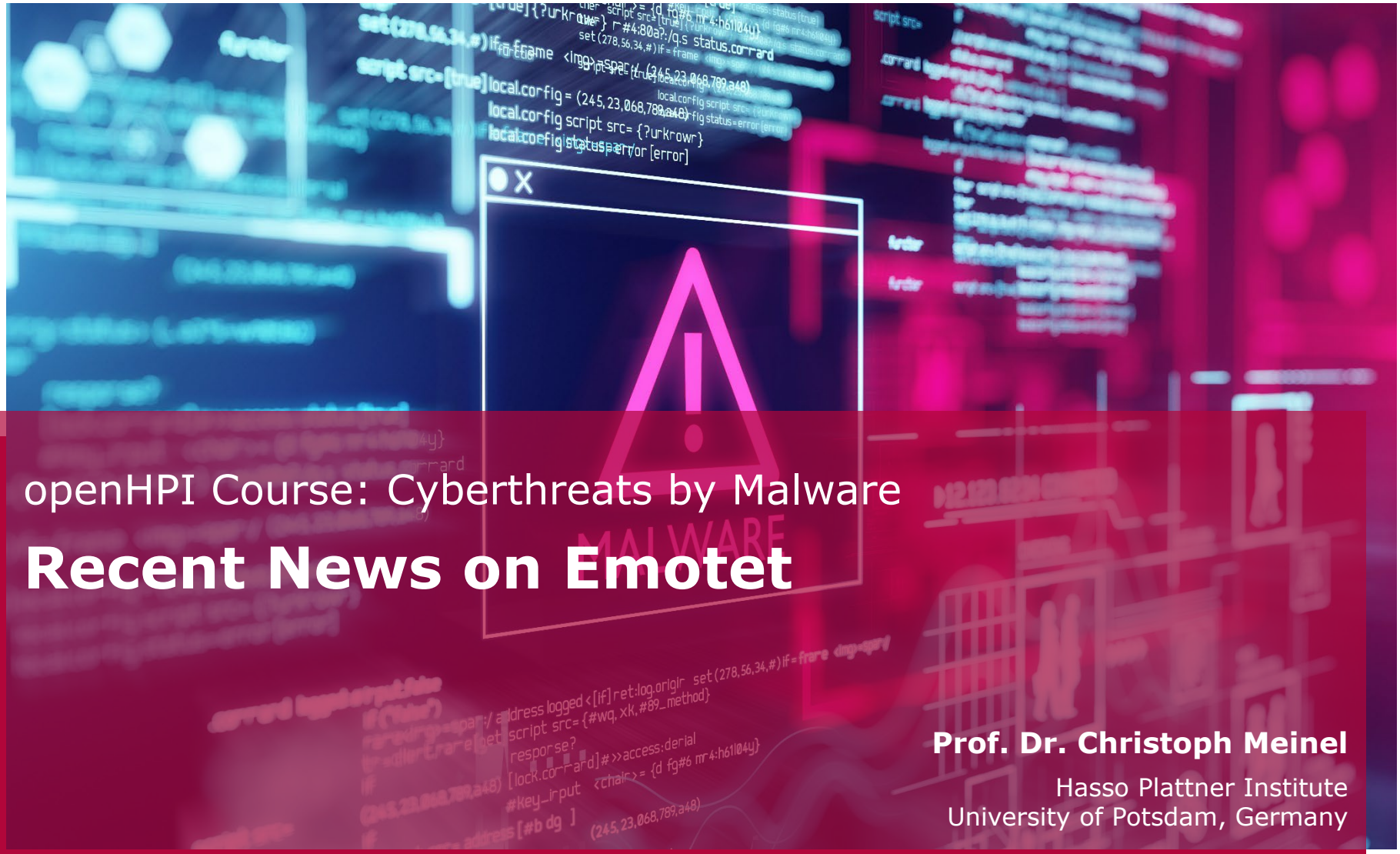


openHPI Course: Cyberthreats by Malware

Recent News on Emotet

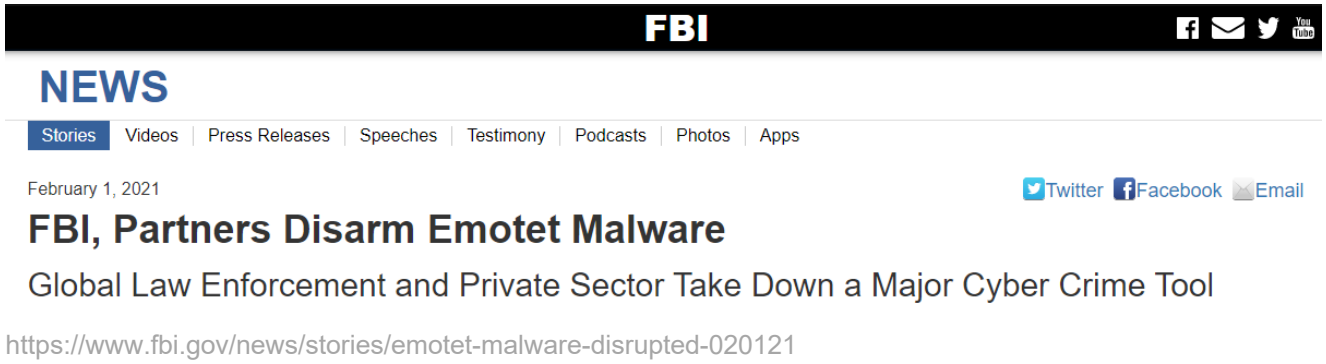
Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Emotet Over The Years

Over the years Emotet has been growing and became more than just a simple malware

- Emotet is able to change its code each time it is called up to avoid detection by antivirus programs
- It utilizes several hundreds of servers across the world with different functionalities to
  - manage the infected computer systems
  - make the network more resilient against takedown attempts
- Emotet has been used by further cybercriminals and malware operators to install other malwares on the victim‘s computer systems, such as TrickBot and Ryuk

Disarming of Emotet Malware (1/3)



https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121

https://www.eurojust.europa.eu/worlds-most-dangerous-malware-emotet-disrupted-through-global-action

Disarming of Emotet Malware (2/3)

On January 2021, law enforcement agencies from across eight countries orchestrated a coordinated takedown on Emotet

- They could gained control over the Emotet network infrastructure and took down the command and control server(s)
- Infected computer systems have been redirected towards law enforcement-controlled infrastructure

Disarming of Emotet Malware (3/3)

On January 2021, law enforcement agencies from across eight countries orchestrated a coordinated takedown on Emotet

- Shortly after, the law enforcements in delivered special payload to remove **Emotet** from all infected computer systems on **April 25th 2021** according to ZDNet

```
1  HANDLE sub_10005F10()
2  {
3    __time64_t v0; // rax
4    HANDLE result; // eax
5    __time64_t Time1; // [esp+0h] [ebp-10h] BYREF
6
7    Tm.tm_year = 121;
8    Tm.tm_mon = 3;
9    Tm.tm_mday = 25;
10   Tm.tm_hour = 12;
11   Tm.tm_min = 0;
12   _time64(&Time1);
13   v0 = _mktime64(&Tm);
14   *&Time1 = _difftime64(Time1, v0);
15   if ( *&Time1 > 0.0 )
16     sub_10005CE0(Time1, HIDWORD(Time1));
17   result = CreateThread(0, 0, StartAddress, 0, 0, 0);
18   if ( result != -1 )
19     result = CloseHandle(result);
20   return result;
21 }
```

MSDN Time Structure Documentation:

tm_mon	Month (0 - 11; January = 0).

April 25 2021

Source: https://twitter.com/MBThreatIntel/status/1354842730711502850

What's Next?

- Law enforcements will try to bring down more malwares and its network infrastructure in the future
- Meanwhile, cybercriminals will try to elude from the law enforcements while developing more advanced and resilient malware to infect more computer systems and profit from the victims
- You could check if your email addresses, usernames, and passwords has been compromised by EMOTET at www.politie.nl/emocheck