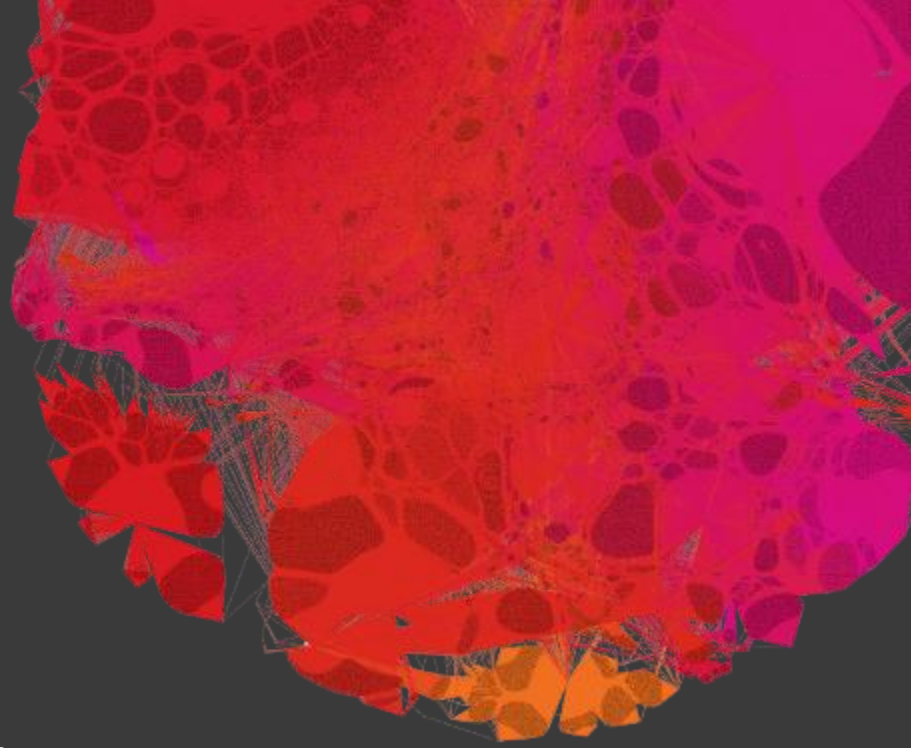
TREND MICRO | cybersecurity institute

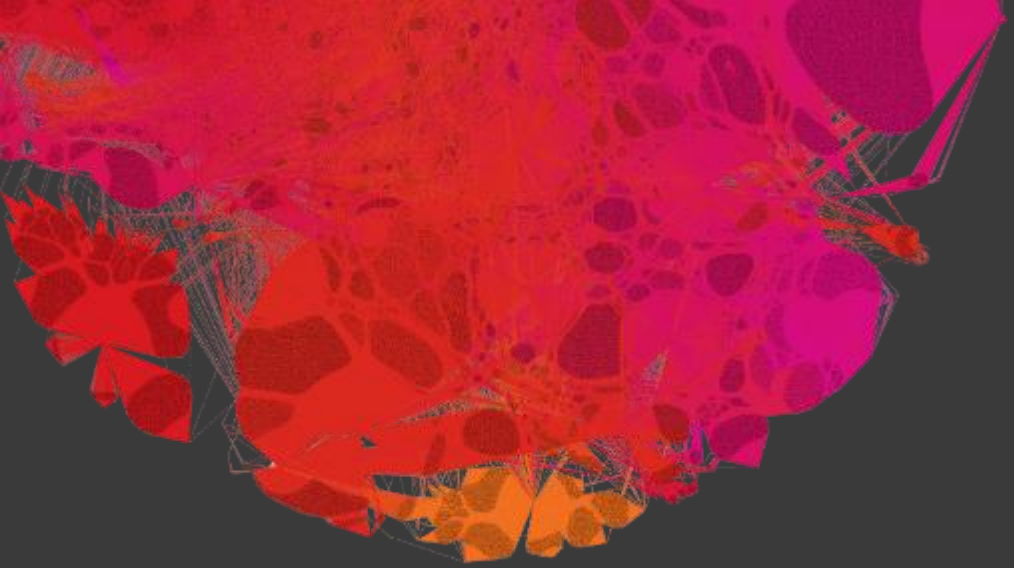


最新のサイバー関連情勢について

2022年3月15日
サイバーセキュリティ・イノベーション研究所
スレット・インテリジェンス・センター

目次

1. 最新の脅威動向
