Exposed Fortinet Fortigate firewall interface leads to LockBit Ransomware (CVE-2024–55591)

By InTheCyber

Published: 2025-11-06 · Archived: 2026-04-29 02:07:47 UTC

10 min read

Oct 30, 2025

Authors: Marco Pedrinazzi (@pedrinazziM), Tommaso Tosi (@_tosto_), Davide Negri

Summary

InTheCyber got engaged in an incident response activity by an enterprise victim of LockBit3.0. The victim had no monitoring solution in place. Most of the logs on critical systems to analyze got encrypted by the threat actor and weak log retention policies did not allow us to reconstruct some dynamics of the attack.

Phase 1: Exploitation of CVE-2024–55591 (Days 1–6)

- **Day 1**: The attacker (TA) exploited **CVE-2024–55591** to bypass authentication and gain super-admin access to a Fortinet Fortigate Firewall.
- **Days 2–4**: The TA created **multiple admin accounts with VPN access**, configured firewall rules for unrestricted access, then deleted and recreated them to evade detection.
- **Day 5**: The TA tested VPN access for 2 minutes.
- **Day 6**: The TA **erased traces** of previous actions.

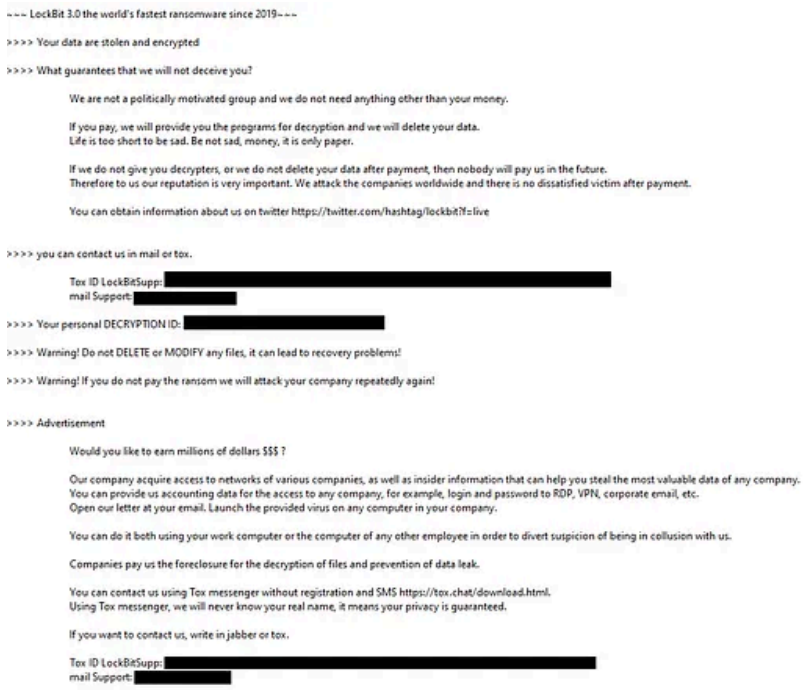
Phase 2: A new threat actor? (Days 7–8)

- **Day 7**: A new attacker (likely an access broker's buyer) used an existing VPN-enabled account to infiltrate the network without brute force. Due to **weak segmentation**, the TA could **move laterally across systems**. Used **RDP** to access domain controllers, backup servers (Veeam), and key machines, and then, the TA extracted **stored credentials** from Firefox browser data. Gained cloud access and modified **MFA settings** for persistence.
- **Day 8**: The TA initiated their actions on Day 8 by **dumping operating system credentials** through access to the **NTDS.dit file**, a critical Active Directory database often targeted for credential theft. They proceeded to **disable the Endpoint Detection and Response (EDR)** system's anti-ransomware features and manipulated alert settings to evade detection. Following this, they compromised multiple **Office365 accounts**, escalated privileges to **Global Administrator** and then unauthorized access to **SharePoint** files

containing stored passwords. Finally, the attacker **destroyed backups** stored on local NAS devices and cloud platforms via Azure App and then they **encrypted virtual machines**, causing significant operational impact and data loss.

