



暴露型ランサムウェアと弊社の対応

2020年6月24日

マクニカネットワークス株式会社

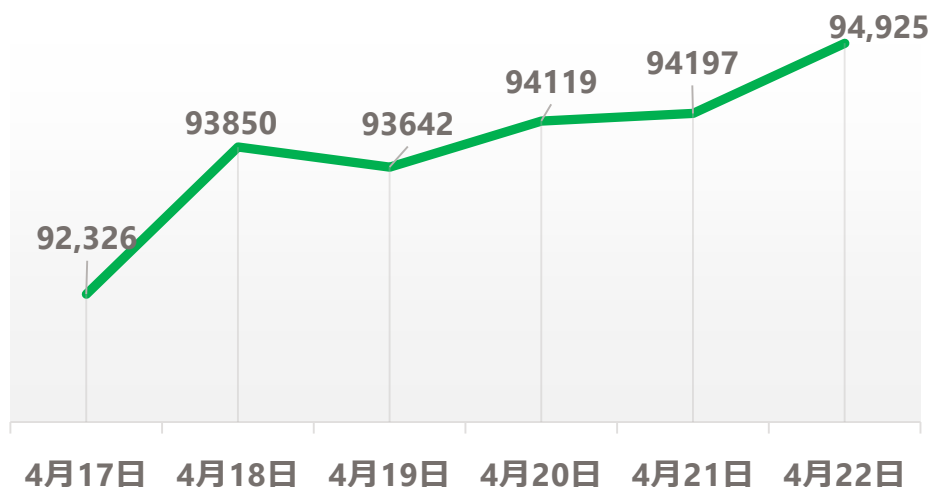
テレワークにおけるリスク観測

- ・ 攻撃されやすいポートが公開された国内のデバイスが増加傾向 *Shodanのデータを弊社集計
- ・ テレワークにより自宅環境で利用されるPCが増加したことが原因と推測

SMB (445/tcp) : ファイル共有サービス

44% 増 65,809 $\rightarrow$ 94,925
2020/3/11 2020/4/22

4月下旬の傾向



SMB関連の脆弱性 :
CVE-2020-0796 (SMBv3の脆弱性)
CVE-2017-0144 (Wannacryでも悪用されたSMBv1の脆弱性)

