働き方の多様化とセキュリティ対策

前田 典彦
株式会社ＦＦＲＩセキュリティ
https://www.ffri.jp/

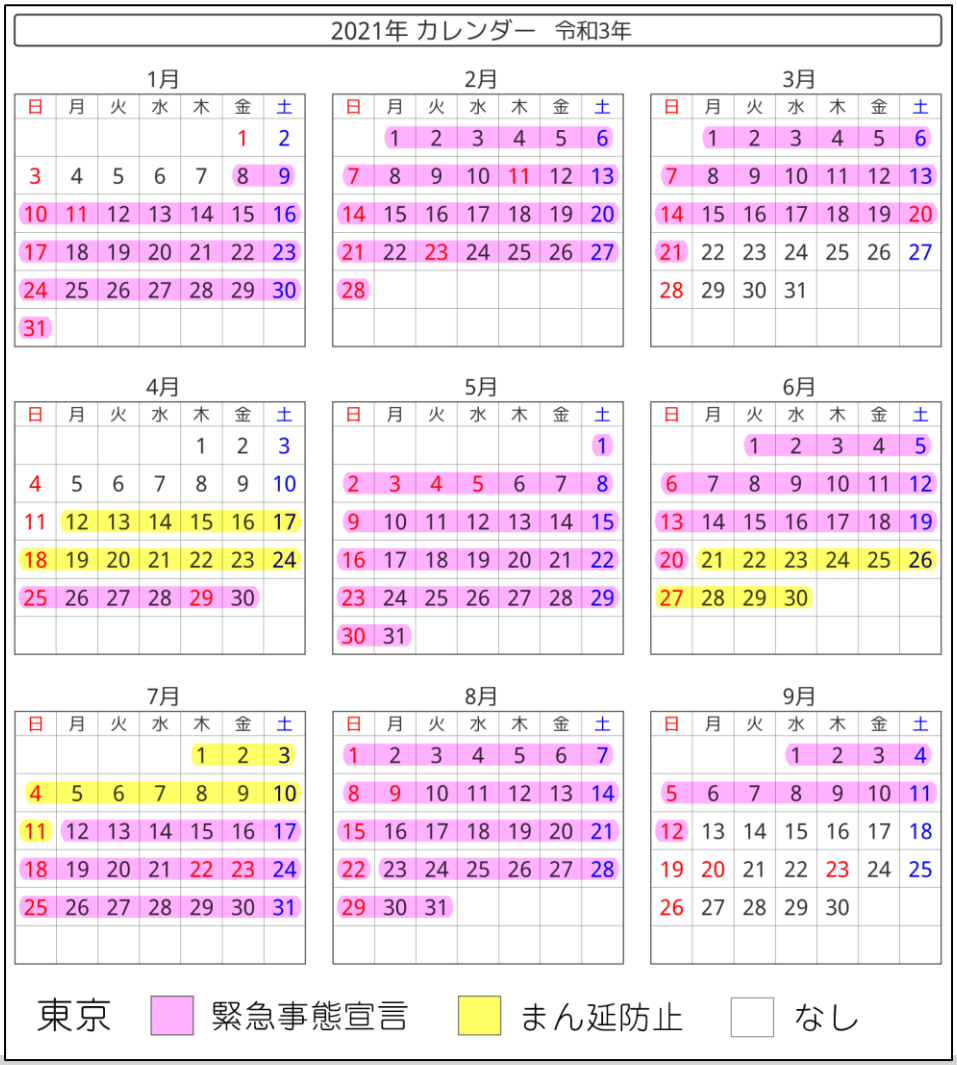
地域SECUNITYサイバーセキュリティセミナー
in Fukuoka
2021年9月28日

自己紹介

前田　典彦
(まえだ　のりひこ)

株式会社FFRIセキュリティ 社長室長、また同社のCSIRTのPoC(日本シーサート協議会加盟)。エバンジェリストとしてサイバーセキュリティ関連情報の発信や普及啓発活動を行う。
UNIXサーバ及びネットワークの構築運用エンジニア業務を約10年経験した後、セキュリティ業界に転身。ウイルス対策ソフトウェアメーカーにて12.5年間調査研究業務・エバンジェリスト活動を経て、2019年7月に株式会社FFRIセキュリティに転職。日本ネットワーク協会(JNSA) 調査研究部会長など、社外NPO法人や各種団体でも活動中。

