DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY

SEPTEMBER 2025

Arachna Ransomware

Date	27 / 09 / 25
Priority	Critical

Executive Summary

This report analyzes a suspicious Windows sample that exhibits strong ransomware-like activity: it drops persistent payloads (pok.exe, RunAsAdmin.kl), hijacks registry/COM entries, disables backup/recovery (shadow copy deletion and bcdedit changes), stops AV/backup services, and sprays ransom-note files (Restore-Files-Guide.hta/.txt) across system and vendor directories. The combination of persistence + deliberate backup/service disruption makes recovery difficult and elevates business-impact risk to critical.

Key Takeaways

This report is for CISOs, incident response leads, SOC analysts, IT operations and forensic teams. The attack was observed on a Windows host with user-level and administrator rights (paths under “C:\Users\<USER>\” and “C:\Users\Administrator\”). It has the potential to impact both workstation and enterprise server environments.

Hunt for the payload path “ %AppData%\Roaming\pok* ”, block the top hashes, and validate off-line/air-gapped backups before any remediation that could destroy evidence.

Indicators of Compromise (IoCs)

Hashes

4c7605574303c35975e0b34ae615268f
8ac407b3b3b9946539d18faefe7b8a36
576a10b52fdae33760574a9d7a8a181a
910f653e66396fdd663d2eb4508ee22e
1c6ca73d1d199f3851bd7eaa5785e504
d8b4afd871b9e0acaac35d88dcf4831a
40cc0c1f60df2fe9b09e7aa9a90941d8

IP

- UDP a83f:8110:0:0:64ca:1f00:0:0:53
- UDP 192.168.0.45:137
- UDP 192.168.0.52:137

Domains

- chocolatey.org
- javadl.oracle.com
- ln.sync.com
- localbitcoins.net
- schemas.microso
- schemas.xmlsoap.org
- www.coindesk.com
- www.reddit.com
- www.twitter.com
- www.wikipedia.com

Technical Analysis

Malicious / Suspicious Registry Activity from the VT Dump

1. Internet & Network Settings Manipulation (T1112 – Modify Registry, T1565 – Network Config)

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\
  - ZoneMap
  - Punycode
  - CreateUriCacheSize
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer*

These can be changed and used to bypass security zones, proxy redirection, or weakening browser protections.

---

2. COM Hijacking & CLSID / Interface Manipulation (T1546.015 – Event Triggered Execution: COM Hijacking)

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\
  - CLSID\{GUIDs}
  - Interface\{GUIDs}
  - WOW6432Node\CLSID\{GUIDs}
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
  - CLSID\{GUIDs}
  - Desktop\NameSpace\{GUIDs}

Malware can register malicious DLLs/EXEs to hijack COM object execution, persistence.

---

3. Command Processor Persistence (T1547.009 – Boot or Log on Autostart Execution: Shortcut Modification / Cmd AutoRun)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor
- HKEY_CURRENT_USER\Software\Microsoft\Command Processor

Attackers set AutoRun commands here so cmd.exe always executes their payload.

---

4. Explorer Hijacking / Shell Modification (T1547.004 – Boot or Logon Autostart: Winlogon / Shell)

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{...}
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{...}

Used for persistence by adding malicious shell folders or fake drives.

---

5. Policy Tampering (T1562 – Impair Defenses, T1112 – Modify Registry)

- HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\
  - Appx
  - CurrentVersion\Internet Settings

Malware may disable security features, prevent app restrictions and weaken sandboxing.

---

6. .NET Framework & Fusion Abuse (T1127 – Trusted Developer Utilities Proxy Execution, T1059.005 – Command/Script via .NET)

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\

- .NETFramework
- Fusion

Indicators of .NET assembly injection or forcing custom runtime configs.

---

7. Security & Crypto Policy Keys (T1562.001 – Disable or Modify Tools, T1484 – Domain Policy Modification)

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy

Altering FIPS algorithm policies can downgrade encryption or enforce weak crypto.

---

8. Image File Execution Options (IFEO) Hijack (T1546.012 – Image File Execution Options Injection)

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options*.exe

Uses classic malware persistence trick — forces debugger or payload execution instead of real EXE.

Likely Benign / Common Noise

These keys are usually touched by normal Windows processes or apps and are not immediately malicious unless combined with the following:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
  - Cryptography*
  - SystemCertificates*
  - Windows NT\CurrentVersion* (general version, product name, etc.)
  - CurrentVersion\SideBySide
  - Windows\CurrentVersion\Winlogon (legitimate if values unchanged, malicious only if Shell/Userinit altered)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters

---

Files Opened

🟥 Malicious
Files strongly tied to the dropped malware (pok folder, software.exe, artifacts in Downloads).