RDP (3389/tcp) : リモートデスクトップサービス

50% 増 71,531 $\rightarrow$ 107,637
2019/6/18 2020/4/22

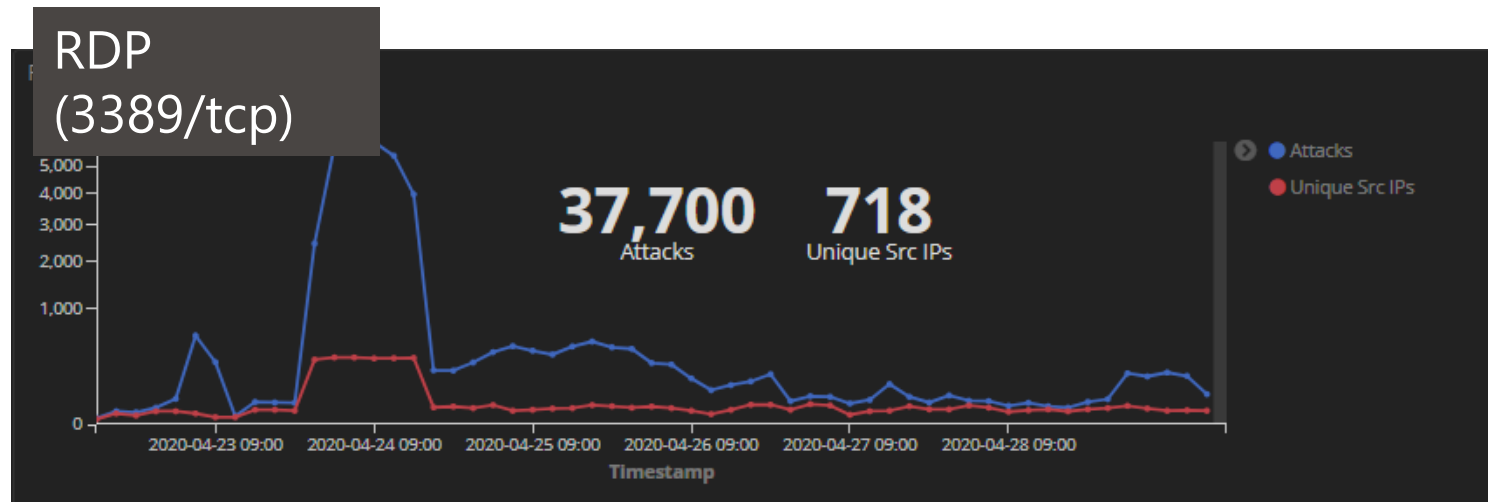
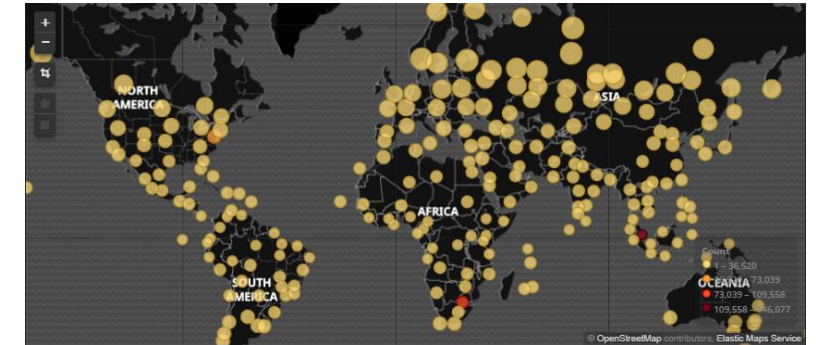
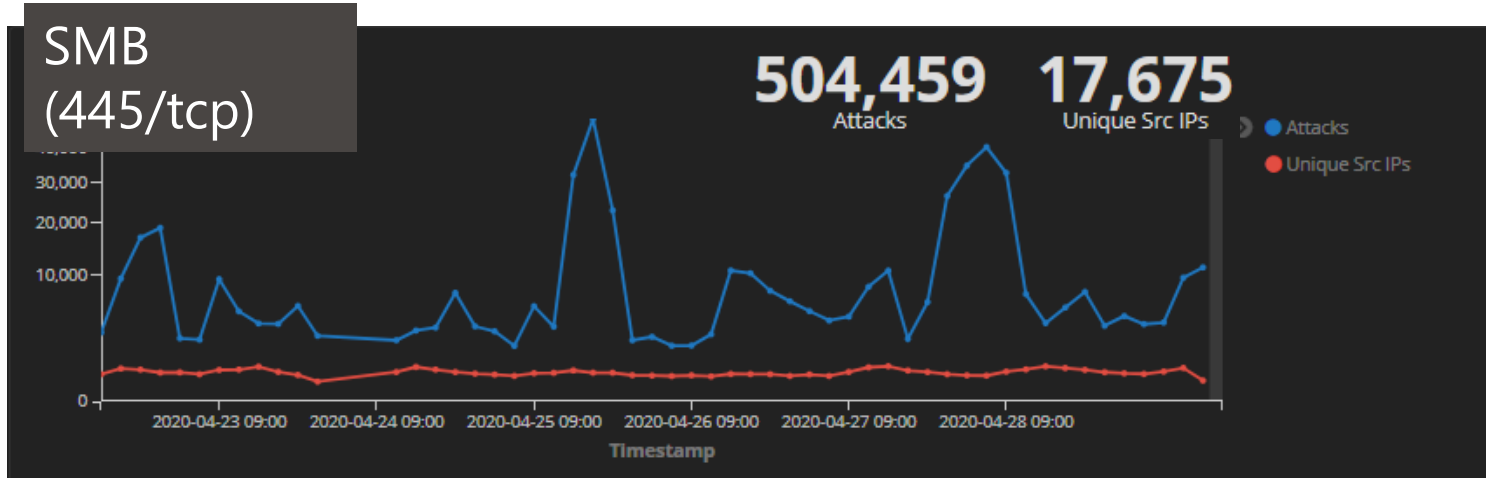
4月下旬の傾向



RDP関連の脆弱性 :
CVE-2019-0708 (BlueKeep)
CVE-2019-1181/CVE-2019-1182 (DejaBlue)

