Blue Planet-works
Safety for the Connected World

サイバーセキュリティの裏側から

2022

Issued by Blue Planet-works

Date Issued
2022.08.17

About Us

革新的な『AppGuard』テクノロジ・プラットフォームをベースとした サイバーセキュリティ製品及びサービスを提供する 日本発のグローバル・サイバーセキュリティ・カンパニー

Blue Planet-works は、2017 年 4 月に日本で設立されました。米国政府機関向けに開発された『AppGuard』と呼ばれていたセキュリティ技術とその事業を買収し、国内外のパートナー企業と共に AppGuard の製品・サービス化に向け開発を進めてまいりました。

サイバー攻撃の手法や攻撃者のプロファイルはここ数年で大きく変化し、より巧妙で組織化されたものとなりました。その攻撃者に対抗するため、「多層防御」として多くのソリューションが開発されてきましたが、その防御の手法は当時から大きく進化していません。AppGuard は、攻撃者とのいたちごっこに終止符を打つべく、従来採用され続けてきた「検知」という手法とは一線を画したゼロトラストの発想のもと開発されました。AppGuard は攻撃そのものを防止し、無効化するセキュリティソフト。独自の特許技術によりシステムに害を与える行為を阻止します。

AppGuard は 2017 年より日本・アメリカをはじめ世界で展開をスタートし、2022 年 6 月末には累計導入企業数が 14,000 社に達する勢いです。中小企業からは彼らが直面する IT セキュリティ運用の煩雑さ及びコスト高に対する効果的なソリューションとして評価をいただき、大企業からは EDR 等を始めとする他のセキュリティ製品との併用によるゼロトラストの構築に大きく貢献するとして高い評価をいただいております。

Contents.

本レポートで報告する指標は、
2021年1月から2022年5月の期間にストーンビートセキュリティ社が行った調査、及び
2021年7月から2022年6月の期間にITガード社が行った調査に基づいています。

01.

はじめに

01. はじめに

新型コロナウイルス（COVID-19）の世界的流行が続く中、我々は新しい生活様式を実践して感染予防と経済活動の両立を図ることが求められています。組織の働き方も半ば強制的ではあるものの変化が生じたことで、IT 化の進展やデジタルトランスフォーメーションを推進する一助となっています。

これらの変化により新たに顕在化してきた様々なリスクがあり、サイバーセキュリティの領域においてもその影響は無視できないものとなっています。今日、国内におけるサイバー犯罪の被害は目に見えて増加しており、もはや対岸の火事とは言えません。日本では特に「Emotet（エモテット）」や「ランサムウェア」による被害が顕著であり、サイバー攻撃によるインシデントが組織にとって甚大な影響をもたらすということを多くの人が認知するところとなりました。

IT化の進展やデジタルトランスフォーメーションの推進は新しい価値を創造して次なるビジネスチャンスにつなげていく一方で組織のシステム依存度を高めることにもなります。その様な状況下で生じるインシデントは、自組織に留まらずサプライチェーン全体にまで波及し、これまで以上に深刻な問題をもたらすリスクを内包しています。前例のない状況に置かれているからこそ、我々は大切なモノを守るためにさらなる努力をしなければなりません。

「サイバーセキュリティの裏側から 2022」は、株式会社 Blue Planet-works が取りまとめたサイバーセキュリティに関するレポートです。ゼロトラスト型エンドポイントセキュリティ「AppGuard」を利用するユーザーの利用実態を調査すると共に、日本国内で観察された最新のサイバー攻撃の動向を株式会社 IT ガード、ストーンビートセキュリティ株式会社の協力の下で取りまとめています。

本レポートは「AppGuard」を利用していただいているユーザーに限らず、以下に挙げる事項を目的としてサイバーセキュリティに関心を持つ全ての方々へ共助の観点から有益な情報を発信していくことを目指しています。

1) 日本国内で発生しているサイバー攻撃被害の実録とその教訓を提供し、同様の被害に遭わないように対策の一助としてもらう。
2) ゼロトラスト製品提供元のセキュリティアドバイザーが日々観測しているサイバーセキュリティの脅威動向を共有することで起こりうる未来をイメージしてもらう。
3) 自社製品の実運用データの分析結果から、ゼロトラスト製品の実力と効果を知ってもらう。

02.

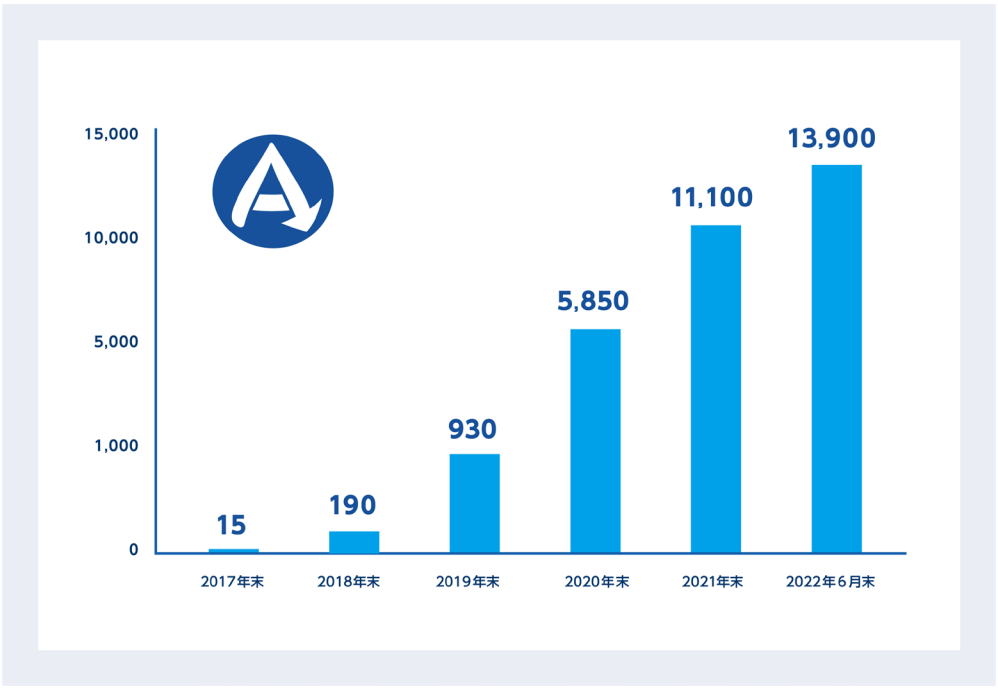
AppGuard利用実態調査

02. AppGuard 利用実態調査

本項では2022年6月末時点における「AppGuard」の利用実態調査の結果を報告します。

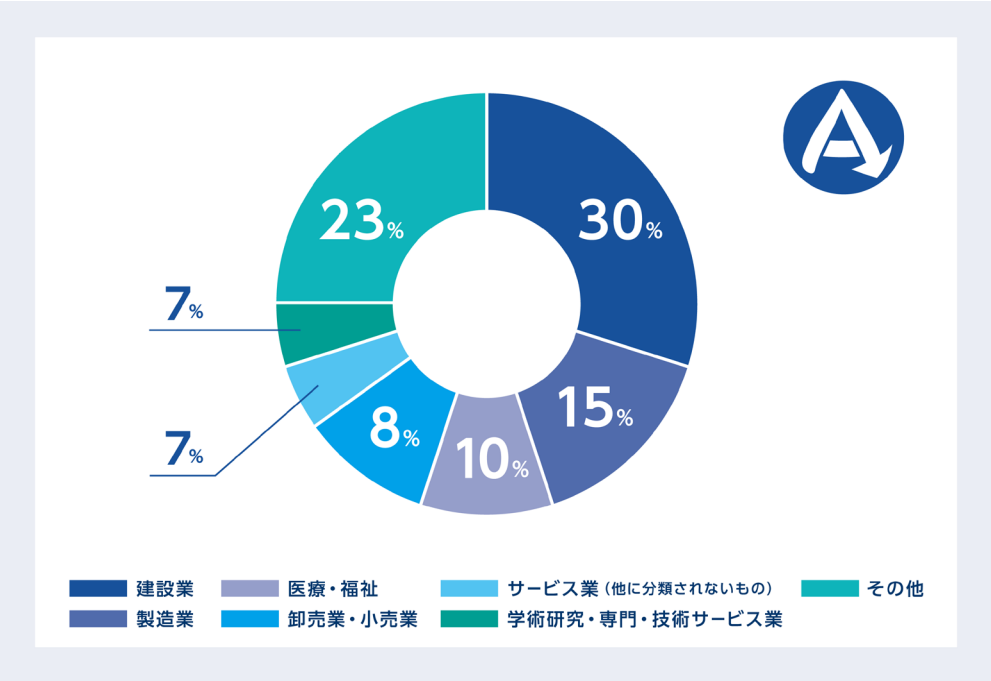
1 累積導入社数とユーザー属性

下図に示されるとおり、2022 年6月末時点で国内累積導入企業数は 14,000 社に届くところまで来ました。国内では 2019 年頃からマルウェア「Emotet」による被害が拡大を始め、さらにはランサムウェアによる国内企業の被害が目立ってきたことからユーザーの多くがセキュリティ対策の見直しを求められたことがAppGuard の成長要因の 1 つになったことが推察されます。



図：AppGuard国内累積導入企業数の推移

業種別で AppGuard を利用するユーザー属性を分類すると、建設業が最も多い結果となりました。本調査で用いた統計データから読み解くと、建設業に分類されるユーザー数が増加傾向にあるタイミングが「Emotet」の活動期間と重なる部分があるため、「Emotet」に感染してしまったことで、その再発防止策として AppGuard が選ばれたのではないかと推察しています。2020 年頃から AppGuard は「Emotet」が用いる攻撃手法であれば 100% 発症を阻止することが可能であることを謳っていたこともあり、多くの被害者の注目を集めることができたのではないでしょうか。なお、「Emotet」への効果としては 2022 年 6 月末時点においても変わっていません。



図：ユーザー属性の業種別割合

2 追加された「信頼された発行元」の傾向分析

AppGuard は起動前制御として「スペースルール」という制御機能を使用します。「スペースルール」は端末内のフォルダ群を 2 つの領域に区分けして監視と制御を行います。管理者権限がなければ変更処理ができないシステムフォルダ等を「システムスペース」に分類し、それ以外のフォルダ（主にユーザープロファイル配下）を「ユーザースペース」に分類しています。前者に対しては配備された実行ファイルに対して起動制御を行わない代わりに外部から攻撃者が悪用する可能性があるアプリケーション（ハイリスクアプリケーション）を通じた書き込みが禁止されます。後者は自由に書き込みができる代わりに配備された実行ファイルに対して起動制御が行われます。起動制御が有効な領域から実行ファイルを起動させる場合、AppGuard のポリシーに登録された「信頼された発行元」のデジタル署名と一致したものを当該実行ファイルが保持しているかどうかで可否が判断されます。

