NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2021年3月版 (第36号)＞(選り抜き版)

2021年3月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

SolarWindsサプライチェーンによる侵害と対策
2020年12月、SolarWinds社のIT管理ソフトウェアとリモート監視ツール製品にマルウェアが混入され、製品を使用している多数の政府組織や企業が侵害される事件がありました。本記事では事件の概要と、高度なサプライチェーン攻撃の対策を解説します。

SolarWindsサプライチェーンによる侵害と対策

1. SolarWindsサプライチェーンによる侵害とは

2002年12月13日、SolarWinds社は、同社のIT管理ソフトウェアとリモート監視ツール製品であるOrion Platformに対して**トロイの木馬型のマルウェア「SUNBURST（※）」**が混入され、Orion Platformのユーザの環境にインストールされていたと公表しました。

Orion Platformは約3万3千の組織で導入されており、SUNBURSTが混入されたOrion Platformをインストールした組織の数は少なくとも1万8千あったとされています。影響を受けた組織の中には、米国の政府組織やグローバルで活動する企業、セキュリティベンダなどが含まれており、SUNBURSTによるバックドアによって、資格情報の窃取や、組織内の機密情報にアクセスされる被害が発生しました。

また、本件と同時期に**Orion Platformの脆弱性を悪用して設置されるWebシェル型のバックドア「SUPERNOVA」**の存在も明らかになりました。

攻撃者がソフトウェアの製造環境(ビルド環境)に侵入していたため、SolarWinds社は同社が使用する**コード署名の証明書を失効し、新しい証明書で署名**する対処を実施しました。

※FireEyeによる名前。別名Solorigate(マイクロソフトによる)

2. 本件の影響を受ける製品

Orion Platformの各バージョンにおけるSUNBURSTとSUPERNOVAと証明書失効(※)の影響有無は以下の通りです。

Orion Platformのバージョン	SUNBURST	SUPERNOVA	証明書失効
2020.2.4	影響無し	影響無し	影響無し
2020.2.1 HF2	影響無し	影響無し	影響有り
2020.2.1 HF1	影響無し	影響有り	影響有り
2020.2.1	影響無し	影響有り	影響有り
2020.2 HF1	影響有り	影響有り	影響有り
2020.2	影響有り	影響有り	影響有り
2019.4.2	影響無し	影響無し	影響無し
2019.4 HF 6	影響無し	影響無し	影響有り
2019.4 HF 5	影響有り	影響有り	影響有り
2019.4 HF 4	影響無し	影響有り	影響有り
2018.2 から 2019.4 HF 3	影響無し	影響有り	影響無し
上記より前のバージョン	影響無し	影響有り	影響無し