SMBやRDPに対する攻撃数の統計（弊社設置のハニーポットから）

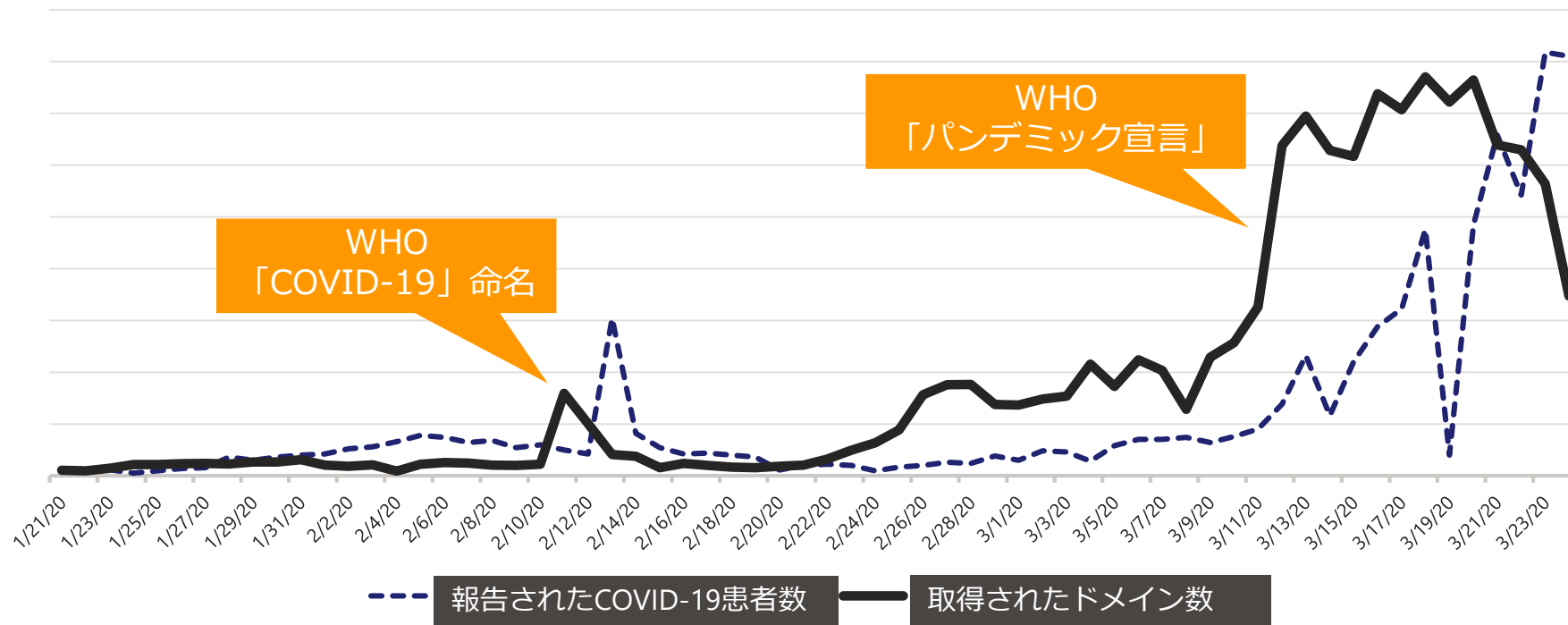
■ 4月22日15:00 ～ 4月29日15:00 1週間分のデータ



SMB/RDPなどのハイリスクポートへの攻撃が実際に発生している。

不審なWebサイトへのアクセスリスク増加について

- 新型コロナウイルスの情報を餌に不正サイトへ誘導する試みが増加していると推測
- covid/corona/c0vidなどを含む疑わしいドメインの取得数が増加傾向



