivations; the ransom note is laden with anti-Israeli and anti-government rhetoric, along with mentions of the recent spate of layoffs across the technology industry.

The main portable executable (PE) module supports command-line options and data encryption optimization for large files.



```
Dear Colleagues,
We're sorry to inform you that we've had to hack Technion network completely and transfer "all" data to our secure servers.
So, keep calm, take a breath and think about an apartheid regime that causes troubles here and there.
They should pay for their lies and crimes, their names and shames. They should pay for occupation, war crimes against humanity,
killing the people (not only Palestinians' bodies, but also Israelis' souls) and destroying the future and all dreams we had.
They should pay for firing high-skilled experts.

Anyway, there is nothing for you (as an individual) to be worried.
That's the task of the administration to follow up our instruction for recovering the network.
But, you can contact us via TOX messenger if you want to recover your files personally. (TOX ID: AB33BC51AFAC64D98226826E70B483593C81CB22E6A3B504F7A75348C38C862F00042F5

Our instruction for the administration:
All your files are encrypted using AES-256 military grade algorithm. So,
        1. Don't try to recover data, because the encrypted files are unrecoverable unless you have the key.
        Any try for recovering data without the key (using third-party applications/companies) causes PERMANENT damage. Take it serious.
        2. You have to trust us. This is our business (after firing from high-tech companies) and the reputation is all we have.
        3. All you need to do is following up the payment procedure and then you will receive decrypting key using for returning all of your files and VMs.
        4. Payment method:
                Enter the link below
                        http://iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad.onion/support
                Enter the ID below and pay the bill (80 BTC)
                        dabda-bt2as4dfa-294jfajks-qti9-bm3xu2
You will receive decrypting key after the payment.

Notice that you just have 48 hours. After the deadline, a 30% penalty will be added to the price.
We put data for sale after 5 days.
Take it serious and don't listen to probable advices of a stupid government.

Good Luck!
"DarkBit"
```

*Figure 1: DarkBit ransom note*

The requested ransom to release the decryptor was 80 Bitcoin (BTC), equating to around USD $1,869,760 at the time of writing. The Haifa-based academic university is currently carrying out incident response activities to determine the scope of the attack, according to a post in Hebrew on their Twitter account, which states:

"The Technion is under cyber attack. The scope and nature of the attack are under investigation. To carry out the process of collecting the information and handling it, we use the best experts in the field, in the Technion and outside, and coordinate with the authorized authorities. The Technion proactively blocked all communication networks at this stage."

## Weaponization and Technical Overview

| | |
|---|---|
| **Weapons** | Golang compiled PE executable |
| **Attack Vector** | Unknown |
| **Network Infrastructure** | TOX, TOR |
| **Targets** | Education |

## Technical Analysis

### Context

On February 12, 2023, Technion – Israel Institute of Technology (IIT) suffered a ransomware attack. The threat actor behind the attack was a previously unknown group – DarkBit, who named themselves and claimed responsibility via a branded .onion website and Twitter page.

To date, the college has not publicly revealed the attack's true extent nor how many computer systems were impacted by the ransomware. The origins of the breach and initial infection vector have not yet been disclosed publicly.

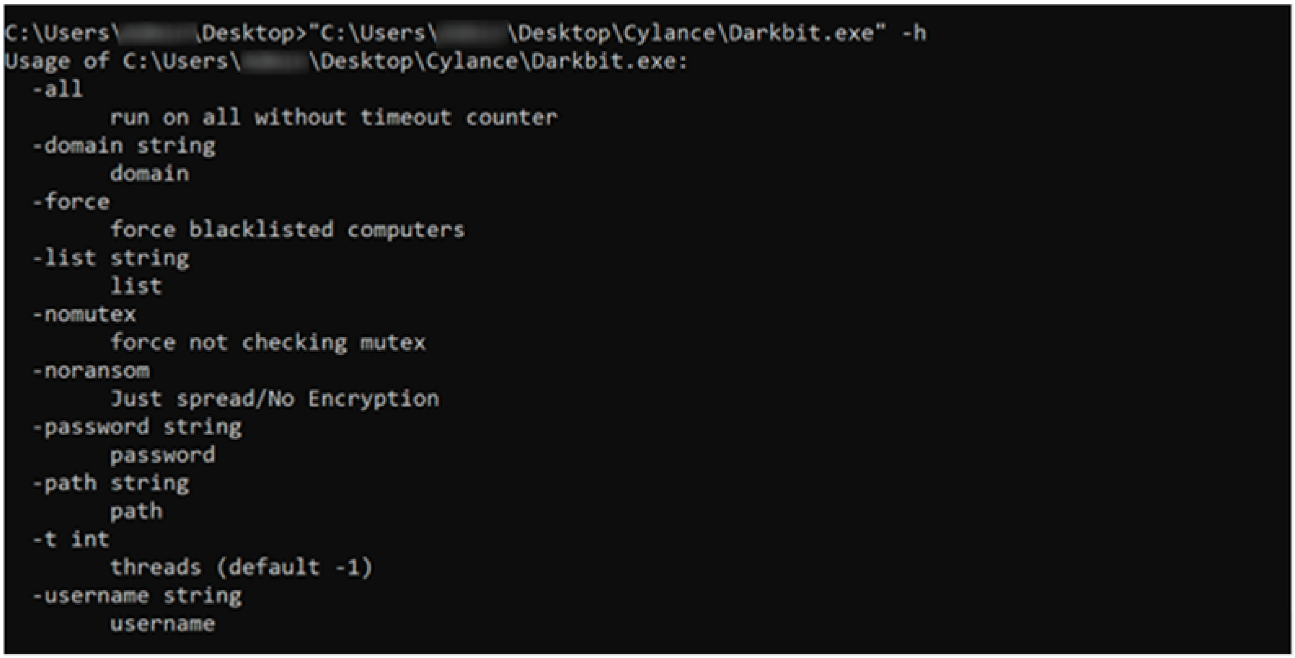
During the attack, affected devices had various files encrypted by the ransomware, with the file extension '.Darkbit' being appended to signify encryption. Additionally, a ransom note with the filename **'RECOVERY_DARKBIT.txt'** was added to all directories compromised by the ransomware.