- C:\Users\<USER>\AppData\Roaming\pok\RunAsAdmin.kl
- C:\Users\<USER>\AppData\Roaming\pok\pok.exe
- C:\Users\<USER>\AppData\Roaming\pok\pok.kl
- C:\Users\Administrator\AppData\Roaming\pok\RunAsAdmin.kl
- C:\Users\<USER>\Desktop\software.exe
- C:\Users\<USER>\Desktop\software.exe.config
- C:\Users\<USER>\Desktop\software.INI
- C:\Users<USER>\Downloads\2a21672372eec44d859a6fb86b9ea6ab848360495a1ace9fc489e6331c72597d.exe

- C:\Users\USER>\Downloads\2a21672372eec44d859a6fb86b9ea6ab848360495a1ace9fc489e6331c72597d.exe.config
- C:\Users\USER>\Downloads\2a21672372eec44d859a6fb86b9ea6ab848360495a1ace9fc489e6331c72597d.INI
- C:\Users\<USER>\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\software.exe.log

🟧 **Suspicious**

Files not inherently malicious but unusual in context — may indicate sideloading, persistence, tampering, or abuse. Worth monitoring:

- C:\Users\<USER>\AppData\Roaming\pok\ (entire folder structure)
- C:\Users\Administrator\AppData\Roaming\pok\
- C:\Users\<USER>\Desktop\CRYPTSP.dll (DLL dropped on Desktop = very unusual)
- C:\Windows\SYSTEM32\MSCOREE.DLL.local (local DLL redirection — common in DLL hijacking)
- C:\Windows\assembly\NativeImages_v4.0.30319_32\rZVNKT3lRTc38ca6461#\ (weirdly named, possibly injected assembly)
- Any <Anonymous Pipe> entries (can be used for IPC in malware process injection).

Malicious / Suspicious File Creations

Category	Count	Example Paths	Notes
Payload (pok.exe, RunAsAdmin.kl)	5	C:\Users\USER>\AppData\Roaming\pok\pok.exe	Main malware payload.
Ransom Notes (.hta/.txt)	120+	C:\ProgramData\Adobe\Restore-Files-Guide.hta C:\ProgramData\Microsoft\Restore-Files-Guide.txt	Spread across vendor/system directories.
Suspicious DLLs	3	C:\Users\<USER>\Desktop\CRYPTSP.dll	Likely sideloading attempt.
Start Menu Infection	10	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AutoIt v3\Restore-Files-Guide.hta C:\ProgramData\Microsoft\Windows\Start Menu\Programs\AutoIt v3\Restore-Files-Guide.txt	Ensures ransomware is launched at reboot via Startup folder.

Hijacking Adobe, Mozilla, OneDrive and Office paths	140+	C:\ProgramData\Adobe\ARM\Restore-Files-Guide.hta C:\ProgramData\Adobe\ARM\Restore-Files-Guide.txt C:\ProgramData\Microsoft Help\Restore-Files-Guide.hta C:\ProgramData\Microsoft Help\Restore-Files-Guide.txt C:\ProgramData\Microsoft OneDrive\setup\Restore-Files-Guide.hta C:\ProgramData\Microsoft OneDrive\setup\Restore-Files-Guide.txt C:\ProgramData\Microsoft\AppV\Setup\Restore-Files-Guide.hta C:\ProgramData\Microsoft\AppV\Setup\Restore-Files-Guide.txt	Ransomware intentionally places ransom instructions in third-party vendors' directories, so the victim sees them during normal use.
Suspicious Custom Microsoft file	1	C:\ProgramData\Microsoft\SmsRouter\MessageStore\SmsInterceptStore.db	Data exfiltration or communication log.
Suspicious Custom Mozilla file	1	C:\ProgramData\Mozilla\UpdateLock-E7CF176E110C211B/profile_count_E7CF176E110C211B.json	Likely tampering with browser update mechanism.

Potentially Normal (but contextually suspicious)

Category	Paths	Notes
System reset logs	C:\$SysReset\AppxLogs\RestoreDownlevelAllUserStore.log C:\$SysReset\Logs\setupact.log C:\$SysReset\Logs\setuperr.log	Normally created during Windows reset/recovery, but ransomware may abuse '$SYSReset' directory as a cover location.
Microsoft caches and DBs	C:\ProgramData\Microsoft\Network\Downloader\qmgr.db C:\ProgramData\Microsoft\Network\Downloader*.log C:\ProgramData\Microsoft\Search\Data\Applications\Windows*.jcp/ *.jtx	Normal for BITS/Windows Search. If timestamps align with ransomware execution, then its highly suspicious.
User account pictures	C:\ProgramData\Microsoft\User Account Pictures*.png / .dat	Normally, part of Windows profile setup. If written at ransomware runtime, then its highly suspicious.

