New Ransomware Operator Exploits Fortinet Vulnerability Duo

forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

March 13, 2025

Between late January and early March, Forescout Research – Vedere Labs identified a series of intrusions based on two Fortinet vulnerabilities. It began with the exploitation of Fortigate firewall appliances — culminating in the deployment of a newly discovered ransomware strain we have dubbed **SuperBlack**.

We attribute these intrusions to a threat actor we are tracking as "Mora_001" which follows our naming convention of using mythology from different regions. In this case, we're using Slavic mythology since the actor uses artifacts in Russian. This actor exhibits a distinct operational signature that blends elements of opportunistic attacks with ties to the LockBit ecosystem.

Mora_001's relationship to the broader Lockbit's ransomware operations underscore the increased complexity of the modern ransomware landscape – where specialized teams collaborate to leverage complementary capabilities. We recently highlighted this trend in our research on zero-day exploits targeting DrayTek routers.

This report details Mora_001's tactics, techniques, and procedures (TTPs), along with recommended detection and mitigation strategies. We will continue monitoring this actor and refining our assessment as we develop our understanding of their relationship to Lockbit.

Mora_001: Overview of a New Ransomware Operator

Here are the key characteristics of the newly identified Mora_001 threat actor exploiting CVE-2024-55591 and CVE-2025-24472 affecting Fortinet devices:

We are tracking Mora_001 as an independent threat actor while recognizing its ties to established ransomware operations based on the following factors:

1. **Consistent post-exploitation patterns** across the incidents we investigated, including:
    1. Creation of identical usernames across multiple victim networks
    2. Overlapping IP addresses used for initial access, post-exploitation, and command-and-control (C2) operations.
    3. Similar configuration backup behaviors in compromised environments
    4. Rapid ransomware deployment within 48 hours when conditions are favorable, with extended reconnaissance in environments with stricter security controls.
2. **Ransomware customization**
   The actor leveraged the leaked LockBit builder, modifying the ransom note structure by removing LockBit branding, and employing their own exfiltration tool.
3. **Relationship to LockBit**
   The ransom note includes the same TOX ID used by LockBit, suggesting a potential link to the infamous ransomware gang. This connection could indicate that Mora_001 is either a current affiliate with unique operational methods or an associate group sharing communication channels.

The post-exploitation patterns observed enabled us to define a unique operational signature that sets Mora_001 apart from other ransomware operators, including LockBit affiliates. This consistent operational framework suggests a distinct threat actor with a structured playbook, rather than multiple operators following a generalized LockBit methodology.

By analyzing the intrusion timeline, overlapping indicators, and operational patterns we can confidently attribute future intrusions to this entity – independent of its exact relationship to LockBit.

Analysis of Intrusions

From Fortinet Firewall Exploits to Ransomware Deployment

Our investigation identified intrusions across multiple environments, traced back to the exploitation of Fortinet firewall vulnerabilities. Below, we present near-complete firewall logs that were instrumental in reconstructing these attack sequences. To protect affected organizations still undergoing remediation, we have redacted dates, timestamps, and other sensitive details.

Initial Access and Persistence

CVE-2024-55591 and CVE-2025-24472 allow unauthenticated attackers to gain `super_admin` privileges on vulnerable FortiOS devices (<7.0.16) with exposed management interfaces.

A proof-of-concept (PoC) exploit was publicly released on January 27, and within 96 hours. we observed active exploitation in the wild using two distinct methods:

- **jsconsole**: Direct exploitation of the WebSocket vulnerability via the jsconsole interface. In logs, this activity appears as jsconsole(IP), with the IP address often spoofed as 127.0.0.1, 13.73.13.73, 8.8.8.8, 1.1.1.1, or other recognizable addresses
- **HTTPS**: Alternative exploitation method using direct HTTPS requests. While this method appears differently in logs, it targets the same underlying vulnerability.

We observed instances where the threat actor leveraged the default PoC exploit as well as slightly modified variants where only minor changes – such as altered usernames and IP addresses – were introduced.