2. ランサムウェアの概要
3. まとめ



最新の脅威動向

サイバー空間脅威概況

ランサムウェア

- FBIから米企業に対し、USBによるランサムウェア攻撃についてアラートを通知
- VPN装置やリモートデスクトップを狙われ、内部へ侵入を許す傾向が多数

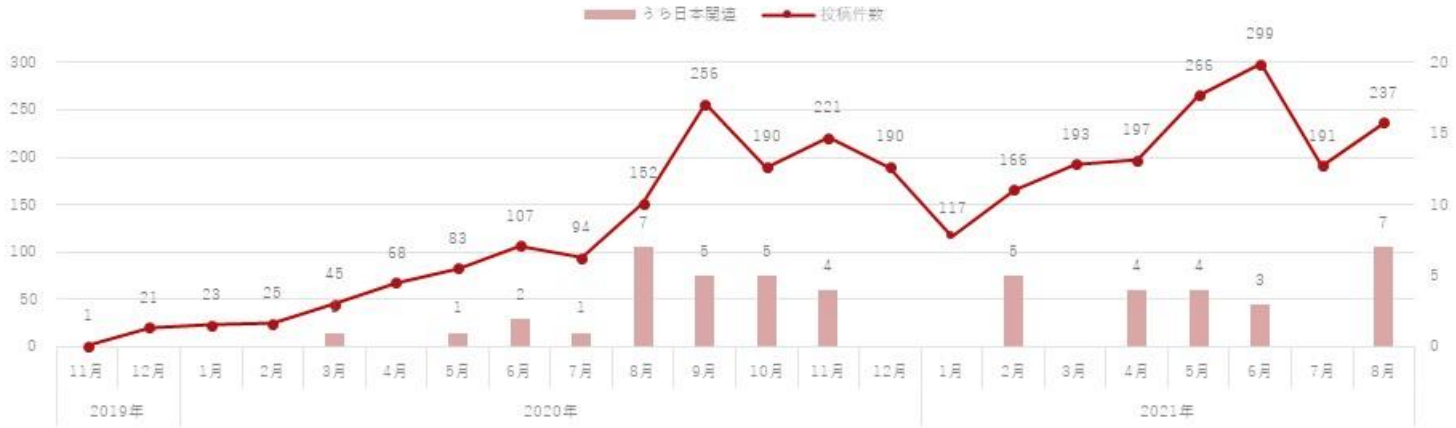
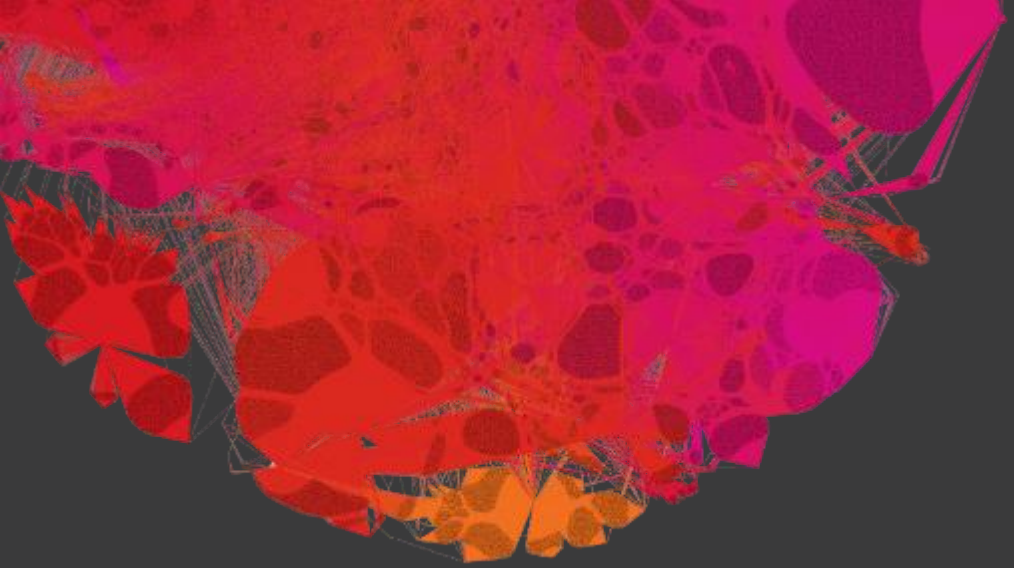


