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。

## ●カプコン、不正アクセスで機密データ奪取される…ランサムウェア感染か

https://mainichi.jp/articles/20201111/k00/00m/040/072000c
https://automaton-media.com/articles/newsjp/20201110-142870/
https://times.abema.tv/news-article/8633189
http://www.capcom.co.jp/ir/news/html/201104.html?_pb_uid=1929

### このニュースをザックリ言うと･･･

- 11月4日(日本時間)、ゲームメーカーのカプコン社より、同社グループのシステムが不正アクセスを受け、同2日未明からメール・ファイルサーバー等にアクセスしづらい障害が発生していると発表されました。

- 同9日には、「RAGNAR LOCKER」と称するサイバー犯罪グループが、同社への攻撃に成功し、顧客や従業員の個人情報および業務上の情報等を含む約1TBのデータを暗号化・ダウンロードしたとする犯行声明をネット上に公開しています。

- RAGNAR LOCKERは同11日午前8時までに1,100万ドル(約11億5,000万円)の身代金を支払うよう同社に要求していましたが、その後同日中に、同社の内部情報とみられるゲームの売上・社員給与の記録や従業員のパスポート画像等、約67GB分のデータをいわゆる「ダークウェブ」上にアップロードしたとされています。

### AUS便りからの所感等

- データを暗号化し、人質に身代金を要求する手口から、ランサムウェアによる攻撃が行われた可能性が各所で指摘されています。

- 先月下旬には、Windowsのドメインコントローラ(DC)の脆弱性をランサムウェアが悪用するケースについて警告が出されており(AUS便り 2020/10/26号参照)、今後もリスクの高い脆弱性がランサムウェアの呼び水になるケースは絶えることはないでしょう。

- 企業・組織の全てのクライアント・サーバー、またリモートワークでの利用も想定される家庭内のPCについても最新のセキュリティパッチを当てて脆弱性を塞ぐこと、感染したPC等から他のPCへの攻撃を食い止められるようUTM等による安全なネットワーク構成をとること、データの暗号化や破壊から確実に復旧できるよう適切なバックアップをとることが肝要です。

毎日新聞

カプコンにサイバー攻撃、情報漏えいか　犯罪集団が声明、大阪府警が捜査

毎日新聞 2020年11月11日 11時55分（最終更新 11月11日 18時53分）　English version

ネットワーク　大阪府　速報　社会

サイバー攻撃を受けたカプコンの本社＝大阪市中央区で2020年11月11日午後3時51分、森口沙織撮影


企業の機密情報を盗んで金銭を要求するサイバー犯罪集団が、大手ゲーム会社「カプコン」（大阪市中央区）にサイバー攻撃を仕掛け、同社の内部情報や個人情報とみられる大量のデータをインターネット上に公開したことが、関係者への取材で判明した。グループは仮想通貨（暗号資産）を要求し、日本時間の11日午前8時までに連絡するよう求めていた。相談を受けた大阪府警が情報収集を進めている。

関係者によると、グループは「RAGNAR LOCKER（ラグナロッカー）」と名乗っている。カプコンのネットワークを攻撃し、同社の顧客や従業員の個人情報、業務情報など約1テラバイト（テラは1兆）のデータを入手したとする英語の犯行声明を9日に公開。取引に応じればデータを消去するとしていた。

AUTOMATON
VERACITY IN GAMING

カプコンの不正アクセス被害は、ランサムウェア攻撃によるものか。攻撃者を名乗るグループが、機密データを人質に約11億円の身代金を要求

By Taijiro Yamanaka - 2020-11-10 15:43

Ragnar_Locker Teamと名乗るグループは11月9日、カプコンの経営陣に宛てた“最後通告”であるとする声明を発表した。これに先立つ11月4日には、カプコンは不正アクセスによるシステム障害の発生を報告しており、今回の声明との関連が指摘されている。

同社は不正アクセスの詳細について明らかにしていないが、セキュリティ関連メディアBleepingComputerは11月6日、カプコンはRagnar_Lockerと呼ばれるランサムウェアによる攻撃を受けたと報じた。ランサムウェア攻撃とは、攻撃者が対象のサーバーなどシステム内のデータを暗号化して利用不可能にし、データを復旧させる代わりに金銭を要求すること。BleepingComputerは、セキュリティ研究家のPancak3氏が入手した、今回カプコンに対して使われたRagnar_Lockerのサンプルを確認したところ、攻撃者とされるRagnar_Locker Teamがカプコンに対して、1100万ドル（約11億5500万円）分のビットコインを“身代金”として要求していることが判明したという。

## ●Googleが報告した「ゼロデイ脆弱性」、WindowsとChromeにて対応

https://jp.techcrunch.com/2020/10/31/2020-10-30-google-microsoft-windows-bug-attack/
https://www.ipa.go.jp/security/ciadr/vul/20201111-ms.html
https://pc.watch.impress.co.jp/docs/news/1284238.html
https://pc.watch.impress.co.jp/docs/news/1288696.html

### このニュースをザックリ言うと・・・

- 10月30日(米国時間)、Googleより、Windowsにおける未修正かつ既に攻撃者に悪用されている、いわゆる「ゼロデイ脆弱性」の存在が発表されました。

- この脆弱性(CVE-2020-17087)は、Chromeブラウザーに存在していた別の脆弱性(CVE-2020-15999)との組合せでの攻撃により、マルウェアがPCを乗っ取ることが可能になるものとされ、主にWindows 7と10が攻撃対象となっているとのことです。