The following log entries illustrate these activities:

```
<46>Jan 31 11:xx:49 xxxx xxx CEF:0|Fortinet|Fortigate|v7.0.13|32001|event:system
success|2|deviceExternalId=xxx FTNTFGTeventtime=xxx xxxtz=+xxx xxx=xx cat=event:system FTNTFGTsubtype=system
xxxlevel=information xxxvd=xxxlogdesc=Admin login successful xxxsn=xxx duser=admin sproc=jsconsole
xxmethod=jsconsole src=127.0.0.1 dst=127.0.0.1 act=login outcome=success reason=none profile=super_admin
msg=Administrator admin logged in successfully from jsconsole
```

```
Feb 01 xx:25:01 xxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event login|4|start=Feb
01 2025 xx:25:01 logver=xxx deviceExternalId=xxx dvchost=xxx vd=root eventtime=xxx tz=-xxx logid=xxx
cat=event subtype=system deviceSeverity=information logdesc=Admin login successful sn=xxx duser=watchTowr
sproc=jsconsole method=jsconsole src=13.37.13.37 dst=13.37.13.37 act=login status=success reason=none
profile=super_admin msg=Administrator watchTowr logged in successfully from jsconsole tz="-xxx"
```

We also observed initial login attempts using randomly generated five-character usernames, likely originating from automated scripts probing for vulnerabilities. These usernames were not added to the local admin user list.

The following activity was recorded:

```
ISP Null from Null used 1 IPs (13.37.13.37)over 26 days. Total attempts: 3269 (Suspicious: 0 [0%], Success:
3252 [99.48%]). Successful users: hoaue,bhqlz,vuiwe,onmne,durtv,nxbww,cwkvy,ussvm,. Failed/Suspicious users:
none. IPs seen in sources: fortinet_fortigate with 3425 total events across all sources. First seen: 2025-
01-30 15:18:55.468+00, Last seen: 2025-03-01 00:37:39.303+00
```

After successfully exploiting the vulnerability and verifying access using randomized usernames, the threat actor consistently created local system admin users in nearly every incident. The newly created accounts included: `forticloud-tech`, `fortigate-firewall` and `adnimistrator` (misspelled administrator):

The following log entries illustrate this activity:

```
{"itime": "xxx", "date": "2025-02-xx", "time": "xx:04:36", "devid": "xxx", "vd": "root", "type": "event",
"subtype": "system", "action": "login", "devname": "xxx", "dstip": "13.37.13.37", "eventtime": "xxx",
"idseq": "xx", "level": "information", "logdesc": "Admin login successful", "logid": "xxx", "logver": "xxx",
"method": "jsconsole", "msg": "Administrator FortiCloud logged in successfully from jsconsole", "profile":
"super_admin", "reason": "none", "sn": "xxx", "srcip": "13.37.13.37", "status": "success", "tz": "-xxx",
"ui": "jsconsole", "user": "FortiCloud"}
```

```
{"itime": "xx", "date": "2025-02-xx", "time": "xx:xx:xx", "devid": "xxxx", "vd": "root", "type": "event",
"subtype": "system", "action": "Add", "cfgattr": "password[*]accprofile[super_admin]", "cfgobj":
"forticloud-tech", "cfgpath": "system.admin", "cfgtid": "xxx", "devname": "xxx", "eventtime": "xxx",
"idseq": "xxx", "level": "information", "logdesc": "Object attribute configured", "logid": "xxx", "logver":
"xxx", "msg": "Add system.admin forticloud-tech", "tz": "-xxx", "ui": "jsconsole(13.37.13.37)", "user":
"FortiCloud"}
```

```
Feb 22 03:xx:10 xxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event Add|4|start=Feb 22
2025 03:xx:10 logver=xx deviceExternalId=xxx dvchost=xxx vd=root eventtime=xxx tz=-xx logid=xx cat=event
subtype=system deviceSeverity=information logdesc=Object attribute configured duser=sys_admin
sproc=ha_daemon act=Add cfgtid=xx cfgpath=system.admin cfgobj=admin_support
cfgattr=accprofile[super_admin]vdom[root]password[*] msg=Add system.admin admin_support tz="-xx"
```

In some cases, instead of relying on a single administrative account for all actions, the threat actor employed a chaining method, where each newly created administrative account was used to generate additional accounts. This approach is likely intended to complicate remediation efforts, making it more difficult to identify and revoke all compromised accounts.