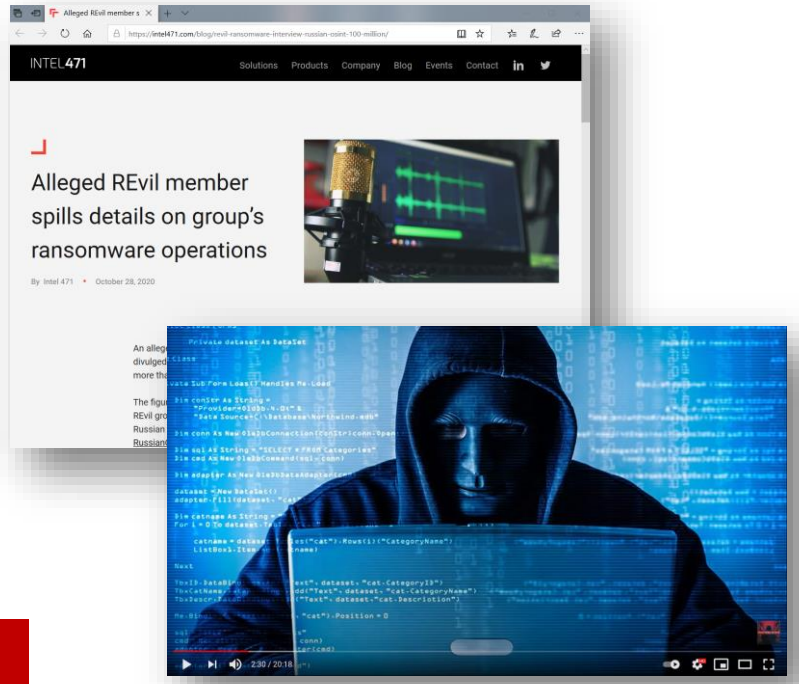
図 ランサムウェアの暴露サイト上に掲載された組織数の推移



ランサムウェア

ランサムウェア開発者へのインタビュー

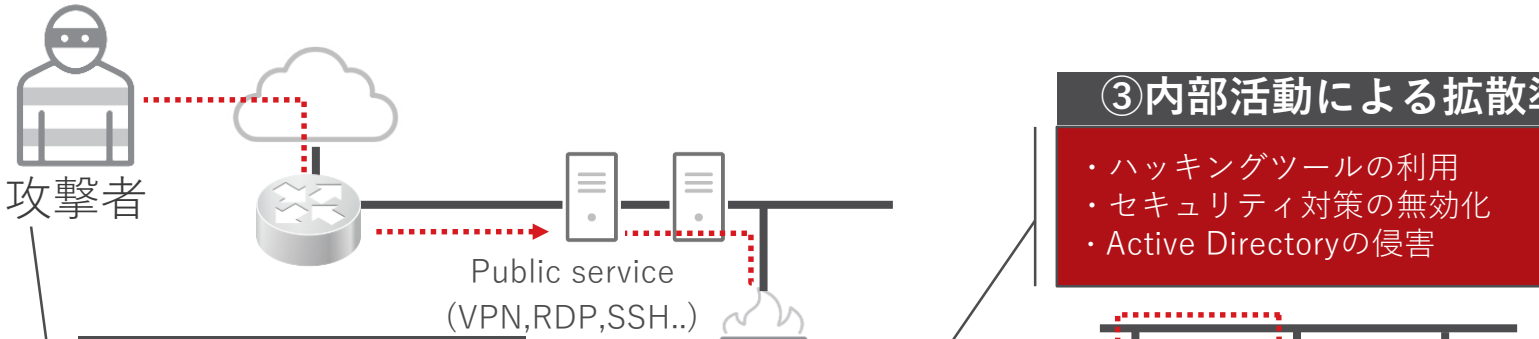
- Sodinokibi（別名：REvil）開発者へのインタビュー
  - ロシア語の話者
  - 年商は年間100億円以上
  - 被害企業の1/3が支払いに応じた
  - 外貨両替のトラベレックス社やテキサス州の行政機関にも攻撃を実施
  - 侵入方法はRDPが一般的
  - 3分で侵入できるケースもある