Files Dropped

Category	Paths	Notes
C:\Users\<USER>\Desktop\software.exe	5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9	RunAsAdmin.kl
C:\Users\user\Desktop\executable.exe	0b2f49a209d901d04cfc23f02cdab022b4601b6c1eadbcfba31d1dcbeb86ee59	C:\ProgramData\chocolatey\lib\KB2919442\KB2919442.nupkg
	7050755f78b60c8d8cf4b5ab77bc7ab4b143a694cc9f974a1239f590ef8f5089	C:\ProgramData\chocolatey\lib\adobereader\adobereader.nupkg
	a74471d42d7b2a73f783aa71e66a412452f0d7d42728e2edf437cf4030f41008	C:\ProgramData\chocolatey\lib\jre8\jre8.nupkg
	77c7708ae344f424a7bc1dcb9cf943bfb15c4920d797ad910d7e616752ffb4ec	C:\Users\user\Desktop\HSXUJGZEKP\WONVOJDAUI.xlsx
	509925a9b7057c080f464e411b133f3638b7d4406d1b469f7fb0c29221dce704	C:\Users\user\Desktop\JWSYIVBBQO\TEDVQCNKDQ.mp3
	7743b3bd15e366fa891cb235fea6ce7d936dba41066923393f58f9e4e9d22659	C:\Users\user\Desktop\WONVOJDAUI.jpg
\Device\ConDrv	43b5390113dcbfa597c4aaa154347d72f660db5f2a0398eb3c1d35793e8220b9	C:\Windows\SysWOW64\wbem\WMIC.exe

Process Created

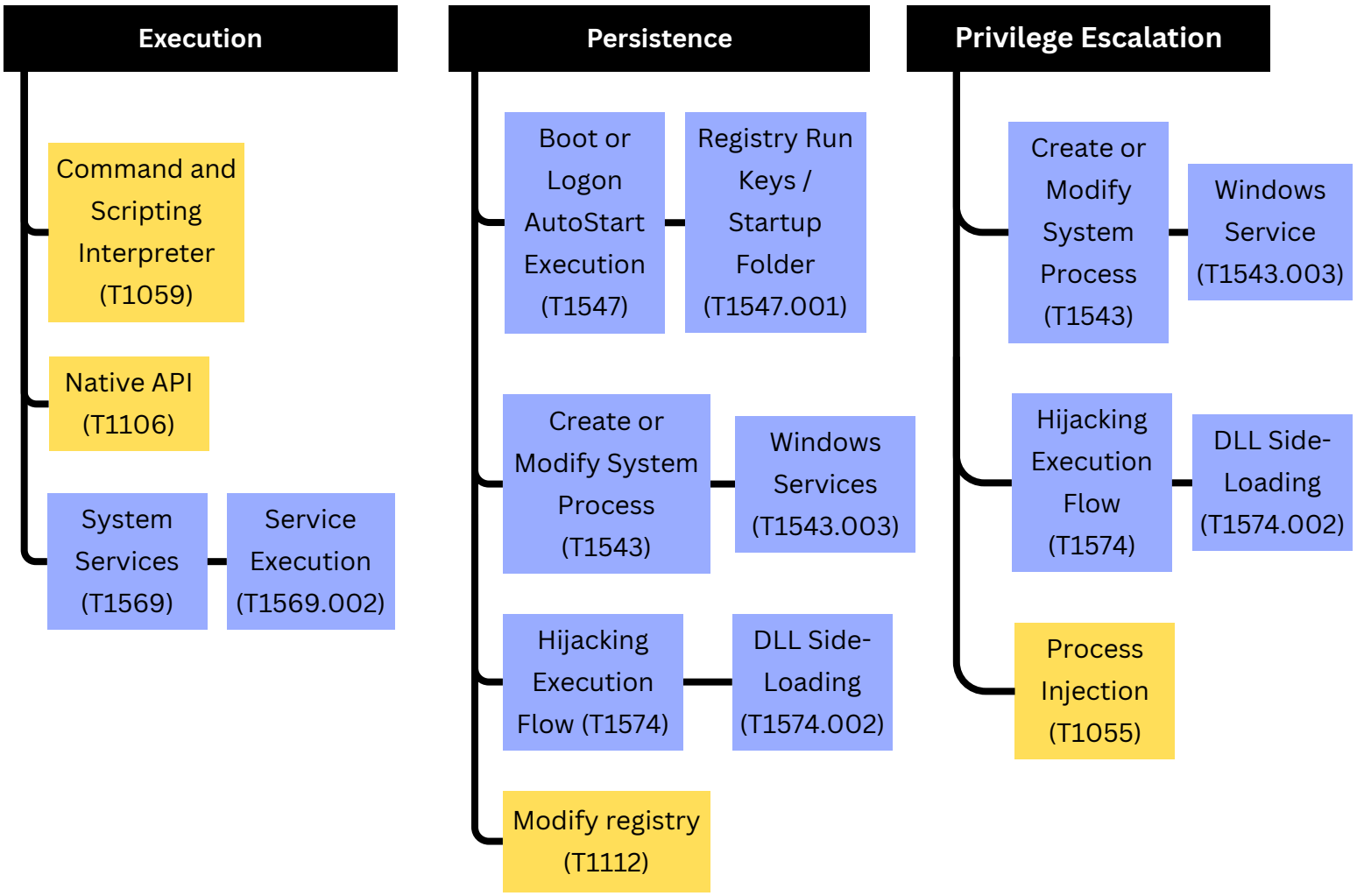
Task	Processes Created
Primary Malicious Process	C:\Users\<USER>\Desktop\software.exe C:\Users\user\Desktop\executable.exe