*以下サイトデータを弊社集計

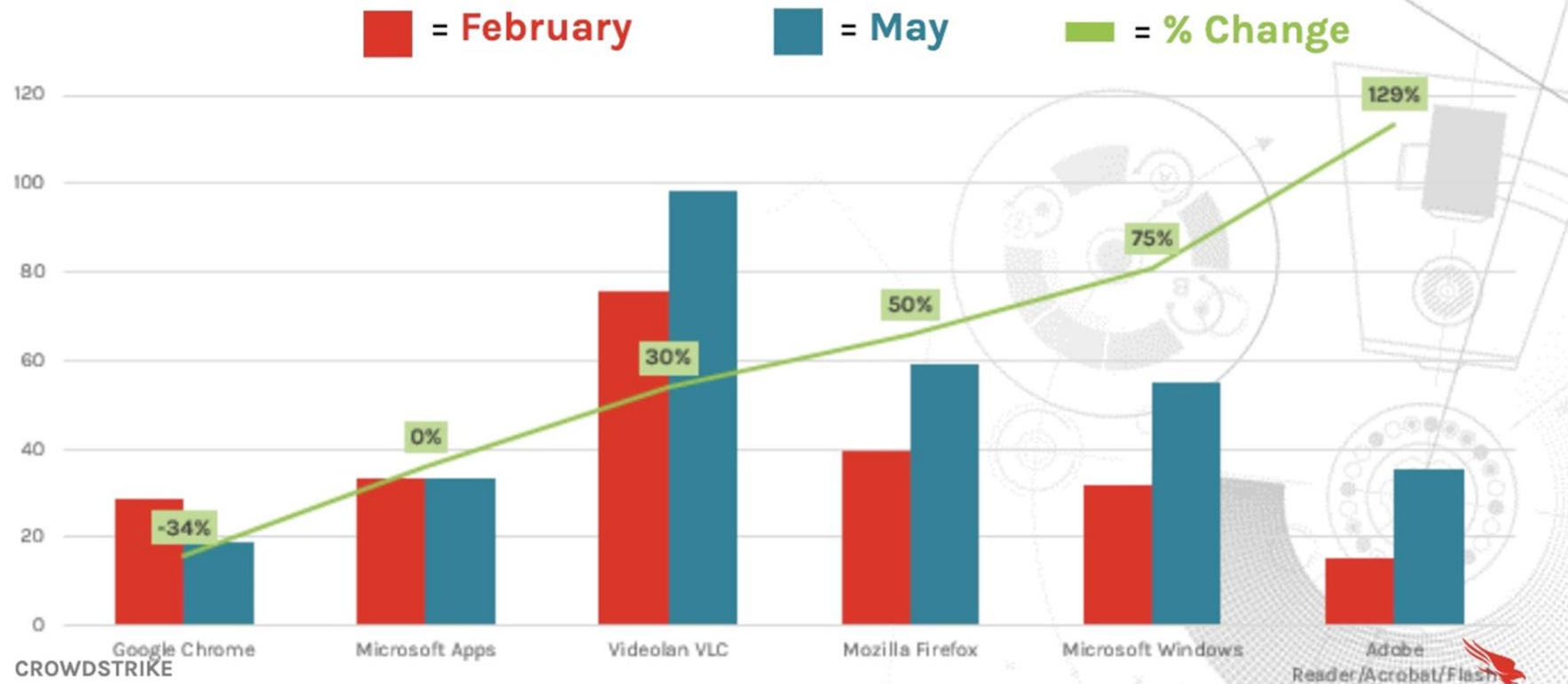
参考: <https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats>

参考: <https://experience.arcgis.com/experience/685d0ace521648f8a5beeeee1b9125cd>

テレワーク中の端末へのパッチ配信の遅延が顕著



WORKSTATION VULNERABILITIES ARE TAKING ABOUT 40% LONGER TO PATCH



Crowd Strike社“Global Vulnerability Management Trends”より抜粋

暴露型ランサムウェア

従来のランサムウェアと暴露型ランサムウェアの違い

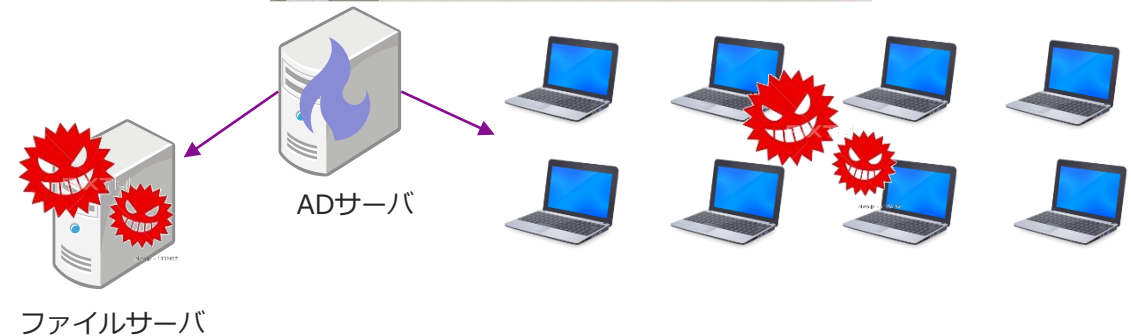
従来のランサムウェア



WannaCryなど

対象：主にクライアントPC、各種サーバ
事象：クライアントPC、サーバの暗号化
及び自己拡散
目的：暗号化解除のために身代金要求
業務復旧のための身代金要求
要求額：数万円程度