本調査では AppGuard を利用するユーザーが「信頼された発行元」にどのようなデジタル署名を登録しているのかを分析し、そこからどのようなビジネスアプリケーションを利用しているのかを推察しています。なお、本調査においては株式会社 IT ガードから提供された 1200 のサンプルデータ（集計期間：2021 年 7 月 1 日～2022 年 6 月 30 日）を基に調査を行っています。このサンプルデータは契約社数ではなくグループ数（1 社の契約テナントに複数のグループが登録される場合がある）に基づいて集計されています。また、本調査は AppGuard のポリシーに登録されたデジタル署名の統計を取っているだけであり、ユーザーがどのような意図で登録したのか又はそのデジタル署名に関連するアプリケーションを実際に利用しているのかは調査の範囲外としています。

① オンライン会議 / ビジネスチャットツール

COVID-19 の影響もあり、多くの組織が在宅勤務やリモートワークを余儀なくされることとなり、直接対面せずともコミュニケーションが可能となるオンライン会議 / ビジネスチャットツールが使用されるようになりました。AppGuard を利用しているユーザーにおいても、その傾向を確認することができます。オンライン会議ツールは組織によって使用するツールが異なるため、相手先のオンライン会議ツールも利用できるようにするために複数のオンライン会議ツールに関連するデジタル署名を登録していると推察されます。

登録された署名	対象アプリケーション	署名登録率
Microsoft Corporation	Teams	100%
Google LLC	Google Meet	73%
Zoom Video Communications, Inc.	Zoom	67%
Cisco WebEx LLC	Cisco WebEx	63%
LINE Corporation	LINE	55%
Slack Technologies, Inc.	Slack	54%
Works Mobile Corporation	LINE Works	52%
LogMeIn, Inc.	Go To Meeting	51%
Polycom, Inc.	Polyビデオ会議	47%
V-cube, Inc.	V-Cubeミーティング	47%

※マイクロソフト社の署名は初期ポリシーで登録されているため登録率は100%となる。

② クラウドストレージサービス

在宅勤務やリモートワークをするユーザーが増えたことで、業務で利用するデータをより効率的に取り扱うためのクラウドストレージサービスが活用される機会が増えています。特に大容量のファイルや機密性の高いファイルをやり取りする場合、メールに授受はセキュリティ上の観点から不向きであるため、細かなアクセス制御や授受の証跡を残せるクラウドストレージサービスは重宝されています。

登録された署名	対象アプリケーション	署名登録率
Microsoft Corporation	One Drive	100%
Google LLC	Google Drive	73%
Dropbox, Inc	Dropbox	56%
Box, Inc.	Box	49%

※マイクロソフト社の署名は初期ポリシーで登録されているため登録率は100%となる。

③ 資産管理ツール

誰もが当たり前の様に利用するアプリケーションではありませんが、組織内の IT 資産やユーザーの行動を把握する目的で導入が進んでいるツールの 1 つです。セキュリティ対策において可視性を高めることは重要であり、今後もこの分野のツールはより一般的に利用されるツールになってくると考えられます。

登録された署名	対象アプリケーション	署名登録率
Sky Co., LTD.	SKYSEA Client View	49%
Intercom, Inc.	MaLion	48%
Motex Inc.	LANSCOPE	48%
HAMMOCK CORPORATION	AssetView	7%

④ エンドポイントセキュリティツール

AppGuard はその性質上、他のエンドポイントセキュリティツールと併用して利用することができます。ユーザーの中にはこれまで利用していたアンチウイルスソフト等を残したまま AppGuard を導入することもあります。また、Adobe Acrobat Reader DC にバンドルされている McAfee のツールや Chrome で利用される ESET のコンポーネント等、エンドポイントセキュリティツールとしては利用していないものの他用途で使用されている関係でデジタル署名は登録されているというケースもあります。

登録された署名	対象アプリケーション	署名登録率
Microsoft Corporation	-	100%
Trend Micro, Inc.	-	50%
Symantec Corporation	-	47%
Cybereason Inc	-	47%
McAfee, Inc.	-	47%
ESET, spol. s r.o.	-	46%
Sophos Limited	-	46%
F-Secure Corporation	-	45%
Kaspersky Lab	-	43%
BROMIUM, INC.	-	7%
AVG TECHNOLOGIES USA, LLC	-	7%

※マイクロソフト社の署名は初期ポリシーで登録されているため登録率は100%となる。

3 ブロックログに基づく阻止された脅威の傾向分析

本調査では AppGuard の「スペースルール」によって起動制御された悪質な実行ファイルの情報から AppGuard 利用ユーザーがどのような脅威に遭遇しているのかを調査しています。なお、本調査においては株式会社 IT ガードから提供された 1129 件のサンプルデータ(集計期間:2021 年 7 月 1 日～2022 年 6 月 30 日)を基に調査を行っています。脅威判定は Google 社が提供する VirusTotal にて AppGuard が出力したファイルハッシュ値を照会しています。

脅威種別	脅威概要	割合
Trojan	マルウェアの一分類であり、主に侵入した端末内に潜伏して悪意ある機能を多数駆使して攻撃者の目的を達成させる悪意あるプログラムを指す。	43%
Malicious	ユーザーにとって不正かつ有害な結果を引き起こすことを目的として作成された悪意あるプログラム (マルウェア) を指す。	39%
Adware	ユーザーにとって不必要な広告を表示又は誘導することで広告収入を得ている迷惑なプログラムを指す。	4%
Downloader	マルウェアを内部に持ち、侵入した端末内で外部との通信を行わずに展開することができる仕組みを実装したプログラムを指す。	4%
Dropper	マルウェアを内部に持ち、侵入した端末内で外部との通信を行わずに展開することができる仕組みを実装したプログラムを指す。	4%
PUP	Potentially Unwanted Programの略で潜在的に悪意ある動きをするプログラムを指す。マルウェアほどの悪質性はないが、健全なものではない。	4%
Emotet	マルウェア「Emotet」のペイロード (Emotetを生成するために実行されるプログラム) を指す。	1%

Virus Total とは
Google 社が運営している Web 上で利用できる無償サービスです。
検査したいファイルをアップロードしたり、ハッシュ値を入力することで、世界中の主要なウイルス対策製品を使用して各製品の検知状況を確認することが出来ます。

https://www.virustotal.com/

世間では「Emotet」の脅威が注視されていますが、実態としてはそれ以外の脅威も数多くユーザーに着弾していることがわかりました。しかし、最終的に発症させたい脅威は異なっていても、それらを発症させるための攻撃手法はいくつかのパターンに分類できます。AppGuard によって阻止された攻撃の中から具体的な攻撃手順と AppGuard が阻止するポイントをいくつか図示します。

1) Emotet (MS Office のマクロ悪用)

この攻撃手法は「Emotet」が利用する最も基本的なものです。MS Excel を悪用した脅威サンプルでは非表示設定になったシートの各セル内に悪質な構文が分割して配置されており、マクロを有効化することでこれらが連結されて 1 つの構文として機能するようになっています。AppGuard は連結された構文を通じて呼び込まれる「Emotet」のペイロードの起動を制御するため発症させることなく攻撃を阻止します。

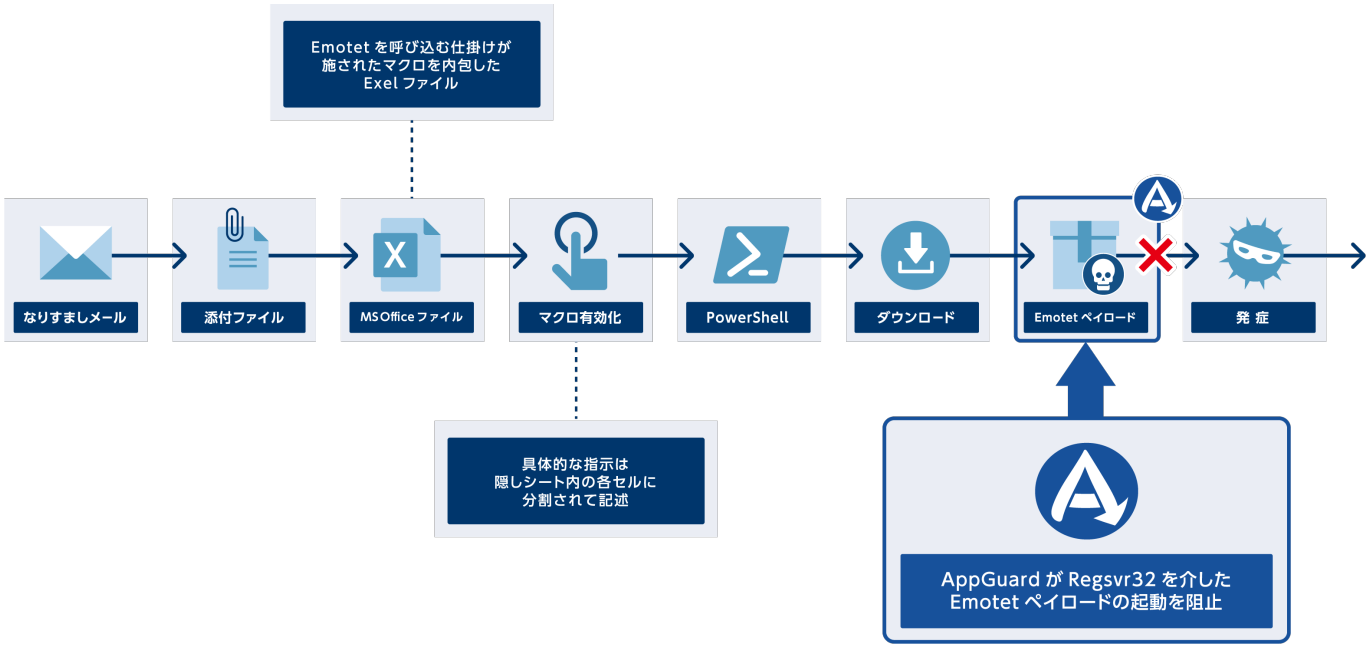


図　Emotet（MS Officeのマクロ悪用）を阻止するポイント

2) Emotet（ショートカットファイルの実行パス悪用）

この攻撃手法は「Emotet」が新たに採用した手口です。MS Office ファイル等のアイコンに偽装したショートカットファイル（.lnk）に設定された実行パスにはコマンドプロンプトを呼び出して特定のコマンドを実行するための構文が埋め込まれています。誤ってこのショートカットファイルを起動すると永続化を目的としたレジストリファイルの改ざんと「Emotet」のペイロードがダウンロードされます。AppGuard はコマンドプロンプトをハイリスクアプリケーション（攻撃者が悪用する可能性があるアプリケーション）として扱うため、レジストリの変更処理を認めず永続化を阻止します。また、ダウンロードされた「Emotet」のペイロードは起動が制御されるため発症させることなく攻撃を阻止します。