System Recovery & Shadow Copy Tampering	cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures
	cmd.exe /C bcdedit /set {default} recoveryenabled no
	cmd.exe /C vssadmin delete shadows /all /quiet
	wmic shadowcopy delete
	wbadmin delete catalog -quiet
	sc delete VSS
Stopping Security and Backup Services	net.exe stop DefWatch /y
	net.exe stop McAfeeDLPAgentService /y
	net.exe stop VeeamTransportSvc /y
	net.exe stop YooBackup /y
	net.exe stop zhudongfangyu /y
Command/Utility Execution	cmd.exe
	sc.exe
	vssadmin.exe
	wbadmin.exe
	WMIC.exe / WmiPrvSE.exe
	conhost.exe

Shell Commands

Task	Shell Commands
	bcdedit /set {default} bootstatuspolicy ignoreallfailures
	bcdedit /set {default} recoveryenabled no
	vssadmin delete shadows /all /quiet
	wmic shadowcopy delete
	wbadmin delete catalog -quiet
	sc delete VSS
Stopping Security and Backup Services	net.exe stop Sophos System Protection Service /y
	net.exe stop Symantec System Recovery /y
	net.exe stop MSExchange /y
	net.exe stop MSSQL$VEEAMSQL2012 /y
	net.exe stop VeeamTransportSvc /y
	net.exe stop MySQL57 /y
	net.exe stop QBCFMonitorService /y
	net.exe stop RTVscan /y
	net.exe stop SavRoam /y
Malware Executables	%SAMPLEPATH%_1_2_a_2a21672372eec44d859a6fb86b9ea6ab848360495a1ace9fc489e6331c72597d.exe
	%SAMPLEPATH%\2a21672372eec44d859a6fb86b9ea6ab848360495a1ace9fc489e6331c72597d.exe