The ransomware boasts several capabilities, including accepting command-line arguments or being run autonomously. It encrypts the victim's device by default, employing Advanced Encryption Standard 256-bits (AES-256) during its encryption routine, and impacts a wide range of file types.

Furthermore, it utilizes the technique of multi-threading for faster and more efficient encryption.

| | |
|---|---|
| **SHA-256** | 9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff |
| **MD5** | 9880fae6551d1e9ee921f39751a6f3c0 |
| **File Name** | N/A |
| **File Size** | 5385216 bytes |
| **File Type** | X64 PE |
| **Compile Date:** | Sat Feb 11 17:10:53 2023 |

Executing the malware via the command-line can be done with multiple optional arguments, as seen below:



```
C:\Users\[redacted]\Desktop>"C:\Users\[redacted]\Desktop\Cylance\Darkbit.exe" -h
Usage of C:\Users\[redacted]\Desktop\Cylance\Darkbit.exe:
  -all
        run on all without timeout counter
  -domain string
        domain
  -force
        force blacklisted computers
  -list string
        list
  -nomutex
        force not checking mutex
  -noransom
        Just spread/No Encryption
  -password string
        password
  -path string
        path
  -t int
        threads (default -1)
  -username string
        username
```

*Figure 2: DarkBit command-line options*

| **Argument** | **Description** |
|---|---|
| -all | Run on all without timeout counter |
| -domain (string) | Domain |
| -force | Force blacklisted computers |

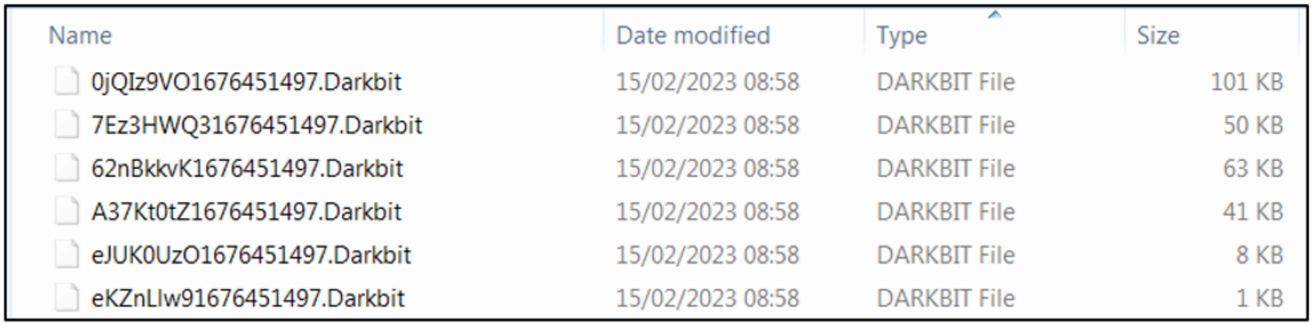
| | |
|---|---|
| -list (string) | List |
| -nomutex | Force not checking mutex |
| -noransom | Just spread/ No encryption |
| -password (string) | Password |
| -path (string) | Path |
| -t (int) | Threads (default -1) |
| -username (string) | Username |

Upon execution, the malware will call vssadmin.exe, the localized Windows® administrative tool for shadow copies.

The malware then attempts to run this command to delete shadow copies in order to prevent the victim organization from performing data recovery:

```
vssadmin.exe delete shadow /all /Quiet
```

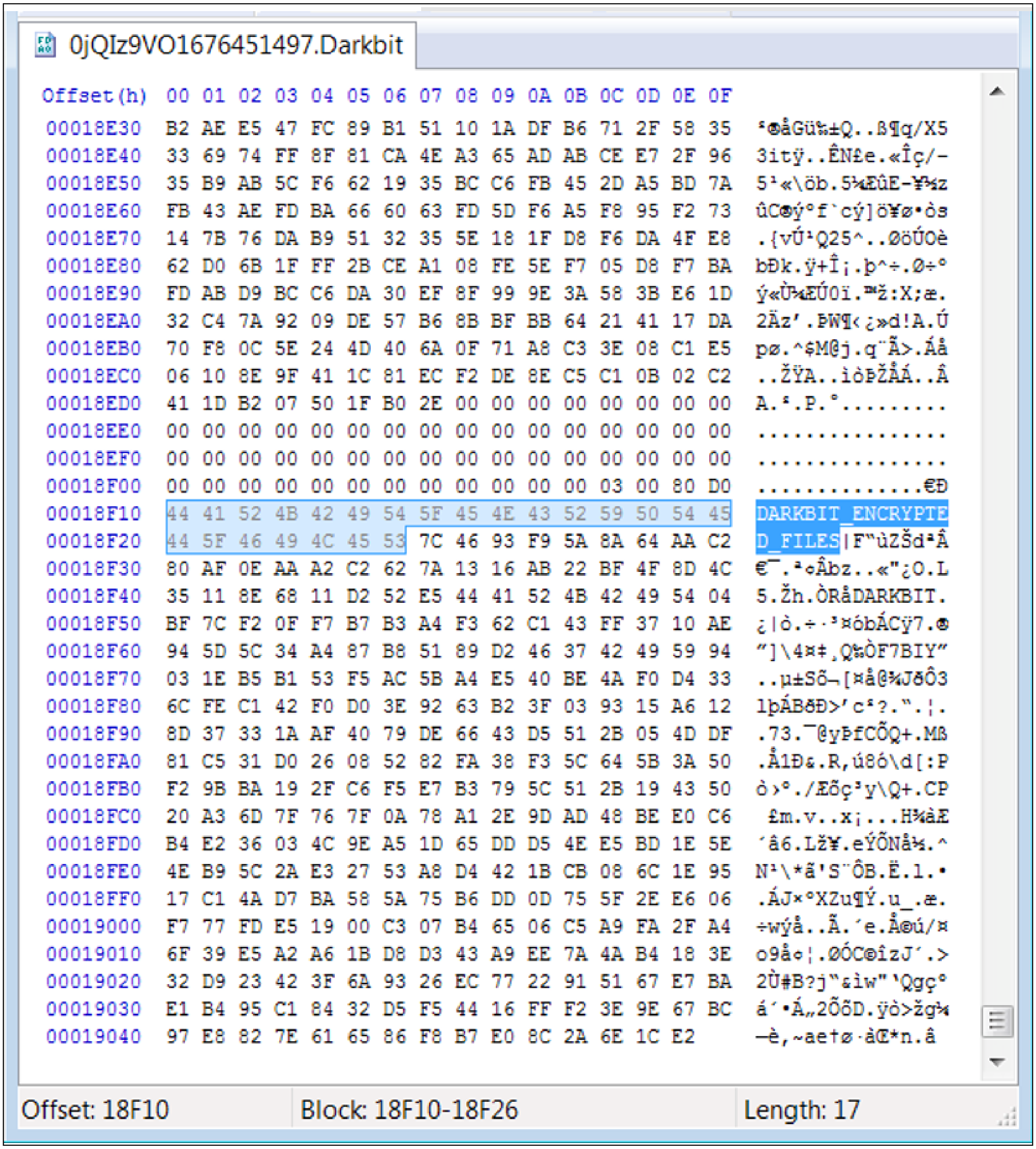
During the file encryption process, file extensions that the malware has not whitelisted are appended with a seemingly randomized name along with the ".Darkbit" file extension. That is appended to all affected files to signify encryption.



