UNC6201 Exploiting a Dell RecoverPoint for Virtual Machines Zero-Day

By Mandiant, Google Threat Intelligence Group

Published: 2026-02-17 · Archived: 2026-04-05 14:25:42 UTC

Written by: Peter Ukhanov, Daniel Sislo, Nick Harbour, John Scarbrough, Fernando Tomlinson, Jr., Rich Reece

---

Introduction

Mandiant and Google Threat Intelligence Group (GTIG) have identified the zero-day exploitation of a high-risk vulnerability in Dell RecoverPoint for Virtual Machines, tracked as CVE-2026-22769, with a CVSSv3.1 score of 10.0. Analysis of incident response engagements revealed that UNC6201, a suspected PRC-nexus threat cluster, has exploited this flaw since at least mid-2024 to move laterally, maintain persistent access, and deploy malware including SLAYSTYLE, BRICKSTORM, and a novel backdoor tracked as GRIMBOLT. The initial access vector for these incidents was not confirmed, but UNC6201 is known to target edge appliances (such as VPN concentrators) for initial access. There are notable overlaps between UNC6201 and UNC5221, which has been used synonymously with the actor publicly reported as Silk Typhoon, although GTIG does not currently consider the two clusters to be the same.

This report builds on previous GTIG research into BRICKSTORM espionage activity, providing a technical deep dive into the exploitation of CVE-2026-22769 and the functionality of the GRIMBOLT malware. Mandiant identified a campaign featuring the replacement of older BRICKSTORM binaries with GRIMBOLT in September 2025. GRIMBOLT represents a shift in tradecraft; this newly identified malware, written in C# and compiled using native ahead-of-time (AOT) compilation, is designed to complicate static analysis and enhance performance on resource-constrained appliances.

Beyond the Dell appliance exploitation, Mandiant observed the actor employing novel tactics to pivot into VMware virtual infrastructure, including the creation of "Ghost NICs" for stealthy network pivoting and the use of iptables for Single Packet Authorization (SPA).

Dell has released remediations for CVE-2026-22769, and customers are urged to follow the guidance in the official Security Advisory. This post provides actionable hardening guidance, detection opportunities, and a technical analysis of the UNC6201 tactics, techniques, and procedures (TTPs).

GRIMBOLT

During analysis of compromised Dell RecoverPoint for Virtual Machines, Mandiant discovered the presence of BRICKSTORM binaries and the subsequent replacement of these binaries with GRIMBOLT in September 2025. GRIMBOLT is a C#-written foothold backdoor compiled using native ahead-of-time (AOT) compilation and packed with `UPX`. It provides a remote shell capability and uses the same command and control as previously

deployed BRICKSTORM payload. It's unclear if the threat actor's replacement of BRICKSTORM with GRIMBOLT was part of a pre-planned life cycle iteration by the threat actor or a reaction to incident response efforts led by Mandiant and other industry partners. Unlike traditional .NET software that uses just-in-time (JIT) compilation at runtime, Native AOT-compiled binaries, introduced to .NET in 2022, are converted directly to machine-native code during compilation. This approach enhances the software's performance on resource-constrained appliances, ensures required libraries are already present in the file, and complicates static analysis by removing the common intermediate language (CIL) metadata typically associated with C# samples.

UNC6201 established BRICKSTORM and GRIMBOLT persistence on the Dell RecoverPoint for Virtual Machines by modifying a legitimate shell script named `convert_hosts.sh` to include the path to the backdoor. This shell script is executed by the appliance at boot time via `rc.local`.

CVE-2026-22769

Mandiant discovered CVE-2026-22769 while investigating multiple Dell RecoverPoint for Virtual Machines within a victim's environment that had active C2 associated with BRICKSTORM and GRIMBOLT backdoors. During analysis of the appliances, analysts identified multiple web requests to an appliance prior to compromise using the username `admin`. These requests were directed to the installed Apache Tomcat Manager, used to deploy various components of the Dell RecoverPoint software, and resulted in the deployment of a malicious WAR file containing a SLAYSTYLE web shell.

After analyzing various configuration files belonging to Tomcat Manager, we identified a set of hard-coded default credentials for the `admin` user in `/home/kos/tomcat9/tomcat-users.xml`. Using these credentials, a threat actor could authenticate to the Dell RecoverPoint Tomcat Manager, upload a malicious WAR file using the `/manager/text/deploy` endpoint, and then execute commands as `root` on the appliance.