MITRE ATT&CK Tactics and Techniques

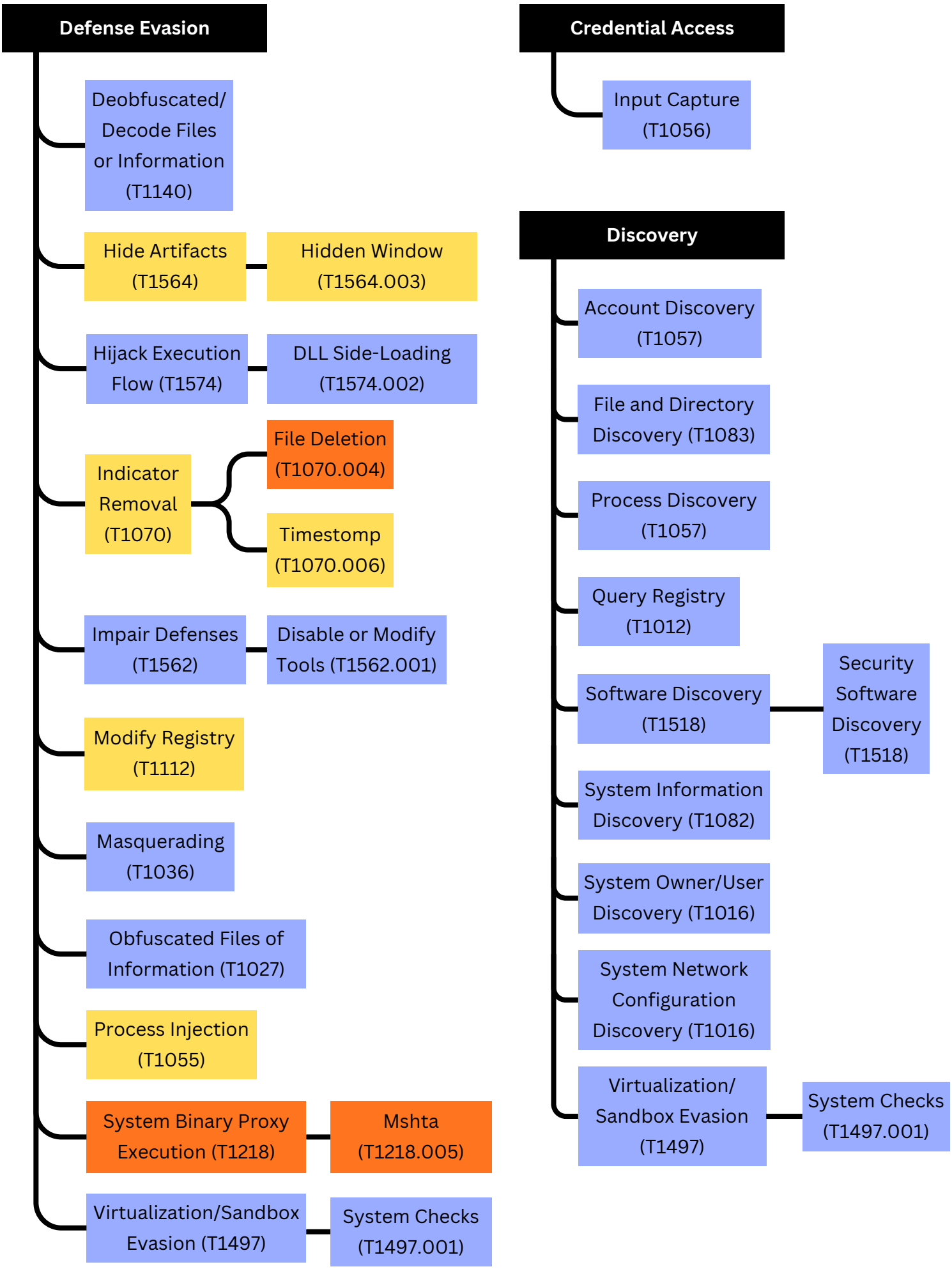


INFO - Informational, not necessarily malicious, but useful context

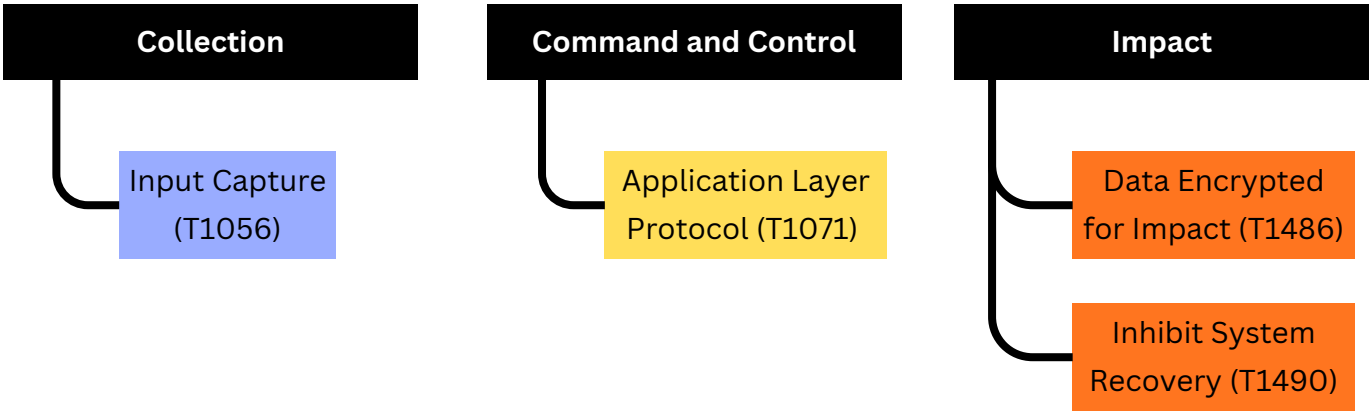
UNKNOWN - Suspicious, not confirmed malicious, needs deep investigation

LOW - Confirmed malicious but lower impact

MITRE ATT&CK Tactics and Techniques



MITRE ATT&CK Tactics and Techniques



X----X----X----X

EDR Freeze

A tool that puts EDRs and Antivirus into Coma State

Introduction

EDR-Freeze is a newly publicized user-mode tool that weaponizes Windows Error Reporting (WER) and the *MiniDumpWriteDump* facility to suspend Endpoint Detection & Response (EDR) and antivirus processes that effectively puts them "*into a coma*" long enough for an attacker to act without being observed.

The technique leverages WerFaultSecure.exe (a WER/PPL component) to invoke *MiniDumpWriteDump* against a security process, and then holds the dumper suspended so the target's process threads remain halted rather than being resumed. This results in a high-leverage, low-footprint primitive that can neutralize monitoring from user mode without needing custom vulnerable drivers.