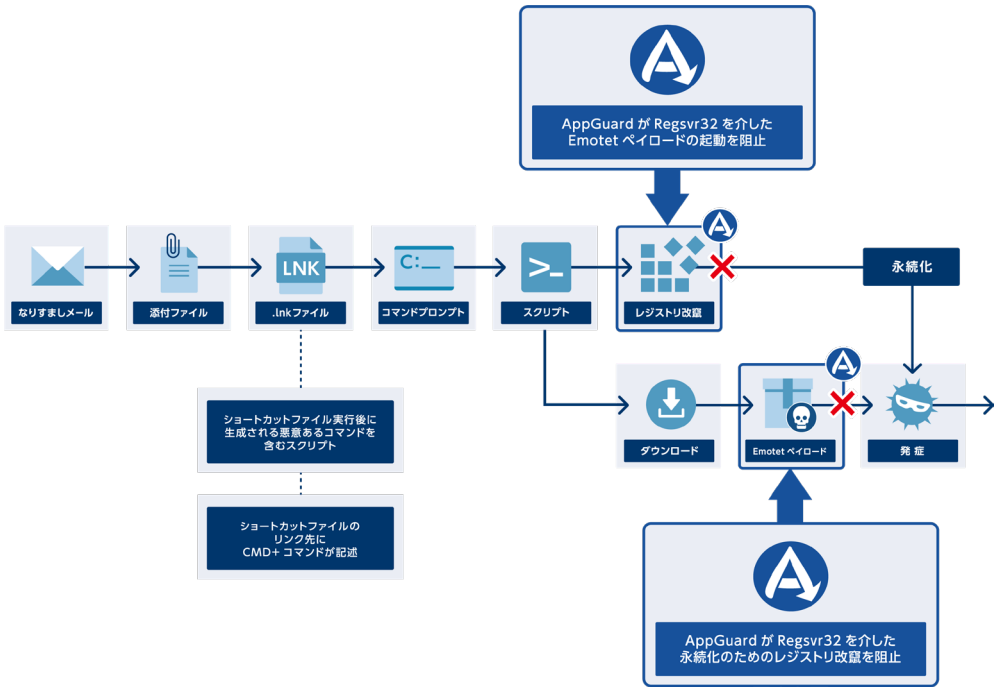


図　Emotet (ショートカットファイルの実行パス悪用) を阻止するポイント

3) WarZoneRAT (MS Excel の Excel アドイン悪用)

この攻撃手法は「Emotet」が用いる MS Office のマクロを悪用したものと似ています。「WarZoneRAT」はメールの添付ファイルに Excel アドイン (.xlam) を格納して送りつけます。ファイルを起動すると Excel アドインの読み込み要求画面が表示され、許可することで「WarZoneRAT」のダウンロードを開始します。AppGuard は Excel アドインを通じて呼び込まれる「WarZoneRAT」のペイロードの起動を制御するため発症させることなく攻撃を阻止します。

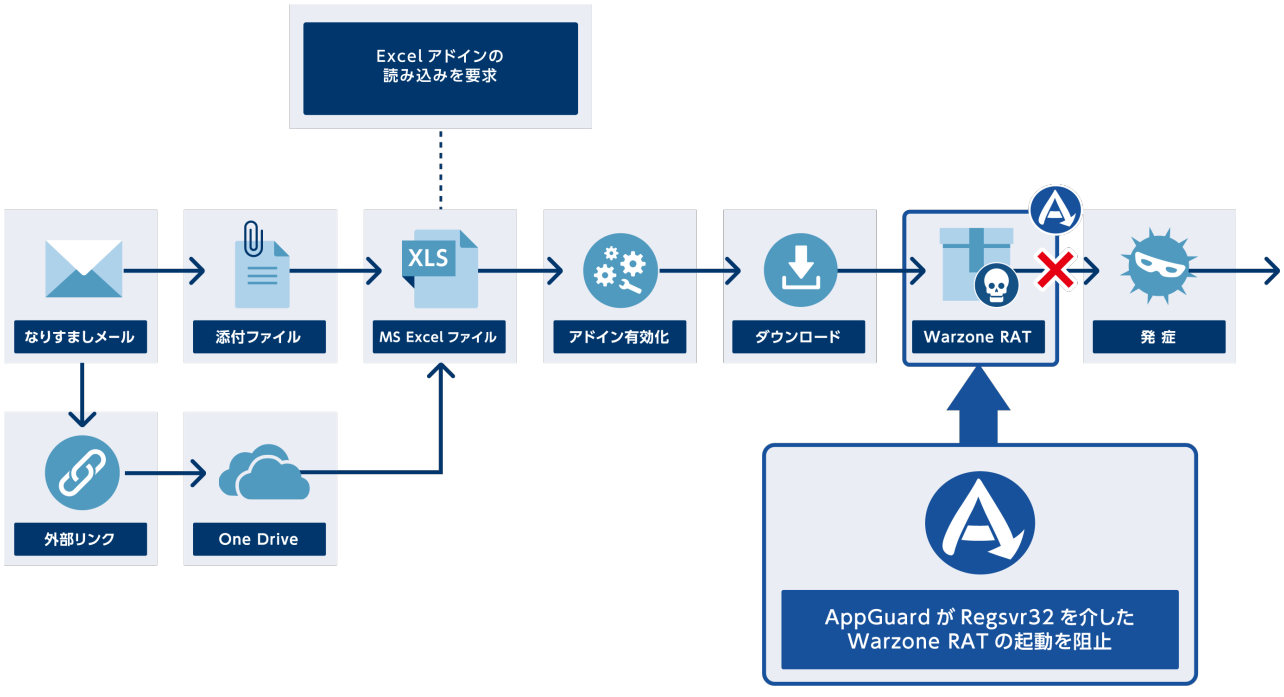


図　WarZoneRAT (MS ExcelのExcelアドイン悪用) を阻止するポイント

4) Chrome Loader (ISO ファイルを悪用)

この攻撃手法は ISO ファイル（光学ディスクの内容を丸ごと 1 つのファイルにアーカイブしたもの）を利用して悪意ある実行ファイルを展開します。Windows 10 では ISO ファイルをダブルクリックするだけで仮想ドライブにマウントできてしまうため、ユーザーが誤って格納されたファイルを起動してしまうリスクがあります。内部に格納された悪意ある実行ファイルを起動すると Dropper として機能して「Chrome Loader」を生成します。AppGuard は ISO ファイル内を「ユーザースペース」として扱うため、格納された悪意ある実行ファイルを起動しようとしても信頼を得る条件（信頼された発行元に登録されたデジタル署名との一致）を満たすことができないため起動を許可せず発症させることなく攻撃を阻止します。

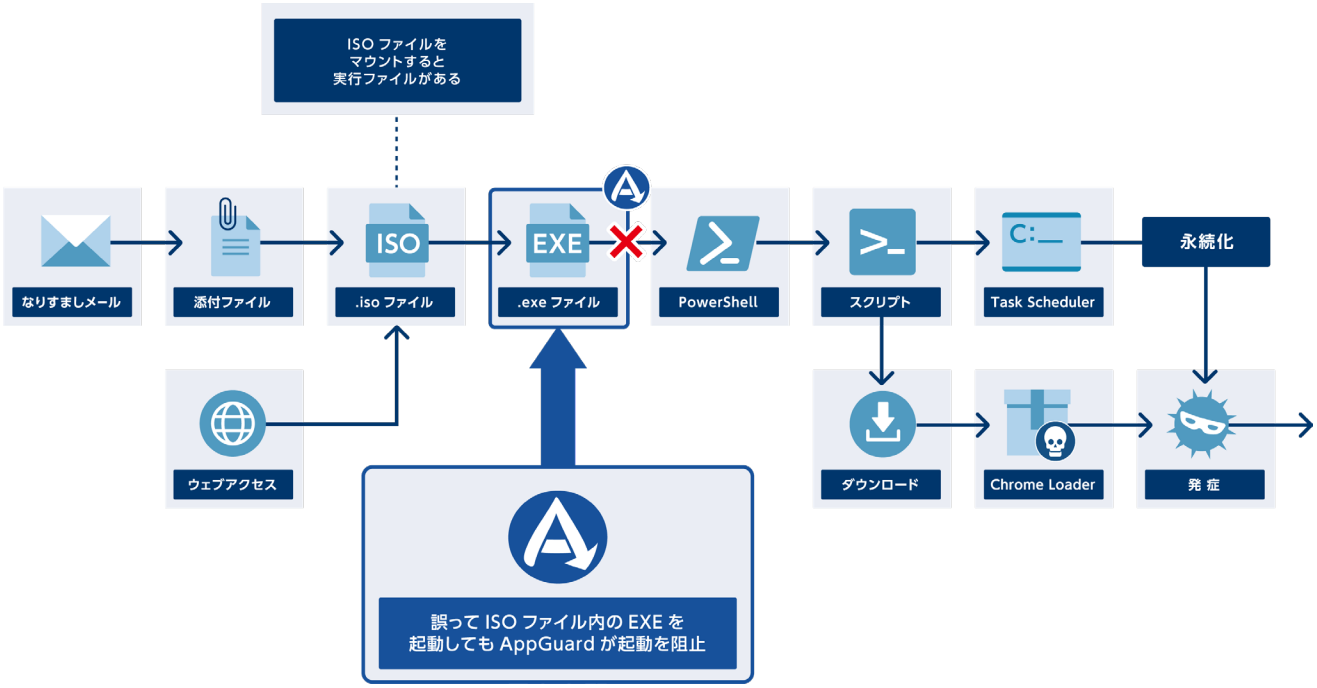


図　Chrome Loader (ISOファイルを悪用) を阻止するポイント

03.