暴露型ランサムウェア



REvil/Sodinokibi, Ryuk,など

対象：ファイルサーバ、クライアントPC
事象：ファイルサーバ、クライアントPCが暗号化
及び内部の情報搾取
目的：暗号化解除のために身代金要求
搾取情報の公開を止めるための身代金要求
要求額：数百万円程度～

----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion [REDACTED]
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.

To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.

If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!

- a) Download and install TOR browser from this site: [https://\[REDACTED\]](https://[REDACTED])
- b) Open our website: [http://\[REDACTED\]](http://[REDACTED])

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:

- a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
- b) Open our secondary website: [http://\[REDACTED\]](http://[REDACTED])

Warning: secondary website can be blocked, thats why first variant much better and more available.

実際に搾取された情報が裏オークションに掛けられた例

The image shows a screenshot of a dark web auction site. The browser address bar displays a .onion URL. The page title is "Happy Blog Auction (new)". The main content area shows a listing for stolen data from a company, with redacted names and URLs. A callout bubble points to the listing, stating that the company's files, accounting documents, client databases, and login data were leaked. Another callout bubble points to the auction details, indicating that the stolen files are being sold as proof of a successful attack, totaling 747.3 GB. A third callout bubble points to the auction start price and time left, showing a minimum deposit of \$50,000, a start price of \$500,000, and a time left of 22 hours, 51 minutes, and 44 seconds. A fourth callout bubble points to a list of files at the bottom of the page, including XLSX files and Opera web documents. A fifth callout bubble points to a screenshot of a company's website, indicating that the stolen information is being displayed there.

攻撃に成功した会社が次々に公開されている

盗み出した情報の画面キャプチャ

盗み出したファイル類を一部「攻撃に成功した証拠」として公開（全体では747.3GB）

\$500,000 からオークション開始
公開まで残り時間22時間

Company files, accounting and working documents of clients, databases. Data for logging into client banks. Audit results of companies.

28, 2019

Scotia Connect – New Sign In Procedures
[https://\[redacted\]](https://[redacted])

User: Andrea Roth

Click to view a

Happy Blog Auction (new)

Blog search Search

[www.\[redacted\]](https://[redacted])

[redacted] inc. is [redacted] headquartered in [redacted] United States. Founded in 2000, the company currently [redacted] with nearly [redacted]

The total data is 747.3 GB

Financial statements, tax

Also confidential informat

Details will be provided to the buyer

Part of the data for public viewing:

[https://\[redacted\]](https://[redacted])

[https://\[redacted\]](https://[redacted])

[https://\[redacted\]](https://[redacted])

[https://\[redacted\]](https://[redacted])