Technical Analysis

Instead of using BYOVD (Bring Your Own Vulnerable Driver) technique in which first we have to install and execute drivers with vulnerabilities to exploit, we can use Windows Error Reporting to put the antivirus process into a state of dormancy. It will be done using uer-mode code and no third-party tools.

The *MiniDumpWriteDump* function, a Windows DbgHelp library, writes a minidump internally by suspending the target process threads to obtain a consistent snapshot and the state for debugging. It is done as threads can modify the memory when the dump is written which can lead to inconsistency.

Attack Primitive

Using *MiniDumpWriteDump* function with a process, it can be put into a suspended state but the function works very quickly and user may not even notice the the targeted process is suspended. A solution for this is to extend the execution time.

Here, we need the EDRs and antivirus processes, but these are protected by PPL (Protected Process Light), so we need to bypass PPL protection for interaction with these processes.

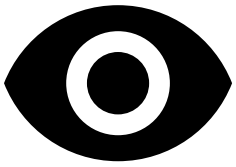
Steps to follow:

Use CreateProcessAsPPL tool to run a process at WinTCB level

CreateProcessAsPPL tool will run a PPL protected process using WerFaultSecure.exe

Use WSASS tool that uses old processes of WerFaultSecure.exe to dump process memory protected by PPL

Provide required parameters like /pid <PID> (process id), /tid <TID> (target thread id), etc. gathered using PPL



Continuously check the targeted process until it goes to suspended state

Once process is in suspended state use OpenProcess with PROCESS_SUSPEND_RESUME privilege and NtSuspendProcess

WerFaultSecure.exe will be in suspended/coma state

Antimalware process will be in suspended state as WerFaultSecure is in coma state

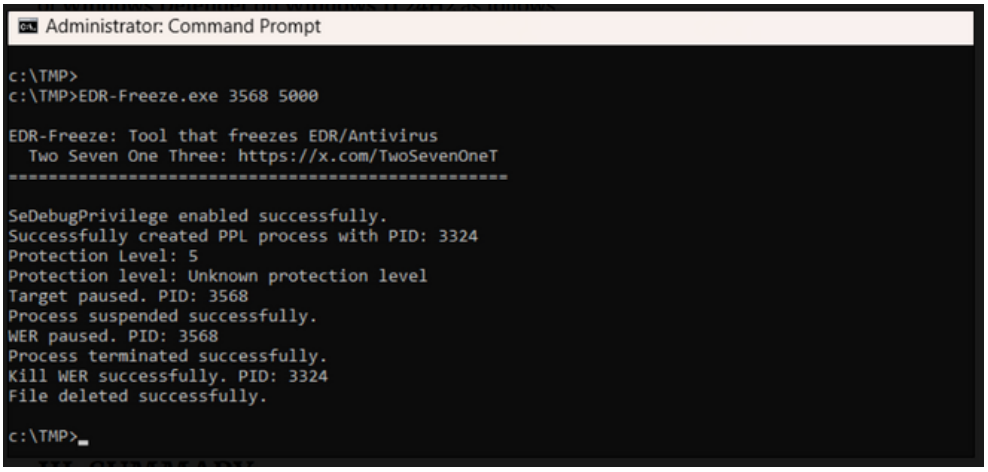
EDR-Freeze Tool

The developer has released the tool to demonstrate this technique. It takes 2 parameters

- PID of the program to be frozen
- Duration for which the process should be in suspended state

This allows attacker to disable security tools, perform malicious actions and when it is done then using security software, resume the suspended process.

A test was done to suspend *MsMpEng.exe* process (a process of Windows Defender on Windows 11 24H2).



Source - EDR-Freeze-Puts-EDRs-Antivirus-Into-Coma

The process *MsMpEng.exe* was successfully suspended for 5000 milliseconds.

Conclusion

As mentioned earlier, the primary flaw in BYOVD attack is it requires drivers with software flaws that can be exploited which can cause dangerous disruptions on targeted computers. This flaw can be fixed with EDR-Freeze by taking use of WerFaultSecure program's software flaw. We can also flexibily control EDR and antivirus programs so that everything runs smoothly.

To prevent EDR-Freeze from being used on the network, we should rely on WerFaultSecure's operating parameters and if it indicates the PID of sensitive programs like LSASS, antivitus software or EDR agents, then a deep investigation should be done.

