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。

●「@creema.jp」のフィッシングメール大量発生、クリーマ社が注意喚起

https://scan.netsecurity.ne.jp/article/2024/10/01/51693.html
https://www.creema.jp/news/1402/detail

このニュースをザックリ言うと･･･

- 9月20日(日本時間)、ハンドメイドマーケットプレイス「creema」を運営するクリーマ社より、企業や官庁を装い、creemaのドメイン名「creema.jp」を使用するフィッシングメールについて注意喚起が出されています。

- 注意喚起によれば、メールはいずれもFrom: (送信元)がsupport@creema.jp、info@creema.jp、または〇〇@creema.jp(ランダムな英数字列や宛先メールアドレスの一部)となっている一方、提示されている事例はヤマト運輸、東京電力、Amazon、クレジットカード各社、税務署、ろうきん等、騙る対象は多岐に及んでいます。

- これらのメールはcreemaへの登録の有無とは関係なく送信されるもので、同社からユーザーのメールアドレス等の個人情報が漏洩した事実はないとしており、受信した場合メール内のURL・ボタン等をクリックしないこと、アクセス先でメールアドレス・パスワード等の個人情報は入力しないことを呼び掛けています。

- この他、携帯電話各社のキャリアメールでなりすましメールを受信しない為の設定手順を紹介しています(GMail等大手メールサービスではなりすましメールに対応済みとしています)。

AUS便りからの所感等

- 同社では以前より、From: で@creema.jpやクリーマ社の@creema.co.jpを使用しながらもcreema以外の組織・サービスを騙るフィッシングメールについて注意喚起を出しています。

- ユーザーがメールの振り分け設定時、「@creema.jp」等のアドレスや、件名や本文で特定の文字列を使用しているものを振り分けるようにしている場合になりすましメールが紛れ込むことを狙っていると考えられますが、今日ではGMail等では迷惑メールと判定したものは振り分け設定に優先して隔離しますし、いよいよ普及が進んでいるSPF・DKIM・DMARCのようなになりすまし対策により、メールサーバー側で受信自体を拒否する等も効率よく行えるようになっています(creemaにおいても「とれる対策はすでに実行済み」と発表しています)。

- メールの件名・内容と送信元アドレスとが明らかに合っていない、いかにも不審なメールには無視するようなリテラシーをユーザー側が持つことは大事ですが、これに依存するだけでいることは今日正しいフィッシング対策ではなく、自組織・取引相手・その他のユーザーを保護する観点から、メールサーバーにおけるシステム面でのなりすまし対策の導入・運用を確実に行うことが重要です。

ScanNetSecurity

脆弱性と脅威／脅威動向

2024.10.1 Tue 8:05

「creema.jp」ドメイン使用し企業や官庁を装った不審メールに注意呼びかけ

株式会社クリーマは9月20日、送信元が同社ドメインとなった不審メールへの注意喚起を発表した。

株式会社クリーマは9月20日、送信元が同社ドメインとなった不審メールへの注意喚起を発表した。

同社では現在、企業や官庁を装い送信元が同社のドメイン「@creema.jp」となったフィッシング詐欺目的の不審メールの急増を確認している。不審メールは同社及び同社が運営するハンドメイド作品の販売サイト「Creema」の会員登録の有無と関係なく、無差別に配信されているという。

同社で確認している事例は下記の通り。

・事例1
メール差出人：ヤマト運輸株式会社
内容：荷物の受け取り日時や場所の指定の案内

・事例2

●Linux・Mac等で使用される印刷システム「CUPS」に脆弱性

https://jvn.jp/vu/JVNVU91741031/
https://x.com/shodanhq/status/1839418045757845925

このニュースをザックリ言うと･･･

- 10月2日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、Linux(およびmacOS等)向け印刷システム「CUPS」に複数の脆弱性(CVE-2024-47176・CVE-2024-47076・CVE-2024-47175・CVE-2024-47177)が報告されたとして注意喚起が出されています。

- 脆弱性の悪用により、CUPSが動作しているサーバー上で任意のコード・コマンドを実行される可能性があり、サーバーを乗っ取られる等の恐れがあります。

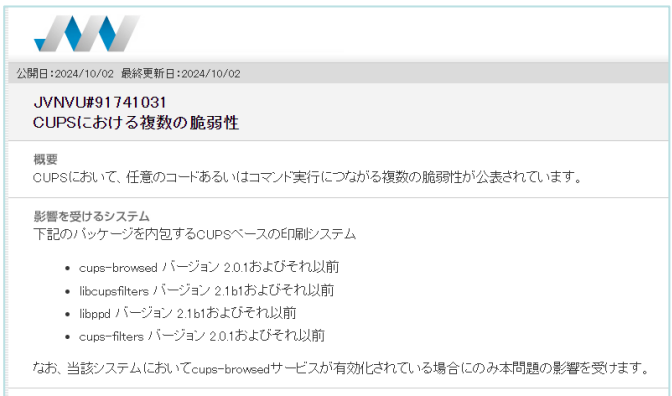
- CUPSの開発元からまだ正式な修正バージョンのリリースはなく、macOSに影響するかも不明ですが、各種Linuxディストリビューションで独自にセキュリティアップデートがリリースされている他、回避策も示されています。