| Name | Date modified | Type | Size |
|---|---|---|---|
| 0jQIz9VO1676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 101 KB |
| 7Ez3HWQ31676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 50 KB |
| 62nBkkvK1676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 63 KB |
| A37Kt0tZ1676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 41 KB |
| eJUK0UzO1676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 8 KB |
| eKZnLlw91676451497.Darkbit | 15/02/2023 08:58 | DARKBIT File | 1 KB |

*Figure 3: DarkBit encrypted files*

Additionally, when a file is encrypted, the string "DARKBIT_ENCRYPTED_FILES" is appended to the now-encrypted code.



0jQIz9VO1676451497.Darkbit

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00018E30  B2 AE E5 47 FC 89 B1 51 10 1A DF B6 71 2F 58 35  ²®åGü‰±Q..ß¶q/X5
00018E40  33 69 74 FF 8F 81 CA 4E A3 65 AD AB CE E7 2F 96  3itÿ..ÊN£e.«Îç/–
00018E50  35 B9 AB 5C F6 62 19 35 BC C6 FB 45 2D A5 BD 7A  5¹«\öb.5¼ÆûE-¥½z
00018E60  FB 43 AE FD BA 66 60 63 FD 5D F6 A5 F8 95 F2 73  ûC®ýºf`cý]ö¥ø•òs
00018E70  14 7B 76 DA B9 51 32 35 5E 18 1F D8 F6 DA 4F E8  .{vÚ¹Q25^..ØöÚOè
00018E80  62 D0 6B 1F FF 2B CE A1 08 FE 5E F7 05 D8 F7 BA  bÐk.ÿ+Î¡.þ^÷.Ø÷º
00018E90  FD AB D9 BC C6 DA 30 EF 8F 99 9E 3A 58 3B E6 1D  ý«Ù¼ÆÚ0ï.™ž:X;æ.
00018EA0  32 C4 7A 92 09 DE 57 B6 8B BF BB 64 21 41 17 DA  2Äz'.ÞW¶‹¿»d!A.Ú
00018EB0  70 F8 0C 5E 24 4D 40 6A 0F 71 A8 C3 3E 08 C1 E5  pø.^$M@j.q¨Ã>.Áå
00018EC0  06 10 8E 9F 41 1C 81 EC F2 DE 8E C5 C1 0B 02 C2  ..ŽŸA..ìòÞŽÅÁ..Â
00018ED0  41 1D B2 07 50 1F B0 2E 00 00 00 00 00 00 00 00  A.².P.°.........
00018EE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00018EF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00018F00  00 00 00 00 00 00 00 00 00 00 00 00 03 00 80 D0  ..............€Ð
00018F10  44 41 52 4B 42 49 54 5F 45 4E 43 52 59 50 54 45  DARKBIT_ENCRYPTE
00018F20  44 5F 46 49 4C 45 53 7C 46 93 F9 5A 8A 64 AA C2  D_FILES|F"ùZŠdªÂ
00018F30  80 AF 0E AA A2 C2 62 7A 13 16 AB 22 BF 4F 8D 4C  €¯.ª¢Âbz..«"¿O.L
00018F40  35 11 8E 68 11 D2 52 E5 44 41 52 4B 42 49 54 04  5.Žh.ÒRåDARKBIT.
00018F50  BF 7C F2 0F F7 B7 B3 A4 F3 62 C1 43 FF 37 10 AE  ¿|ò.÷·³¤óbÁCÿ7.®
00018F60  94 5D 5C 34 A4 87 B8 51 89 D2 46 37 42 49 59 94  ”]\4¤‡¸Q‰ÒF7BIY”
00018F70  03 1E B5 B1 53 F5 AC 5B A4 E5 40 BE 4A F0 D4 33  ..µ±Sõ¬[¤å@¾JðÔ3
00018F80  6C FE C1 42 F0 D0 3E 92 63 B2 3F 03 93 15 A6 12  lþÁBðÐ>'c²?.".¦.
00018F90  8D 37 33 1A AF 40 79 DE 66 43 D5 51 2B 05 4D DF  .73.¯@yÞfCÕQ+.Mß