Another common exploitation method we observed involved the threat actor using the `fortigate-firewall` account to exploit CVE-2025-24472 rather than CVE-2024-55591. The difference lies in the exploitation technique. Fortinet updated its advisory on February 11 to include CVE-2025-24472 after one of the victims we investigated contacted them to confirm our findings.

The following log entries illustrate this activity:

```
"Local_Process_Access" "Local_Process_Access" "root" "" "" "none" [192.168.1.179]:54145 [192.168.142.132]:80
```

```
{"itime": "xxx", "date": "2025-02-xx", "time": "xx:30:44", "devid": "xxxx", "vd": "root", "type": "event",
"subtype": "system", "action": "login", "devname": "xxxx", "dstip": "xxx.xxx.xxx.xx", "eventtime": "xx",
"idseq": "xxx", "level": "information", "logdesc": "Admin login successful", "logid": "xxx", "logver":
"xxx", "method": "https", "msg": "Administrator fortigate-firewall logged in successfully from https(80.66.8
8.90)", "profile": "super_admin", "reason": "none", "sn": "xx", "srcip": "80.66.88.90", "status": "success",
"tz": "-0500", "ui": "https(80.66.88.90)", "user": "fortigate-firewall"}
```

We also observed the addition of the PoC user “watchTowr” which was later removed by the threat actor after gaining access.

The following log entry illustrates this activity:

```
Feb 05 xx:38:21 xxxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event Delete|4|start=Feb
05 2025 xx:38:21 logver=xxx deviceExternalId=xxx dvchost=PIT-FG101E-FW1 vd=root eventtime=xxx tz=-0500
logid=xxx cat=event subtype=system deviceSeverity=information logdesc=Object configured duser=watchTowr
sproc=jsconsole(13.37.13.37)act=Delete cfgtid=xxx cfgpath=system.admin cfgobj=fortigate-firewall msg=Delete
system.admin fortigate-firewall tz="-0500"
```

After creating local administrator accounts, the threat actor downloaded the firewall configuration file, which contains critical information, including policies, routes, keys and VPN configurations. Additionally, logs indicate configuration changes made by the threat actor, suggesting modifications to system settings.

notice	System configuration backed up	User admin backed up the configuration from jsconsole(127.0.0.1)	jsconsole(127.0.0.1)	admin
alert	Configuration changed	Configuration is changed in the admin session	https(80.66.88.90)	fortigate-firewall

The actor created a scripted automation task to resynchronize the forticloud-sync user with a super_admin profile and a known password daily at a specified time. This ensures that even if the local account is manually removed from the firewall, it will automatically be recreated via “system.automation-action.

The following log entries illustrate this activity:

```
Feb 27 xx:13:49 xxxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event Add|4|start=Feb 27
2025 xx:13:49 logver=700120523 deviceExternalId=xxx dvchost=xxx vd=root eventtime=xx x tz=-xxx logid=xxx
cat=event subtype=system deviceSeverity=information logdesc=Object attribute configured duser=forticloud-
tech sproc=jsconsole(192.248.155.218)act=Add cfgtid=xxxx cfgpath=syst em.automation-action
cfgobj=Forticloud-Sync cfgattr=action-type[cli-script]minimum-interval[0]description[Automatically Syncing /
Updating the device - user definition]script[config system admin\nedit f orticloud-sync\nset password
#^(agT2^R96R-S_l4Y^HS#^\nset accprofile super_admin\nend\nexit]accprofile[super_admin] msg=Add
system.automation-action Forticloud-Sync tz="-XX"
```

```
Feb 27 xx:13:49 xxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event Add|4|start=Feb 27
2025 xx:13:49 logver=xxx deviceExternalId=xxx dvchost=xxx vd=root eventtime=xxx tz=-xx l ogid=xxx cat=event
subtype=system deviceSeverity=information logdesc=Object attribute configured duser=forticloud-tech
sproc=jsconsole(192.248.155.218)act=Add cfgtid=xx cfgpath=system.automati on-trigger cfgobj=Forticloud-Sync
cfgattr=description[Automatically Syncing / Updating the device]trigger-type[scheduled]trigger-
frequency[daily]trigger-hour[15]trigger-minute[30] msg=Add system.aut omation-trigger Forticloud-Sync tz="-
xxx"
```

System and Network Discovery

When the firewall had VPN capabilities, the threat actor created local VPN user accounts with names resembling legitimate accounts but with an added digit at the end. These newly created users were then added to the VPN user group, enabling future logins. This tactic was likely intended to evade detection during casual administrative reviews, and to maintain persistent access even if the initial entry points were discovered. The actor then manually assigned a password to the newly created users.