The earliest identified exploitation activity of this vulnerability occurred in mid-2024.

Newly Observed VMware Activity

During the course of the recent investigations, Mandiant observed continued compromise of VMware virtual infrastructure by the threat actor as previously reported by Mandiant, CrowdStrike, and CISA. Additionally, several new TTPs were discovered that haven't been previously reported on.

Ghost NICs

Mandiant discovered the threat actor creating new temporary network ports on existing virtual machines running on an ESXi server. Using these network ports, the threat actor then pivoted to various internal and software-as-a-service (SaaS) infrastructures used by the affected organizations.

iptables proxying

While analyzing compromised vCenter appliances, Mandiant recovered several commands from Systemd Journal executed by the threat actor using a deployed SLAYSTYLE web shell. These iptable commands were used for Single Packet Authorization and consisted of:

- Monitoring incoming traffic on port 443 for a specific HEX string
- Adding the source IP of that traffic to a list and if the IP is on the list and connects to port 10443, the connection is ACCEPTED
- Once the initial approved traffic comes in to port 10443, any subsequent traffic is automatically redirected
- For the next 300 seconds (five minutes), any traffic to port 443 is silently redirected to port 10443 if the IP is on the approved list

```
 iptables -I INPUT -i eth0 -p tcp --dport 443 -m string --hex-string <HEX_STRING>
iptables -A port_filter -i eth0 -p tcp --dport 10443 --syn -m recent --rcheck --name ipt -j ACCEPT
iptables -t nat -N IPT
iptables -t nat -A IPT -p tcp -j REDIRECT --to-ports 10443
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 --syn -m recent --rcheck --name ipt --seconds 300 -j IP
```

Remediation

The following investigative guide can assist defenders in analyzing Dell RecoverPoint for Virtual Machines.

Forensic Analysis of Dell RecoverPoint Disk Image

The following artifacts are high-value sources of evidence for incident responders conducting full disk image analysis of Dell RecoverPoint for Virtual Machines.

- Web logs for Tomcat Manager are stored in `/home/kos/auditlog/fapi_cl_audit_log.log`. Check log file for any instances of requests to `/manager`. Any instances of those requests should be considered suspicious
    - Any requests for `PUT /manager/text/deploy?path=/<MAL_PATH>&update=true` are potentially malicious. `MAL_PATH` will be the path where a potentially malicious WAR file was uploaded
- Uploaded WAR files are typically stored in `/var/lib/tomcat9`
- Compiled artifacts for uploaded WAR files are located in `/var/cache/tomcat9/Catalina`
- Tomcat application logs located in `/var/log/tomcat9/`
    - Catalina - investigate any `org.apache.catalina.startup.HostConfig.deployWAR` and `org.apache.catalina.startup.HostConfig.deployWAR` events
    - Localhost - Contains additional events associated with WAR deployment and any exceptions generated by malicious WAR and embedded files
- Persistence for BRICKSTORM and GRIMBOLT backdoors on Dell RecoverPoint for Virtual Machines was established by modifying `/home/kos/kbox/src/installation/distribution/convert_hosts.sh` to include the path to the backdoor

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included IOCs in a free GTI Collection for registered users.

File Indicators

Family	File Name	SHA256
GRIMBOLT	support	`24a11a26a2586f4fba7bfe89df2e21a0809ad85069e442da98c37c4add369a0c`
GRIMBOLT	out_elf_2	`dfb37247d12351ef9708cb6631ce2d7017897503657c6b882a711c0da8a9a591`
SLAYSTYLE	default_jsp.java	`92fb4ad6dee9362d0596fda7bbcfe1ba353f812ea801d1870e37bfc6376e624a`
BRICKSTORM	N/A	`aa688682d44f0c6b0ed7f30b981a609100107f2d414a3a6e5808671b112d1878`
BRICKSTORM	splisten	`2388ed7aee0b6b392778e8f9e98871c06499f476c9e7eae6ca0916f827fe65df`
BRICKSTORM	N/A	`320a0b5d4900697e125cebb5ff03dee7368f8f087db1c1570b0b62f5a986d759`
BRICKSTORM	N/A	`90b760ed1d0dcb3ef0f2b6d6195c9d852bcb65eca293578982a8c4b64f51b035`
BRICKSTORM	N/A	`45313a6745803a7f57ff35f5397fdf117eaec008a76417e6e2ac8a6280f7d830`