00018FA0  81 C5 31 D0 26 08 52 82 FA 38 F3 5C 64 5B 3A 50  .Å1Ð&.R‚ú8ó\d[:P
00018FB0  F2 9B BA 19 2F C6 F5 E7 B3 79 5C 51 2B 19 43 50  ò›º./Æõç³y\Q+.CP
00018FC0  20 A3 6D 7F 76 7F 0A 78 A1 2E 9D AD 48 BE E0 C6   £m.v..x¡...H¾àÆ
00018FD0  B4 E2 36 03 4C 9E A5 1D 65 DD D5 4E E5 BD 1E 5E  ´â6.Lž¥.eÝÕNå½.^
00018FE0  4E B9 5C 2A E3 27 53 A8 D4 42 1B CB 08 6C 1E 95  N¹\*ã'S¨ÔB.Ë.l.•
00018FF0  17 C1 4A D7 BA 58 5A 75 B6 DD 0D 75 5F 2E E6 06  .ÁJ×ºXZu¶Ý.u_.æ.
00019000  F7 77 FD E5 19 00 C3 07 B4 65 06 C5 A9 FA 2F A4  ÷wýå..Ã.´e.Å©ú/¤
00019010  6F 39 E5 A2 A6 1B D8 D3 43 A9 EE 7A 4A B4 18 3E  o9å¢¦.ØÓC©îzJ´.>
00019020  32 D9 23 42 3F 6A 93 26 EC 77 22 91 51 67 E7 BA  2Ù#B?j"&ìw"'Qgçº
00019030  E1 B4 95 C1 84 32 D5 F5 44 16 FF F2 3E 9E 67 BC  á´•Á„2ÕõD.ÿò>žg¼
00019040  97 E8 82 7E 61 65 86 F8 B7 E0 8C 2A 6E 1C E2     —è‚~ae†ø·àŒ*n.â
```

Offset: 18F10 | Block: 18F10-18F26 | Length: 17

*Figure 4: Encrypted file's contents*

### DarkBit Ransomware Filetype Exclusion List

| | | | | | | |
|---|---|---|---|---|---|---|
| msilog | log | ldf | lock | theme | msi | sys |
| wpx | cpl | adv | msc | scr | key | ico |
| dll | hta | deskthemepack | nomedia | msu | rtp | msp |

| | | | | | | |
|---|---|---|---|---|---|---|
| idx | ani | 386 | diagcfg | bin | mod | ics |
| com | hlp | spl | nls | cab | diagpkg | icl |
| ocx | rom | prf | themepack | msstyles | icns | mpa |
| drv | cur | diagcab | exe | cmd | shs | Darkbit |

**DarkBit File-Specific Exclusion List**

| | |
|---|---|
| Thumbs.db | Desktop.ini |
| Darkbit.jpg | Recovery_darkbit.txt |
| System volume information | |

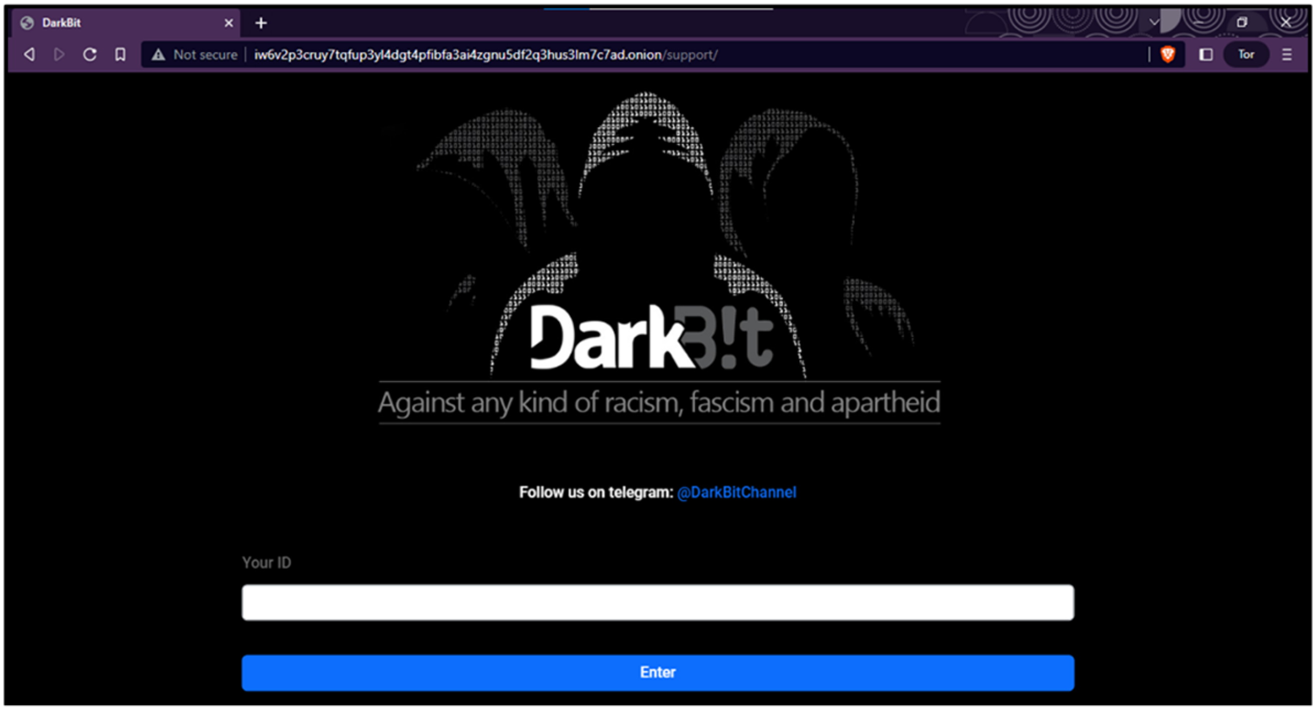
When it comes to encrypting files larger than 25MB, the malware is instructed (depending on the target file size) to divide those files into parts, with each part being a specific size, and then to encrypt them.

| Max file size (MB) | Parts | Part size (bytes) |
|---|---|---|
| 1000 | 2 | 12000 |
| 4000 | 3 | 10000 |
| 7000 | 2 | 20000 |
| 11000 | 3 | 30000 |
| 51000 | 5 | 30000 |
| 1000000 | 3 | 1000000 |
| 5000000 | 5 | 1000000 |
| 6000000 | 20 | 10000000 |

**Network Infrastructure**

The DarkBit group has a .onion webpage accessible to the TOR network. Under the DarkBit logo, the site includes the provocative subheading, “*Against any kind of racism, fascism and apartheid,*” leading one to believe this might be a hacktivist group. The ransom note includes its address, offering "support" to the victim.

| URL |
|---|
| hxxp://iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad[.]onion/support |


