muratec

「Emotet」終息も束の間、新たなランサムウェア被害が拡大

「Cring」とは？そしてその防御策は

昨年世間を騒がせたマルウェア「Emotet」（エモテット）がようやく終息に向かったのも束の間、今年に入って新たなランサムウェア「Cring」（クリング）が流行し始め、国内企業にも被害が広がっています。

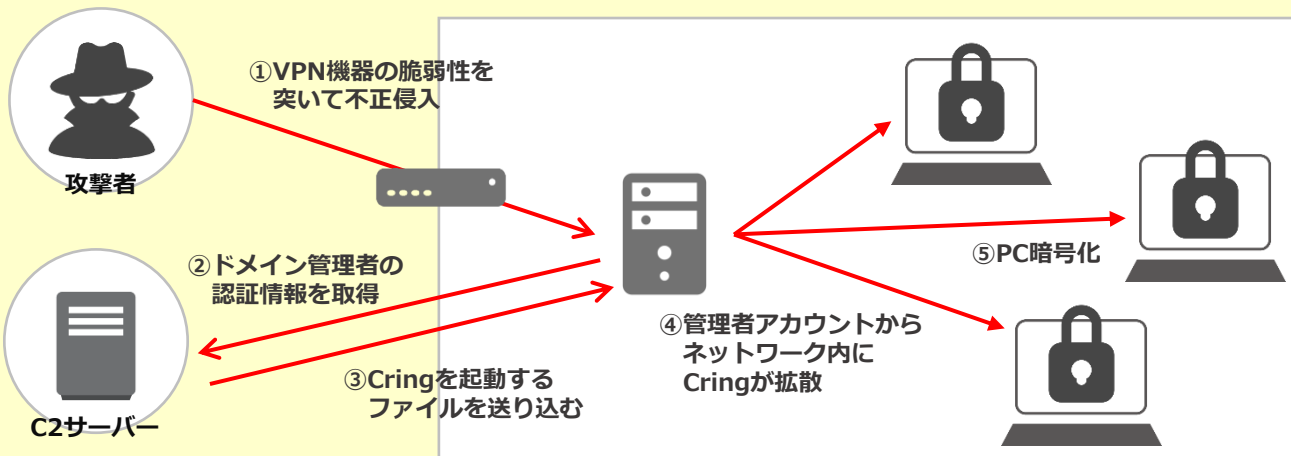
トレンドマイクロ社によると、2021年1～4月にインシデント対応支援したランサムウェア被害のうち約7割が「Cring」によるものだったと報告されています。

「ランサムウェア（Ransomware）」とは？

悪質なウイルスソフトの一種で、感染した**PCをロックしたりファイルを暗号化したりして使用不能にし、元に戻すのと引き換えに「身代金」を要求**する不正プログラムです。

さらに最近は、データの暗号化だけでなく**「身代金を支払わないとデータを暴露するぞ」と脅しをかける、「二重脅迫」の手口**が増加しています。この被害に遭った会社が**身代金支払いを拒む姿勢を貫いたことで、内部情報が暴露されるという事件**も実際に起こりました。

「Cring」の攻撃の突破口として悪用されたのは、2019年に公表されていたFortinet社のVPN製品の脆弱性（CVE-2018-13379）でした



（参照元：カスペルスキー社・トレンドマイクロ社の公開記事）

他にもPulse SecureやPalo Alto、Ciscoといった各種VPN製品で既知の脆弱性を悪用したサイバー攻撃が増加。

コロナ禍でテレワーク需要が高まり、リモート接続にVPN利用が定着する中でこうした過去の脆弱性が攻撃者の標的になっているのです。

ひいてはVPNの安全性を疑問視する声も出てくる事態に…

IGP　5年リース　月額　24,000円（税別）
TM-BOX　5年リース　月額　18,000円（税別）

VPNは安全でない？

答えはYES&NO ― そもそも100%安全なソフトウェアはありません

VPN自体は、インターネット上に暗号化トンネルを構築して通信を行うという安全性の高い技術です。

しかしVPNに限らずソフトウェアに脆弱性は付きもの。残念ながら「100%瑕疵のない製品」は無いというのが現実です。

JPCERT/CC（https://www.jpcert.or.jp/）では日々多岐にわたるソフトウェアの脆弱性を公開し、いち早く対策を施すように注意喚起を行っています。


