ウォッチガードレポート：ファイルレスマルウェア攻撃が900%増、クリプトマイナーが復活、ランサムウェア攻撃が減少

2020年第4四半期インターネットセキュリティレポート：エンドポイント攻撃の大幅増、暗号化マルウェア比率の増加、IoTデバイスを標的とした新たなエクスプロイトなど

2021年4月28日（水） ー
企業向け統合型セキュリティソリューション（ネットワークセキュリティ／セキュアWi-Fi／多要素認証/エンドポイントプロテクション）のグローバルリーダであるWatchGuard（R）Technologiesの日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、代表執行役員社長 谷口
忠彦、以下ウォッチガード）は、四半期毎に発行している「インターネットセキュリティレポート」の最新版（2020年第4四半期）を発表しました。レポートには、2020年6月
にウォッチガードがPanda
Securityを買収したことに伴い、エンドポイントの脅威インテリジェンスに基づく新たな知見が盛り込まれています。また、中でも注目すべきは、ファイルレスマルウェアとクリプトマイナー攻撃の割合がそれぞれ約900%と25%増加したのに対して、2020年はランサムウェアペイロード（ユニーク数）が2019年と比較して48%減少したことを明らかにしています。さらに、ウォッチガード脅威ラボでは、2020年Q4では暗号化されたマルウェアの検知が前期比で41%増加し、ネットワーク攻撃が2018年以降最も増えたことを突き止めています。

ウォッチガードのCTO、Corey
Nachreiner（コリー・ナクライナー）は次のように述べています。「前期および2020年を通じて、洗練された回避型の脅威戦術が増加したことは、多層型のエンドツーエンドセキュリティプロテクションの導入が必須となっていることを物語っています。攻撃はあらゆる方面から仕掛けられており、サイバー犯罪者はファイルレスマルウェア、クリプトマイナー、暗号化された攻撃などを多用し、リモートロケーションのユーザおよび従来のネットワーク境界の中にいる社内ユーザの両方を標的にしています。今日の効果的なセキュリティとは、エンドポイントの検知とレスポンス、ネットワーク防御、そしてセキュリティアウェアネストレーニングや厳格なパッチ管理などの基本的な予防措置を重視することです。」

ウォッチガードが四半期ごとに発行しているインターネットセキュリティレポートには、進化し続ける最新のマルウェア、エンドポイント、ネットワーク攻撃のトレンドに関して、企業、パートナー、そして顧客が身を守るために役立つ情報を提供しています。以下に2020年Q4の主な調査結果を紹介します：

ファイルレスマルウェア攻撃が急増 -
2020年はファイルレスマルウェアの割合が2019年に比べて888%増加しました。これらの脅威は特に危険であり、従来のエンドポイントプロテクションのクライアントによる検知を回避し、ユーザが不正リンクをクリックする、あるいは知らずに感染したWebサイトを訪れるだけで被害に遭っ

てしまいます。PowerSploitや
CobaltStrikeといったツールキットにより、攻撃者は稼働中の他のプロセスに不正コードを容易に注入することができ、ユーザのプロテクション機能がオリジナルのスクリプトを特定し、除去しても稼働し続けることができます。エンドポイントの検知／レスポンスソリューションと予防的なアンチマルウェアを両方実装することで、こうした脅威を特定することができます。

2019年の小康状態からクリプトマイナーによる被害が上昇

2018年の初頭に実質的に全ての暗号通貨の価格が暴落してから、クリプトマイナーの感染は大幅に減少し、2019年には亜種の検知が633件（ユニーク数）と最低になりました。とはいえ、攻撃者は既存のボットネット感染にクリプトマイナーモジュールを追加し、被害者から不当に収入を得る一方で、ネットワークを他のサイバー犯罪に悪用することを続けていました。結果として、2020年Q4に暗号通貨の価格が再び上昇し始めると、クリプトマイナーマルウェアの検知数が2019年と比較して25%増加し、昨年は850（ユニーク数）もの亜種が発見されました。

ランサムウェア攻撃の数が引き続き減少 -

2020年は2年続けてランサムウェアペイロード（ユニーク数）が減少し、最高を記録した2018年の5,489件、そして2019年の4,131件から2,152件（ユニーク数）にペイロードが減りました。これらの数字は、ランサムウェアの亜種に世界中の膨大な数のエンドポイントが感染したことを示しています。これらの検知は主に、WannaCryおよび関連する亜種を検知するために2017年に導入されたシグニチャにより検知されており、WannaCryが表舞台に登場してから3年以上にわたりランサムウォーム戦術がいまだに生き延びていることを示しています。ランサムウェアの数が着実に減少したことは、攻撃者がこれまでの的を絞らない広範囲な攻撃から、医療機関や製造業などダウンタイムが許されない被害者を対象とした高度な標的型攻撃へとシフトし続けていることを示唆しています。