Network Indicators

Family	Indicator	Type
GRIMBOLT	`wss://149.248.11.71/rest/apisession`	C2 Endpoint

GRIMBOLT	`149.248.11.71`	C2 IP

YARA Rules

G_APT_BackdoorToehold_GRIMBOLT_1

```
 rule G_APT_BackdoorToehold_GRIMBOLT_1
{
  meta:
    author = "Google Threat Intelligence Group (GTIG)"
  strings:
    $s1 = { 40 00 00 00 41 18 00 00 00 4B 21 20 C2 2C 08 23 02 }
    $s2 = { B3 C3 BB 41 0D ?? ?? ?? 00 81 02 0C ?? ?? ?? 00 }
    $s3 = { 39 08 01 49 30 A0 52 30 00 00 00 DB 40 09 00 02 00 80 65 BC 98 }
    $s4 = { 2F 00 72 00 6F 00 75 00 74 00 65 79 23 E8 03 0E 00 00 00 2F 00 70 00 72 00 6F 00 63 00 2F 00 73 00 6
  condition:
    (uint32(0) == 0x464c457f) //linux
    and all of ($s*)
}
```

G_Hunting_BackdoorToehold_GRIMBOLT_1

```
 rule G_Hunting_BackdoorToehold_GRIMBOLT_1
{
    meta:
        author = "Google Threat Intelligence Group (GTIG)"

    strings:
        $s1 = "[!] Error : Plexor is nul" ascii wide
        $s2 = "port must within 0~6553" ascii wide
        $s3 = "[*] Disposing.." ascii wide
        $s4 = "[!] Connection error. Kill Pty" ascii wide
        $s5 = "[!] Unkown message type" ascii wide
        $s6 = "[!] Bad dat" ascii wide
    condition:
        (
            (uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x00004550) or
            uint32(0) == 0x464c457f or
            uint32(0) == 0xfeedface or
            uint32(0) == 0xcefaedfe or
            uint32(0) == 0xfeedfacf or
            uint32(0) == 0xcffaedfe or
            uint32(0) == 0xcafebabe or
```

```
            uint32(0) == 0xbebafeca or
            uint32(0) == 0xcafebabf or
            uint32(0) == 0xbfbafeca
        ) and any of them
}
```

G_APT_BackdoorWebshell_SLAYSTYLE_4

```
 rule G_APT_BackdoorWebshell_SLAYSTYLE_4
{
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
                $str1 = "<%@page import=\"java.io" ascii wide
                $str2 = "Base64.getDecoder().decode(c.substring(1)" ascii wide
                $str3 = "{\"/bin/sh\",\"-c\"" ascii wide
                $str4 = "Runtime.getRuntime().exec(" ascii wide
                $str5 = "ByteArrayOutputStream();" ascii wide
                $str6 = ".printStackTrace(" ascii wide
        condition:
                $str1 at 0 and all of them
}
```

Google Security Operations (SecOps)

Google Security Operations (SecOps) customers have access to these broad category rules and more under the “Mandiant Frontline Threats” and “Mandiant Hunting Rules” rule packs. The activity discussed in the blog post is detected in Google SecOps under the rule names:

- Web Archive File Write To Tomcat Directory
- Remote Application Deployment via Tomcat Manager
- Suspicious File Write To Tomcat Cache Directory
- Kbox Distribution Script Modification
- Multiple DNS-over-HTTPS Services Queried
- Unknown Endpoint Generating DNS-over-HTTPS and Web Application Development Services Communication
- Unknown Endpoint Generating Google DNS-over-HTTPS and Cloudflare Hosted IP Communication
- Unknown Endpoint Generating Google DNS-over-HTTPS and Amazon Hosted IP Communication

Acknowledgements

We appreciate Dell for their collaboration against this threat. This analysis would not have been possible without the assistance from across Google Threat Intelligence Group, Mandiant Consulting and FLARE. We would like to specifically thank Jakub Jozwiak and Allan Sepillo from GTIG Research and Discovery (RAD).

Posted in

- Threat Intelligence