JVN Japan Vulnerability Notes

JVN 脆弱性レポートの読み方の更新について (2021-04-16)

新着リスト

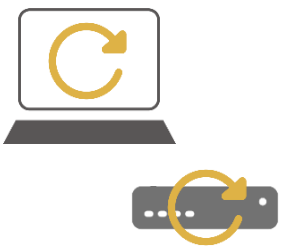
JVNVU#92160646:	Advantech 製 iView における複数の脆弱性 [2021/06/04 10:30]
JVN#64064138:	スマートフォンアプリ「ATOM - スマートライフ」におけるサーバ証明書の検証不備の脆弱性 [2021/06/03 12:00]
JVNVU#91051134:	Siemens 製品に対するアップデート (2021年5月) [2021/06/03 09:45]
JVNVU#94926489:	Hillrom 製 Welch Allyn medical device management tools に複数の脆弱性 [2021/06/02 13:30]
JVN#91691168:	スマートフォンアプリ「goo blog（gooブログ）」におけるアクセス制限不備の脆弱性 [2021/06/02 12:00]
JVN#98239374:	Zettlr におけるクロスサイトスクリプティングの脆弱性 [2021/06/02 10:00]
JVNVU#92862829:	バッファロー製ルータ WSR-1166DHP3 および WSR-1166DHP4 における複数の脆弱性 [2021/05/31 16:30]
JVNVU#93332929:	複数のトレンドマイクロ株式会社製品の脆弱性に対するアップデート (2021年5月) [2021/05/31 16:00]
JVNVU#90340376:	Dnsmasq における複数の脆弱性 (DNSpooq) [2021/05/28 18:20]
JVNVU#94613356:	GENIVI Alliance 製 dlt-daemon にヒープベースのバッファオーバーフローの脆弱性 [2021/05/28 14:30]
JVNVU#91343607:	Sensormatic Electronics 製 VideoEdge に境界条件の判定に関する脆弱性 [2021/05/28 14:30]
JVNVU#98845656:	MesaLabs 製 AmegaView における複数の脆弱性 [2021/05/28 14:30]
JVNVU#98060539:	三菱電機製 MELSEC iQ-R シリーズの MELSOFT 交信ポートにおけるリソース枯渇の脆弱性 [2021/05/28 13:10]
JVNVU#95111565:	ISC DHCP におけるバッファオーバーフローの脆弱性 [2021/05/28 10:00]
JVNVU#98263390:	Pulse Secure 製 Pulse Connect Secure にバッファオーバーフローの脆弱性 [2021/05/27 13:00]

脆弱性レポート一覧

ではどうすればよいのでしょうか？

【対策１】とにかく最新状態にアップデート！

Cringに狙われたFortinet社の脆弱性も、2019年の公開と同時に対策パッチが提供され、Fortinet社も繰り返し注意を呼びかけていたものでした。今回その対策を怠った機器が狙われたのです。
脆弱性とはつまり「弱点」なので、公開されたら早急に対処することが重要です。OS、アプリケーション、ネットワーク機器のファームウェアを常に最新状態にアップデートすることで、製品性能を十分に保つことができます。



【対策２】万が一に備えてデータをバックアップ

ランサムウェアによってPCがロックされたりデータが暗号化されると、たとえ身代金を払ってもデータを復元できるとは限りません。また昨今の攻撃は非常に巧妙化しており、多重に不正プログラムが仕掛けられている可能性も高く、安全性を考えるとPCは初期化せざるを得ません。
そうした事態に備え、業務データは日頃から定期的にバックアップを取っておくことが、業務への影響を最小限にするために重要です。

InformationGuard Plus でセキュリティ対策を

適切なファームウェアアップデート

重大な脆弱性が確認されたときは、UTM稼働中の機台はムラテックの管理ポータルから適切にファームウェアアップデートを実施し、機器の安全性を保ちます。

多層的なバックアップ機能

PCからストレージ、ストレージから外部HDDまたはクラウドへと、業務データを多層的にバックアップできる機能を標準搭載。万一の事態に備えて大切なデータを安全に守ります。

株式会社　一進堂　TEL048-464-3515