DarkBit
Not secure
iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad.onion/support/
Tor
DarkB!t

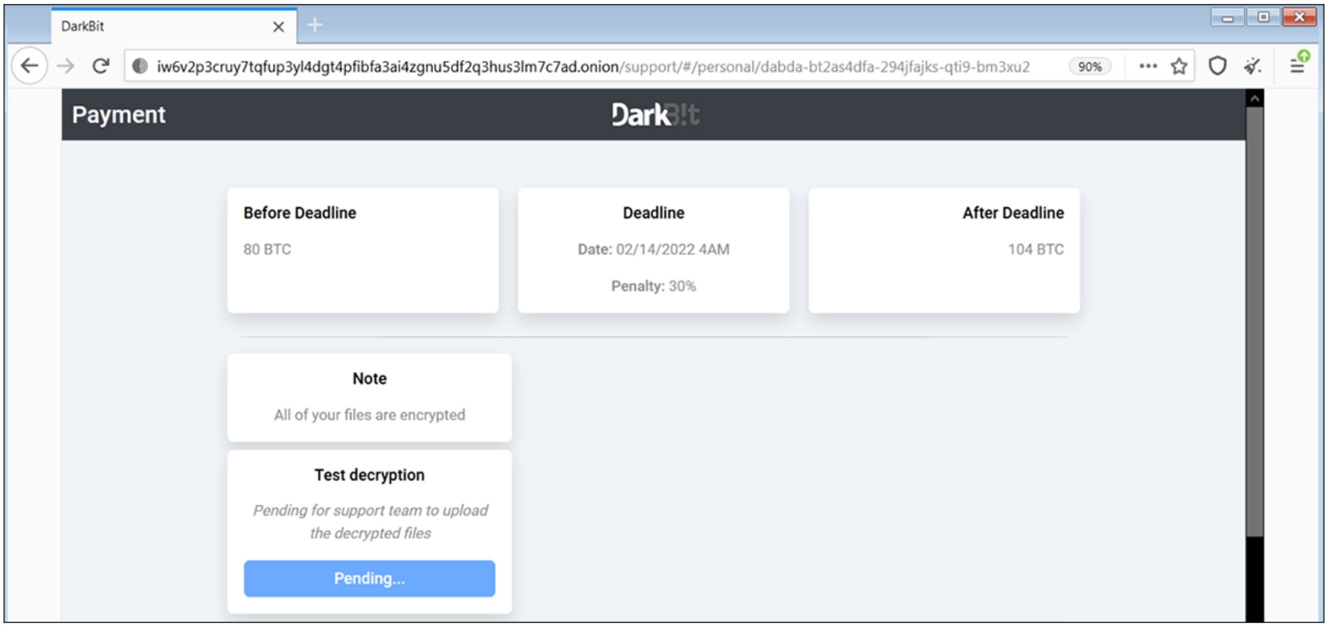
Against any kind of racism, fascism and apartheid

Follow us on telegram: @DarkBitChannel

Your ID

*Figure 5: DarkBit "support" page*

As an additional extortion method, 48 hours after its initial attack, the ransomware group demanded a further 30% penalty (24 BTC) to pressurize the university into immediately paying the specified sum.


DarkBit
iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad.onion/support/#/personal/dabda-bt2as4dfa-294jfajks-qti9-bm3xu2
90%
Payment
DarkB!t

| Before Deadline | Deadline | After Deadline |
|---|---|---|
| 80 BTC | Date: 02/14/2022 4AM<br>Penalty: 30% | 104 BTC |

**Note**

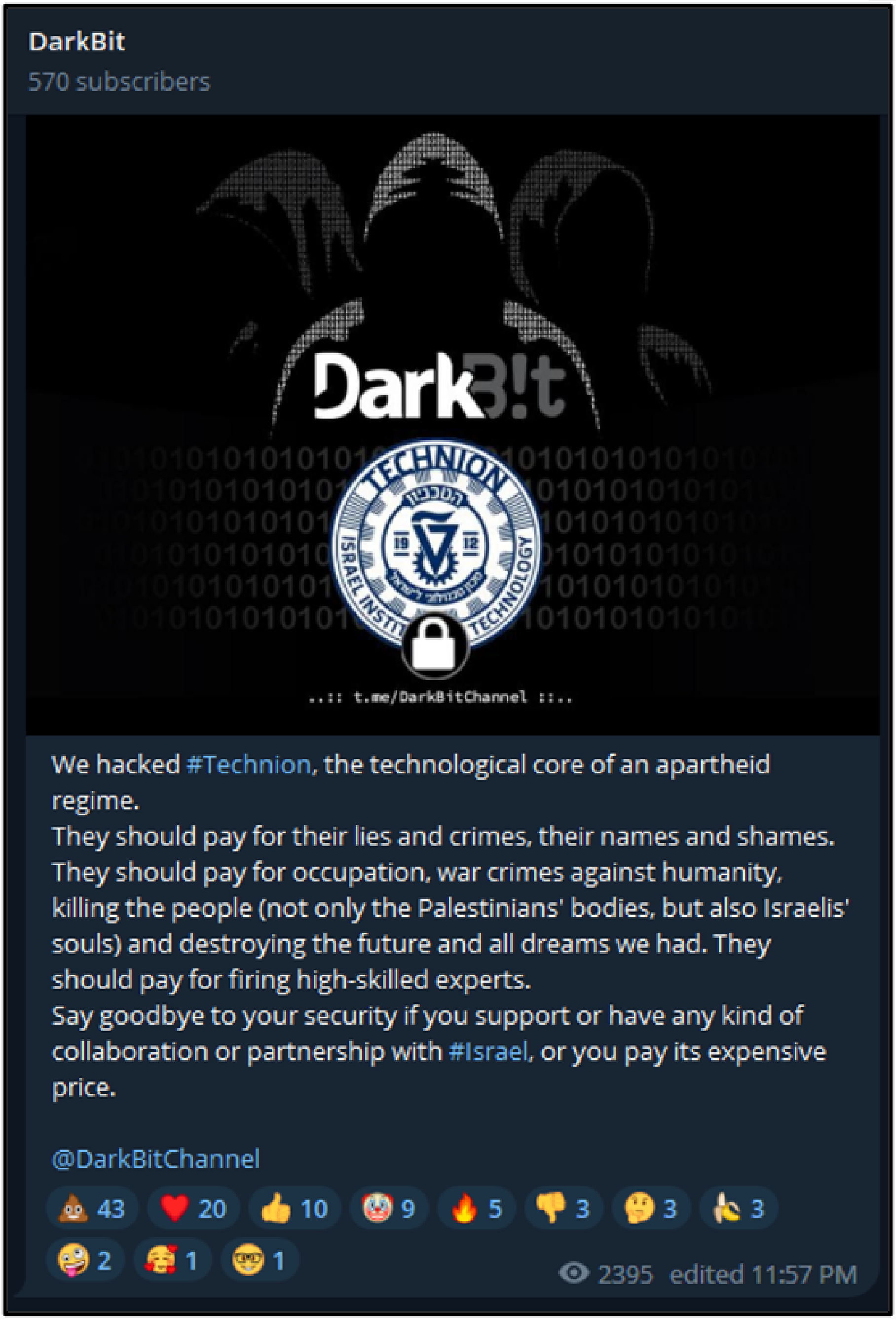
All of your files are encrypted

**Test decryption**

*Pending for support team to upload the decrypted files*

*Figure 6: Victim payment information page*

Furthermore, the DarkBit group has a Telegram account where it was last noted to be boasting about the hack of the university, citing more anti-Israeli rhetoric.



DarkBit
570 subscribers

We hacked #Technion, the technological core of an apartheid regime.
They should pay for their lies and crimes, their names and shames.
They should pay for occupation, war crimes against humanity, killing the people (not only the Palestinians' bodies, but also Israelis' souls) and destroying the future and all dreams we had. They should pay for firing high-skilled experts.
Say goodbye to your security if you support or have any kind of collaboration or partnership with #Israel, or you pay its expensive price.

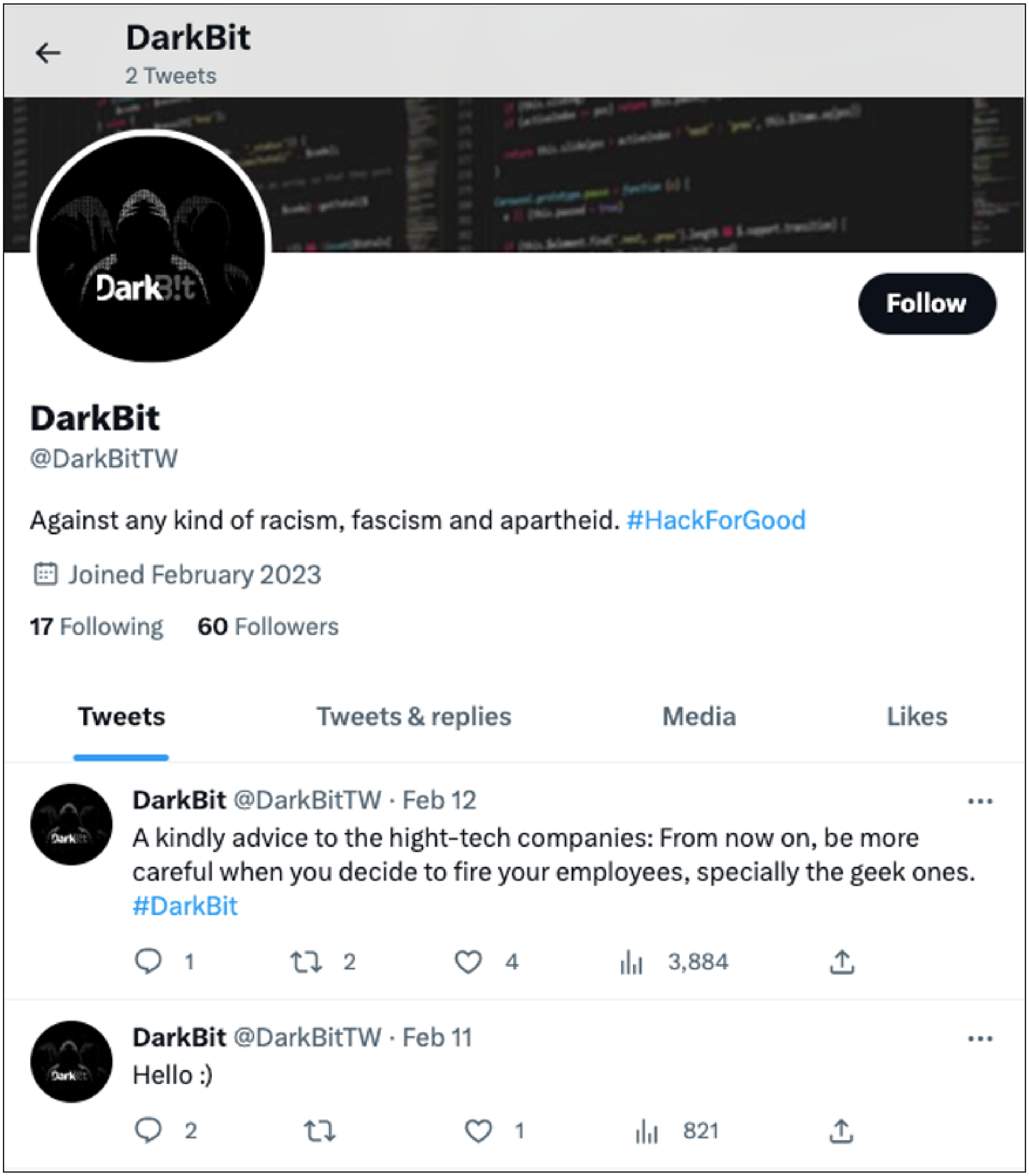
@DarkBitChannel

💩 43 ❤️ 20 👍 10 🤡 9 🔥 5 👎 3 🤔 3 🍌 3
🤪 2 🥰 1 🤓 1 👁 2395 edited 11:57 PM

*Figure 7: The DarkBit ransomware group’s Telegram page*

DarkBit also has a Twitter page containing similar political messaging as was seen in the ransom note, with the Twitter handle (@)DarkBitTW. It promotes the hashtag “#HackForGood”.

A Tweet from the account dated Feb 12th gives us a little more insight into the possible motivations of the threat actor, stating: “A kindly advice to the hight-tech [sic] companies: From now on, be more careful when you decide to fire your employees, specially [sic] the geek ones. #DarkBit”.


DarkBit

2 Tweets

DarkBit

@DarkBitTW

Against any kind of racism, fascism and apartheid. #HackForGood

Joined February 2023