Analysis

Press enter or click to view image in full size



~~~ LockBit 3.0 the world's fastest ransomware since 2019~~~

>>>> Your data are stolen and encrypted

>>>> What guarantees that we will not deceive you?

We are not a politically motivated group and we do not need anything other than your money.

If you pay, we will provide you the programs for decryption and we will delete your data.
Life is too short to be sad. Be not sad, money, it is only paper.

If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

You can obtain information about us on twitter https://twitter.com/hashtag/lockbit?f=live

>>>> you can contact us in mail or tox.

Tox ID LockBitSupp: [redacted]
mail Support: [redacted]

>>>> Your personal DECRYPTION ID: [redacted]

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!

>>>> Advertisement

Would you like to earn millions of dollars $$$?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.

You can do it both using your work computer or the computer of any other employee in order to divert suspicion of being in collusion with us.

Companies pay us the foreclosure for the decryption of files and prevention of data leak.

You can contact us using Tox messenger without registration and SMS https://tox.chat/download.html.
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, write in jabber or tox.

Tox ID LockBitSupp: [redacted]
mail Support: [redacted]

Ransom Note

Phase 1: Exploitation of CVE-2024–55591

This stage is related to days from 1 to 6 of the attack.

Day 1

Initial access — Exposed FW management leads to authentication bypass and a new super admin

On day 1, the TA created a new super-admin account by exploiting CVE-2024–55591. This vulnerability allowed the TA to bypass authentication using an alternate path or channel vulnerability affecting FortiOS and gain super-admin privileges via crafted requests to the Node.js web socket module. The threat actor exploited this vulnerability since the firewall's management console was exposed to the Internet.

Day 2, 3, 4, 5 and 6

Persistence — A new admin accounts with VPN access

On day 2, the super-admin account created by the threat actor created 5 local users and added them to the `ADMIN` group. The local user's name is a 6-character string made of random characters.
~~~

On day 3, the super-admin account created by the threat actor added a new local user following the same pattern as on day 2 but granting the user VPN access. In particular the threat actor,

- Adds `user.local` `<REDACTED>`
- Adds a new `firewall.address` `object_172_all_iZ`

```
subnet[172.16.0.0 255.240.0.0]
```

- Adds `firewall.address` `object_10_all_iZ`

```
subnet[10.0.0.0 255.0.0.0]
```

- Adds `firewall.address` `object_192_all_iZ`

```
subnet[192.168.0.0 255.255.0.0]
```

- Adds `vpn.ssl.web.portal` `<REDACTED>`

```
tunnel-mode[enable]ip-pools[SSLVPN_TUNNEL_ADDR1_<REDACTED>]split-tunneling-routing-address[10_all_iZ
```

- Adds `vpn.ssl.settings:authentication-rule` `<REDACTED>`

```
users<REDACTED>]portal[<REDACTED>]
```

- Changed SSL setting
- Edits `vpn.ssl.settings`

```
status[enable->enable]
```

- Adds `firewall.policy` `<REDACTED>`. This rule allows the created user above to access all internal network subnets over any service or port, without restriction, at any time. All traffic is logged.

```
name[<REDACTED>]srcintf[ssl.root]dstintf[any]action[accept]srcaddr[SSLVPN_TUNNEL_ADDR1_<REDACTED>]ds
```

On day 4, the super-admin account created by the threat actor deletes what they did on the firewall on day 3 but creates again a new user and grants it VPN access doing the same operations as in day 3.

On day 5, the threat actor connected to the victim's infrastructure via VPN for 2 minutes, no other activity was found in that timeframe, and we assumed the TA wanted to test the VPN connection.

On day 6, the TA deletes all activities done on the FW on day 4.

Get InTheCyber's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The source IPs from where the TA logged in are 45.55.158.47,37.19.196.65

Phase 2: A new threat actor?