The following log entries illustrate this activity:

```
{"itime": "xxx", "date": "2025-02-xx", "time": "18:04:01", "devid": "xxx", "vd": "root", "type": "event",
"subtype": "system", "action": "Add", "cfgattr": "type[password]passwd[ENC ]", "cfgobj": "xxx1", "cfgpath":
"user.local", "cfgtid": "11075652", "devname": "xxxx", "eventtime": "xxx", "idseq": "xxxx", "level":
"information", "logdesc": "Object attribute configured", "logid": "xxxx", "logver": "xxxx", "msg": "Add
user.local xxx1", "tz": "-xxx", "ui": "GUI(89.248.192.55)", "user": "fortigate-firewall"}
```

```
{"itime": "xxx", "date": "2025-02-xx", "time": "xx:04:01", "devid": "xxxx", "vd": "root", "type": "event",
"subtype": "system", "action": "Edit", "cfgattr": "member[ xxx1]", "cfgobj": "VPN Users", "cfgpath":
"user.group", "cfgtid": "xxx", "devname": "xxxx", "eventtime": "xxx", "idseq": "xxx", "level":
"information", "logdesc": "Object attribute configured", "logid": "xxx", "logver": "xxx", "msg": "Edit
user.group VPN Users", "tz": "-xx", "ui": "GUI(89.248.192.55)", "user": "fortigate-firewall"}
```

FortiClient VPN disconnected	2025-02-xxTxx:48:32Z	2025-02-xxT00:00:00Z	xx1
FortiClient VPN connected	2025-02-xxTxx:04:15Z	2025-02-xxT00:00:00Z	xx1

tunnel-up	Russia	vpn	XX1	event	89.248.192.55		89.248.192.55
tunnel-up	Russia	vpn	XX1	event	89.248.192.55	10.1.1.1	89.248.192.55

In environments without VPN capabilities or where the actor was unable to add VPN users, they attempted to log in to other firewalls using the credentials created on the initial compromised firewall. This was done through two distinct methods:

High Availability (HA) Configuration Propagation

For firewalls configured in HA mode, the threat actor forced HA functionality to propagate the compromised configuration to additional firewalls within the same cluster. By triggering the HA sync process, they ensured that their backdoor accounts and automation scripts were replicated across the devices.

Relevant log entry:

```
Feb 27 xx:13:49 xxx CEF:0|Fortinet|FortiGate-101E|7.0.12,build0523 (GA)|xxx|system event
Add|4|start=Feb 27 2025 xx:13:49 logver=xx deviceExternalId=xxx dvchost=xxxx vd=root eventtime=xxx tz=-
xxx logid=xxx cat=event subtype=system deviceSeverity=information logdesc=Object attribute configured
duser=forticloud-tech sproc=ha_daemon act=Add cfgtid=xxx cfgpath=system.automation-stitch
cfgobj=Automatically Syncing cfgattr=description[Automatically Syncing / Updating the
device]trigger[Forticloud-Sync] msg=Add system.automation-stitch Automatically Syncing tz="-xxx"
```

Authentication Infrastructure Abuse

For firewalls configured to use TACACS+ or RADIUS, the threat actor attempted to VPN into the network. This method could succeed if any of the locally created users were also synchronized with Active Directory (AD) or via a Radius Community secret, allowing authentication through the Network Policy Server (NPS).