17 Following 60 Followers

DarkBit @DarkBitTW · Feb 12

A kindly advice to the hight-tech companies: From now on, be more careful when you decide to fire your employees, specially the geek ones. #DarkBit

1 2 4 3,884

DarkBit @DarkBitTW · Feb 11

Hello :)

2 1 821

*Figure 8: DarkBit's Twitter page*

### Targets

*Figure 9:  DarkBit targets*

At the time of writing, the only known target of this new group has been the Technion - Israel Institute of Technology. However, given that DarkBit has set up a support site for victim interaction and payment facilitation, combined with their seemingly political motivations, new targets may come up in Israel in the near future.

## Attribution

Given the political theme behind the attack and the political and institutional rhetoric posted on the threat group's web pages, there may be other factors at play here besides financial motivation. Due to the note about tech layoffs on its Twitter page, it is conceivable that a disgruntled employee or group of employees may be behind this ransomware attack, unless this is simple misdirection.

Based on the code analysis, BlackBerry cannot link this group to any publicly known ransomware groups.

## Conclusions

Ransomware is no longer about financial gain. We have noted a growing trend where ransomware is used as a weapon in geopolitics. This trend began a few years ago in Ukraine. Today we now see it in Israel, used against one of the largest universities in the country. We should expect more ransomware attacks with geopolitical motivations as time goes by.

Ransomware is used as a blunt tool by threat actors because upon deployment, it immediately disrupts systems, causing reputational and financial damage; it may also result in financial benefit to the threat actor if the ransom is paid. Finally, the messages displayed on the ransomware's support pages and sites offer threat actors a public place to spread their own flavor of geopolitical propaganda.

## APPENDIX 1 – Indicators of Compromise (IoCs)

| | |
|---|---|
| **Hashes (md5, sha-256)** | 9880fae6551d1e9ee921f39751a6f3c0<br>9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff |
| **Ransom Note** | recovery_darkbit.txt |
| **Mutex in the System** | Global\dbdbdbdb |
| **Network Indicators** | hxxp://iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad[.]onion/support<br>TOX ID:<br>AB33BC51AFAC64D98226826E70B483593C81CB22E6A3B504F7A75348C38C862F00042F5245AC |

## APPENDIX 2 – Applied Countermeasures

### Yara Rules

