3.『Operation Blotless攻撃キャンペーンに関する注意喚起』

要約

- Living Off The Land(LOTL)戦術と呼ばれる攻撃に対する警戒が高まっている。
- LOTL 戦術とは、正規ツールを駆使して攻撃を行う手法であり、検知が難しいという特徴がある。初期侵入経路として SSL-VPN 製品の脆弱性を悪用した攻撃が多い。
- 将来の攻撃に備えるためには、脆弱性対策が重要であり、インフラとアプリケーションの両面で考慮する必要がある。これには、ASM ツールや SBOM(SCA)ツールの活用により、脆弱性のリスクを低減することが期待される。
- 脆弱性を可視化し、基本的なパッチの適用を行うことが攻撃を防ぐための重要な対策である。

概要

2024 年 6 月 25 日、JPCERT/CC は『Operation Blotless 攻撃キャンペーンに関する注意喚起』を発表し、環境寄生型(LOTL:Living Off The Land)戦術を利用するサイバー攻撃キャンペーン「Operation Blotless」に対して注意を喚起しました(*1) 。

LOTL 戦術は、以前から持続的な標的型攻撃(APT:Advanced Persistent Threat)を行う攻撃者が使用する高度な手法として、米国のサイバーセキュリティに関する主要な連邦機関の一つである CISA (Cybersecurity and Infrastructure Security Agency)からも注意喚起が行われ、国際的にも広く認知されている攻撃手法です。2023 年以降、日本の組織を標的にした攻撃活動が確認されており、JPCERT/CC だけでなく、NISC(内閣サイバーセキュリティセンター)も注意を呼びかけています(*2)。

出典:JPCERT/CC『Operation Blotless 攻撃キャンペーンに関する注意喚起』(*1)

出典:NISC『Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起』(*2)

LOTL 戦術は検知されにくい

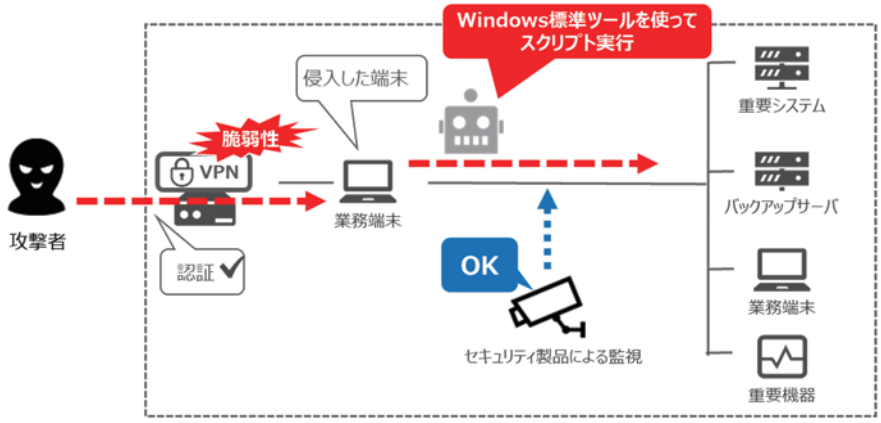
LOTL 戦術の特徴は、マルウェアを使用せずに、正規ツールを駆使してサイバー攻撃を行うことです。商用ツールやオープンソースのツールなど、組織内にあっても不審ではないツールや、OS などの侵入した環境に必ずある機能を操作することで、セキュリティ製品やログの監視・調査を回避します。

特に、近年のランサムウェア攻撃では、Microsoft の PowerShell が頻繁に悪用されているといわれて

(*1) JPCERT/CC『Operation Blotless 攻撃キャンペーンに関する注意喚起』

(*2) NISC『Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起』

います。PowerShell は、通常の Windows に搭載されているスクリプト言語と実行環境です。攻撃者は、セキュリティ製品による検知を回避するため、マルウェアを送り込むことなく、不正なスクリプトを入力して PowerShell を利用し、別のマルウェアをダウンロードするなどの不正な行動を促します。



出典：大和総研作成

環境寄生型（LOTL：Living Off The Land）戦術

Volt Typhoon の攻撃活動との関連

JPCERT/CC は、この注意喚起において、特定の国の組織的なサイバー攻撃グループ「Volt Typhoon」による同様の攻撃を例にあげ、具体的な対策の提案をしています。Volt Typhoon は、2021 年頃から活動が確認され、2023 年 5 月に Microsoft がその活動を指摘したことで注目を浴びました。ただし、現時点では Operation Blotless が Volt Typhoon による攻撃活動だけであるかどうかは確定していません。Volt Typhoon は、先述の LOTL 戦術を徹底しているため、攻撃の痕跡がほとんど残らず、また、1 回の侵害期間が短く、侵害範囲も限定的であるため、被害現場にはほとんど証拠が残らないといわれています。これらの点が共通していると考えられています。

将来の攻撃に備えるには

Volt Typhoon は、初期侵入経路として SSL-VPN 製品の脆弱性を悪用した攻撃を頻繁に行っています。脆弱性対策は非常に重要であり、インフラ面では、インターネットからアクセス可能な IT 資産を特定し、それらのリスク（脆弱性など）を継続的に検出・評価する ASM（Attack Surface Management）ツールの使用が考えられます。JPCERT/CC も本注意喚起の文面において ASM の利用を推奨しています。なお、本冊子 P.17 では ASM の動向について詳しく紹介しています。

また、アプリケーション面では OSS の脆弱性に慎重な対応が求められます。OSS はコスト効率が高く、柔軟性に優れるため、多くの企業や組織が利用しています。しかし、コードの品質やセキュリティの脆弱性が見落とされる可能性があるため、攻撃者が脆弱性を見つけ出しやすいという点に留意が必要です。これには、SBOM（SCA）ツール(*1)を活用することで、ソフトウェア構成要素を把握し、脆弱性のリスクを継続的に低減することが期待されます。

これらのツールを活用して脆弱性を可視化し、基本的なパッチの適用を行うことが、攻撃を防ぐための重要な対策となります。セキュリティ意識を高め、適切な対策を講じることで、企業や組織の情報資産を守ることができます。安全な環境を維持するために、脆弱性対策の重要性を常に意識することが必要です。

（蓮見　将生）

(*1) 大和総研『サプライチェーンリスクマネジメントを支援する SBOM とは？背景や導入の注意点を解説』
SBOM（ソフトウェア部品表）を作成、共有、活用、管理することができるツールのこと。SBOM 管理ツール、OSS 管理ツール、ソフトウェア構成解析（SCA）ツールなどとも呼ばれる。