※真偽のほどは定かではないが、ランサムウェアが注目されているとは言える

出典:
https://intel471.com/blog/revil-ransomware-interview-russian-osint-100-million/
https://www.youtube.com/watch?v=ZyQCQ1VZp8s&feature=youtu.be

ランサムウェア攻撃の全体像



①ターゲット選定

・外部公開サービスのスキャン
-RDP, VPN, SSH 等
・応答から利用バージョン、脆弱性有無の判断

②侵入

・VPNサービス等の脆弱性
・安易なID,パスワード

③内部活動による拡散準備

・ハッキングツールの利用
・セキュリティ対策の無効化
・Active Directoryの侵害

④最終目的・ランサム感染

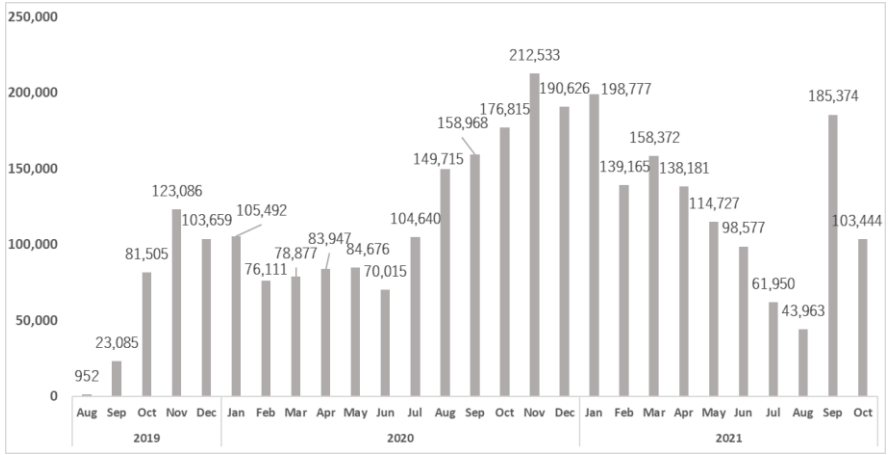
・遠隔実行
・GPO機能による配信・実行
・データ暗号化＋情報リーク

狙われる「外部との接点」：VPN

- 露出したサーバやVPNなどのネットワーク機器に対する遠隔攻撃
  - 脆弱性攻撃：VPN、Exchangeサーバ（CVE-2020-0688）
  - 認証の突破（漏えい情報の利用、アカウントリスト型/ブルートフォース攻撃）

公表時期	社名	CVE	CVSS v3
2019年4月	Pulse Secure ※	CVE-2019-11539	7.2(重要)
2019年4月	Pulse Secure ※	CVE-2019-11510	8.8(重要)
2019年5月	Fortinet ※	CVE-2018-13379	7.5(重要)
2019年7月	Palo Alto Networks ※	CVE-2019-1579	8.1(重要)
2020年1月	Citrix Systems ※	CVE-2019-19781	9.8(緊急)
2020年7月	F5 Networks ※	CVE-2020-5902	9.8(緊急)
2021年2月	SONICWALL	CVE-2021-20016	9.8(緊急)
2021年3月	F5 Networks ※	CVE-2021-22986	9.8(緊急)
2021年4月	Pulse Secure ※	CVE-2021-22893	10.0(緊急)
2021年8月	CISCO	CVE-2021-1609	9.8(緊急)
2021年8月	CISCO	CVE-2021-1610	7.2(重要)

