日本関連のハクティビスト活動を観測 -
ウィズセキュア、8 月の脅威レポートを発表

～ 福島の処理水放出に起因するハクティビズム、今後欧米の環境団体に影響を与える可能性 ～

2023 年 9 月 14 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 8 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。日本に関連する項目としては、ハクティビスト活動が急増、特に日本関連の攻撃が目立っています。これは福島原発からの処理水放出に起因するサイバー攻撃であり、環境問題に関連したサイバー攻撃の初のケースとなります。レポートではまた、新たに登場したランサムウェアや日本でも多くのユーザーを持つ WinRAR の脆弱性などについても取り上げています。

●ハクティビズム

ハクティビズムは政治的な意思表示や目的実現のためのハッキングの使用です。この 1 ヶ月間、環境活動に関連するサイバー攻撃がより顕著になっていることです。福島原発からの海洋への処理水放出に対して、『Anonymous Italia』とインドネシアのグループ『VulzSec』が環境活動に関連するサイバー攻撃を引き起こし、「#OpJapan」という攻撃キャンペーンを実施しています。このキャンペーンは環境活動に関連するサイバー攻撃としての初の事例であり、今後ヨーロッパやアメリカでの同様の他団体の戦術に影響を及ぼす兆候である可能性も考えられます。また、親ロシア派のハクティビストグループはウクライナに援助を提供する国々を中心に DDoS 攻撃を続けています。

●8 月新たに観測されたランサムウェア

『Metaencryptor』
ダークウェブ上で活発なリークサイトを持ち、マルチポイントで恐喝ランサムウェアを操作しています。8 月 17 日、彼らは異なる被害者に関する 12 の投稿を行いましたが、これは彼らが比較的長期に渡って侵害を行ってきた可能性を示しています。ターゲットのうち 5 つがドイツ企業であることから、日和見的な攻撃ではなくターゲットを絞ったものだと考えられます。

『INC Ransom』
このグループはオーストリアのホテルとオランダの電力会社をリークサイトに掲載しています。彼らの最近の攻撃が Huntress 社によって分析され、同社発行のレポートには IOC (侵害の指標) と TTP (戦術・技術・手順) が含まれています。サイバー犯罪のプロフェッショナル化により、それらの多くは他の攻撃グループと共通点が見られます。

『Cloak』
このグループについてはほとんど知られていませんが、これまでにリークサイトに 24 の被害者をリストアップしています。被害者は様々なセクターに属するグローバル企業であり、攻撃は日和見的なものであると考えられます。

●WinRAR での脆弱性

多くのユーザーを持つファイル圧縮・解凍ソフトである WinRAR には、CVE-2023-40477 と CVE-2023-38831 という 2 つの既知の脆弱性が確認されています。前者は既に積極的に悪用されており、被害者が悪意のある.rar ファイルを開くというアクションが必要ですが、攻撃者にとっては何らかの口実のもとにユーザーとの間にその対話のキッカケを作り出すことは容易であるため、更なる悪用の可能性は高いと言えます。後者は一見無害なファイルを含む特別に細工された.zip ファイルが関係し、実際には別のディレクトリに格納された悪意のあるコードが実行されます。

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、現在のサイバー脅威の状況について以下のように語っています。
「8 月にも多くの新しいランサムウェアやソフトウェアにおける脆弱性が発見されています。脅威は常に進化しており、ユーザーは常にベンダーからのアップデートを確認しソフトウェアを最新の状態に保ち、リスクの低減を図ることはもちろんのこと、安全なバックアップや企業自体としてのセキュリティ防衛戦略の策定・実施を行うべきです。」

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。