AUS便りからの所感

- CUPSはLinux等のマシンに接続されたプリンターをLAN上で共有するといった用途に使われます。

- 複合機をはじめとしたIoT機器のサーチエンジン「Shodan」では、CUPSサービスに外部からアクセス可能なサーバーが世界で少なくとも75,000台確認されているとしています。

- 複合機等と同様、本来第三者に公開されるべきものではなく、ゲートウェイやファイアウォールにおいてUPnP等による不必要な公開設定がされないよう注意すべきです。


公開日:2024/10/02 最終更新日:2024/10/02

JVNVU#91741031
CUPSにおける複数の脆弱性

概要
CUPSにおいて、任意のコードあるいはコマンド実行につながる複数の脆弱性が公表されています。

影響を受けるシステム
下記のパッケージを内包するCUPSベースの印刷システム

- cups-browsed バージョン 2.0.1およびそれ以前
- libcupsfilters バージョン 2.1b1およびそれ以前
- libppd バージョン 2.1b1およびそれ以前
- cups-filters バージョン 2.0.1およびそれ以前

なお、当該システムにおいてcups-browsedサービスが有効化されている場合にのみ本問題の影響を受けます。

●マルウェア入りAndroidアプリの配布事例、相次いで報告される

https://news.mynavi.jp/techplus/article/20240927-3032403/
https://www.threatfabric.com/blogs/octo2-european-banks-already-under-attack-by-new-malware-variant
https://www.lifehacker.jp/article/2409necro-trojan-malware-has-infected-11-million-android-devices/
https://securelist.com/necro-trojan-is-back-on-google-play/113881/

このニュースをザックリ言うと･･･

- 9月24日(現地時間)、オランダのセキュリティ企業ThreatFabric社より、Androidに侵入、インターネットバンキングを狙うマルウェア「Octo2」について注意喚起が出されています。

- Octo2は「Exobot」および「Octo(別名: ExobotCompact)」の亜種とされ、「Google Chrome」「NordVPN」「Enterprise Europe Network」といったAndroidアプリに偽装する形で配布が確認されたとしています。

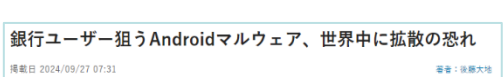
- また同じくセキュリティ企業のKaspersky社より、Androidに感染するトロイの木馬「Necro」が広まっているとの事例が報告されています。

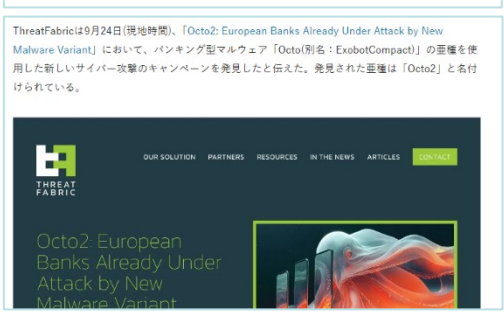
- こちらは「Spotify」「WhatsApp」の改造版を称するアプリの他、Google公式のPlayストアで配布されているアプリにも感染しているとされ、1,100万台以上のAndroid端末が影響を受けているとしています。

AUS便りからの所感

- ThreatFabric社では2023年12月にAndroidに侵入する別のマルウェアについて注意喚起を行った際、Android 13から導入された、有害とみられるアプリに警告を表示する「制限付き設定」を解除するよう誘導する動きがあったことに言及しており、Playストア以外からのインストール時に警告が表示されないよう、あるいはユーザーに無視するようにしてマルウェアを感染させようと様々な手口をとっている様子が窺えます。

- Playストアからインストールするアプリでも同様ですが、インストール時や実行時に不必要に権限や設定変更を要求してくるアプリに対しては安易に従わず、アプリストアのレビューやSNS上での報告がないか確認し、普段から信頼のおける必要最低限のアプリのインストールに留めるよう心掛けましょう。


銀行ユーザー狙うAndroidマルウェア、世界中に拡散の恐れ
掲載日 2024/09/27 07:31
著者：後藤大地


ThreatFabricは9月24日(現地時間)、「Octo2: European Banks Already Under Attack by New Malware Variant」において、バンキング型マルウェア「Octo(別名：ExobotCompact)」の亜種を使用した新しいサイバー攻撃のキャンペーンを発見したと伝えた。発見された亜種は「Octo2」と名付けられている。