```
rule Darkbit_Ransomware {
meta:
        description = "Yara rule based of the DarkBit Ransomware code"
        author = "The BlackBerry Research & Intelligence team"
        date = "2023-02-14"
        last_modified = "2023-02-15"
        distribution = "TLP:White"
        version = "1.0"
        sha256 = "9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff"
        md5 = "9880fae6551d1e9ee921f39751a6f3c0"

strings:
        $4538285_63 = { 9? 9? 9? 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? C6 ?? ??
?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 66 ?? E8 ?? ?? ?? ?? 48 ?? ?? 84 ?? 0F 85 }
        $5891110_63 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 4C ?? ?? 48 ??
?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 4C ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? 0F 1F ?? ?? ?? 48 ?? ?? 0F 8E }
        $7545077_63 = { 48 ?? ?? ?? ?? ?? ?? 0F 1F ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ??
E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? 0F 84 }
        $5903045_63 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? B9 ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ??
?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? 4C ?? ?? 0F 1F ?? ?? ?? 48 ?? ?? 73 }
        $5127463_63 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ??
?? ?? 4C ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? ?? ?? 4C ?? ?? 0F 9E ?? 48 ?? ?? ?? ?? ?? ?? ?? 48
}
        $6072198_63 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ??
?? B9 ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 9? 48 ?? ?? 0F 84 }
        $4935722_63 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ??
?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 84 ?? 0F 85 }
        $4976425_63 = { 41 ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 4F ?? ?? ?? 4D ?? ?? ?? 41 ?? ?? ?? 0F 11 ??
?? ?? ?? ?? ?? 4F ?? ?? ?? 4D ?? ?? ?? 41 ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? 74 }
        $4527589_63 = { 48 ?? ?? ?? ?? 48 ?? ?? 0F B7 ?? ?? ?? 0F B7 ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 48 ??
?? ?? ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 9? 48 ?? ?? 7D }
        $4716056_63 = { 0F B6 ?? ?? ?? 0F B6 ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 48 ?? ??
48 ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? 66 ?? ?? ?? ?? B8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? C3 }
        $5798030_63 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F 1F ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ??
48 ?? ?? ?? ?? 9? 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? 83 ?? ?? ?? ?? ?? ?? 75 }
        $6047533_63 = { 0F B6 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? 48 ??
?? ?? ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 44 ?? ?? ?? ?? ?? 48 ?? ?? 48 }
        $7558727_62 = { 31 ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ??
?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? B9 ?? ?? ?? ?? BF ?? ?? ?? ?? E8 ?? ?? ?? ?? 0F 1F ?? 48 ?? ?? 0F 84 }
        $4266979_62 = { 48 ?? ?? ?? 48 ?? ?? 8B ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? FF D? 48 ?? ?? ?? ?? 0F B6 ??
?? 83 ?? ?? 88 ?? ?? 0F B6 ?? ?? BE ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? 66 ?? 74 }
        $5892010_62 = { 4B ?? ?? ?? 49 ?? ?? ?? 49 ?? ?? ?? ?? 49 ?? ?? ?? ?? 8B ?? ?? ?? ?? ?? ?? 4C ?? ??
?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 49 ?? ?? 0F 8F }
        $5132165_62 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 9? E8
?? ?? ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? ?? ?? 4C ?? ?? 0F 9E ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? EB }
        $6850214_62 = { 44 ?? ?? ?? ?? ?? 8B ?? 89 ?? ?? ?? 8B ?? ?? 89 ?? ?? ?? 8B ?? ?? 89 ?? ?? ?? 8B ??
?? 89 ?? ?? ?? 0F 10 ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? C3 }
        $4976188_62 = { 41 ?? ?? ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 4B ?? ?? ?? 48 ?? ?? ?? 0F 10 ?? 0F 11 ?? ??
?? ?? ?? ?? 4B ?? ?? ?? 48 ?? ?? ?? 0F 10 ?? 0F 11 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? ?? 0F 85 }
        $4610524_62 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ??
?? ?? ?? ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? 84 ?? 0F 85 }
        $6072616_61 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? B9 ?? ?? ?? ?? 0F 1F ?? E8 ?? ?? ??
?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 66 ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 0F 84 }