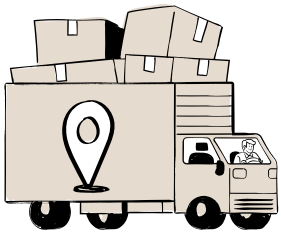
X----X----X----X

Asahi Group Cyberattack Highlights Rising OT Security Risks in Manufacturing

Introduction

On September 29, 2025, Asahi Group Holdings which is a major Japanese brewer / beverage company, announced a system failure caused by a cyberrattack, affecting its domestic operations. The attack forced the company to suspend their multiple operations like -

Order Processing



Shipment Operations

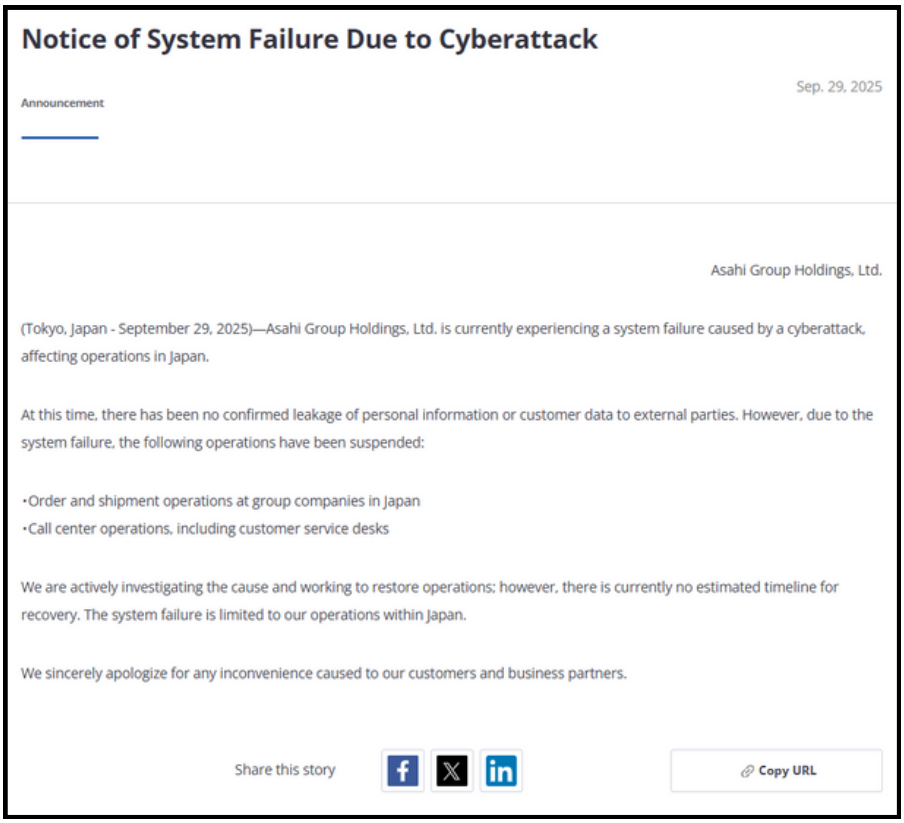
Call Center / Customer Service

The production at multiple factories is believed to be impacted, with machinery or control systems inaccessible or offline.

With a portfolio that includes not just its flagship Asahi beer but also the Peroni brand and Nikka whisky, Asahi Group Holdings is a huge player in the global beverage sector.

The retail and hospitality industries, which depend on steady supply, are immediately impacted by any disruption in its manufacturing and delivery network.

The company has acknowledged the event and is actively mitigating the disruption but they have not provided a timeline for full recovery.



Notice of System Failure Due to Cyberattack

Announcement

Sep. 29, 2025

Asahi Group Holdings, Ltd.

(Tokyo, Japan - September 29, 2025)—Asahi Group Holdings, Ltd. is currently experiencing a system failure caused by a cyberattack, affecting operations in Japan.

At this time, there has been no confirmed leakage of personal information or customer data to external parties. However, due to the system failure, the following operations have been suspended:

・Order and shipment operations at group companies in Japan
・Call center operations, including customer service desks

We are actively investigating the cause and working to restore operations; however, there is currently no estimated timeline for recovery. The system failure is limited to our operations within Japan.

We sincerely apologize for any inconvenience caused to our customers and business partners.