COVID-19



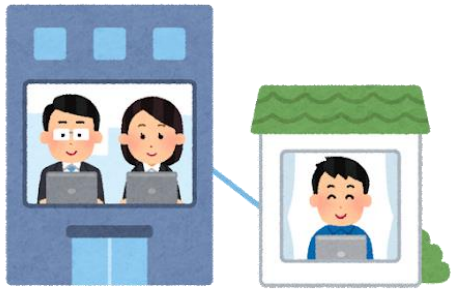
- 東京は、もはや「緊急事態が【普通の事態】」の状態
- (9月中旬以降、状況は多少落ち着いてきたか？←イマココ)
- とにかく「3密」を回避、人流の抑制
- 特にオフィスワーカーには、自宅勤務・テレワークが求められるご時世
- post(or with) COVID-19 時代にリモートワークはどうなるか

リモートワーク

- リモートワーク (work at/from home, telework) は、おそらく無くならない
- 出社勤務でなくても、業務効率が {上がる | 保てる} { 職種 | 性格 } の集団が一定数存在する
- それを容認する会社・組織も一定数存在する

- 出社勤務と在宅勤務が並列・混在することが普通になる

- リモートワークを支えるIT技術
- IT技術活用の安全性担保

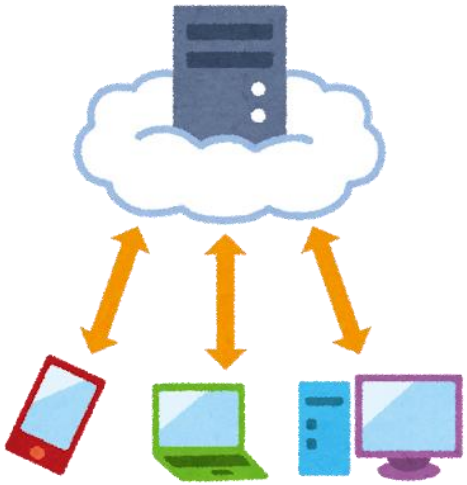


リモートワークを支えるITとセキュリティ

- リモートアクセス (VPN, RDPなど)
- クラウドサービス

- CASB (Cloud Access Security Broker)
- CSPM (Cloud Security Posture Management)
- SASE (Secure Access Service Edge),
- etc, etc…

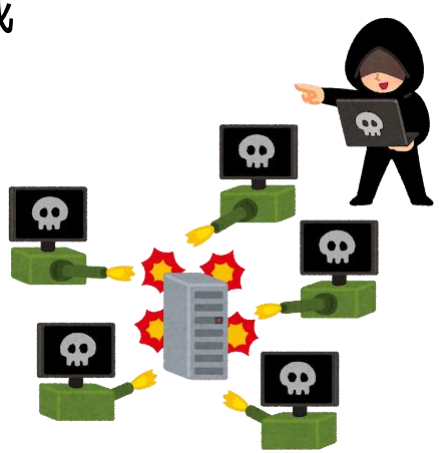
- セキュリティオーケストレーション
- ゼロトラスト



攻撃者の目線で考えてみる

- 攻撃者の手法は臨機応変

- 境界型で防御する組織を攻める
- リモートワークを実施している組織を攻める
- クラウドサービスを攻める
- 比較的攻略しやすい組織 → 防御力が高い組織
- サプライチェーン攻撃
- 個人を攻略 → 組織を攻略



例えば、VPN

FORTINET Blog | Business & Technology | Threat Research | Industry Trends | Partners | Customer Stories | PSIRT Blogs | CISO Collective | Subscribe

PSIRT BLOGS

Malicious Actor Discloses FortiGate SSL-VPN Credentials

By Carl Windsor | September 08, 2021

Fortinet has become aware that a malicious actor has recently disclosed SSL-VPN access information to 87,000 FortiGate SSL-VPN devices. These credentials were obtained from systems that remained unpatched against FG-IR-18-384 / CVE-2018-13379 at the time of the actor's scan. While they may have since been patched, if the passwords were not reset, they remain vulnerable.