※コード署名に使用した証明書が失効した場合、署名されたプログラムは信頼されないプログラムと扱われ、失効日以降に使用できなくなります。

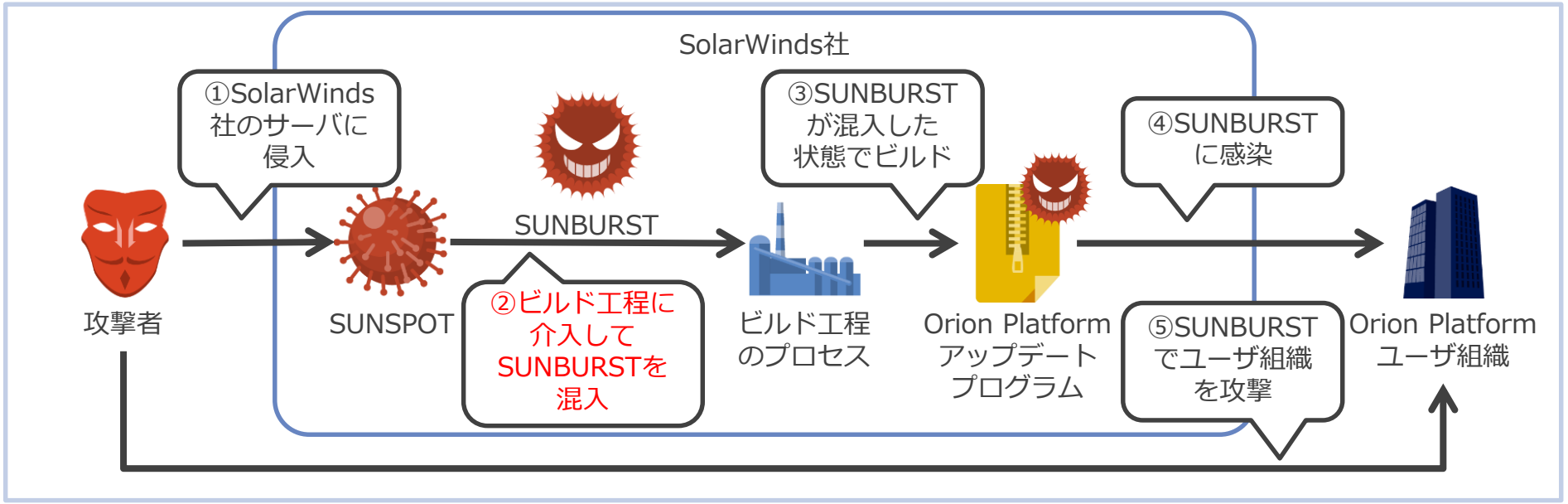
3. タイムライン

時期	出来事
2019年9月4日	攻撃者がSolarWinds社にアクセス
2019年9月12日 ～11月4日	攻撃者がOrion Platformへテストコードを挿入
2020年2月20日	攻撃者がトロイの木馬型マルウェア「SUNBURST」のコンパイルとデプロイ
2020年3月～6月	攻撃者によるバックドアが含まれるOrion Platformを配布
2020年6月4日	攻撃者がビルドVMからマルウェアを削除
2020年12月8日	FireEyeが「国が後援する攻撃者がFireEyeのネットワークに侵入し、同社のRed Team侵入テストツールを盗んだ」と発表
2020年12月13日	FireEyeがOrion Platformに対するサプライチェーン攻撃を発表
2020年12月13日	SolarWindsがOrion Platformに関するセキュリティアドバイザリを公開
2020年12月13日	米国の国土安全保障省が緊急指令21-01を発行し、連邦政府機関に影響を受けるデバイスを切断するように指令
2020年12月15日	SolarWindsが修正したOrion Platformをリリース
2020年12月16日	マイクロソフトがSUNBURSTをMicrosoft Defender Antivirusで隔離対応
2020年12月17日	US-CERTがアラートAA20-352Aを公開

4. 本件の原因

SolarWinds社は本件の原因を調査中としていますが、現時点では**Orion Platformのビルド工程に介入する「SUNSPOT」と呼ばれるマルウェア**が活動していたことが判明しています。

SUNSPOTは、Orion Platformのビルドに関係するプロセスの実行を監視して、**ソースコードを挿入することによってSUNBURSTを混入**させていました。また、ソースコード挿入によって発生したビルドエラーから攻撃を発見されるのを防ぐためにハッシュ値の検証プロセスにも介入していました。



5. 影響を受けた主な組織と本件の影響

SUNBURSTの被害を受けた主な組織および本件の影響は以下の通りです。これらの情報は現在も更新されているため、今後も新たな組織が追加されたり被害の詳細が公表されたりする可能性があります。

組織名	影響
FireEye	Red Team用に開発していた攻撃ツールの窃取
米国財務省	攻撃者が数十の電子メールアカウントを侵害
マイクロソフト	攻撃者がソースコードの一部を閲覧

また、日本の代理店のひとつである株式会社アクシスは、本件の注意喚起の中で「弊社のお客様の多くは、この時期にモジュールの入れ替えなどを実施されていないことを確認いたしましたが、いくつかのお客様にて、その可能性があることを把握しております。」と記載しており、**日本においても本件の影響があった**と推測されます。

6. Orion Platform導入組織向けの対応 (1/2)

SolarWinds社からOrion Platformを導入している組織向けに本件に対応したバージョンが提供されており、アップグレードが推奨されています。

Orion Platform のバージョン	SUNBURST	SUPERNOVA	証明書失効	推奨される対応内容
2020.2.4	影響無し	影響無し	影響無し	(不要)
2020.2.1 HF2	影響無し	影響無し	影響有り	2020.2.4へアップグレード
2020.2.1 HF1	影響無し	影響有り	影響有り	
2020.2.1	影響無し	影響有り	影響有り	
2020.2 HF1	影響有り	影響有り	影響有り	
2020.2	影響有り	影響有り	影響有り	
2019.4.2	影響無し	影響無し	影響無し	(不要)
2019.4 HF 6	影響無し	影響無し	影響有り	2020.2.4または 2019.4.2へアップグレード
2019.4 HF 5	影響有り	影響有り	影響有り	
2019.4 HF 4	影響無し	影響有り	影響有り	
2018.2 から 2019.4 HF 3	影響無し	影響有り	影響無し	
上記より前のバージョン	影響無し	影響有り	影響無し	2020.2.4へアップグレード または緩和策の実施 または使用の中止

6. Orion Platform導入組織向けの対応 (2/2)

US-CERTは、本件に関するアラート「AA20-352A」を公開しています。特に、Orion Platformを導入している組織が実施するべき対応内容を記載しています。