Relevant log entry:

```
network policy server denied access to a user. contact the network policy server administrator for more
information. user: security id: s-1-0-0 account name: admin account domain: xxx fully qualified account
name: xxx\admin client machine: security id: s-1-0-0 account name: - fully qualified account name: -
called station identifier: xx.xxx.xx.xx calling station identifier: xxx.xxx.xxx.xxx nas: nas ipv4
address: xx.xxx.xxx.xx nas ipv6 address: - nas identifier: xxxxx nas port-type: virtual nas port: 5
radius client: client friendly name: xxx client ip address: xxx.xxx.xx.xx authentication details:
connection request policy name: virtual private network (vpn) connections network policy name: -
authentication provider: windows authentication server: xxx.xxx.xx@local authentication type: extension
eap type: - account session identifier: xxxx logging results: accounting information was written to the
local log file. reason code: 21 reason: an nps extension dynamic link library (dll) that is installed
on the nps server rejected the connection request.
```

To identify potential paths for lateral movement, the threat actor leveraged built-in FortiGate dashboards to gather environmental intelligence beyond what was available in the previously downloaded configuration file.

The threat actor accessed the following FortiGate dashboards:

- **Status Dashboard**: Displays system metrics and status indicators.
- **Security Dashboard**: Provides insights into threat detection, vulnerability assessments, and compromised hosts.
- **Network Dashboard**: Shows routing details, DHCP status, SD-WAN performance, and VPN connections.
- **Users & Devices Dashboard**: Lists endpoint devices, FortiClient connections, user authentication, and quarantined devices.
- **WiFi Dashboard**: Monitors wireless networks, access points, client connections, and wireless security alerts.

Relevant log entry:

```
{"itime": "xx","date": "2025-02-xx","time": "xx:07:59","devid": "xxx","vd": "root","type":
"event","subtype": "system","action": "Edit","cfgattr": "gui-dashboard:--------","cfgobj": "fortigate-
firewall","cfgpath": "system.admin","cfgtid": "xxx","devname": "xxx","eventtime": "xxxx","idseq":
"xxxx","level": "information","logdesc": "Object attribute configured","logid": "xxx","logver":
"xxxx","msg": "Edit system.admin fortigate-firewall","tz": "-xx","ui": "GUI(80.66.88.90)","user":
"fortigate-firewall"}
```

Lateral Movement and Ransomware Deployment

Using firewall configurations, dashboard insights, and established network access (via VPN or direct authentication), the attackers moved laterally within the network, prioritizing high-value targets including file servers, authentication servers and domain controllers, database servers and other network infrastructure devices.

The actor primarily relied on Windows Management Instrumentation (WMIC) for remote system discovery and execution, and SSH to access additional systems, particularly servers and network devices.

In one confirmed case, the attacker focused on identifying and compromising file servers, which became primary targets for data exfiltration and ransomware deployment. Instead of encrypting the entire network, the attacker selectively encrypted file servers containing sensitive data.

The encryption was initiated only after data exfiltration, aligning with recent trends among ransomware operators who prioritize data theft over pure disruption.

Analysis of Ransomware and Infrastructure

The ransomware strain observed in these incidents closely resembles LockBit 3.0 (LockBit Black). The primary differences lie in the ransom note left after encryption and a custom data exfiltration executable. Due to these modifications, we have designated this variant “SuperBlack”.

Ransomware Pivots

Here is the ransom note left by the threat actor:

The note contains a Tox chat ID (`DED25DCB2AAAF65A05BEA584A0D1BB1D55DD2D8BB4185FA39B5175C60C8DDD0C0A7F8A8EC815`), which is linked to LockBit 3.0. Since Tox chat IDs are typically used by Ransomware-as-a-Service (RaaS) groups and affiliates, this suggests that the actor behind these intrusions is either a current or former affiliate leveraging LockBit’s leaked builder, or an independent threat actor reusing LockBit’s infrastructure and tools.

The note retains LockBit 3.0’s HTML template structure, but removes branding elements such as the header “`~~~LockBit 3.0 the world's fastest ransomware since 2019~~~`” and the actor’s leak site (`lockbitaptxxx[.]onion`).

Using the Tox chat ID from the ransom note, we identified four additional similar notes on VirusTotal:

- `c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404`
- `f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513`
- `813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2`
- `782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045`

One of those was linked to sample `d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88`, which has an import hash of `914685b69f2ac2ff61b6b0f1883a054d`. This import hash has previously been associated with BlackMatter, LockBit, and BlackMatte ransomware.

This sample serves as the primary executable responsible for encryption, which then downloads additional files to the infected machine. One of those is a wiper with hash `917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2`.