        $4442442_61 = { 4C ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? 44 ?? ?? ?? ?? ?? ?? ?? 45 ?? ?? ?? 41 ?? ?? ??
41 ?? ?? ?? 47 ?? ?? ?? 45 ?? ?? ?? 41 ?? ?? ?? 44 ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? 45 ?? ?? 0F 8E }
        $4448822_61 = { 48 ?? ?? ?? ?? 0F 1F ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ??
?? 48 ?? ?? ?? ?? 8B ?? 89 ?? C1 ?? ?? C1 ?? ?? 01 ?? C1 ?? ?? 41 ?? ?? C1 ?? ?? 29 ?? 85 ?? 0F 8C }
        $4726213_61 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 40 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? 4C ?? ??
4C ?? ?? E8 ?? ?? ?? ?? 4C ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 0F B6 ?? ?? ?? 4C ?? ?? ?? ?? 48 }
        $5127401_61 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? E8 ??
?? ?? ?? 48 ?? ?? ?? ?? 4C ?? ?? ?? ?? 4C ?? ?? 0F 9E ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? ?? ?? EB }
        $4357770_61 = { 48 ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ??
?? 48 ?? ?? ?? ?? 0F 10 ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? 0F 10 ?? ?? ?? ?? ?? 0F 11 ?? ?? ?? 31 ?? EB }
        $5046026_60 = { 48 ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ??
?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? FF D? 66 ?? 48 ?? ?? ?? 0F 85 }
        $6918301_60 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? 0F 10 ?? ?? ??
?? ?? ?? 0F 11 ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? 0F 10 ?? ?? ?? ?? ?? ?? 0F 11 ?? ?? EB }
        $5651196_60 = { 0F 1F ?? ?? E8 ?? ?? ?? ?? 9? 66 ?? ?? ?? ?? ?? ?? ?? ?? ?? C6 ?? ?? ?? ?? ?? ?? ??
C7 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 66 ?? ?? ?? ?? ?? ?? ?? ?? ?? C6 ?? ?? ?? ?? ?? ?? ?? 31 ?? EB }
        $5735857_60 = { E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ??
48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 0F 1F ?? ?? E8 ?? ?? ?? ?? 83 ?? ?? ?? ?? ?? ?? 75 }
        $5058799_60 = { 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ??
?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F BA ?? ?? 73 }
        $4987306_60 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ??
?? 48 ?? ?? ?? 81 E? ?? ?? ?? ?? 44 ?? ?? ?? ?? 41 ?? ?? ?? 4C ?? ?? 9? 0F B6 ?? 40 ?? ?? ?? 75 }
        $4491881_60 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ??
?? 48 ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? 66 ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? 0F 82 }
        $5384124_60 = { 0F 1F ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ??
?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? 83 ?? ?? ?? ?? ?? ?? 75 }
        $6212553_60 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 9? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ??
?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F 1F ?? ?? 48 ?? ?? 0F 84 }
        $5991938_60 = { 4C ?? ?? 48 ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? 0F 94 ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ??
?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 4C ?? ?? ?? ?? ?? ?? ?? 89 ?? 48 }
        $4975050_60 = { 48 ?? ?? ?? ?? ?? ?? ?? 0F 10 ?? 0F 11 ?? ?? ?? ?? ?? ?? 0F 10 ?? ?? 0F 11 ?? ?? ??
?? ?? ?? 0F 10 ?? ?? 0F 11 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F 1F ?? 48 ?? ?? ?? 0F 8F }
        $7558357_59 = { 31 ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ??
?? ?? ?? ?? ?? ?? E8 ?? ?? ?? ?? B9 ?? ?? ?? ?? BF ?? ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? 0F 84 }
        $5152831_59 = { 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ??
0F 1F ?? ?? ?? E8 ?? ?? ?? ?? 48 ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? 48 }
        $4347563_59 = { 48 ?? ?? ?? ?? 66 ?? ?? ?? 48 ?? ?? 48 ?? ?? 48 ?? ?? 9? 9? 48 ?? ?? ?? 48 ?? ?? ??
?? ?? ?? ?? ?? ?? 48 ?? ?? 48 ?? ?? 48 ?? ?? ?? 66 ?? ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? 0F 83 }
        $6022661_59 = { 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 0F 1F ?? E8
?? ?? ?? ?? E8 ?? ?? ?? ?? 83 ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 89 ?? 48 }
        $6139378_59 = { 88 ?? ?? ?? 44 ?? ?? ?? ?? ?? C6 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? FF D?
48 ?? ?? ?? ?? 0F B6 ?? ?? ?? 48 ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? ?? 48 ?? ?? ?? ?? ?? ?? C3 }

    condition:
        uint16(0) == 0x5A4D and filesize < 10MB and all of them
}
```

**Related Reading**:

## About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back