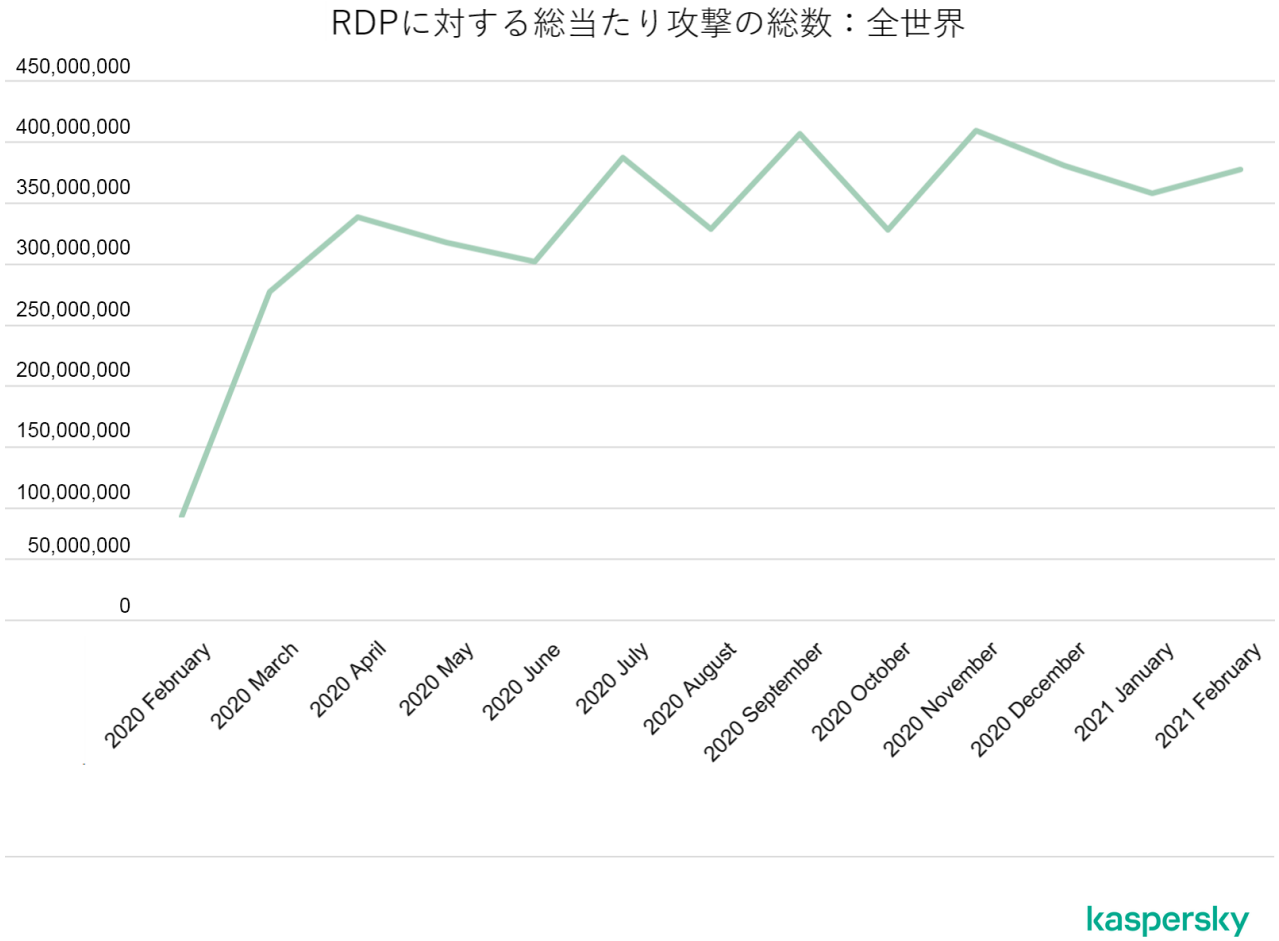
This incident is related to an old vulnerability resolved in May 2019. At that time, Fortinet issued a PSIRT advisory and communicated directly with customers. And because customer security is our top priority, Fortinet subsequently issued multiple corporate blog posts detailing this issue, strongly encouraging customers to upgrade affected devices. In addition to advisories, bulletins, and direct communications, these blogs were published in August 2019, July 2020, April 2021, and again in June 2021.

Fortinet is reiterating that, if at any time your organization was running any of the affected versions listed below, even if you have upgraded your devices, you must also perform the recommended user password reset following upgrade, as per the customer support bulletin and other advisory information. Otherwise, you may remain vulnerable post-upgrade if your users' credentials were previously compromised.

Again, if at any time your organization was running an affected version listed in the original advisory, Fortinet recommends immediately taking the following steps to ensure

出典：Fotinet PSIRT Blogs https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

例えば、RDP



出典：Kaspersky Daily https://blog.kaspersky.co.jp/attacks-on-rdp-during-pandemic-year/30354/

ランサムウェア被害事例

- 富士フイルム https://www.fujifilm.com/jp/ja/news/list/6642
- JBS(ブラジル食肉加工大手) オーストラリア部門・北米部門 https://jp.reuters.com/article/cyber-jbs-idJPKCN2DD2II
- ヘルスサービスエグゼクティブ（HSE）および保健省（DoH）（アイルランド） https://www.programmersought.com/article/33118478406
- やまびこ https://www.technadu.com/japanese-power-tool-maker-yamabiko-claimed-victim-babuk/273865/
- Colonial Pipeline（米国） https://www.bnnbloomberg.ca/colonial-pipeline-paid-hackers-nearly-us-5m-in-ransom-1.1603285
- Guilderland Central School （米国） https://securityaffairs.co/wordpress/117281/cyber-crime/school-district-albany-ransomware.html
- ブロワード郡公立学校（米国） https://securityaffairs.co/wordpress/117281/cyber-crime/school-district-albany-ransomware.html

