報道関係者各位

ウィズセキュア、月次脅威レポートで
新規のマルウェア攻撃グループについて注意喚起

～ 6 月はマルウェアを使用した攻撃が増加、企業は積極的かつ強固な防御策を ～

2023 年 7 月 27 日
ウィズセキュア株式会社

先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、本年 6 月の同社の月次脅威ハイライトレポートを発表しました。本レポートで最も懸念すべきこととして取り上げられたのは同月におけるランサムウェア攻撃の増加です。ランサムウェアは、貴重なデータを暗号化し、複合化のための身代金を要求する悪意のあるソフトウェアであり、サイバー犯罪者にとって大きな収益源となっています。

6 月には発生した重要なインシデントの 1 つが、ロシアの新しいサイバー犯罪グループ『Clop』による、欧米を中心に 350 万人ものユーザーを持つファイル転送サービス『MOVEit』の脆弱性を悪用したランサムウェア攻撃です。この攻撃により多数の企業が侵害を受け貴重なデータが漏えいし、脅迫の対象となる可能性があります。レポートでは、この攻撃が広範囲に影響を及ぼし、MOVEit の数千ものインスタンスに影響を与え、機密性の高い個人情報が流出する可能性があることを取り上げています。

また BYOVD (Bring Your Own Vulnerable Driver) 手法の脅威が高まっていることも注目すべき点です。BYOVD は、攻撃者が正規のドライバの脆弱性を悪用し、アンチウィルスや EDR (エンドポイントの検知と対応) ソリューションをバイパスまたは無効化する目的で採用する防御回避戦略です。同レポートでは、『Terminator』と名付けられた BYOVD エクスプロイトの出現について言及し、より強固な防御の重要性を強調しています。

その他のトピックとしては、中国の APT (Advanced Persistent Threat) グループ『Volt Typhoon』の活動を取り上げています。Volt Typhoon は Living off the land 攻撃 (アクセス先システムに存在するリソースの流用) やカスタム Web シェルを利用してシステムを侵害しています。ウィズセキュアは、Volt Typhoon が米国の重要インフラのセキュリティとレジリエンスにもたらす重大なリスクを指摘しています。

こうしたサイバー脅威に関して、ウィズセキュアの日本法人であるウィズセキュア株式会社でサイバーセキュリティ技術本部長を務める島田秋雄 (しまだ　あきお) は次のように述べています。
「当社の脅威ハイライトレポートは企業や団体がサイバー脅威から防衛するうえでの実践的な対応方法を提供し、ランサムウェアのリスクの軽減を目的としています。今回のレポートに掲載されているこれらのインシデントは、脅威が

進化していること、そして組織が常に警戒を怠らず、ランサムウェア攻撃が発生した場合に重要なデータを回復できるよう、安全なバックアップを行うことの重要性、プロアクティブかつ強固なセキュリティ防衛戦略を実施する必要性を表しています。」

ウィズセキュアの脅威ハイライトレポート (英語) は以下のページでご覧いただけます。
https://www.withsecure.com/en/expertise/research-and-innovation/research/monthly-threat-highlights-report

ウィズセキュア Web サイト:
https://www.withsecure.com/jp-ja/
ウィズセキュアプレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure について

ウィズセキュアは、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を検出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立されたウィズセキュアは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。
詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の発信をおこなっています。