Our hypothesis is that an initial access broker was involved in this campaign who gained access in `<REDACTED>` and sold the access in `<REDACTED>` (roughly a month later) to another attacker. This stage is related to days 7 and 8 of the attack.

Day 7

Initial access — A valid local account with VPN access

On day 7, the threat actor started the compromise of the victim's infrastructure by using the VPN connection from an account already present on the FW, no signs of brute force were detected. The threat actor kept the VPN connection active through all days 7 and 8. The IP from where the TA connected is 154.18.187.108.

Discovery

There was no indication of reconnaissance activities conducted by the attackers. It is believed they had access to both firewall logs and configurations, allowing them to assess firewall policies and identify key systems to target.

The threat actor was able to move laterally across most systems in the network due to insufficient network segmentation (with all targets being in the same subnet) and weak password policies, which enabled access to multiple servers with a single credential set.

The limited access to logs and the lack of network segmentation contributed to the success of the attack.

Lateral Movement via RDP & Defense Evasion via valid accounts & Initial access to the cloud & Persistence

The threat actor used RDP to connect to the domain controller and other machines in the victim's network. The account used for the connections was Administrator (Domain admin).

The threat actor connected via RDP to the backup machine (Veeam server) using the Domain admin account and the local Administrator account.

To evade detection, the threat actor used valid local and domain accounts.

The threat actor then created on the desktop of the backup machine a file called *1.csv*. This file contained the passwords to access several systems which later got compromised. We assume the TA acquired these credentials by reading files specific to the target browser (Firefox, in this case) which had all those credentials saved.

The threat actor later proceeded to log in on the cloud account `<REDACTED>@<REDACTED>` (*account1*, as reference) from 154.18.187.108, using either stolen or guessed credentials and then registered their contact information for MFA, ensuring persistence. Next, the system required to provide password reset information and the attacker entered their recovery details, granting even a stronger persistent access.

Day 8

Credential access — OS Credential Dumping by accessing the Ntds.dit file on volume shadow copy

On day 8, the TA connected again via RDP to the Domain Controller and it is able to dump OS credentials by accessing the Ntds.dit file on volume shadow copy. We assume that the file was exported since it was saved on `c:\windows\temp1\Active Directory\ntds.dit`

Defense Evasion — Disabled the EDR's anti-ransomware features

Later, the threat actor visited the web management console of the EDR from the backup machine's browser, where they disabled several features. Among these, disabling the anti-ransomware modules had the most significant impact, along with altering the email notification settings. The threat actor visited from the web browser all the target systems listed in the `1.csv` file created on day 7.

Credential access attempt

Next, the TA saved the SYSTEM registry hive on the Desktop of the Domain Controller which we believe was an attempt to get credentials via the registry hive dumping. SAM and SECURITY hives were not saved on the Desktop, and we did not detect any attempts to dump the hives on the machine, therefore we cannot determine if this technique succeeded or not.

Lateral movement to the cloud & Privilege Escalation

The TA compromised another account `<REDACTED>@<REDACTED>` (responsible for the *ADSync service)* (*account2*, for reference) because when the TA attempted to log in (again from 154.18.187.108) the password was expired and Office365 allowed the TA to change it and set the information required for the self-service password reset. Later, the TA added its own Authenticator to complete the MFA.

TA compromised 30 minutes later one account with Global Admin privileges on Office365 `<REDACTED>@<REDACTED>` (*account3*, for reference) via Password Hash Sync. The TA granted access to this account access a Veeam Azure App, which allowed the TA to delete the cloud backups.

Credential access — Searching for interesting files in SharePoint

The threat actor from this compromise was able to access the victims' enterprise SharePoint and access sensitive files and, especially, Excel files with passwords shared and available to everyone. The threat actor moved to the Trash and deleted several emails related to new role grants for this account. Next, the TA from the Global Admin account on Office365 reset the password of this account and the other two compromised accounts.

