SolarWinds社のServ-Uの脆弱性を狙う攻撃：Falcon Completeが即座に対処、GRACEFUL SPIDERを阻止

October 21, 2021 | Alex Clinton - Tasha Robinso | 最前線から

＊原文は CrowdStrike Blog サイト掲載：
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/

このブログ記事では、SolarWinds 社の Serv-U の脆弱性を狙う最近の攻撃に、**CrowdStrike Falcon Complete**™ が素早く対応したケースを紹介します。SolarWinds は、2021 年 7 月にこの脆弱性について**報告**するとともに、これを解決するための修正プログラムをリリースしました。National Vulnerability Database（NVD）では、この詳細について **CVE-2021-35211** で報告しています。

Falcon Complete チームは、複数の顧客環境内で埋め込まれた活動を特定し、影響を受けたシステムの封じ込めを行って無力化し、以降のラテラルムーブメントなどのアクティビティを阻止しました。調査では、攻撃者が追加のツールを展開しようとしていたことが判明し、それがおそらく**ランサムウェア**攻撃の準備であったと見ています。この攻撃に特異的な点は、多段階のコンポーネントオブジェクトモデル（COM）を用いた永続化メカニズムが使用され、信頼されるプロセスの代わりに、攻撃者による任意のコードの実行を可能にしていたことでした。侵害活動の発見において、技術を活用したマシンベースの検知機能は非常に有効です。しかし、高度な技術を備えた今日の攻撃者らは、信頼されるプロセスを悪用することで環境へのアクセスを可能にしているため、脅威を追跡して無力化するには、人間の専門知識が必要であることは明らかです。

この記事で紹介するイベントは、CrowdStrike Intelligence が確認した攻撃者グループ GRACEFUL SPIDER が関与していたものです。GRACEFUL SPIDER は、東ヨーロッパやロシアをベースに活動していると推測されています。この攻撃者グループは世界のさまざまな業種の企業を標的としてきました。その代表的な収益化手法は、詐取したデータを人質に暗号通貨による身代金の支払い要求、身代金が支払われない場合に盗んだデータを使っての恐喝、被害者のアカウントから金銭の送金盗取、犯罪者の闇市場での決済カードデータの販売などがあります。

最初の検知

この攻撃者らの侵入後、活動の初期段階で、**CrowdStrike Falcon®** が MFT サーバー上で WINLOGON.EXE を親プロセスとするリバースシェルの実行を検知しました。SYSINFO.EXE のバイナリを分析すると、攻撃者がターゲットホストにアクセスする目的で、オープンソースの Meterpreter ベースのリバースシェル「TinyMet」を使用していたことがわかりました。さらに、これらのプロセスのネットワークテレメトリー情報からは、不審な IP との通信を試みていたことが判明しました。

図 1：TinyMet シェルの実行

その後すぐに、SVCHOST.EXE を親プロセスとするエンコードされた PowerShell の実行が検知されました。この PowerShell をデコードすると、ランダムな変数名を使用しており、レジストリキーから取得した内容を実行しようとしていました。これらは正当なスクリプトにはありえないことで、悪意のあるものであることがわかりました。