- Chrome側では10月20日の時点で脆弱性を修正したバージョンがリリースされており、11月11日(日本時間)にはWindows側でも、マイクロソフト(以下MS)よりリリースされた月例のセキュリティパッチで対応が行われています。

### AUS便りからの所感

- GoogleではChrome側での対応後、事前にMSに連絡をとり、一週間以内に対応するよう依頼していましたが、期限内に対応されなかったことから情報を公開、Windowsでの対応は結局月例のパッチでの対応となっています。

- 一方のChromeについても複数のゼロデイ脆弱性への対応によるセキュリティリリースが続き、11月だけでも3度アップデートが行われています(11月16日時点の最新バージョンは86.0.4240.198)。

- 最も根本的な対策として、Windowsがセキュリティパッチが適用された最新のバージョンとなっているかの確認が重要となりますが、通常設定では自動更新が行われるChrome(およびChromeと同じエンジンを使うEdgeブラウザー)でも同様に、最新バージョンになっているか確認を行うようにしてください。

Googleがいまだに悪用されているWindowsのゼロデイバグを公表

2020年10月31日 by Zack Whittaker

Google（グーグル）が、現在のところ公表されていないWindowsの脆弱性について、その詳細を明らかにした。同社によると、その脆弱性は現在でもハッカーが頻繁に悪用しているという。グーグルはMicrosoft（マイクロソフト）に、1週間の修復猶予期間を与えている。そしてその締切が過ぎた米国時間10月30日の午後、脆弱性の詳細を公表した。

この脆弱性には名前がなく「CVE-2020-17087」というラベルが付いている。被害は主にWindows 7とWindows 10で生じている。

脆弱性を発見したグーグルのセキュリティグループであるProject Zeroによると、このバグによりWindowsの自分のユーザーアクセスのレベルを上げることができるという。Windowsの脆弱性とChromeの別のバグを一緒に用いるが、後者はグーグルが先週公表しフィックスしている。新しいバグでは、通常は他のアプリケーションから隔離されているChromeのサンドボックスを逃れて、オペレーティングシステムの上でマルウェアを動かすことができる。

## ● Ubuntuに脆弱性、管理者権限ユーザーを勝手に作成される恐れ

https://gigazine.net/news/20201113-ubuntu-make-administrator-vulnerability/

### このニュースをザックリ言うと・・・

- 10月10日(現地時間)、コード管理サイト「github」のエンジニアより、Linuxディストリビューションの一つ「Ubuntu」に、管理者権限を持つユーザーが作成可能な脆弱性が存在すると発表されました。

- 発表における動画解説では、Ubuntuが稼働するホストにログイン可能な一般ユーザーがサーバー上で細工を行うことにより、Ubuntuの初期設定画面を呼び出し、そこで管理者権限を持つユーザーを作成する様子が紹介されています。

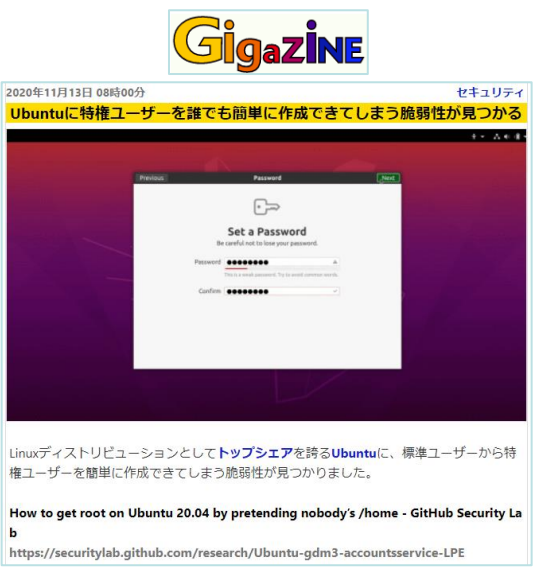
- 脆弱性はUbuntu 16.04～20.10のデスクトップバージョンに存在し、11月3日に修正パッチがリリースされたとのことです。

### AUS便りからの所感

- 脆弱性はUbuntuで独自に追加されたコードに存在するもので、Ubuntuの派生元となるDebianや、別系統となるCentOS・RHELには存在しないとのことです。

- Ubuntu上でGUI(X Window System・Wayland)が稼働しているケースでのみ問題となりますが、Linuxサーバーを GUI上で管理することも珍しくなく、組織内の悪意のある人間が悪用することが考えられます。

- Linuxにおいては、全てのソフトウェアパッケージを一括してアップデートする仕組みを確実に活用し、OSを最新に保つルーチンを確立すること、またパッケージからではなくソースからコンパイルしたソフトウェアについても、古いバージョンを放置せずに管理することが重要です。



GIGAZINE

2020年11月13日 08時00分 セキュリティ

Ubuntuに特権ユーザーを誰でも簡単に作成できてしまう脆弱性が見つかる



Linuxディストリビューションとしてトップシェアを誇るUbuntuに、標準ユーザーから特権ユーザーを簡単に作成できてしまう脆弱性が見つかりました。

How to get root on Ubuntu 20.04 by pretending nobody's /home - GitHub Security Lab
https://securitylab.github.com/research/Ubuntu-gdm3-accountsservice-LPE