実録：
ランサムウェアを取り巻く攻撃者の動向

03. 実録:ランサムウェアを取り巻く攻撃者の動向

1 攻撃経路の変化

本項では猛威を奮うランサムウェアに関連する動向と国内で発生したランサムウェア被害の中から興味深い事例をレポートします。ストーンビートセキュリティ株式会社の報告によれば、ランサムウェアによる被害は同社が実施した国内フォレンジック調査対応事案の約 30% を占めており、調査期間中（2021 年 1 月～2022 年 5 月）においては「Emotet」に次ぐ被害となっています。

従来、ランサムウェアの感染経路としてはメールに添付されたファイルをトリガーとして発症するケースが大半でしたが、最近はリモートアクセス機能を提供するネットワーク機器を経由して内部ネットワークに侵入されるケースや、外部公開されたシステムの脆弱性を突いた不正アクセスによってランサムウェアに感染させられる事案が増加傾向にあります。

2 RaaSビジネスとIAB(Initial Access Broker)の台頭

ランサムウェアによる被害が拡大する背景としては、攻撃者にとって容易かつ効率的に金銭を稼ぐ手段となっていることが挙げられます。数年前から RaaS（Ransomware-as-a-Service）と呼ばれるランサムウェアを使った攻撃をパッケージ化した仕組みが登場し、今や世界中に様々な RaaS グループが存在しています。RaaS グループの組織構造は各グループで様々ではありますが、主に「開発部門」「サポート部門」「交渉部門」といった構造になっています。ロシアの RaaS グループである「Conti」には、人事部門が存在しており、新メンバーのスカウトや組織内での報酬管理といった一般的な企業に近い組織形態を持つグループも存在しています。他にも RaaS グループは「アフィリエイト」と呼ばれる攻撃の実行役を担うパートナーを各所で募ったり、他の犯罪グループと手を組む等、サイバー攻撃におけるエコシステムを構築しています。

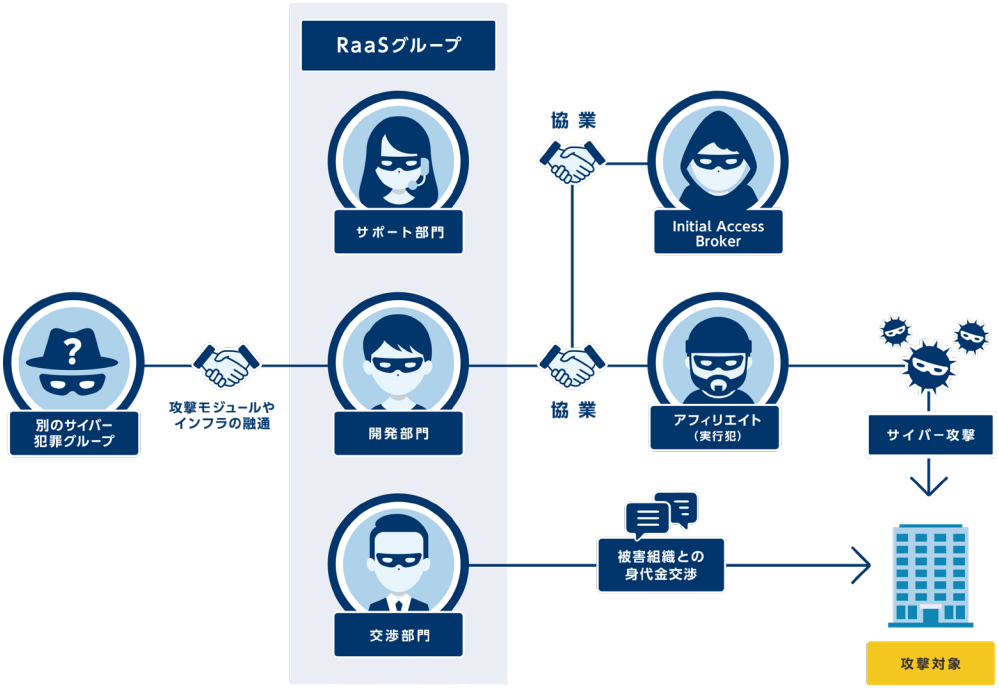


図　RaaSグループにおけるエコシステム

このエコシステムの中でも存在感を増して台頭してきているのが IAB (Initial Access Broker) です。彼らは、攻撃対象のネットワークやシステムに侵入するための情報を専門に扱っているサイバー犯罪者です。例えば、彼らが取り扱うものとして、セキュリティパッチが適用されていないネットワーク機器の所在や接続アカウント、脆弱な認証方式を採用している外部公開システムの存在等が挙げられます。

これまでは実行犯となる攻撃者自らが攻撃対象を地道に攻略していく必要がありましたが、手頃な価格で国や業種などを条件に攻撃可能な対象の情報を IAB から入手することで、攻撃者は短時間かつ容易に攻撃対象のネットワークやシステムへ侵入することができるようになりました。その結果、従来から使われてきたメールやウェブアクセスという選択肢に加えて、前述のリモートアクセス機能を提供するネットワーク機器や脆弱な外部公開システム等の新たな侵入経路を通じた被害が増加することとなりました。

下図は、Fortinet 社が提供するネットワーク機器において外部から到達が可能であり、かつ、CVE-2018-13379 の脆弱性が未修正である機器の一覧がハッカーフォーラムで公開されていた様子です。

Initial Access Broker とは
「初期アクセス (Initial Access)」の確立は攻撃者目線で見るとサイバー攻撃のスタートであり最大の難関であると言えます。
Initial Access Brokerより初期アクセスの情報を購入することによって攻撃の初期で最も難しいフェーズを時間短縮し、効率的に攻撃を展開することが可能となります。

CVE(Common Vulnerabilities and Exposures) とは
日本語では共通脆弱性識別子といい、個別製品に存在する脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子です。MITRE 社は世界 80 を超える脆弱性情報サイトと連携をして脆弱性情報の収集と重複のない採番を行うことで世界中で統一さらた識別子を元に脆弱性情報を管理することを目的としています。
識別子構成は CVE +〈西暦〉+〈連番〉(その年で何番目に登録されたか) で表されます。

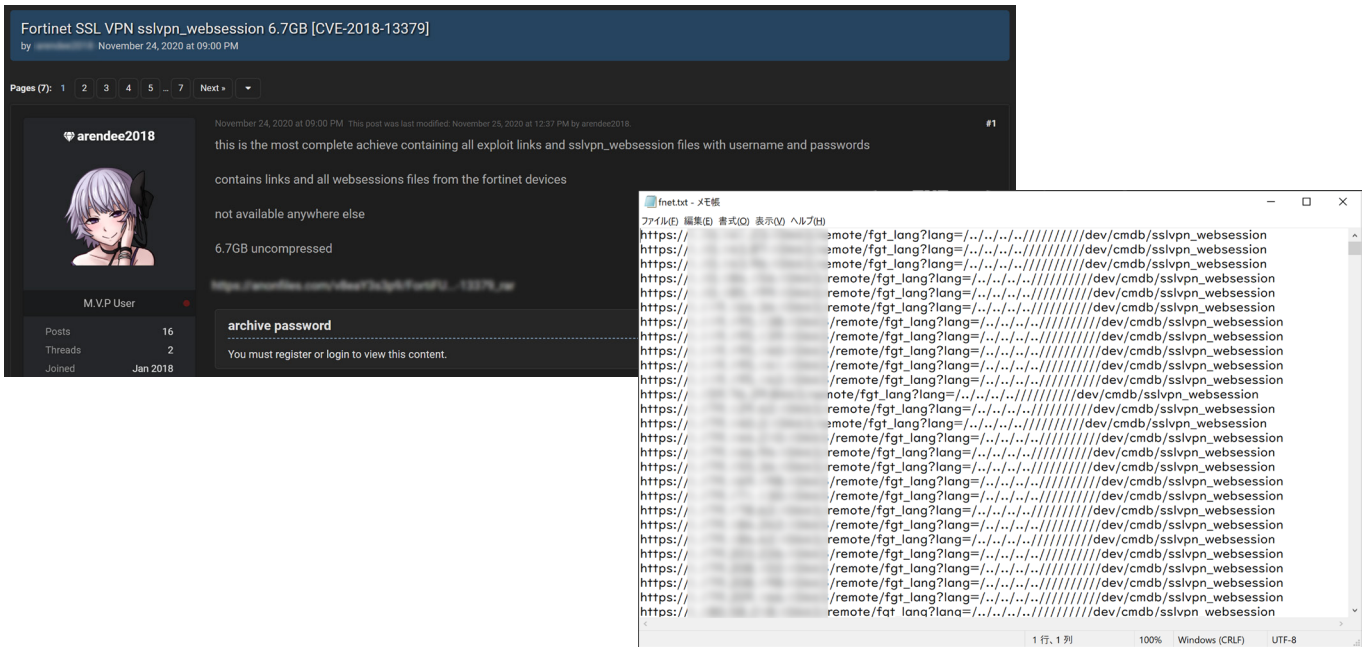
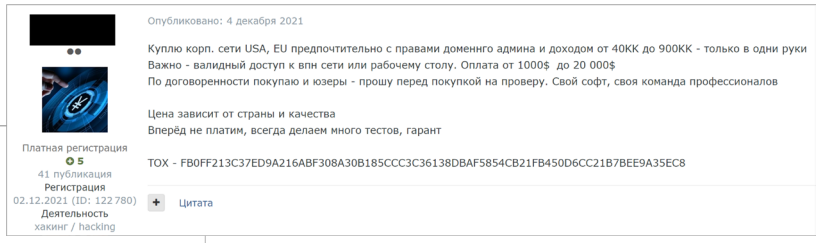


図　ハッカーフォーラムに投稿されたCVE-2018-13379未修正機器一覧

ハッカーフォーラム上では、金銭を要求しない形で公開されるものもあれば、IABを通じて金銭を伴う取引によって攻撃者の手に渡る情報もあります。下図の様に「Initial Access を欲しがる人(攻撃者)」と IAB を結びつける場も存在しています。ここでは、自身が欲している条件を提示して該当する情報を持つ IAB を探す人物や、自身が持っている侵入経路に関連する情報を宣伝する IAB が確認できます。



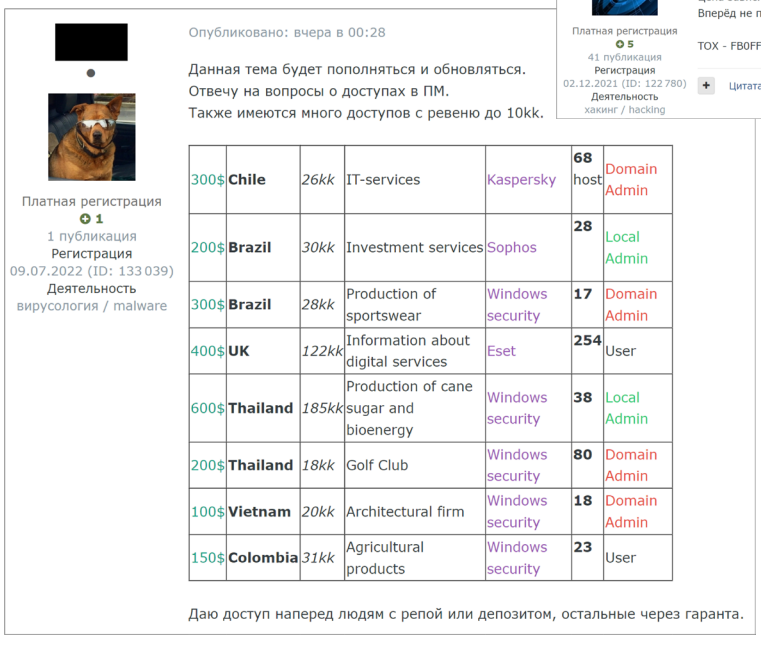


図　企業へのInitial Accessを買い求めるアフィリエイトの投稿

図　IABが投稿したVPN及びRDPアカウントの販売広告

3 インサイダー(内部協力者)の勧誘

一部の RaaS グループでは、IAB を利用せず攻撃対象組織の従業員を買収しようと試みていることがわかっています。例えば、RaaS グループの 1 つである「LockBit」は運営するリークサイト内で高額な報酬を餌に攻撃対象の組織に侵入するためのメールアカウント、VPN や RDP 等の情報提供や、わざとマルウェアに感染してもらうといった話を持ち掛けていたことが確認されています。