We have designated this wiper component as “WipeBlack” which has been observed in previous ransomware incidents tied to LockBit and BrainCipher. BrainCipher, in turn, has been linked to SenSayQ, EstateRansomware, and RebornRansomware. Additionally, the wiper’s builder is associated with the leaked LockBit builder, reinforcing its connection to LockBit-linked ransomware operations.

The wiper file is designed to remove evidence of the ransom executable after encryption.

It exhibits anti-forensic patterns common to our ransom executable (via the ransom note) and BrainCipher/Lockbit intrusions. It dynamically resolves Windows APIs to obstruct static analysis, and uses named pipes for command execution and communication. We identified a function that creates a named pipe using an obfuscated string, decrypted using the key `0x3105DFDE`. It implements custom operation codes for issuing commands and allocates a 1MB buffer in `sub_402a78` to overwrite the ransom executable with random data, effectively erasing it post-encryption.

Observable Network Pivots

The threat actor leveraged information from the compromised firewall’s configuration file and dashboards to pivot deeper into the internal network. To maximize their scope, they attempted to log into multiple firewalls and accounts. We observed IP address `185.147.124[.]34` performing some of these actions.

This IP was previously associated with malicious web requests to multiple edge devices. It has SSH fingerprint `fa3f3f12cee3c18aa50ea8b8e38708cad06875e617164baca8f8ee7156459249`.

Port 7000 was found open on this IP, revealing a tool called “VPN Brute v1.0.2” containing Russian language content.

The VPN Brute tool is designed to brute force multiple edge devices, including:

- RDWeb (Remote Desktop Web Access)
- PulseSecure (referred to as “Dana” in some sections)
- OWA (Outlook Web Access)
- GlobalProtect (Palo Alto Networks)
- Fortinet
- Cisco
- BIG-IP (F5 Networks)
- Citrix

Additionally, VPN Brute can rotate through multiple proxy servers (both SOCKS and HTTPS) for each request or set of requests. This allows them to replace blocked or failed proxies dynamically with fresh ones. It also allows the operator to control credential processing by setting the number of credential strings per thread, and defining maximum or minimum credentials per client request.

We identified 15 additional IP addresses running VPN Brute v1.0.2 and v1.1.0 (listed in the Indicators of Compromise (IoCs) section. The newer versions introduce checkbox-based options for added functionality, including:

- “Продолжить поиск после успешного гуда” (“Continue searching after successful discovery”) – suggesting the tool can keep brute-forcing even after finding valid credentials.
- “Включить комбинационный режим” (“Enable combination mode”) – allowing custom username and password combinations.
- “Сканировать ханипоты” (“Scan honeypots”) – helping to detect honeypots to avoid detection.

Recommended Mitigations

The intrusions we investigated highlight the increasing trend of exploiting perimeter security appliances for initial access. The rapid transition from vulnerability disclosure to active exploitation significantly narrows the window for organizations to apply critical updates.

To mitigate these threats, organizations must adopt a defense in depth approach by properly segmenting networks and implementing layered security controls that can limit attackers’ ability to achieve their objectives.

As of this writing, the highest number of exposed FortiGate firewalls are in the United States (7677), India (5536) and Brazil (3201). We recommend the following actions for FortiGate users:

- **Patch vulnerable systems**: Apply FortiOS updates addressing CVE-2024-55591 and CVE-2025-24472 immediately.
- **Restrict management access**: Disable external management access to firewalls whenever possible.
- **Audit administrator accounts**: Regularly review all administrator accounts and remove any unauthorized or unexpected users.
- **Examine automation settings**: Check for unauthorized automation tasks, particularly those set to run daily or during off-hours.
- **Review VPN users**: Audit all VPN users and groups for slight variations of legitimate usernames or recently created accounts without clear business justification.
- **Enable comprehensive logging**: A common gap in investigations is the lack of comprehensive logging. Ensure the following are enabled: CLI audit logs on FortiGate, HTTP/S traffic logs to/from firewalls, Network Policy Server (NPS) auditing for authentication events, Authentication system auditing set to record both success and failures (rather than just failures). Comprehensive logging enhances detection, investigation and proactive threat hunting.

Go deeper. Watch our on-demand webinar of our 2024 Threat Roundup — and see what to expect in 2025.