Execution & Impact — Encrypted VMDKs and destroyed backups

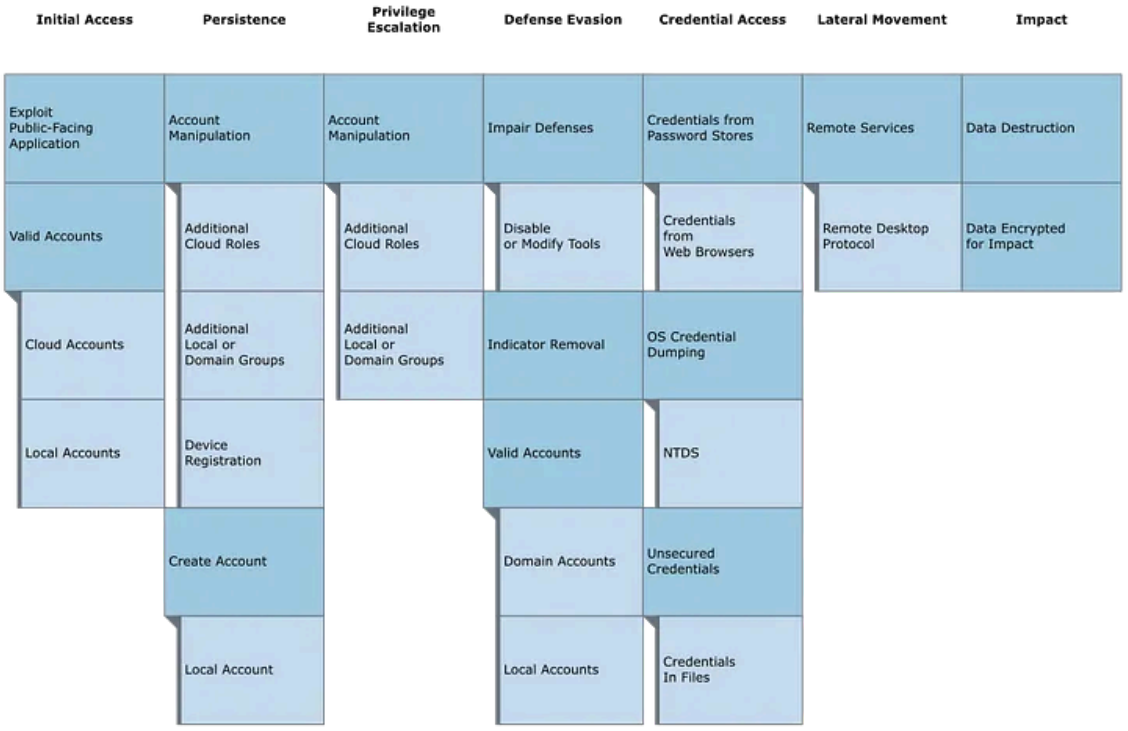
The threat actor encrypted the virtual machine files of the victim's enterprise and deleted all the backups. We could not get any logs on the ESXi nodes and on the VSphere node. The backups were stored on several NASs (virtualized, destroyed by accessing the VMs) and in the cloud (destroyed by using the AzureApp).

By the analysis of the outbound network traffic, we excluded the threat actor's exfiltrated data since the amount of data in the days of the attack was very small and aligned to the baseline of the previous days before the attack.

InTheCyber did not observe any trace of command and control activity since the threat actor was able to move laterally using RDP by having VPN access.