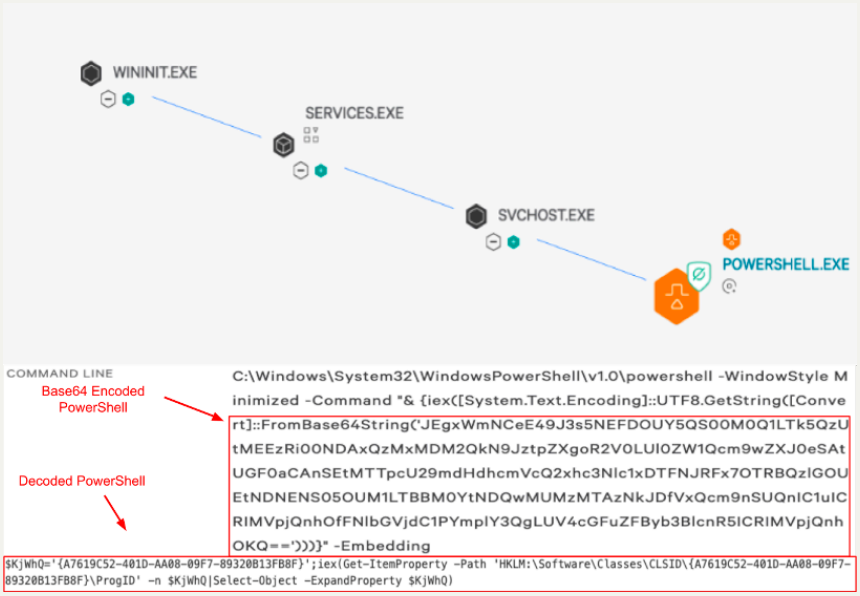

図 2：エンコードされた PowerShell の実行

これらのアクションはいずれも Falcon によって阻止されました。しかし、不審なインフラに頻繁に接続を試みていること、悪質な PowerShell スクリプトを実行していること、そのソースが不明であることから、デバイス上にまだ未解決の脅威が存在していることは明らかでした。問題のホストは直ちに封じ込めと隔離を行い、その後の活動を阻止する一方で、Falcon Complete は脅威のソースを究明すべく調査を続けました。

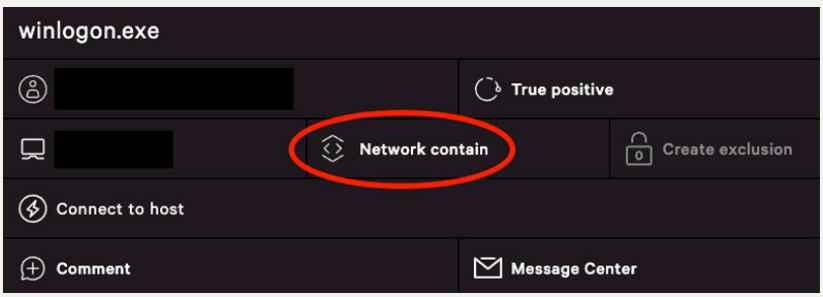

図 3：ネットワーク隔離

悪質なアクティビティが、正規の Windows プロセスや SYSTEM ユーザーアカウントを使用して実行されていたことから、このホストへの攻撃ベクトルは、ユーザーに対するフィッシングなどではなく、公開されたエクスプロイトによる侵害であったことが疑われました。さらに、不審なアクティビティの一部が正規の WINLOGON.EXE プロセスを使用して実行されていたことから、プロセスインジェクションが用いられた可能性が濃厚でした。

その後、Falcon Complete チームは、さらなる状況把握とアクティビティの発生源特定のために、エンドポイント・アクティビティ・モニタリング（EAM）のデータを調べることにしました。

EDR（エンドポイントでの検知と対応）データの調査

入手した検知情報を確認し、問題のアクティビティが悪意のあるものであることを確認した Falcon Complete は、脅威の全容解明に向けて調査を進めました。

では、何が起こったかを大まかに説明いたします。

足場の確保

以降の悪質な活動を防ぐために、Falcon Complete チームは、攻撃者がどのようにしてホストに足がかりを得たのかを特定する必要がありました。

それまでに確認したデータから、同チームは、攻撃者が一般向けのサービスを悪用してこのホストにアクセスしたのではないかと推測しました。Falcon Complete が、そのデバイス上で実行中のプロセスを確認すると、このデバイスは SolarWinds Serv-U FTP サーバーであることがわかりました。さまざまなソースで関連するプロセスのハッシュを探すと、このソフトウェアのバージョン番号がわかりました。

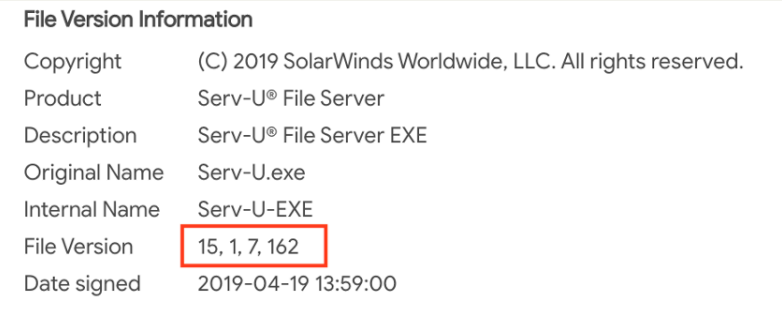

図 4：SolarWinds Serv-U のバージョン情報

このバージョンを急いで調べると、最近米国国土安全保障省 **CISA** が発表した「CVE-2021-35211」を含む既知のエクスプロイトが複数存在することがわかりました。