Watch the webinar

Acknowledgements*: We acknowledge Ameer Mane and Swapnil Randhave for their efforts in sweeping customer environments using extracted intelligence.*

TTPs and Detection Opportunities

TECHNIQUE	ARTIFACT	DETECTION OPPORTUNITY
Exploit Public-Facing Application	local_access_token	Monitor HTTP/S connections to external IP of the firewall to find local_access_token in the URL

Privilegeescalation	“profile”: “super_admin”	Monitor for profile with string super_admin in “Admin login successful” logs or with [super_admin->super_admin]password[*] or [super_admin]vdom[root]password[*]
Create Account:Local Account	“Add system.admin forticloud-tech”	Monitor for newly added local users on the firewall by checking “Object attribute configured” with msg “Add system.admin <user_name“
External RemoteServices	member[hostname <user_list>]type[password]passwd[ENC base64]	Monitor for newly added users to VPN groups by checking “Object attribute configured” with msg “Edit user.group VPN Users” and “Add user.localxxx1″
ModifyAuthenticationProcess	“Configuration changed”	Monitor for any changes to the configuration of the firewall.
Data fromConfigurationRepository	“System configuration backed up”	Monitor for any config downloads
ScheduledTask/Job	[config system admin\nedit forticloud-sync\nset password#^(agT2^R96R-S_l4Y^HS#^\nset accprofilesuper_admin\nend\nexit]accprofile[super_admin]	Monitor for system commends “config system admin” to find scripts added to local firewall that will sync through fortigate’s inbuilt automation process
Create Account:Local Account	msg=Delete system.admin fortigate-firewall	Monitor for newly added local users on the firewall by checking “Object attribute configured” with msg “Delete system.admin <user_name“
External RemoteServices	“cfgattr”: “gui-dashboard:———“,”cfgobj”: “fortigate-firewall”,”cfgpath”: “system.admin”,”cfgtid”: “xxx”,”devname”: “xxx”,”eventtime”: “xxxx”,”idseq”: “xxxx”,”level”: “information”,”logdesc”: “Object attribute configured”,”logid”: “xxx”,”logver”: “xxxx”,”msg”: “Edit system.admin fortigate-firewall”,”tz”: “-xx”,”ui”: “GUI(80.66.88.90)”,”user”: “fortigate-firewall”	Monitor GUI access from External IP addresses by using “cfgpath”: “system.admin” in combination with “ui”: “GUI(<ip address>)”

IoCs

The indicators of compromise (IoCs) below are available on the Forescout Vedere Labs threat feed.

IPs	89.248.192[.]55 94.154.35[.]208 80.66.88[.]90 185.147.124[.]31 96.31.67[.]39 94.156.177[.]187 170.130.55[.]164 185.147.124[.]10 109.248.160[.]118 213.176.64[.]114 57.69.19[.]70 185.147.124[.]34 192.248.155[.]218 185.147.124[.]55 176.53.147[.]5 80.64.30[.]237 193.143.1[.]65 185.224.0[.]201 5.181.171[.]133 94.156.227[.]208 95.217.78[.]122 77.239.112[.]0 192.248.155[.]218 185.95.159[.]43 95.179.234[.]4 217.144.189[.]35 45.15.17[.]67 185.147.124[.]34
File hashes	c994b132b2a264b8cf1d47b2f432fe6bda631b994ec7dcddf5650113f4a5a404 f383bca7e763b9a76e64489f1e2e54c44e1fd24094e9f3a28d4b45b5ec88b513 813ad8caa4dcbd814c1ee9ea28040d74338e79e76beae92bedc8a47b402dedc2 782c3c463809cd818dadad736f076c36cdea01d8c4efed094d78661ba0a57045 d9938ac4346d03a07f8ce8b57436e75ba5e936372b9bfd0386f18f6d56902c88 917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2
User names	adnimistrator fortigate-firewall admin_support newadmin forticloud-tech newadminuser newadminz renewadmin admin-vpn-access admin-vpn-access-work adminp0g it_manager
Commands	[config system admin\nedit forticloud-sync\nset password #^(agT2^R96R-S_l4Y^HS#^\nset accprofilesuper_admin\nend\nexit]accprofile[super_admin]