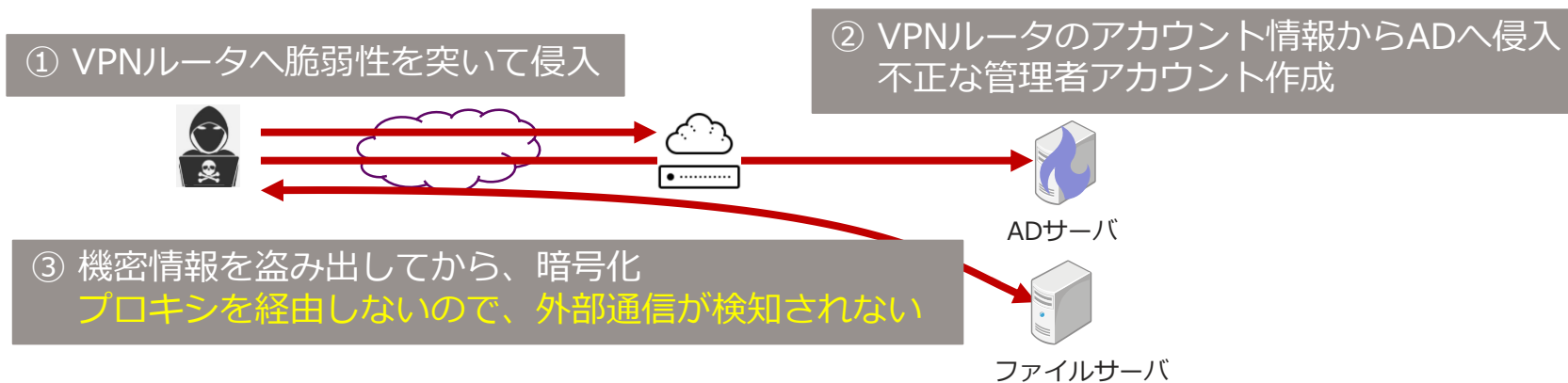
Minimum deposit: \$50,000 Top bid: --

Start price: \$500,000 Current price: \$1,500,000

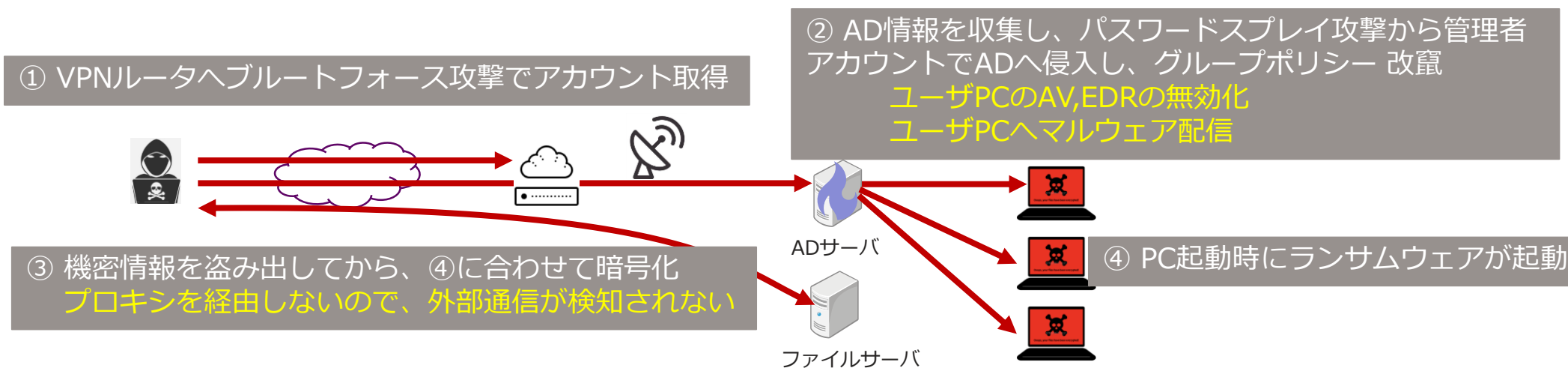
Opened Time left: 22 hours, 51 minutes and 44 seconds

9,916	7,243	XLSX File	5/7/2020 4:45 ...	C56CFD6A
924,389	902,829	XLSX File	1/30/2019 11:3...	S2DA66D1
3,374,276	2,903,027	Opera Web Docu...	1/22/2019 6:56 ...	3081B234
395,264	77,848	XLS File	1/24/2019 12:1...	99F208E3
331,897	313,921	Opera Web Docu...	10/30/2017 5:4...	2FEEC590
2,556,664	2,145,840	XLSX File	0/6/2010 6:17	BE01ABD3

被害例 1) VPNルータの脆弱性から侵入され、ADサーバが乗っ取られファイルサーバが暗号化

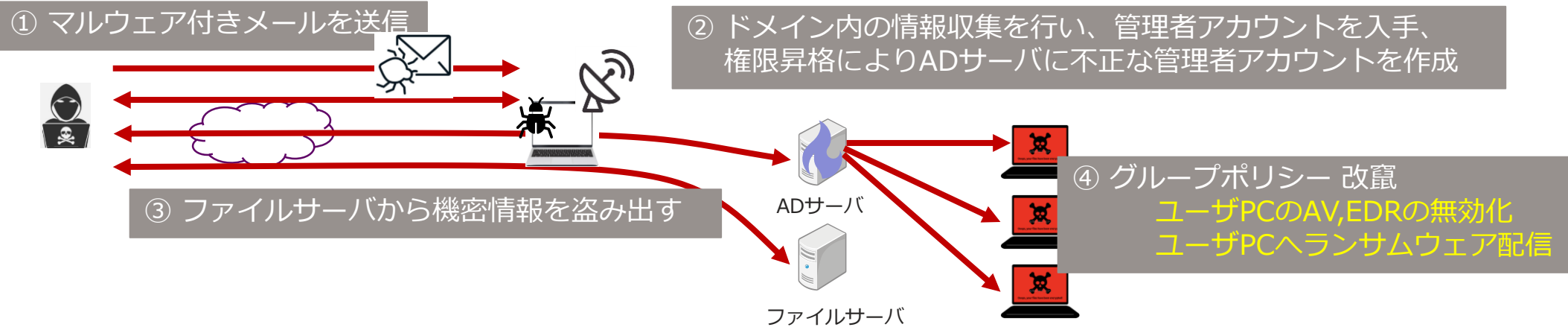


被害例 2) VPNルータのアカウントから侵入され、ADサーバが乗っ取られユーザPCが暗号化

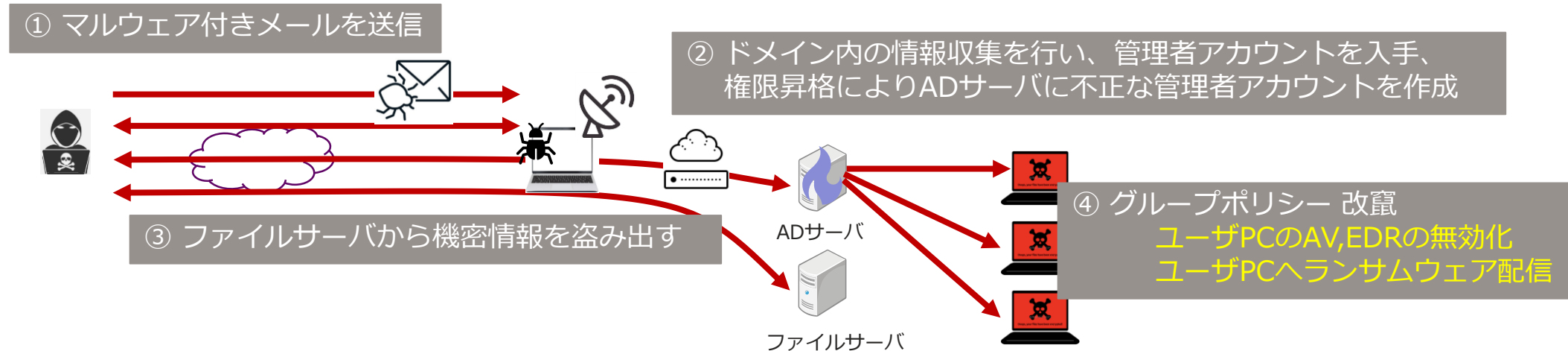


暴露型ランサムウェアの手口と被害②

被害例 3) メール添付ファイルから侵入、ADサーバが乗っ取られユーザPCが暗号化



被害例 4) メール添付ファイルから侵入、ADサーバが制圧乗っ取られユーザPCが暗号化 (VPN経由※)

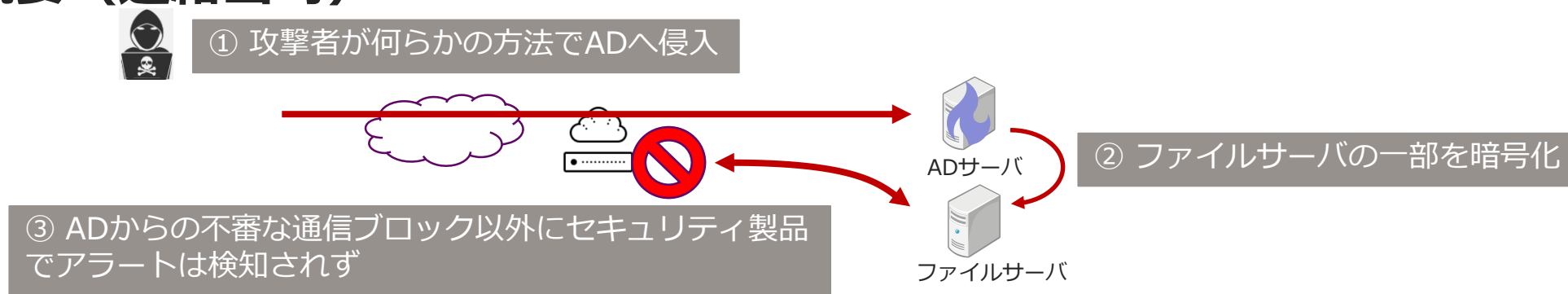


※ VPN経由でユーザが利用中に感染して直接インターネット通信する場合には、外部通信で検知できない

暴露型ランサムウェアに対する弊社の対応

■ X社の事案

■ 被害概要（連絡当時）



- サーバ群、リモートアクセス端末から社内NWを経由した通信において、セキュリティ機器での不審な通信ブロックは事象発生前後の時間帯でAD以外に確認できず
- X社では調査用にADのイメージを取得し、その後バックアップイメージからADを事案前の状態に復元済み
- 暗号化されたファイル内容の特定とバックアップからの復元を計画中

■ X社からの依頼事項

- ADサーバ、ファイルサーバのフォレンジックによる被害範囲の詳細調査
- サーバの復旧やテレワークによる事業再開に向けた支援

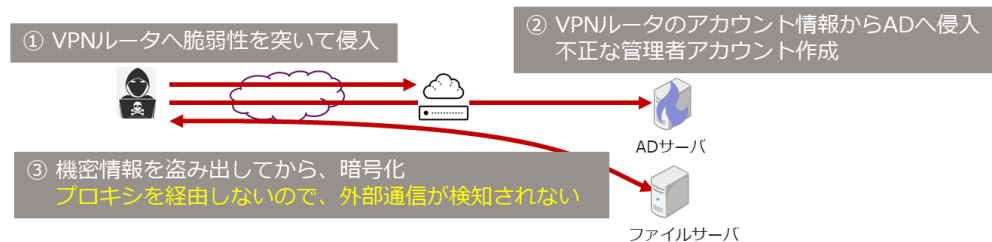
▶ 弊社からの調査提案内容

- ▶ ランサムウェア特定のため、脅迫文の提供
- ▶ 攻撃者の侵入経路、事象の再発を考慮したADイベントログとVPNログ、Proxyログ等のセキュリティ製品以外のログ調査

▶ 調査の結果、X社が認識していなかった被害

- ▶ VPNの脆弱性パッチが適用されておらず、VPN経由でADへ侵入し、暗号化対象と推測されるデータのアップロードをVPN経由で実施
- ▶ REvilランサムウェア実行の数ヶ月前にも偵察のためか、侵入した痕跡も発見（同攻撃者かは不明）

被害例 1) VPNルータの脆弱性から侵入され、ADサーバが乗っ取られファイルサーバが暗号化



2次被害や再発を防ぐため、VPNパッチ適用、アカウントリセット、プレスリリース準備など攻撃に対する適切な調査と対処が必要。

サービス項目	サービス詳細	費用	コメント
ActiveDirectory脅威診断 スポットサービス	ActiveDirectoryに対する脅威を分析してレポートします。	有償	2020年6月24日～9月30日の間、 無償で実施（法人様向け）
ActiveDirectoryにおける脅威 月次レポートサービス	ActiveDirectoryに対する脅威を継続分析し、 月次レポートとして提供します。	有償	
ActiveDirectory監視サービス	ActiveDirectoryへの攻撃を継続的に監視するだけでなく、不審な挙動が検出された場合はリモートから対処を実施します。 ・不審なアカウントの無効化 ・追加で調査に必要な情報の収集	有償	

このような事案がありましたら、ぜひご一報ください。

お問合せ

貴社のお役に立てるような
ご提案活動をさせて頂く所存です。

ご依頼等ございましたら、何なりとお申し付けください。
今後ともよろしくお願い申し上げます。

【 お問い合わせ先 】

マクニカネットワークス株式会社

第2営業統括部第2営業部

S&J製品担当

Tel: 045-476-2010

Email: sec-service@cs.macnica.net

URL: <https://www.macnica.net/sandj/>

- 本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。