別のケースとして、2020 年 8 月に米国テスラ社が保有するネバダ州にあるギガファクトリーへサイバー攻撃を仕掛けるために 100 万ドルの報酬を餌にして従業員を買収しようと接触があったことが米国司法省によって発表されています。幸いにして従業員はこの誘いに乗らず、FBI に通報したことで事なきを得ましたが、攻撃者は様々な方法を使って攻撃対象を攻略しようとしていることがわかります。テクノロジーに基づく対策が重要であることは変わりませんが、組織として攻撃者からの甘い誘惑に乗らない様に従業員の倫理観を高める取り組みも併せて検討していくことが推奨されます。

Alert (AA22-152A)
Russian National Arrested for Conspiracy to Introduce Malware into a Nevada Company's Computer Network

https://www.justice.gov/opa/pr/russian-national-arrested-conspiracy-introduce-malware-nevada-companys-computer-network

図　従業員を買収しようと接触があったことをTwitterで公開したテスラ社

4 データを暗号化せずに身代金を要求するサイバー恐喝グループ

2022 年 6 月 1 日、CISA (米国国土安全保障省サイバーセキュリティインフラセキュリティ庁) より「Karakurt」というサイバー恐喝グループのアラートが公表されました。「Karakurt」は攻撃対象を侵害した際にデータの暗号化は行わず、データの窃取のみを行います。主な窃取対象は雇用記録、健康記録、財務関連情報、知財情報、個人情報等が挙げられています。彼らは、データを盗み出すと被害者に対して盗み出したデータのサンプルを提示した上で、情報の公開又は第三者への売却を材料にして身代金の支払いを要求します。

Alert (AA22-152A)
Karakurt Data Extortion Group

https://www.cisa.gov/uscert/ncas/alerts/aa22-152a

また、特徴的なのは身代金の支払いを早期、かつ確実なものとするために被害者から盗み出したメールアドレスリストや電話番号を使って、従業員、取引先、顧客等に対してデータの漏洩を防ぐために被害者が「Karakurt」に対して早期に支払いを行うように促して欲しいとメッセージを送りつけるのです。CISA の報告では「Karakurt」が別のグループが以前に盗み出したデータを入手し、それは自分たちが改めて盗み出したものだと主張して身代金の支払いを要求するケースも確認されています。

「Karakurt」の様にデータの暗号化を伴わず、盗み出したデータを使って恐喝行為のみを行うグループは以前から複数確認されていますし、多くの RaaS グループはデータ暗号化＋データ漏洩の二重恐喝をトレンドとして活動するようになっています。ランサムウェア感染＝データ暗号化と結びつけるユーザーも多く、その対策としてバックアップが推奨されていますが、ランサムウェア対策としては併せてデータの漏洩対策も検討する必要があります。

データ漏洩は関係者、取引先や顧客にまで影響が及ぶ可能性があります。今や事業の推進が自組織のみで完結するケースは少なく、様々なステークホルダーを巻き込んでいます。外部に公開すべきではないデータが漏洩した場合、社会的な信用が大きく低下する恐れがあり、データの暗号化同様に気を配らなければなりません。

本項で紹介した「Karakurt」は何か特別な脅威であり、これまでとは違った取り組みが必要であると思うかもしれません。しかし、CISA の報告を読む限りでは「Karakurt」も他のサイバー犯罪者たちと同様に、未施錠のドアとも言える脆弱性を悪用して攻撃対象のネットワークへ侵入しています。IAB という厄介な存在も暗躍していますが、第一に必要なことは自組織における攻撃対象となり得るポイントを減らす基本的な取り組みであるということを理解しておく必要があります。

5 進化するランサムウェア

ランサムウェアは前述のとおり、攻撃者の間でエコシステムが構築され、彼らが金銭を獲得するための優れたビジネスモデルが確立しつつあります。RaaS グループ間でアフィリエイトを獲得するための競争も確認されている中で、ランサムウェア自体も進化の兆しを見せています。

① 暗号化処理の高速化
攻撃者がランサムウェアによる暗号化を身代金要求の手段として利用する場合、システム管理者に検知されないように暗号化処理を完遂させる必要があるため、暗号化処理速度の向上は重要課題の 1 つとなります。

下表は株式会社 Blue Planet-works が 2022 年 6 月 14 日に実施した主要な RaaS ファミリーによるファイル暗号化速度の計測結果になります。暗号化速度にバラツキはあるものの「LockBit 2.0」や「Babuk」が利用するランサムウェアの暗号化速度は他を圧倒しています。

ランサムウェアファミリー	中央値 (1GBの暗号化速度)	100GB換算 (中央値×100GB)
LockBit 2.0	33秒	55分
Babuk	39秒	65分
BlackMatter	46秒	76分40秒
Revil	56秒	93分20秒
Hive	1分03秒	105分
Conti	1分12秒	120分
BlackCat	1分35秒	158分20秒
PYSA	1分37秒	161分40秒
CLOP	2分07秒	211分40秒

この計測結果を踏まえると、EDR 等の IoC (Indicator of Compromise：侵害の指標) /IoA (Indicator of Attack：攻撃の指標) に基づく検知システムを利用していたとしても、暗号化が開始されてしまうと検知から対処までの時間的な猶予がなく、業務の継続性に大きな影響が生じると考えられます。特にネットワーク内で同時多発的に暗号化処理を開始されるとさらに対処が困難となります。

ランサムウェア対策を検討する上で、侵入から発症するまでの間に検知・対処できることが望ましいですが、実現するためには状況に応じた検知ルールの追加・修正や SOC のスキルレベルに大きく依存してしまうため、その不確実性を払拭しきるのは並大抵のことではありません。現実的には、侵入の阻止や発症の阻止といった異なるアプローチの検討も併せて視野に入れて対策を検討する必要があります。

マルウェアとプログラム言語

マルウェアの歴史はコンピューターの歴史に追随し、約 40 年以上前からその存在が確認されています。
コンピューター黎明期に最も広く普及したコンピューター言語が C 言語ファミリーと呼ばれる言語群であり、当然のようにマルウェアもこれらの言語で作成され現在も踏襲されています。
しかし、IT 技術の進化は時を追うごとに加速しその技術革新に合わせる形で多くの新しいコンピューター言語が誕生しています。
これら比較的新しいコンピューター言語は AI やアプリケーションの開発などで重宝される存在でありつつ、サイバーセキュリティの観点では、解析できるアナリストが少ない、検体母数の少なさによる脅威情報不足などの問題を抱え、検知が非常に難しくなっています。

② アンチウイルスで検知できない言語で書かれたマルウェア

マルウェアを構成するプログラム言語としては C 言語ファミリーが一般的ですが、最近では Go、Rust、Nim、D、Python といった異なるプログラム言語で書かれたマルウェアが台頭してきています。これらのプログラム言語で書かれたマルウェアを難読化処理することで、従来のマルウェアと比べてもリバースエンジニアリング (マルウェアの構造分析を行い検出するための情報を得ること) を困難にすることができます。また、その性質からクロスコンパイル (単一のソースコードを元にして異なる OS 環境向けに実行可能なものとして生成すること) できるものも多く、Windows 以外の OS に対しても流用できるため、攻撃者にとっては検出されにくく使いやすいというメリットがあります。

また、現時点では多くのセキュリティ対策ツールがこれらのプログラム言語で構成されたマルウェアの解析に必要となる機能実装が十分にできていない状況が攻撃者にとっては魅力的です。
他のプログラム言語で構成される対象はマルウェア本体とマルウェアを呼び込むドロッパーが挙げられます。前者は前述のとおり、それ自体が検知されにくくなり、他 OS への多面展開が容易になります。後者は侵入後にバックドアとして機能することから、マルウェア本体を再コーディングしなくて良いため、様々なマルウェアを展開する上で使いまわしができるメリットがあります。

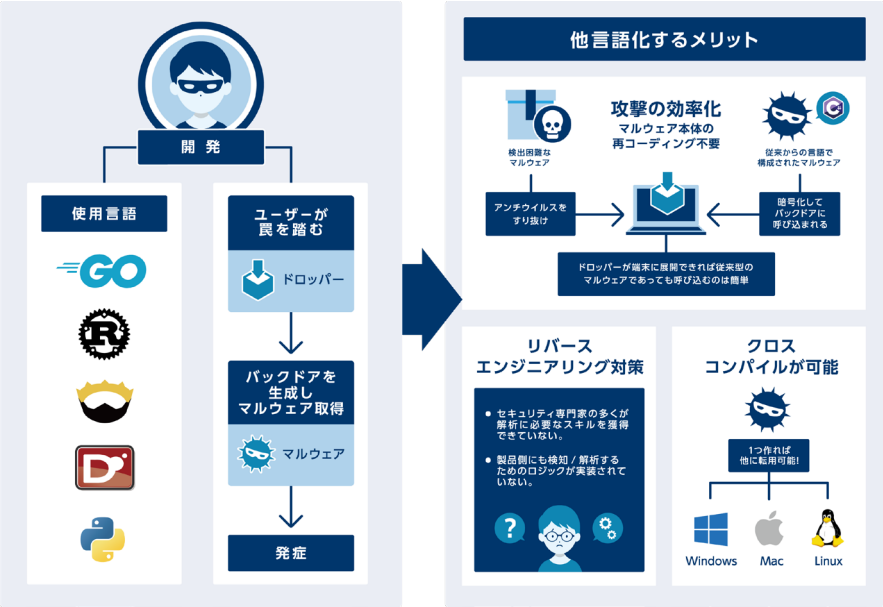
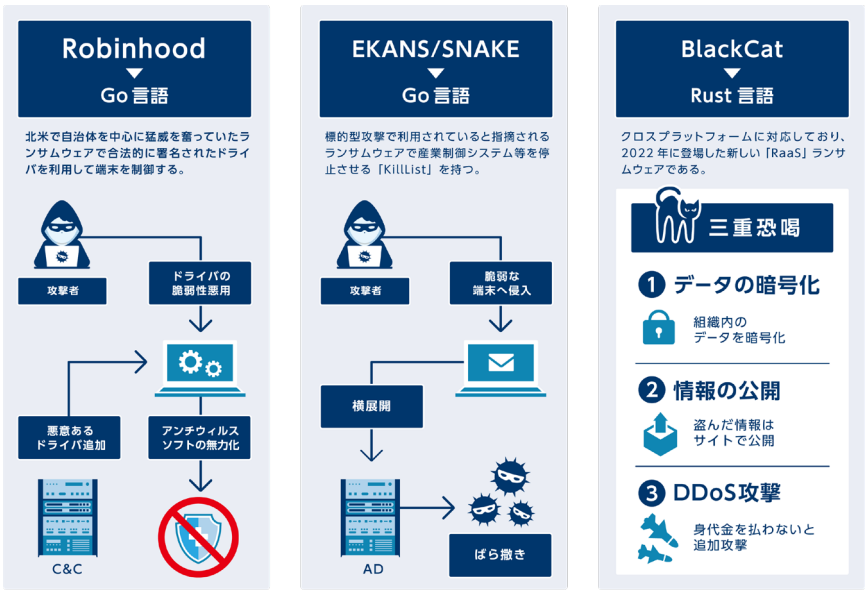