今回の調査では、正規の WINLOGON.EXE プロセスが悪用されていることに着目しました。これは、プロセスインジェクションによってステルス性の強化を目論む攻撃者グループがよく使う手法です。次の EAM 検索を行って、ホスト上のプロセスインジェクションの試行を特定しました。

```
(event_simpleName=*Reflective* OR DetectName=*Reflective* AND ReflectiveDllName!=NULL) OR (event_simpleName=*Inject* OR event_simpleName=*inject*)

| table _time aid event_simpleName ComputerName InjectorImageFileName InjecteeImageFileName  Reflective* Injected* CallStackModuleNames SourceThreadModule TargetThreadModule ParentProcessId_decimal TargetProcessId_decimal ContextProcessId_decimal
```

event_simpleName	ComputerName	InjectorImageFileName	InjecteeImageFileName
ProcessInjection	[redacted]	\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\System32\winlogon.exe
InjectedThread			
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\explorer.exe
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\explorer.exe
InjectedThread			
ProcessInjection		\Device\HarddiskVolume1\Windows\System32\lsass.exe	\Device\HarddiskVolume1\Windows\System32\winlogon.exe
ProcessInjection		\Device\HarddiskVolume1\Program Files\RhinoSoft\Serv-U\Serv-U.exe	\Device\HarddiskVolume1\Windows\System32\lsass.exe

図 5：プロセスインジェクションの連鎖（クリックで拡大）

図 5 を見ると、Serv-U.exe が最初に lsass.exe に注入され、続いて lsass.exe が winlogon.exe に注入されたことがわかります。また、Lsass.exe は、explorer.exe にも注入されました。このインジェクションの連鎖から、Serv-U が感染元であることが確認されました。さらに、Falcon の Process Timeline ダッシュボードを使用して、最初に侵害が行われた IP を特定することができました。

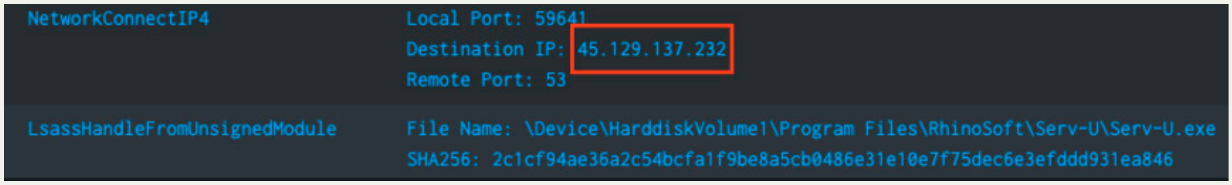

図 6：Falcon Process Timeline：Serv-U

Process Timeline で、関連する時間帯に注入された各プロセスを確認すると、攻撃者が、先に確認された TinyMet シェル、Cobalt Strike ビーコン（Falcon によって阻止）、AdFind のコピーなど、追加のツールを展開しようとしていたことがわかりました。TinyMet や Cobalt Strike のようなツールは、GRACEFUL SPIDER などのサイバー犯罪者グループが、環境へのアクセス権を販売・移譲する際によく使われます。これらのリモートアクセスツール（RAT）や AdFind（一般的には環境の列挙に使用）は、攻撃者がランサムウェアを展開する前の初期のステップでよく使用されます。ランサムウェアのブローカーネットワークが増加していることから、ホスト上でランサムウェアが検知された場合には、迅速な対応が必要であることは明白です。

永続化

侵害が発見された場合、Falcon Complete は、インシデントを解決する前に、必ずホストとお客様の環境がクリーンな状態となるようにします。次の段階は、攻撃者がホスト上の足場を維持するために使用したメカニズムを特定することでした。さまざまな永続化メカニズムの可能性を探りましたが、ホスト上の定期タスクを調べたところ、COM レジストリオブジェクトを利用した多段階の実行チェーンの存在がすぐに明らかになりました。

感染元が特定されたものの、このホストでは、WinLogon とは関係のない、Base64 でエンコードされた PowerShell スクリプトが実行されていることを何度か検知しています。このことから、攻撃者はホスト上で永続化メカニズムを確立しており、検知の頻度が高いことから、おそらくは定期タスクを使用していたと考えられます。