ランサムウェア被害事例（つづき）

- ボルティモア郡公立学校（米国）
- プリングフィールド公立学校（米国）
- フェアファックス郡公立学校（米国）
  https://securityaffairs.co/wordpress/117281/cyber-crime/school-district-albany-ransomware.html
- 鹿島建設 海外グループ会社
  https://www3.nhk.or.jp/news/html/20210428/k10013003291000.html
- カプコン https://www.capcom.co.jp/ir/news/html/210413.html
- ビジョンケアUS（HOYAのアメリカ子会社）
  https://www.bloomberg.co.jp/news/articles/2021-04-21/QRWN3GT0G1LM01
- 岡野バルブ製造https://www.nikkei.com/article/DGXZQOJC275VR0X20C21A4000000/

ランサムウェア被害事例（さらにつづき）

- 日産証券 https://xtech.nikkei.com/atcl/nxt/news/18/10211/
- ニューヨーク市 法務部https://www.nytimes.com/2021/06/07/nyregion/cyberattack-law-department-nyc.html
- Travelex (英外貨両替大手) https://jp.cointelegraph.com/news/uk-company-paid-23m-ranson-in-bitcoin-to-cybercriminals
- LogicalNet (MSP/ホスティング事業)
- オールバニー国際空港 (米ニューヨーク州) https://itnews.org/news_resources/128660
- Digital Dental Record と PerCSoft が共同開発した「DDS Safe」(米国・医療記録の保存とバックアップを行うソリューション) https://japan.zdnet.com/article/35141974/
- Synoptek (MSP/ITコンサル) https://www.barracuda.co.jp/ransomware-scourge-returns-with-a-vengeance/
- Acer (台湾PCメーカー) https://gigazine.net/news/20210322-acer-revil-ransomware/

代表的なランサムウェア攻撃集団

- 最近の傾向・潮流は、完全に「暴露型ランサムウェア」
- (以下、**赤太字**は代表的なランサムウェア攻撃集団名)

- サーバーアプリケーションの脆弱性の悪用（ゼロデイも含む）
  - **DearCry**によるMicrosoft Exchangeのゼロデイ脆弱性悪用
- リモートアクセス環境の脆弱性悪用（VPNサーバーの脆弱性、RDP設定不備など）
  - **Ryuk**、**REvil**が多用する
- サプライチェーン攻撃
  - **REvil**によるMSP経由の攻撃など
- フィッシングメールによる認証情報窃取、添付ファイル展開によるマルウェア感染
- ボットネットを基盤としたマルウェア配信
  - **Conti**, **DoppelPaymer**が多用する
- 2020年中の数カ月間に、大企業を中心に2500万米ドル超の利益を上げたとされる**Netwalker**
- 2021年5月、米国東海岸における燃料供給の約半分を担うColonial Pipeline社を操業停止に追い込んだ**DarkSide**

ランサムウェア その目的

- お金

- 侵入できれば何でも良い
- 手段も標的も選ばない
- 完全に暴露型にシフト

ランサムウェア 侵入の典型例

- VPN脆弱性を悪用
- フィッシングメール
- ボットネットを使用
- クラウドサービスへの侵入
- 不用意なリモートアクセス設定を悪用
- “human operated”
- サプライチェーン攻撃も実在

※サイバーセキュリティに関わるサプライチェーンリスクにおける留意点

- 委託先・取引先からの情報漏洩、攻撃展開
- 災害などで部品供給元が絶たれる話
- 機器等にバックドアが仕掛けてられている話
- ソフトウェア配布時における事故の例

- ランサムウェア攻撃者集団が使う手法は、その他の攻撃者も当然使用している

ランサムウェア被害に遭ったら・・・

- 善後策としてのバックアップ
- 暗号化脅迫型か、暴露型か
- 身代金を払うべきか、払わざるべきか
- サイバー保険の検討

- 要点は、迅速な復旧を第一とすること。
- 情報漏えい時の対処方針を予め決めておくこと。

クラウドサービスの性質と留意点

- クラウドサービスの脆弱性（設定不備によるユーザーが意図しない挙動）

  例：ゲストユーザセキュリティポリシーのベストプラクティス(Salesforce)

  https://help.salesforce.com/s/articleView?id=000355945&type=1

→脆弱性として取り扱われない問題に気付ける「アンテナの高さ」、「横のつながり」

エンドポイントの強化

- 境界線型防御
- ゼロトラスト

どのモデルであっても、エンドポイント(PC)は存在する

- アンチウイルス (AV)
- 次世代型アンチウイルス (NGAV)
- EDR (Endpoint Detection and Response)

ありがとうございました。

前田 典彦
株式会社FFRIセキュリティ

地域SECUNITYサイバーセキュリティセミナー
in Fukuoka
2021年9月28日