暗号化された回避型のマルウェア攻撃が2桁成長

4四半期連続でマルウェアの全般的な数が減少しているにもかかわらず、ウォッチガードがQ4にネットワーク境界で検知した全ての攻撃の約半数（47%）が暗号化されていました。さらに、HTTPS接続経由で配信されたマルウェアは41%増加しており、暗号化されたゼロデイマルウェア（アンチウイルスシグニチャを回避する亜種）はQ3と比較して22%増えました。

IoTデバイスやルータを標的にしたボットネットマルウェアが最大の脅威に

Q4では、Linux.Genericウイルス（「The
Moon」としても知られる）がウォッチガードのマルウェア検知トップ10リストに新たなに登場しました。このマルウェアは、サーバネットワークの一部として、IoTデバイスやルータなどのコンシューマグレードのネットワークデバイスを直接標的とし、あらゆる脆弱性をエクスプロイトします。ウォッチガードの調査により、攻撃者が仕組んだインフラの中に存在するARMプロセッサ向けに作成されたLinuxに特化したマルウェア、およびMIPSプロセッサ向けに作成されたペイロードであることが判明し、IoTデバイスに対する回避型攻撃であることは明白です。

サプライチェーン攻撃の危険性を物語るSolarWindsへの不正アクセス -

国が関与したとされる今回のSolarWinds経由の洗練されたサプライチェーン攻撃は、今後数年間にわたってセキュリティ業界全体に大きな影響を与えることになると予測されます。影響はSolarWindsのみならず、著名なFortune
500企業、セキュリティ大手企業、そして米政府をも含む約100社にまで拡大しました。ウォッチガードによる詳細なインシデント分析により、今日の相互につながるデジタルエコシステムにおいて、サプライチェーン攻撃に対する防御の重要性が明らかになりました。

マルチペイロード方式でメールスキャナーを欺く新手のトロイの木馬 -

Trojan.Script.1026663が、ウォッチガードのQ4における最も広く普及したマルウェア検知リストのトップ5に入りました。攻撃は、ユーザに添付の注文リストを確認することを求めるメールから始まります。次に添付ドキュメントが一連のペイロードと不正コードを起動させ、ユーザのマシンに最終目的とする攻撃Agent Tesla remote access
trojan（RAT）とキーロガーをロードさせます。

ネットワーク攻撃の数が2018年のピーク時の数を凌駕
Q4のネットワーク攻撃の総検知数は5%増加し、2年以上ぶりに記録を更新しました。また、ネットワーク攻撃シグニチャのユニーク数が着実に増加し、Q3と比べて4%増となっています。これは、世界でリモートワークが継続されているにもかかわらず、相変わらず企業のネットワーク境界が狙われており、攻撃者が引き続きオンプレミスのアセットを標的にしていることを示しています。

今期、ウォッチガードのアプライアンスは2,600万件以上のマルウェア（1デバイス当たり456件）、350万件近いネットワーク脅威（1デバイスあたり77件の検知）をブロックしています。また、Fireboxで455件（ユニーク数）の攻撃シグネチャをブロックしており、Q3と比較して4%増加しています。四半期ごとに発行されるウォッチガードの調査レポートは、脅威ラボの調査活動をサポートするためのデータ共有に賛同いただいている、ウォッチガーアプライアンスオーナーによる匿名のFireboxデータに基づいています。さらに、レポートの新たなエンドポイント脅威インテリジェンスでは、92ヵ国にわたる170万のエンドポイントから250万件（ユニーク数）のペイロードアラートに基づき、2020年における特定のマルウェア攻撃やトレンドに関する深い洞察を提供しています。

本レポートの全編では、2020年Q4におけるその他のマルウェアや攻撃のトレンドの詳細、悪名高いSolarWinds経由のサプライチェーン攻撃の詳細分析、そして読者向けの主要なセキュリティベストプラクティスを紹介しています。

レポート全文は以下よりダウンロードできます。
https://www.watchguard.com/wgrd-resource-center/security-report-q4-2020（英語）

*日本語レポートは後日公開予定。

【WatchGuard Technologiesについて】
WatchGuard (R) Technologiesは、ネットワークセキュリティ、セキュアWi-Fi、多要素認証、高度なエンドポイントプロテクション、ネットワークインテリジェンスを提供するグローバルリーダとして、全世界で約10,000社の販売パートナーとサービスプロバイダより80,000社以上の企業にエンタープライズクラスのセキュリティ製品とサービスを提供しています。ウォッチガードのミッションは、中堅・中小企業や分散型企業を含むすべての企業がエンタープライズレベルのセキュリティをシンプルに利用できるようにすることです。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、数多くのパートナーを通じて、国内で拡大する多様なセキュリティニーズへのソリューションを提供しています。詳細は https://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向はTwitter（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法はSecplicityJPまでアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社

〒106-0041
東京都港区麻布台1-11-9 BPRプレイス神谷町5階
マーケティング担当
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： https://www.watchguard.co.jp