ホスト上で最近登録された定期タスクを探すと、Windows レジストリ内に、ある COM オブジェクトを示す 1 つのタスクが見つかりました。

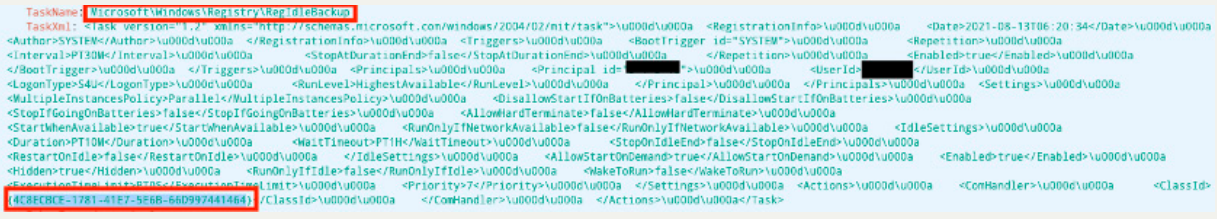

図 7：定期タスクの登録（クリックで拡大）

この定期タスクは、多くの Windows ホストで見られる既知のデフォルトの定期タスクです。攻撃者にとって格好のターゲットであり、攻撃者らの悪質な COM オブジェクトを示すものです。Windows レジストリ内の COM オブジェクトは、目立つことなく、自動実行が可能であるため、マルウェアを隠すのには絶好の場所であると言えます。この機能は、Windows 上のさまざまなソフトウェアによって正当な用途で利用されていますが、このケースでは、悪質なコードを実行させるために悪用されていました。

この時点で、Falcon Complete は、このホスト上で Falcon Real Time Response（RTR）機能を実行して、さらなる分析を行いました。RTR 機能はアナリストにホスト上のシェルを提供します、これを利用し EAM 内で発見されたデータを素早く検証、補完することができます。調査が完了したら、さらに RTR を使用して、ホスト上の悪質なアーティファクトの修復を行うことができます。RTR を使用してこの COM オブジェクトを調査したところ、2 つ目の COM オブジェクトのレジストリキーを示す TreatAs キーが確認されました。

図 8：悪質な COM オブジェクト（クリックで拡大）

2 つ目のレジストリキーを調べると、図 2 に示すように、Base64 でエンコードされた PowerShell（実行を試みていたスクリプト）が見つかりました。これをデコードすると、3 つ目の COM ベースのレジストリキーの内容をプルして実行するための PowerShell コマンドが見つかりました。

3 つ目のキーの内部のスクリプトはエンコードされており、未使用のコードを使用して簡易的に難読化されていました。デコードして難読化を解除すると、このスクリプトはホストの EventLog を消去できることが確認できました。しかし、その主な機能は、4 つ目のレジストリキー内の DLL をメモリにロードすることでした。

図 9：悪質な PowerShell スニペット

CrowdStrike Intelligence チームがこの DLL を分析したところ、ホスト名とドライブのシリアル番号を使って計算された 5 つ目（最後）のレジストリキーにペイロードが埋め込まれていたことが確認されました。この場所からロードされたマルウェアは、FlawedGrace と呼ばれる、GRACEFUL SPIDER に特有の RAT でした。

この永続化チェーンでは、展開された追加のツールを除く、悪質なコンテンツの大半をメモリ内に保持しており、比較的ステルス性が高いことがわかります。

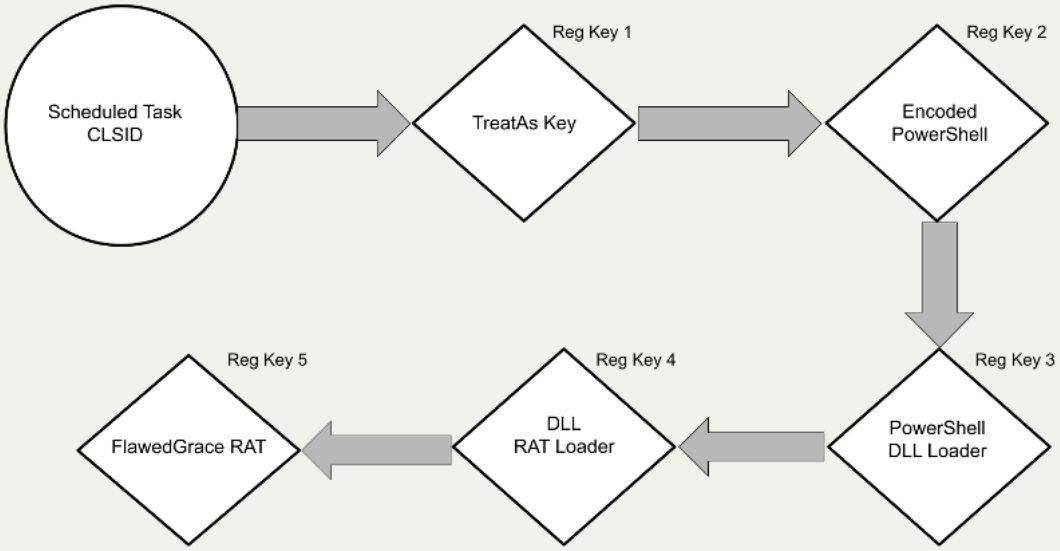

図 10：永続化チェーン

Falcon Complete チームによるこの永続化メカニズムの分析、ならびにプロアクティブな脅威ハンティングを提供する **CrowdStrike Falcon OverWatch™** と、CrowdStrike Intelligence チームとの連携により、今回のインシデントが GRACEFUL SPIDER によるものであることがすぐに判明しました。また、被害を受けたお客様の環境において、悪質なアーティファクトを特定することができました。

