ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●ウクライナをターゲットとする「ワイパー型」マルウェアが相次いで確認

https://www.eset.com/jp/blog/welivesecurity/caddywiper-new-wiper-malware-discovered-ukraine/
https://msrc-blog.microsoft.com/2022/03/01/cyber-threat-activity-in-ukraine-analysis-and-resources-ja/

このニュースをザックリ言うと･･･

- 2月下旬以降、セキュリティベンダーのESET社より、ウクライナの組織をターゲットとしているとみられるワイパー型(感染したPCのデータを消去する)マルウェアの存在が同社ブログで相次いで発表されています。

- 2月25日(現地時間)に同社から最初に発表されたのは「HermeticWiper」で、同23日、ロシアがウクライナへの侵攻を開始する数時間前からこれを用いた破壊的な攻撃が行われたとしています。

- 次いで3月10日の発表では、今度はロシアの侵攻が開始した直後の2月24日に、ウクライナ政府のネットワークに対し「IsaacWiper」と呼ばれる別種による攻撃が行われたとのことです。

- さらに3月24日には、同21日に「CaddyWiper」と呼ばれる3種類目のマルウェアが確認されたことが発表されています。

AUS便りからの所感等

- HermeticWiperは、WindowsのSMB(ファイル共有プロトコル)やWMI(組織向け管理機能)でLAN上に拡散した他、「HermeticRansom」と呼ばれるランサムウェアも攻撃に用いられたとされており、また2021年に不正に取得されたコードサイン証明書による署名がされていたとのことです(攻撃が確認された直後に証明書は無効化されています)。

- HermeticWiper・IsaacWiper・CaddyWiperはそれぞれ作りが大きく異なるとされ、別々の組織による攻撃の可能性が示唆されています。

- そしてこの他にも、同じくウクライナをターゲットとするランサムウェア「WhisperGate」の存在が、1月にMicrosoft等から発表されています。

- これらのマルウェアのターゲットが「ウクライナを支持する世界の国々」へ拡大する可能性は決して皆無とは言えず、全ての組織においてアンチウイルスやUTM等により、マルウェアへの感染の抑制や、内部での感染時の被害の軽減等を図ることが肝要です。

●テレワーク普及、退職者による機密漏えい…IPA「内部不正防止ガイドライン」5年ぶりの改訂

https://www.itmedia.co.jp/news/articles/2204/07/news082.html
https://www.ipa.go.jp/about/press/20220406.html

このニュースをザックリ言うと・・・

－4月6日(日本時間)、IPAより、「組織における内部不正防止ガイドライン」の第5版が公開されました。

－内部不正による情報セキュリティ事故を防ぐため、2013年3月の公開以後、2014・2015・2017年と改訂されていたもので、今回近年の事業環境の変化や情報漏えい対策技術の進歩などを踏まえ、5年ぶりの改訂となっています。

－第5版の主な改訂のポイントとして「テレワークの普及に伴う対策」「退職者関連対策」「ふるまい検知等の新技術活用に伴う対策」の3つが挙げられています。

AUS便りからの所感

－前述のポイントのうち「テレワークの普及に伴う対策」はオンラインストレージ・クラウドサービスの利用拡大等への対応、「退職者関連対策」は営業秘密の漏えいルートとして中途退職者が最も多いとされた2021年の調査結果を踏まえてのもの、「ふるまい検知等の新技術活用に伴う対策」についてはAIの活用による検知の採用にあたっての役職員の人権・プライバシーを保護する観点からの運用を取り上げています。

－過去に当ガイドラインを活用して組織内での対策の整備を行っていた場合でも、今回の改訂ポイントに着目し、追加対策を行うべき箇所があれば着実に押さえていき、法規的あるいは技術的に内部不正の発生や成立を抑え込めるような体制を引き続き整えて頂ければ幸いです。

ITmedia NEWS

IPAの「内部不正防止ガイドライン」、5年振りに更新 テレワーク普及など踏まえ改訂

2022年04月07日 11時21分 公開　[ITmedia]

情報処理推進機構（IPA）は4月6日、内部不正による情報セキュリティ事故を防ぐためのガイドライン「組織における内部不正防止ガイドライン」を2017年振りに改訂した。コロナ禍によるテレワークの普及や個人情報保護法の改正、技術の進展などを踏まえ、新たに必要になった対策を追記した。

●Windows・sudo等の古い脆弱性を悪用する攻撃、米CISAが注意喚起

https://news.mynavi.jp/techplus/article/20220407-2315628/
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/06/cisa-adds-three-known-exploited-vulnerabilities-catalog

このニュースをザックリ言うと・・・

－4月6日(現地時間)、米国土安全保障省(DHS)に属するセキュリティ機関CISAより、同機関が公表している「Known Exploited Vulnerabilities Catalog(既知の悪用された脆弱性のカタログ)」に3件の脆弱性を追加したと発表されました。

－追加されたのは、2021年1月発表のsudo(Linuxで管理者等の権限でコマンドを実行するツール)の脆弱性(CVE-2021-3156)、2017年3月発表のWindows SMB(ファイル共有等を行うプロトコル)v1の脆弱性(CVE-2017-0148)、および2021年5月発表のWindows HTTPプロトコルスタックの脆弱性(CVE-2021-31166)となります。

AUS便りからの所感

－sudoの脆弱性はサーバーに別途侵入済みの攻撃者あるいは正規のログイン可能なユーザーが悪意をもって攻撃を行う場合、SMBv1の脆弱性はサーバー側が当該プロトコルを受け付ける設定の場合(v2ないしv3のみ受け付けるよう設定可能)、HTTPプロトコルスタックの脆弱性はサーバーがWebサーバー等として稼働している場合に影響を受ける可能性があり、未対策の場合、最悪サーバー等を乗っ取られる恐れもあるものです。

－いずれの脆弱性も昨年およびそれ以前に発表、セキュリティアップデートがリリース済みのものであるため、これらを含めたあらゆる脆弱性や攻撃の影響を抑制できるよう、随時サーバー・クライアントのOSやソフトウェアを最新に保つ運用、加えて不要なサービスへのアクセスを制限する等の強固な設定による防御を強く推奨致します。

TECH+ Powered by マイナビニュース

SudoやSMBv1のサイバー攻撃への活発な悪用を確認、更新を

2022/04/07 10:47　著者：後藤大地

米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA: Cybersecurity and Infrastructure Security Agency)は4月6日(米国時間)、「CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA」において、「Known Exploited Vulnerabilities Catalog」に3個の脆弱性を追加したと伝えた。これら脆弱性はサイバー犯罪者によって積極的に悪用されていることが確認されている。

CVE番号	脆弱性内容
CVE-2021-3156	Sudo Heap-Based Buffer Overflow Vulnerability
CVE-2021-31166	Microsoft HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2017-0148	Microsoft SMBv1 Server Remote Code Execution Vulnerability