TTP

Press enter or click to view image in full size



Indicators

```
154.18.187.108
45.55.158.47
37.19.196.65
```

Detection

We built the following Sigma rules to detect the activities performed on the firewall based on what we observed during the Incident Response activity. The sigma rules are available here in the Sigma official repository.

```
title: FortiGate - New Administrator Account Created
id: cd0a4943-0edd-42cf-b50c-06f77a10d4c1
status: experimental
description: Detects the creation of an administrator account on a Fortinet FortiGate Firewall.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/390485493/config-system-admin
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.persistence
    - attack.t1136.001
logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Add'
        cfgpath: 'system.admin'
    condition: selection
falsepositives:
    - An administrator account can be created for legitimate purposes. Investigate the account detai
level: medium
```

```
title: FortiGate - New Local User Created
id: ddbbe845-1d74-43a8-8231-2156d180234d
status: experimental
description: |
    Detects the creation of a new local user on a Fortinet FortiGate Firewall.
    The new local user could be used for VPN connections.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/109120963/config-user-local
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.persistence
    - attack.t1136.001
logsource:
```

```
    product: fortigate
    service: event
detection:
    selection:
        action: 'Add'
        cfgpath: 'user.local'
    condition: selection
falsepositives:
    - A local user can be created for legitimate purposes. Investigate the user details to determine
level: medium
```

```
title: FortiGate - VPN SSL Settings Modified
id: 8b5dacf2-aeb7-459d-b133-678eb696d410
status: experimental
description: |
    Detects the modification of VPN SSL Settings (for example, the modification of authentication ru
    This behavior was observed in pair with the addition of a VPN SSL Web Portal.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/114404382/config-vpn-ssl-sett
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44546/44546-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.persistence
    - attack.initial-access
    - attack.t1133
logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Edit'
        cfgpath: 'vpn.ssl.settings'
    condition: selection
falsepositives:
    - VPN SSL settings can be changed for legitimate purposes.
level: medium
```

```
title: FortiGate - Firewall Address Object Added
id: 5c8d7b41-3812-432f-a0bb-4cfb7c31827e
status: experimental
description: Detects the addition of firewall address objects on a Fortinet FortiGate Firewall.
references:
```

```
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/306021697/config-firewall-add
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.defense-evasion
    - attack.t1562
logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Add'
        cfgpath: 'firewall.address'
    condition: selection
falsepositives:
    - An address could be added or deleted for legitimate purposes.
level: medium
```

```
title: FortiGate - New VPN SSL Web Portal Added
id: 2bfb6216-0c31-4d20-8501-2629b29a3fa2
status: experimental
description: |
    Detects the addition of a VPN SSL Web Portal on a Fortinet FortiGate Firewall.
    This behavior was observed in pair with modification of VPN SSL settings.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/113121765/config-vpn-ssl-web-
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.persistence
    - attack.initial-access
    - attack.t1133
logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Add'
        cfgpath: 'vpn.ssl.web.portal'
    condition: selection
```

```
falsepositives:
    - A VPN SSL Web Portal can be added for legitimate purposes.
level: medium
```

```
title: FortiGate - New Firewall Policy Added
id: f24ab7a8-f09a-4319-82c1-915586aa642b
status: experimental
description: Detects the addition of a new firewall policy on a Fortinet FortiGate Firewall.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/333889629/config-firewall-pol
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.defense-evasion
    - attack.t1562
logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Add'
        cfgpath: 'firewall.policy'
    condition: selection
falsepositives:
    - A firewall policy can be added for legitimate purposes.
level: medium
```

```
title: FortiGate - User Group Modified
id: 69ffc84e-8b1a-4024-8351-e018f66b8275
status: experimental
description: |
    Detects the modification of a user group on a Fortinet FortiGate Firewall.
    The group could be used to grant VPN access to a network.
references:
    - https://www.fortiguard.com/psirt/FG-IR-24-535
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/398/event
    - https://docs.fortinet.com/document/fortigate/7.6.4/cli-reference/328136827/config-user-group
    - https://docs.fortinet.com/document/fortigate/7.6.4/fortios-log-message-reference/44547/44547-l
author: Marco Pedrinazzi @pedrinazziM (InTheCyber)
date: 2025-11-01
tags:
    - attack.persistence
```

```
    - attack.privilege-escalation

logsource:
    product: fortigate
    service: event
detection:
    selection:
        action: 'Edit'
        cfgpath: 'user.group'
    condition: selection
falsepositives:
    - A group can be modified for legitimate purposes.
level: medium
```

In case you were wondering, these were us during the incident response activity ❤

Press enter or click to view image in full size