図　様々なプログラム言語を用いて構成されるマルウェアやドロッパー

かつて国内大手製造業を襲ったランサムウェアも従来とは異なるプログラム言語で構成されていたことがわかっており、セキュリティ対策に注力していた組織においても、その検出が非常に困難であったことが伺い知れます。



注意：図示するマルウェアの動きは当該マルウェア発見当時のものです。現時点で流通する最新版とは挙動が異なる場合があります。

図　従来とは異なるプログラム言語で構成されたマルウェアの例

6 ランサムウェアによる国内インシデント事例

本項ではストーンビートセキュリティ株式会社が実施した国内で実際に発生したランサムウェアによる侵害事案のフォレンジック調査から、非常に高度な手法が用いられていた事案の詳細を紹介します。フォレンジック調査とは、侵害されたデバイスやネットワークに残された攻撃の痕跡からインシデントの原因や影響範囲を調査するものです。この事案では、いわゆる「マルウェア」と定義されるもの（対象へ害を与えたり、悪用することを目的としたソフトウェア）が利用されておらず、攻撃対象となった Windows OS が標準機能として提供しているツールや機能だけを悪用して暗号化が行われました。

① インシデント概要
ある日の未明、企業 A が保有するサーバーの大部分（約 250 台）と一部のクライアント端末のデータが何者かによって暗号化され、サーバーが正常稼働できなくなり、業務停止に陥りました。

② インシデントタイムライン

Day 0	海外のIPアドレス（TOR経由で接続元を匿名化）から社内ネットワークへリモートアクセス（第三者によって窃取された正規アカウントによる不正ログイン）が行わる。
約2週間後	
Day 1 深夜	本格的な攻撃が開始される。攻撃開始から約1時間後にさらに2名の攻撃者が加わる。
Day 2 未明	Active Directory のAdministratorのパスワードが変更され、ドメインのポリシー設定変更が行われる。Active Directoryから他のデバイス（約250台）へRDP接続が行われて被害が拡大（バックアップサーバー、業務システム、ファイルサーバーを含む約250台のデバイス内にあるデータが暗号化）する。攻撃者によって脅迫文が提示され、業務停止に陥る。

③ 原因の特定

フォレンジック調査によって明らかになった攻撃の全体像は下図のとおりです。

図 攻撃の全体像

1) 社内ネットワークへの接続方法

Active Directory のイベントログを調査したところ、攻撃者は外部から VPN 接続を確立した状態で Active Directory へ RDP 接続していたことが確認されました。そのため、攻撃者は事前に VPN 機器との間に VPN 接続を確立するための正規の ID・パスワードを保持していたことになります。VPN 機器を調査したところ、使用していた VPN 機器のバージョン情報からアカウント情報を窃取可能な脆弱性（CVE-2021-22893）が未修正の状態であったことが確認されたことから、攻撃者はこの脆弱性を悪用して VPN 機器内に保存されていた ID・パスワードを窃取したと考えられます。

2) Active Directory の侵害方法

Active Directory を調査したところ、Active Directory を稼働させている Windows Server が長期に渡って Windows Update が実施されていないことがわかりました。また、2020 年に発見された「Zerologon(CVE-2020-1472)」が悪用可能な状態であったこともわかりました。管理者への聞き取り結果として、脆弱性への対策の必要性は理解していたものの、業務が多忙であったことから対策が後回しになっていたようです。

「Zerologon」は Active Directory が配下のクライアントと通信をする際に利用される「MS-NRPC (Netlogon Remote Protocol)」の暗号化処理における実装の不備によってドメイン管理者権限を第三者に取得されてしまう極めて危険な脆弱性です。侵害時に保全したデータから同じ条件の Active Directory 環境を再現したところ、「Zerologon」を悪用して管理者権限を取得できることが確認できたことと、イベントログからこの脆弱性を悪用して Active Directory の管理者権限パスワードが外部から変更されたことが確認されました。

3) 攻撃対象デバイスの侵害方法
Active Directory の管理者権限が攻撃者に取得された場合、同一ドメインに所属するクライアント端末やサーバーに対してリモートログオンが可能となります。攻撃者はネットワーク上で稼働していたほぼ全てのサーバーに RDP 接続を行った上で、データの暗号化を行っています。

④ フォレンジック調査で明らかになったこと

1) 複数の攻撃者によって手動で攻撃が展開されていた
VPN 機器のログや侵害されたサーバーのイベントログ、RDP 接続時のキャッシュ情報等から、本件は少なくとも 3 名の攻撃者によって実行されたことが確認されました。Day 0 時には 1 名で攻撃が開始され、その後の Day 1 午後に同じ攻撃者が再度侵入、他の 2 名は Day 1 深夜の攻撃開始後に参加しています。そのため、最初に侵入した 1 名が本件の首謀者であり、後から侵入した 2 名は協力者に相当する人物であったと想定されます。

2) マルウェアが利用されない攻撃手法
本件が一般的にイメージされるサイバー攻撃と異なる点は、マルウェアを一切使用していないという点です。攻撃者にとっては、マルウェアを使用する方が攻撃の一部又は全部を自動化できる利点はありますが、一方でセキュリティ対策ツールにより検知されるリスクがあります。本件では、Windows の正規サービスを活用しつつ、暗号化においても正規の暗号化ツール (BitLocker) を利用しているため、データの暗号化が行われるまでシステム管理者に気づかれることなく攻撃が遂行されていました。一連の手口から、セキュリティ対策ツールの検知ロジックや回避テクニックに精通している熟練の攻撃者であったことが伺えます。

3) 外部への情報漏洩
ランサムウェアは要求した身代金を手に入れるために、データの暗号化を実施する前にこれらのデータを持ち出すことがあります。本件でも情報漏洩の調査が行われましたが、以下の 3 つの理由により情報漏洩には至っていないと判断されました。

外部への データ転送量	VPN機器のログから攻撃者が接続していた時間は約3時間であることがわかりました。また、外部へ転送されたデータ量はわずか10MB程度と小さく、RDP接続そのものによるデータ量を踏まえると、VPN及びRDP接続のセッショントラヒックの転送量の範囲に留まっていると考えられました。
データを 持ち出した痕跡	通常、攻撃者が外部にデータを持ち出す際にはファイルの収集や圧縮、送信といった一連の操作が行われ、これらの操作に対する痕跡が対象機器上に記録されますが、調査時において情報持ち出しを裏付ける操作の痕跡は確認できませんでした。
データ転送が 容易ではなかった 可能性	侵入されたサーバーの中にはファイルサーバーやバックアップサーバーがあり、ディスクサイズ、ファイルサイズ共に非常に大きいものであったため、それらのデータを短時間で外部に送信することは容易ではなかったと考えられます。

⑤ 攻撃者の目的

暗号化の被害に遭ったデバイスのデスクトップには「ファイルを暗号化した。復号キーが欲しければ仮想通貨で要求額を支払え」という内容が記載された脅迫文が大量に作成されていました。前述のとおり、情報の持ち出しが目的ではなかったとすれば、純粋にデータの暗号化による金銭の要求が攻撃者の目的であったと考えられます。

⑥ AppGuard が導入されていた場合

本件において AppGuard が使われていた場合、どうなっていたでしょうか？ 調査結果に基づいて考察します。まず、AppGuard は Windows OS を対象とした製品であるため、VPN 機器を通じた内部ネットワークへの侵入及びポートスキャンを阻止することはできません。しかし、Active Directory の存在が攻撃者に知られたとしても AppGuard が導入されていることで、以下に示すとおり「Zerologon (CVE-2020-1472)」を悪用して Active Directory を掌握することはできません。結果として、Active Directory を踏み台とした攻撃者の最終目的を阻止することが可能です。

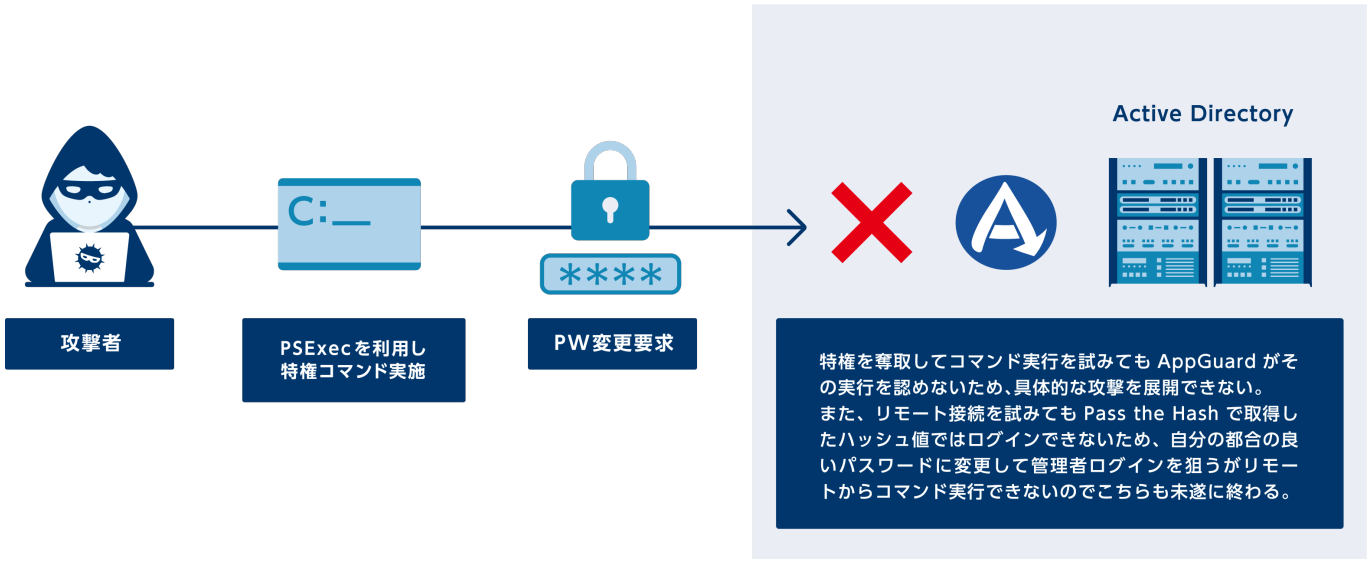


図　Zerologonを悪用した攻撃を阻止するAppGuard

Active Directory に導入された AppGuard は、ポリシーに基づいて内外から干渉ができないロックダウン状態を作り出します。攻撃者は「Zerologon」の脆弱性を悪用して特権コマンドを Active Directory に送り込もうとしますが、AppGuard によって外部から Active Directory に対するコマンドの実行が許可されないため、パスワードの変更を含めて一切の干渉が成立せず、攻撃のライフサイクルを分断することが可能です。

7 ランサムウェア被害に遭わないために意識すべきこと

「(6) ランサムウェアによる国内インシデント事例」で取り上げた侵害事案では、VPN 機器のファームウェア更新が適切に行われていれば内部ネットワークへの侵入を防ぐことができました。また、Active Directory においても定期的な脆弱性対応 (OS・ソフトウェア) が行われていれば「Zerologon」の脆弱性を悪用されず、管理者権限を取られることもなく被害の拡大を最小限に留めることができたはずです。

セキュリティインシデント全般に言えることですが、基本的な対策を徹底することでインシデントの発生を防ぐ、又は極小化することが可能です。平時の状態から安全な状態を維持する取り組み (脆弱性管理、設定の棚卸し、アクセス制御、認証等) ができているか、今一度点検・確認されることを強く推奨します。

また、フォレンジック調査のプロフェッショナルであるストーンビートセキュリティ株式会社は、インシデント発生時における効果的な調査を実現するために推奨すべき事項として以下を挙げています。

① ログ取得期間の見直し
Windows OS は仕様としてイベントログを生成します。イベントログはフォレンジック調査において非常に重要であり、イベントログの有無で調査の難易度は大きく変わります。残念ながら初期設定値で取得できるイベントログの期間は短く、インシデント発生時点のログが残っていないというケースはよく見られます。実際に保存するログはログの量、ディスク容量を考慮する必要がありますが、少なくとも 3 ヶ月程度はログを保存するように設定することが推奨されます。

② 取得するログの種類の見直し
ファイルへのアクセス履歴は Windows OS の初期設定では記録されず、監査ログを有効にする必要があります。ただし、取得するログの種類を増やすとディスク容量がひっ迫する恐れがあります。システム構成や環境を考慮の上、取得するログの種類について検討することが推奨されます。

③ 可視性を高めるためのツールの活用
フォレンジック調査においては、プログラムの実行やプロセスの挙動を抑えることが重要になります。そのため、遡ってプロセスの実行及び追跡が可能となるEDR 等のセキュリティ対策ツールの活用が推奨されます。

④ 環境の保全
自組織でなんとかしようとして色々と着手したことによって、情報が錯乱して追跡調査が困難になるケースも多いため、外部の専門家に協力を要請する場合には保全を最優先とすることが推奨されます。

⑤ 複数のフォレンジック事業者のリストアップ
外部の専門家に協力を要請する前提なのであれば、複数のフォレンジック事業者をあらかじめリストアップしておくことで、いざという時にスムーズに対応を進めることが可能となります。流行性のあるマルウェアが猛威を振るっていた場合、一時的にフォレンジック事業者側の人的リソースに余裕がなくなることも想定され、いざという時に協力を得ることができない可能性があります。そのため、特定の事業者だけではなく、複数の事業者にコンタクトできるようにしておき、対応できる事業者と早期に見つけられる様にしておくことが推奨されます。

04.

実録：
Penetration Testから読み解く攻撃の手口

04. 実録: Penetration Test から読み解く攻撃の手口

1 狙われるActive Directory

Penetration Test（以下、ペネトレーションテスト）とは、システムに残存する脆弱性や設定不備を利用して組織への侵入を試み、侵入された際のリスクを明らかにすることを目的としたテストです。本項では、ストーンビートセキュリティ株式会社が実施した企業 A に対する Active Directory へのペネトレーションテストの結果から、昨今のサイバー攻撃において被害拡大の要因ともなっている Active Directory に内在するリスクを紹介します。

ランサムウェアを扱うサイバー攻撃者の多くはランサムウェアを効率的に配布するために Active Directory を侵害する傾向が多く見られます。Active Directory は Windows ドメインを統合管理する仕組みであるため、管理者権限を奪取された場合にグループポリシーを利用してランサムウェアをドメイン配下の端末に配布されるだけでなく、ドメインに登録されている全てのアカウント情報が攻撃者に窃取されてしまう懸念があります。

本項では組織の内部ネットワークに攻撃者が何らかの方法で侵入した状態を想定し、その状態から内部ネットワークで稼働する Active Directory を探し出し、管理者権限を奪取するまでの流れを再現することで対策のポイントを導き出していきます。

2 Active Directoryの管理者権限を奪取するまでの流れ

下図に示されるとおり、ペネトレーションテストの結果として、攻撃者（ペンテスター）は企業Aが運用するActive Directoryに対して「Zerologon（CVE-2020-1472）の脆弱性」と「SMBでの匿名ログイン」の2通りの攻略方法が存在することを確認しています。

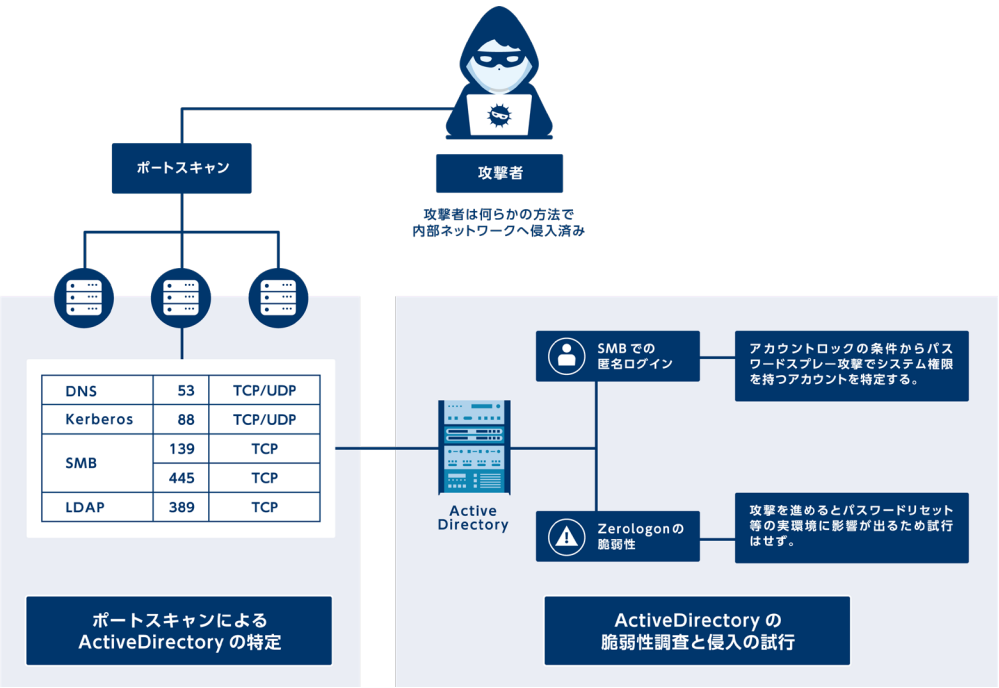


図　攻撃者がActive Directoryへ侵入するまでの流れ

① ポートスキャンによるActive Directoryの特定

攻撃者（ペンテスター）が対象にポートスキャンを実行することでオープンポートやサービス、ソフトウェア情報を収集することができます。また、オープンポートやサービス名から対象機器のサーバー種別についても推測可能な場合があります。

SMB
(Server Message Block)とは
ネットワーク間でのファイル共有やプリンター共有等の実行を容易に行うプロトコルです。

攻撃者（ペンテスター）の端末からポートスキャンを実行した際に、あるホストからの応答でDNS（53/TCP、UDP）、Kerberos（88/TCP、UDP）、SMB（139/TCP、445/TCP）、LDAP（389/TCP）サービス等が動作していることが確認できました。これらのサービスが動作していたことから、このホストがActive Directoryであると推測することができます。

② Active Directoryの脆弱性調査と侵入の施行

ポートスキャンによってActive Directoryと推測されたホストに対して、今度は専用のツールを使って脆弱性のスキャンを実施したところ「Zerologonの脆弱性」と「SMB（Server Message Block）での匿名ログインが有効」であることが判明しました。

1) Zerologon の脆弱性

Zerologon の脆弱性は CVE-2020-1472 として定義され非常に深刻度の高い（CVSS v3 基本値：10.0[緊急]）脆弱性として知られています。この脆弱性を悪用することでリモートから Active Directory の管理者権限を奪取することが可能であり、この攻撃によってドメイン全体を攻撃者に掌握される危険性があります。

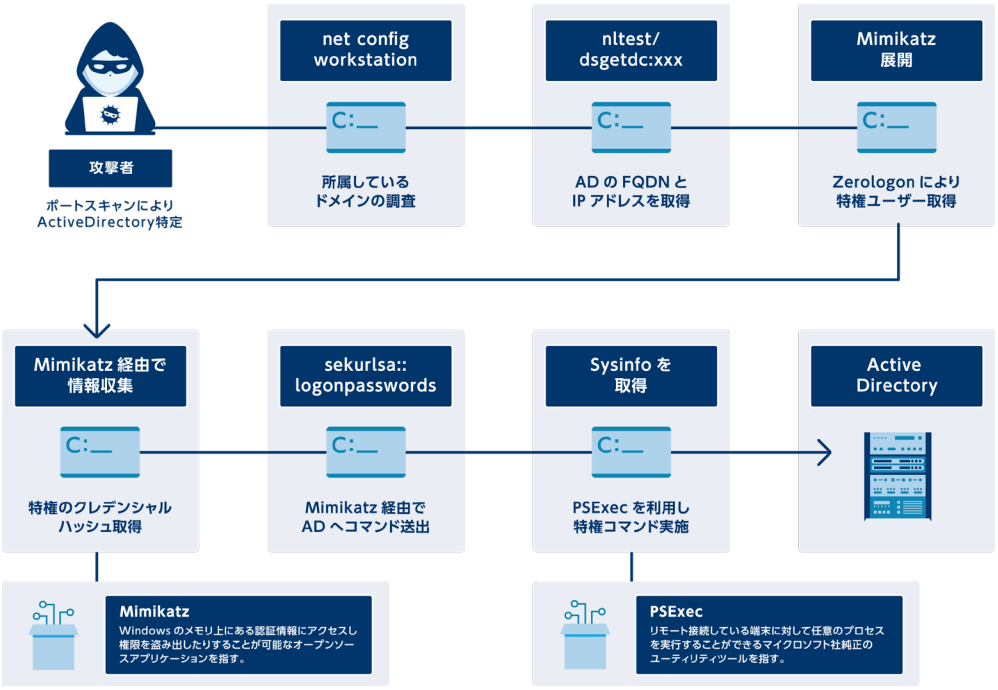


図　Zerologonを悪用した攻撃の流れ

本項で取り上げているペネトレーションテストでは、対象ホストが企業 A の本番環境で利用されている Active Directory であるため、Zerologon の脆弱性を悪用してパスワードリセット等を試みて管理者権限を奪取するところまでは攻撃を進めていません。しかし、この脆弱性が残存しているという事実は、攻撃者にとって容易に Active Directory を掌握できることを意味します。