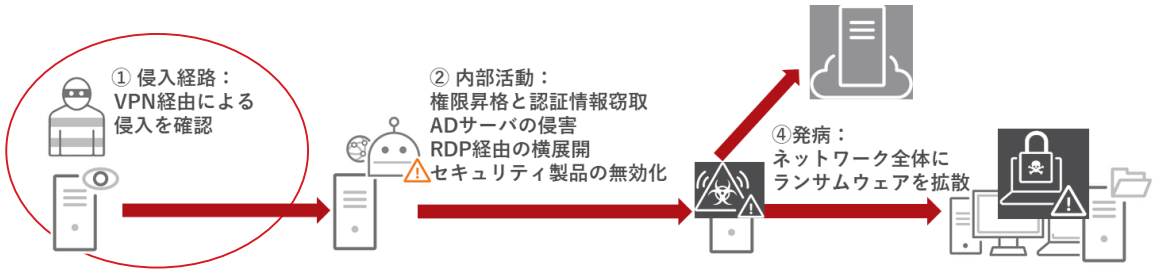
図：主なVPNの脆弱性一覧



グラフ：全世界における主なVPN脆弱性攻撃通信の検知数推移（左図　※を集計）

外部との接点を狙う攻撃：ランサムウェア

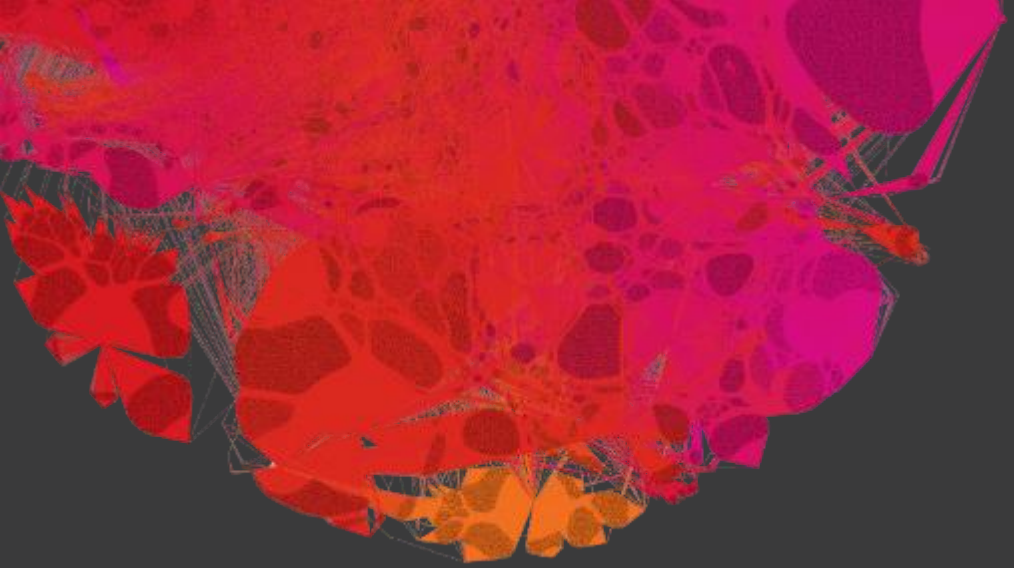
- ランサムウェア攻撃の侵入経路の中で、特にVPN経由が顕著化



図：「LockBit 2.0」の侵入方法

図：「LockBit 2.0」の感染画面例

2021年1~8月のインシデント対応の中で、特にVPN経由での侵入が確認されている「Cring」、「LOCKBIT」の被害が全体のおよそ7割



まとめ

被害に遭わないための対策

1. **セキュリティ対策製品を常に最新に保つ（運用の徹底）**
   - 不正メール、不正サイト、不正ファイル対策機能の利用
2. **脆弱性・設定不備対策**
   - ソフトウェアのバージョンアップ
   - IPS（不正侵入防止システム）などの仮想パッチの利用
   - クラウドサービスなどに対してCSPM（Cloud Security Posture Management）を利用してセキュリティの設定ミスや各種ガイドライン等への違反有無を確認
3. **侵入を前提とした対策**
   - ゼロトラストアーキテクチャ（NIST SP800-207）のアプローチ
   - 攻撃者が嫌がる環境づくりが重要
4. **重要ファイルのバックアップ**
5. **最新のサイバー犯罪・攻撃の手口を知る**
   - 例えば、Officeのマクロ機能を実行できないようにすることでEMOTETへの対策となる
     「警告を表示せずにすべてのマクロを無効にする」に設定することで「コンテンツの有効化」を表示させないことも有効