Share this story

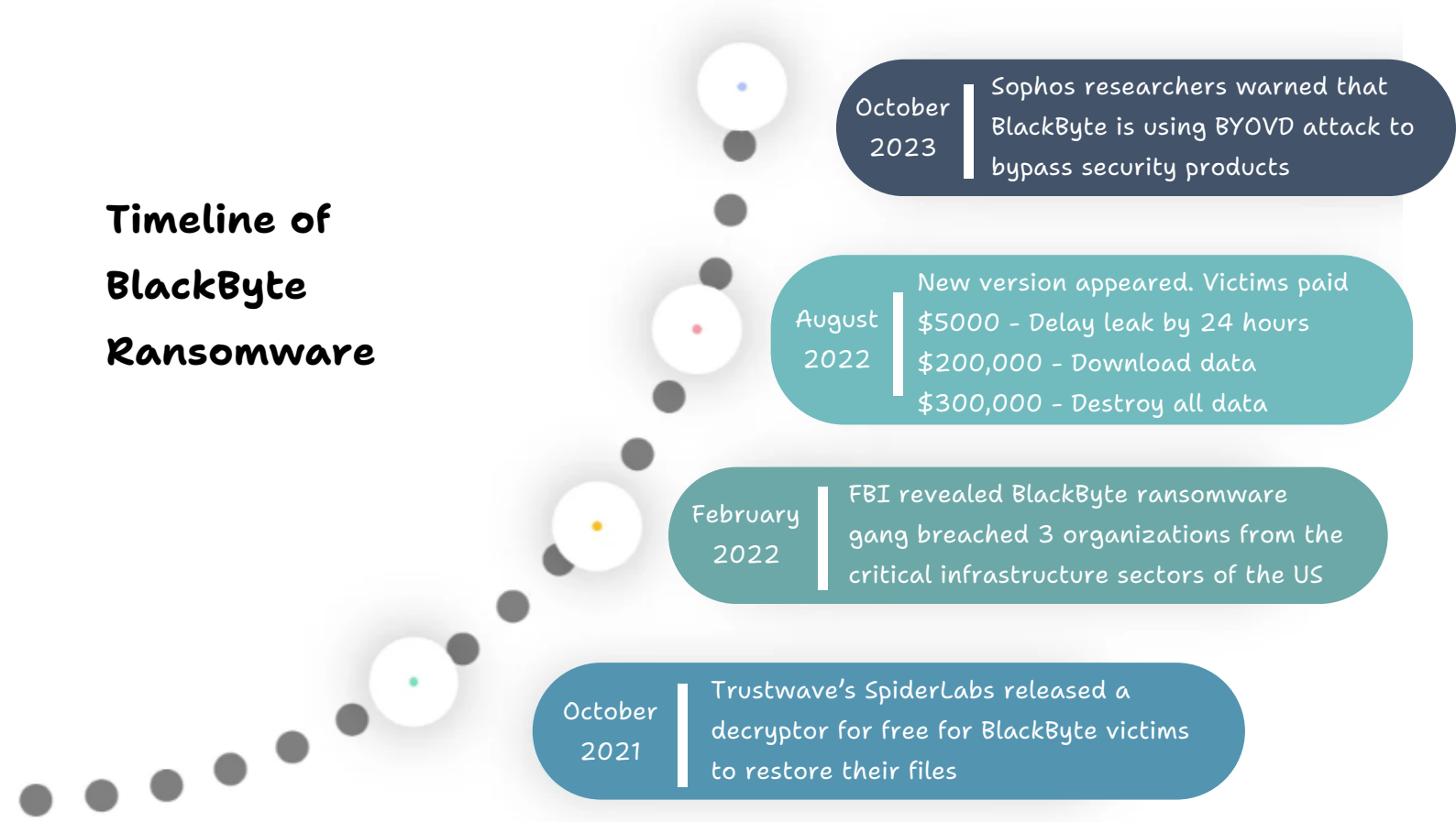
Copy URL

Source - Asahi Group Holdings notice

BlackByte Ransomware

The BlackByte ransomware group took credit for the attack on Japanese beer and beverage company Asahi Group. They claim to have stolen a large number of documents, probably in gigabyte size, from the Asahi Group including financial and sales report.

They are demanding $500k for buying the data and $600k to delete all of the stolen data.



Threat Patterns & Likely Attack Vectors

Though Asahi Group has not publically disclosed all details, typical patterns to watch for based on industry precedent:

- File encrypting ransomware or wiper malware targeting production or control servers.
- Lateral movement from IT to OT / ICS / MES / SCADA systems.
- Exploitation of unpatched vulnerabilities or weak access control.
- Supply chain / third-party software or vendor compromise as initial mechanisms.
- Attackers likely to disable monitoring, logging, or failover mechanisms.
- Time-of-attack coordination (e.g., midnight, weekends) to maximize disruption.

Implications for Similar Organizations

As this attack targeted the intersection of IT and OT/production systems, organizations with similar profiles of manufacturing, beverage/food and drink, large-scale supply chains, etc. should take this as a red flag. Key implications:

Operational Disruption Risk

Even without data exfiltration, attackers can cripple production, logistics, and downstream customer functions like ordering and shipping.

Supply Chain & Brand Impact

Extended downtime can damage customer realtionships, break supply commitments and lead to financial losses or reputational damage.

Deep Intrusion Capability

The scale suggests that the attacker had deep access into the control systems or the core infrastructure of Asahi Group Holdings.

X----X----X----X

Sources / References

VIrustotal Analysis of Arachna Ransomware

Zero Salarium: A tool that puts EDRS and Antivirus Into a Coma State
CreateProcessAsPPL tool
WSASS tool
EDR-Freeze tool

BlackByte ransomware group hits japanese beverage giant asahi group
Asahi Group Proof Block

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips