Phishing, Malware und Co.

Aktuelle Bedrohungen und Auswirkungen

Martin Fruhmann, MSc BSc

FH JOANNEUM
University of Applied Sciences

Über mich

Martin Fruhmann

- Studium IT & Mobile Security @ FH JOANNEUM
- Lehrender @ FH JOANNEUM
  - Netzwerk Technologien
  - Netzwerk Security
  - IT-Security
  - Penetration Testing
  - Phishing
- Sieger ACSC 2018 (Studentenwertung)


Darkside
Darkside
darksic [redacted] .onion/ [redacted]
Your network has been locked!
You need pay $ 2,000,000
190.363 BTC (+10%) - 22537.751 XMR
After payment we will provide you universal decryptor for all network.
Don't worry, we are good decryption specialists.
How to decrypt files ?

Colonial Pipeline US - Ransomware

- Initialer Angriff
  - Altes VPN Passwort
- DarkSide Ransomware (RU)
  - Ransomware as a Service (RaaS)
  - Data Exfiltration & Encryption

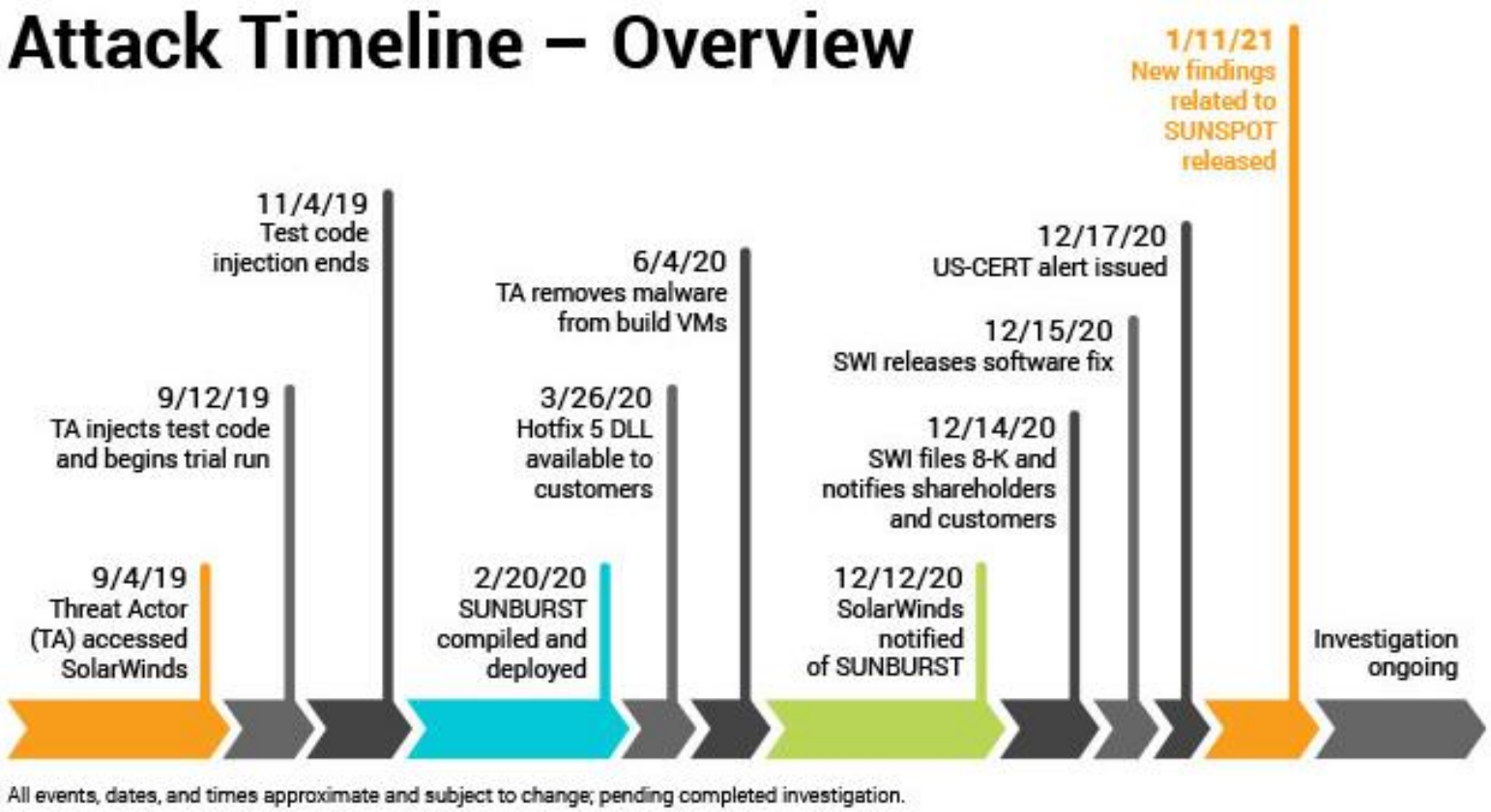
- Ransom:

- 75 Bitcoins paid – 4,4Mio$
- 63,7 Bitcoins recovered – 2,4Mio$

https://blog.malwarebytes.com/ransomware/2021/05/threat-spotlight-darkside-the-ransomware-used-in-the-colonial-pipeline-attack/

https://en.wikipedia.org/wiki/Colonial_Pipeline_cyber_attack

Solarwinds - Supply-Chain Attack

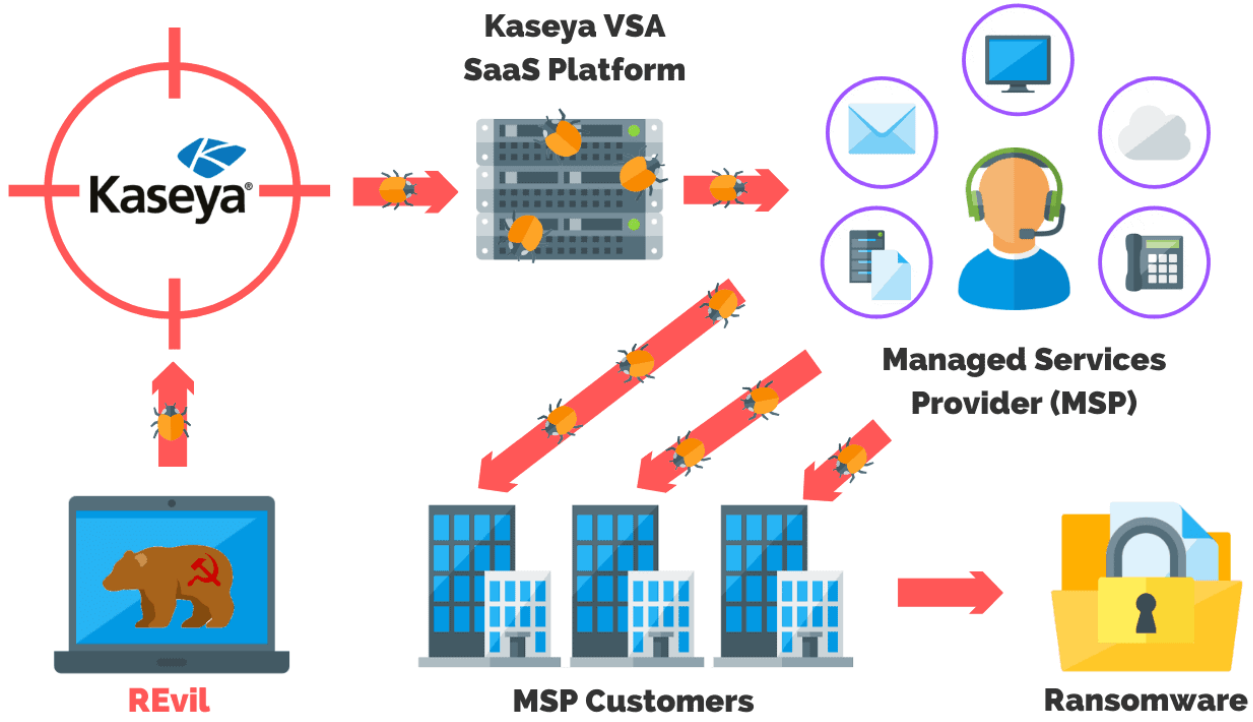


- 18.000 Kunden betroffen
- SUNBURST
  - HTTP Backdoor
- FireEye Red Team Tools gestohlen

https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/

Kaseya - Supply Chain Ransomware

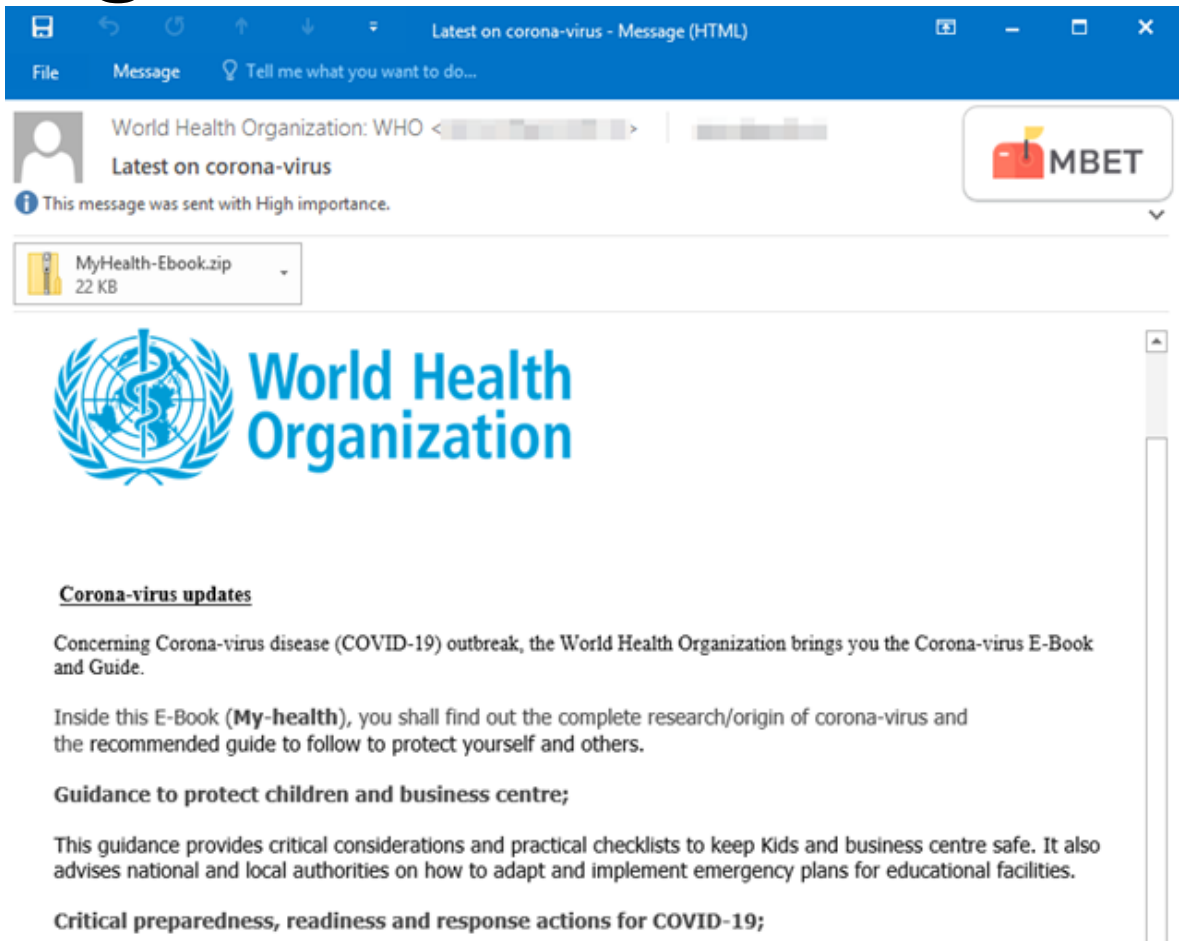
- Remote Monitoring & Management Software
- Zero-Day Vulnerability
  - CVE-2021-30116
- REvil Ransomware
- 60 Kunden (Managed Service Provider)
  - ca. 1500 Endkunden betroffen
- > 1 Million Systeme infiziert
- Insgesamt 70 Mio$ ransom



https://purplesec.us/kaseya-ransomware-attack-explained/

COVID-19 themed Phishing

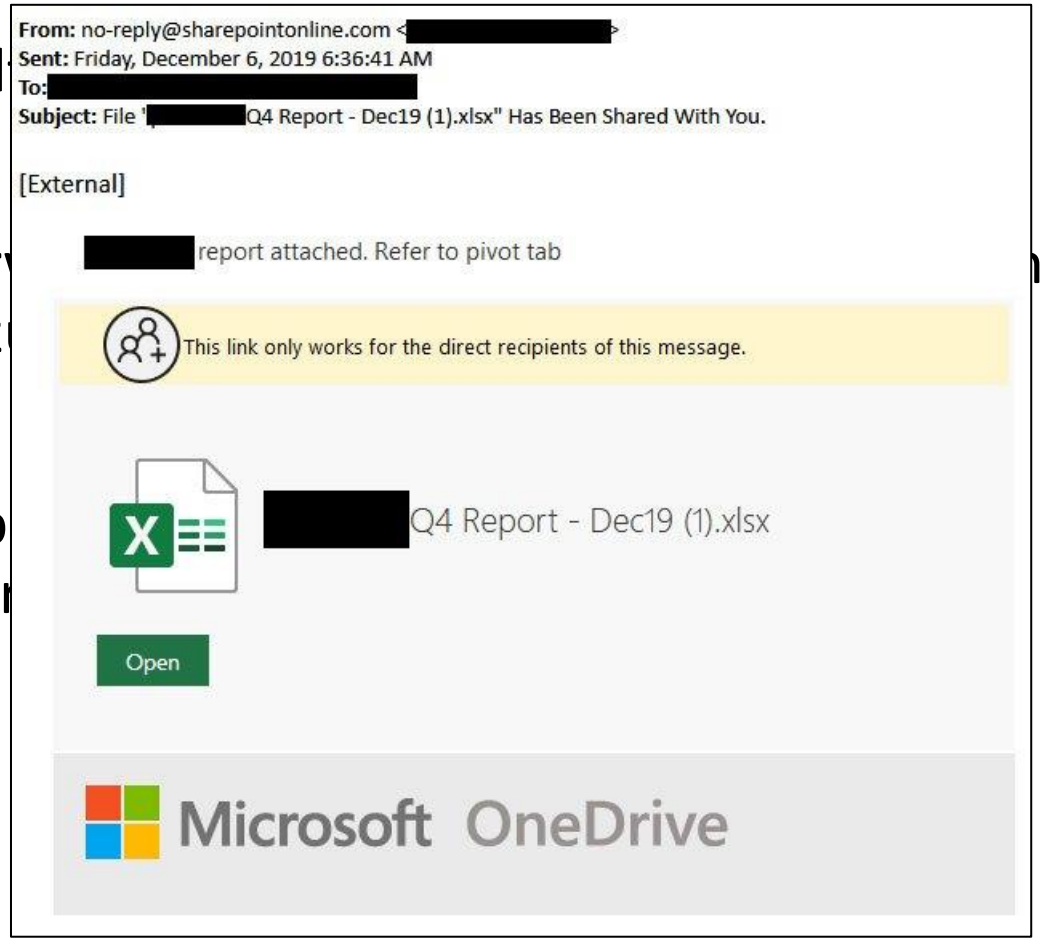
- World Health Organization (WHO)
- Neues Coronavirus E-Book
- FormBook Malware
  - Zugriff auf Clipboard
  - Keylogging
  - Stehlen von Browser Daten

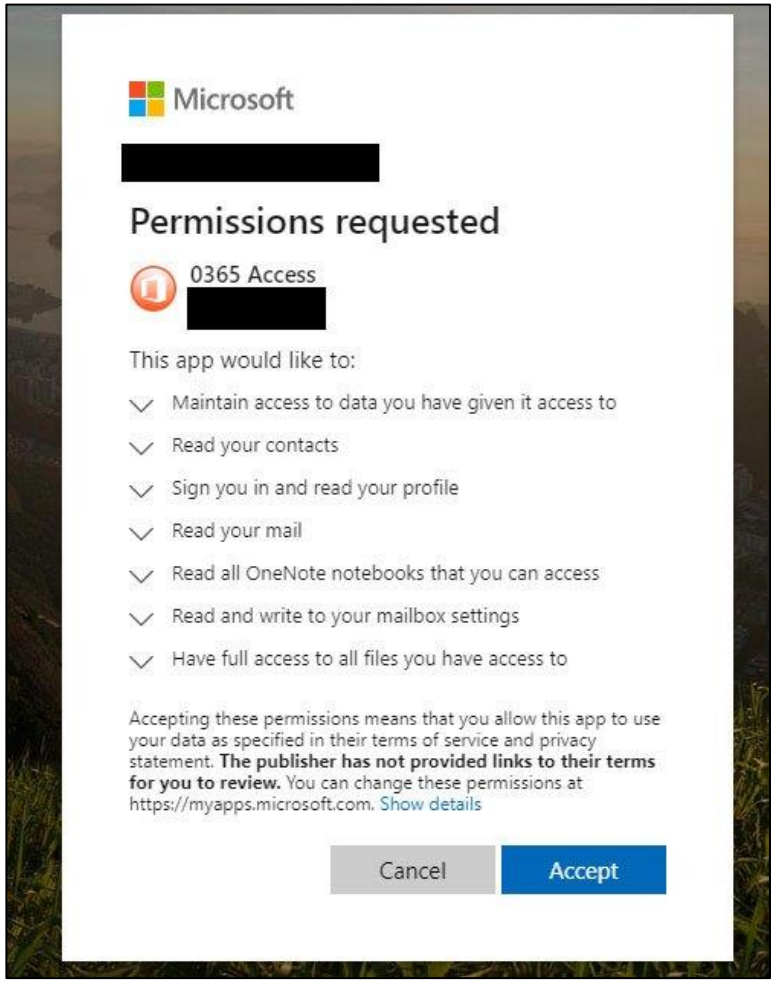


https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

Phishing for O365 Accounts with OAuth

- Ziel
- Ver
  abz
- Arb
  auf



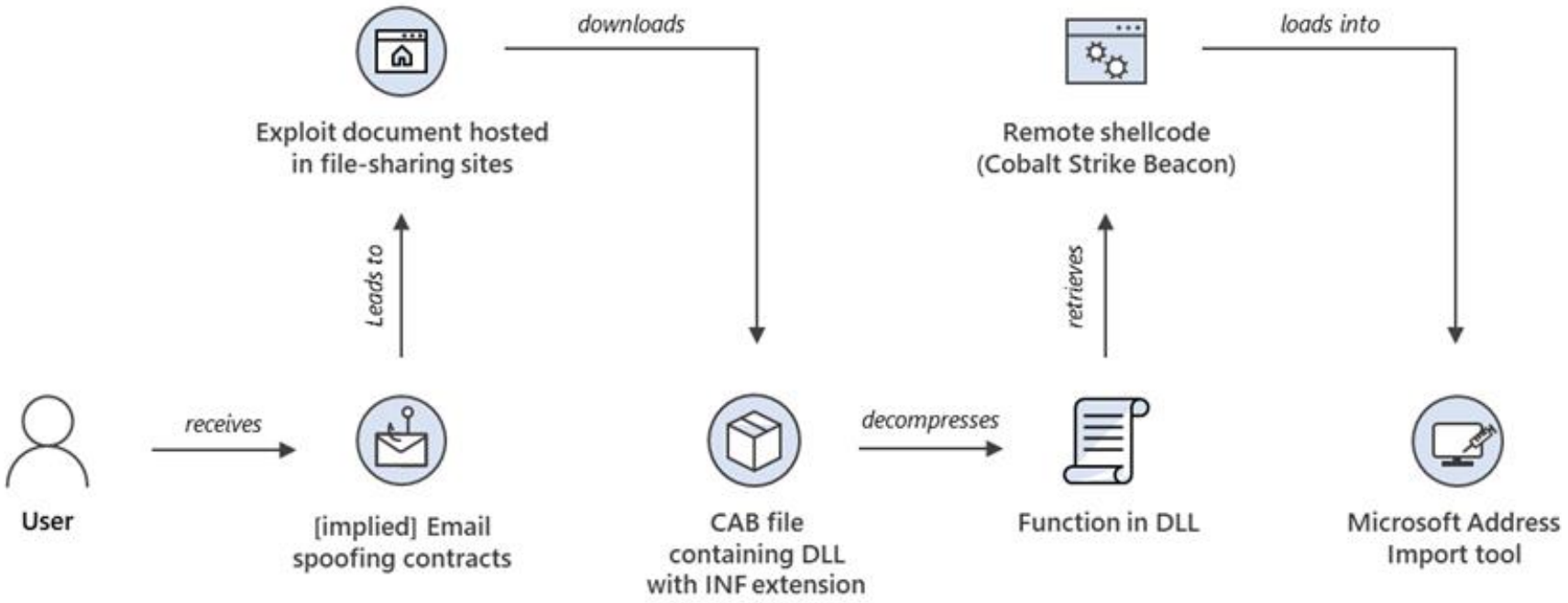


https://www.bleepingcomputer.com/news/security/phishing-attack-hijacks-office-365-accounts-using-oauth-apps/

CVE-2021-40444 – MSHTML Zero-Day

- Zero-Day Remote Code Execution in MSHTML
- Reported nach ersten Angriffen
- MSHTML in Office Dokumenten zur Darstellung von Web Content

CVE-2021-40444 – MSHTML Zero-Day



https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

Schutzmaßnahmen

- Software Updates
- Awareness Schulungen
- Passwort Richtlinien
- Datensicherung
- Regelmäßige Sicherheitsüberprüfungen