レメディエーション

トリアージと調査が完了した後、Falcon Complete チームは、このインシデントに関連するホスト内のあらゆる悪質なアーティファクトを修復しました。これにはすべての永続性メカニズムが含まれます。本ケースでは、次のような特定の難しい COM レジストリオブジェクトでした。

HKLM\Software\Classes\CLSID\{unique ID_1}\TreatAs

HKLM\Software\Classes\CLSID\{unique ID_2}\LocalServer

HKLM\Software\Classes\CLSID\{unique ID_2}\ProgID

HKLM\Software\Classes\CLSID\{unique ID_2}\VersionIndependentProgID

EAM で確認された追加のツール（TinyMet シェルおよび AdFind）は、最終的に Falcon センサーによってブロックされ、隔離されました。これらはディスク上では発見されず、追加の修正措置は不要でした。調査を進める中で、チームはホスト上に注入されたプロセスを複数確認しています。システムを完全にクリーンな状態にし、再感染を防ぐために、元凶である Serv-U.exe を含め、これらのプロセスを終了させました。

被害を受けたお客様には、Falcon Complete による修復の説明とともに、今後の攻撃を防ぐために、攻撃を示すすべての兆候と、システムに適用可能なパッチのリストを提供しました。また Falcon Complete は以下をお客様にアドバイスしました：

・関連する IP を境界領域でブロックすること
・影響を受けたシステム上のすべてのユーザーアカウントのパスワードをリセットすること（LSASS が侵害されたため）
・すべての利用可能なパッチを早急に適用すること

このお客様は、データの流出やランサムウェアの拡大を防ぐために、それらの対応を速やかに行いました。

関連する C2 アクティビティ

46.161.40[.]87 - Injected WinLogon

179.60.150[.]26 - TinyMetShell C2

179.60.150[.]32 - Cobalt Strike C2

45.129.137[.]232 - remote IP contacted by exploited Serv-U.exe process

まとめ

Falcon Complete は、外部に公開されている Serv-U MFT サーバー上のアクティブな攻撃活動を特定し、その活動を封じ込め、攻撃者がその目的を達成するのを阻止しました。同チームは、EAM、Falcon Process Timeline ダッシュボード、Falcon RTR、およびいくつかのオープンソースインテリジェンス（OSINT）を活用して、侵害活動を迅速にシャットダウンしました。

関連するアーティファクトを除去し、悪用された脆弱なアプリケーションを特定した後、同チームは、影響を受けるすべてのお客様に対して、外部公開された脆弱な MFT サーバーにパッチを適用し、さらなる攻撃からビジネスを保護し、さらに他のサーバーの脆弱性をチェックするために必要となる喫緊の情報を迅速に提供することができました。

ホストにタイムリーにパッチが適用されなかった稀なケースでは、GRACEFUL SPIDER が舞い戻り、Cobalt Strike ビーコンの配信を試みることが知られています。この試みは、Falcon エージェントによってすぐさまブロックされました。このような攻撃は、GRACEFUL SPIDER のような攻撃者グループが、標的とする組織内に足がかりを確保するために、永続性とステルス性を併せ持つ戦術を採用していることを示しています。幸いなことに Falcon では、今回のようにメモリ内に多く残された攻撃用コードを迅速に特定・調査し、修復するためのテレメトリー機能とツールを提供しています。

Falcon Complete チームは、Falcon OverWatch および CrowdStrike Intelligence の各チームと密接に連携し、膨大なスキルセットを活用して、組織が攻撃者グループを迅速に調査・特定できるようにすることで、「Stop Breaches - 侵害の阻止」という我々のミッションを後押ししています。

その他のリソース

- Falcon Completeの詳細については、製品Webページをご覧ください。
- ホワイトペーパーをご一読ください。CrowdStrike Falcon Complete：Instant Cybersecurity Maturity for Organizations of All Sizes（英語）
- 2020年にCrowdStrikeが追跡した攻撃者については、2021年CrowdStrikeグローバル脅威レポートをご一読ください。
- CrowdStrikeの次世代型AVをお試しください：Falcon Prevent™の無料トライアル

原文：Stopping GRACEFUL SPIDER: Falcon Complete's Fast Response to Recent SolarWinds Serv-U Exploit Campaign
https://www.crowdstrike.com/blog/how-falcon-complete-stopped-a-solarwinds-serv-u-exploit-campaign/