ステップ1
- フォレンジックのために、影響を受けるバージョンのOrion Platformをインストールしている全てのインスタンスのシステム(メモリとOS)を保全する
- 新しい特権ユーザまたはサービスのアカウントを確認する

ステップ2
- 影響を受けるバージョンのOrion Platformをネットワークから直ちに切断するか、電源を切る
- 攻撃者が使用する全てのアカウントと、マルウェアの永続化設定を特定して削除する

ステップ3
- Orion Platformが監視している全てのホストが侵害されていると想定した脅威を調査する
- 信頼できるソースを使用してOrion Platformを再構築する
- Orion Platformで使用しているアカウントをリセットする

Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
<https://us-cert.cisa.gov/ncas/alerts/aa20-352a> をもとに作成

7. 本件を踏まえた対策

本件では、大きく2種類の被害者が発生しました。

1. Orion Platform製品を利用しているユーザ組織(Microsoftなど)
2. Orion Platform製品を開発・提供しているSolarWinds社

本件のようなサプライチェーンへの侵害に対する対策は、**製品・サービスを利用する「ユーザ」**と、**製品・サービスを開発・提供する「サプライヤ」**で異なります。

次ページ以降では、ユーザとサプライヤの各々の立場の対策を解説します。

8. ユーザの対策

高度なサプライチェーン攻撃は、既存のシグネチャやIoCベースの対策では防ぐことが極めて難しく、完全に防ぐことや攻撃を早期に検知することは困難です。そのため、防御のためのシステムの導入だけでなく、導入する製品・サービスの管理体制やインシデント対応体制を整備するなどの幅広いリスク管理が重要です。

システムの主な対策

- エンドポイント保護製品の導入
- EDRの導入
  ※不審なアクティビティを検知するためのシステム・体制も必要です

制度・体制の主な対策

- 信頼できる委託先、取引先組織、サービスの選定
  (組織やサービスの信頼性評価や品質基準の導入)
- インシデント報告・対応体制などの運用規則の整備
- 契約内容の確認
  (組織間の取引や委託契約における情報セキュリティ上の責任範囲を明確化)

9. サプライヤの対策

サプライヤの立場から見た場合の、本件の原因と対策は以下の2点です。

1．ビルド環境への侵入

ビルド環境が攻撃者によって侵害されると、ソースコードや証明書の真正性を厳密に管理しても、本件のようにソフトウェアの信頼性が損なわれる事態となります。

ビルド環境へ侵入させないために、開発環境を既知の脆弱性や攻撃方法から守る対策を行う必要があります。また、開発に関する外部システムの連携やリモートアクセスの部分においても対策を行うことが重要です。

2．マルウェアが混入されたソフトウェアの配布

攻撃者はソースコードの改ざんだけでなく、ビルドされた不正なプログラムをSolarWinds社の証明書でデジタル署名する権限も持っていました。

仮に、ビルド環境の侵害によって製品にマルウェアが混入された場合でも、デジタル署名や最終的にソフトウェアをリリースするシステムのプロセスや権限をビルド環境と分離することで、ユーザへのマルウェア配布を防ぐことができます。

また、EDRは自動化されたビルドやリリースのプロセスに介入する不審な活動を監視する有効な対策といえます。

10. まとめ

SolarWinds社のIT管理製品は、多くの組織に導入されていたため、インシデントの影響範囲が広く、甚大な被害となりました。

本件のようなサプライチェーンにおける高度な攻撃は、「ユーザ」と「サプライヤ」の２つの立場に分けて対策を行う必要があります。

製品・サービスを利用する「ユーザ」の立場では、従来のシグネチャやIoCベースのセキュリティ対策では防げないため、システムだけでなく制度・体制を含めた、より包括的なセキュリティ対策をする必要があります。

製品・サービスを開発・提供する「サプライヤ」の立場では、仮に攻撃者によって侵害されてもユーザに影響がないように製品・サービスの開発・生産環境に対するセキュリティ対策を実施することが重要です。

11. 参考URL

- SolarWinds : SolarWinds Security Advisory
  https://www.solarwinds.com/sa-overview/securityadvisory
- cyber.dhs.gov : DHS Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise
  https://cyber.dhs.gov/ed/21-01/
- US-CERT : US-CERT Alert (AA20-352A) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
  https://us-cert.cisa.gov/ncas/alerts/aa20-352a
- SolarWinds : New Findings From Our Investigation of SUNBURST
  https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst
- FireEye : Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
  https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- IPA：情報セキュリティ10大脅威 2021 ～よもや自組織が被害に！呼吸を合わせて全力防御！～
  https://www.ipa.go.jp/files/000088835.pdf#page=42
- METI：サイバーセキュリティ経営ガイドライン
  https://www.meti.go.jp/policy/netsecurity/mng_guide.html

NTT DATA

Trusted Global Innovator