CVSS (Common Vulnerability Scoring System) とは
共通脆弱性評価システムと略されます。
IT システムの脆弱性に対する共通の評価を提供するための仕組みです。評価はその危険度に応じて 0.0 ～ 10.0 のスコアで表示され、数値が大きくなるほど危険度が高く緊急な対処が必要だとされています。

2) SMB での匿名ログインが有効化

SMB での匿名ログインが有効化されている場合、攻撃者は認証情報なしに Active Directory に対して接続が可能となるため、ドメインに登録されたユーザー名やパスワードポリシー、アカウントロックに関する設定等の様々な情報を取得されてしまう危険性があります。

ポートスキャンによって Active Directory と推察された対象ホストに対して SMB での匿名ログインを利用することで、攻撃者（ペンテスター）は約 500 件のユーザー名やパスワードポリシー、アカウントロックに関する情報を入手することができました。入手したパスワードポリシーから、設定可能なアカウントパスワード要件が脆弱（複雑性の設定要件なし）で文字長は 8 文字以上であることが判明します。また、アカウントロックに関する情報からは、5 回の認証失敗で対象

アカウントがロックされることも確認できました。これらの情報を活用することで、攻撃者（ペンテスター）は脆弱な設定となっているアカウントの有無を調査することができます。

一般的に脆弱な設定となっているアカウントを特定する手段として、「ブルートフォース攻撃」と呼ばれる手法が利用されます。「ブルートフォース攻撃」は、特定のユーザー名に対してパスワードを総当りする攻撃ですが、前段の調査によって「5 回の認証失敗で対象アカウントがロック」される設定となっていることから、攻撃者は総当りによるアカウントロックを回避するために「パスワードスプレー攻撃」へ切り替える判断が可能となります。

「パスワードスプレー攻撃」とは、少ないパスワードリストを活用して総当りすることで脆弱なアカウントを特定する攻撃手法です。本項で取り上げているペネトレーションテストでは、よく使われるパスワードの中から「password」、「12345678」の 2 つと「ユーザー名(ユーザー名=パスワード)」の計 3 つをパスワードリストとして利用しました。

この対象ホストに対しては、アカウントロックされない範囲で約 1500 回（約 500 ユーザー× 3 つのパスワード）の認証試行を行い、脆弱なパスワードを使用しているユーザーを 10 分弱で約 40 件も特定することができました。これらのアカウントに対してどういった権限が付与されているのか調査したところ、システム権限を持ち、あらゆるコマンドを実行可能な Domain Admins グループに所属するアカウントが含まれていました。この時点で攻撃者は Active Directory の管理者権限を奪取したことになります。

Domain Admins グループに所属するアカウントを奪取した攻撃者（ペンテスター）は Active Directory へ侵入した後、登録されている全アカウントのパスワード情報の抽出を行い、約 5000 件のパスワードハッシュを取得することに成功しました。

パスワードハッシュとはパスワードの保存形式であり、パスワードはハッシュ関数によりハッシュ化された値（ハッシュ値）で格納されています。ハッシュ化することで Active Directory で管理されたパスワード情報が漏洩した場合でも、元のパスワードが特定されないようにする利点があります。しかし、脆弱なパスワードを使用していた場合、容易にハッシュ値から元のパスワードを特定することが可能です。本項においても取得した約 5000 件のハッシュ値に対して、攻撃者（ペンテスター）は約 2 時間で 1000 件以上のパスワードをパスワードハッシュから特定することに成功しました。

3 ペネトレーションテストから読み解くActive Directoryへの配慮

本項で紹介したActive Directoryへのペネトレーションテストの結果からActive Directoryを運用する上で配慮すべき事項と推奨される対策を以下に示します。

配慮すべき事項	推奨される対策
脆弱性の残存	深刻度が高く、かつ、攻撃への転用が容易な脆弱性に対する管理及び解消/緩和策の徹底
SMBでの匿名ログインが有効	匿名ログインの無効化
脆弱なパスワード設定	よく使われるパスワード (Worst Password) は利用せずに強固な認証を実現するための仕組みやパスワードポリシーの適用
利用されていない不要なアカウント	退職者など不要となったアカウントの削除徹底

「Zerologon (CVE-2020-1472) の脆弱性」の様に、既知の脆弱性を悪用される場合もありますが、SMBサービスの脆弱な仕組みを足掛かりとしてActive Directoryへ侵入し、管理者権限を持つアカウントのパスワード情報を取得されてしまうこともあります。

実際の攻撃者はActive Directoryにバックドア用のアカウントを追加することで、永続的な接続を確保することもあります。また、昨今は「3.実録：ランサムウェアを取り巻く攻撃者の動向」で紹介した事例の様に侵入したシステム内の情報探索や情報窃取後にランサムウェアを実行して業務停止に追い込む事例も数多く確認されています。

本項でご紹介した様に修正パッチの未適用や脆弱なパスワードの使用等、基本的な対策が実施されていないことがシステムへの侵入やアカウントの漏洩につながります。また、適切なパスワードポリシーを設定していたとしても、そのパスワードポリシーを設定する以前の古いアカウントが削除されないまま残っていると、それを悪用されることもあります。

セキュリティ対策を万全に行っている組織やシステムであっても、第三者によるペネトレーションテスト等の棚卸しを定期的に実施し、リスクを可視化して適切な対応を施していくことが重要です。

4 脆弱性管理プロセスの構築

ストーンビートセキュリティ株式会社が2021年1月から2022年5月までに実施したペネトレーションテストにおいては、全体の約 80% 以上のシステムで何らかの脆弱性が残存していることが報告されています。その中の約 5% が OS やソフトウェアに起因する深刻度の高い脆弱性であり、本項で取り上げた「Zerologon（CVE-2020-1472）の脆弱性」に代表される悪用された場合に深刻な被害に直結するものばかり確認されています。

脆弱性への対策としては主に修正パッチを適用することになりますが、修正パッチを適用する作業は、適用後にシステムの動作に影響を及ぼす懸念があるため事前検証が必要になる等、管理者にとっては手間を要するものではあります。しかしながら、万一、脆弱性が攻撃に悪用されてしまい、ネットワーク内で深刻な被害が生じた場合は緊急対応や復旧作業等で非常に多くの時間を割かざるを得ない状況になります。また、さらに調査・対応をフォレンジック事業者に依頼すると多額の費用も発生します。もし、速やかな修正パッチの適用が難しい場合には、根本対策（修正パッチの適用）を実施するまでの期間は緩和策（例：AppGuard を利用する）を講じる等、計画的かつ柔軟な対応が求められます。

OS やソフトウェアの脆弱性は日々新しいものが公開されており、その中には深刻度の高いものも多数含まれています。また、ユーザーの実環境においては数年前の古い脆弱性が残存しているものや、サーバー機器以外のネットワーク機器（UTM 製品やその他アプライアンス製品等）においても深刻な脆弱性が残存しているのが実態です。そのため、管理対象のシステムにおいては、公開された脆弱性情報を定期的に確認し、リスクを評価した上で、脆弱性対策を計画的に実施することが非常に重要となります。また、脆弱性への対応を日々の運用業務に組み込んで、脆弱性対策を着実かつ継続的に実施できるような仕組み（脆弱性管理プロセス）を構築することが推奨されます。

OS やソフトウェアの脆弱性に対応するための脆弱性管理プロセス（脆弱性の識別、優先順位付け、パッチの入手、パッチの適用、パッチ適用状況の検証）は、各組織のシステム環境や運用状況に応じて構築する必要があります。現在、脆弱性管理プロセス構築時の参考となるガイドラインとしては、米国国立標準技術研究所（NIST）が発行する「Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (NIST SP800-40 Rev.4)」があります。また、少し古いですが国内でも IPA から日本語訳も公開されています。本書には、脆弱性管理プロセスの各フェーズにおけるベストプラクティスが網羅的に説明されており、本書の内容に沿って脆弱性管理プロセスを構築することが推奨されています。

Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (NIST SP800-40 Rev.4)

パッチおよび脆弱性管理プログラムの策定（日本語訳PDF）

Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways (NIST SP1800-31)

2022 年 4 月 に は、「Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways (NIST SP1800-31)」が発行されています。こちらには、前述の「NIST SP800-40 Rev.4」で説明されている修正パッチ管理プロセスを組織に実装する際、ツールを導入して自動化や省力化を図る方法が詳しく解説されています。脆弱性管理プロセスにおいて、管理対象システムの数が多い場合は管理の手間も増大しますので、プロセスの自動化を進めて省力化を図ることも重要です。

05.

セキュリティアドバイザーの視点から

05. セキュリティアドバイザーの視点から

本項では株式会社 Blue Planet-works のセキュリティアドバイザーが、近い将来、今よりも身近な脅威となる可能性がある事案について取り上げます。

1 つ目の事案はマルウェアに組み込まれる正規の署名済みドライバーについてです。脅威を検出するセキュリティツールは日々進化をしていますが、攻撃者もそれらを回避するために様々な手法を展開します。本項で例示しているウクライナに投入された「HermeticWiper」やいくつかのランサムウェアにおいて正規のアプリケーションソフトで利用されているドライバーが悪用されていることが確認されており、今後も正規のドライバーがマルウェアに実装されて悪用されるケースは増えていくと考えられます。

2 つ目の事案はソフトウェアサプライチェーン攻撃についてです。SolarWinds 社や Kaseya 社の製品が攻撃者に悪用されて合法的な処理プロセスを通じてそれらを利用する世界中の組織に対して大規模なインシデントが立て続けに引き起こされました。システム認証でのなりすましを排除する完全な認証を使用していたとしても、不本意に侵害されたソフトウェアサプライチェーンの脆弱性によって閉域環境であっても攻撃を展開することが可能であり、他の攻撃手法と比べても阻止することが非常に難しいことがわかっています。今後も注目度が高く、極めて危険性の高い攻撃手法となります。

1 マルウェアに組み込まれる正規の署名済みドライバー

Go、Rust、Nim、D、Python 等の言語で構成されたマルウェアが増加傾向にある一方でマルウェアに実装されるコンポーネントに正規のアプリケーションで利用されているドライバーが転用されるケースが確認されています。本項では 2022 年 2 月 23 日にウクライナに投入されたワイパー型マルウェア「HermeticWiper」を実例として紹介します。

① ワイパー型マルウェアとは
ワイパー型マルウェアは、対象端末内のデータ又は特定領域を消去して使用不能にすることを目的として使われる標的型のマルウェアです。最近では主にマスターブートレコード（MBR）を別の情報で上書きすることによって短時間でシステムを破壊します。他のマルウェアと異なり、攻撃対象は国が関与するインフラ施設等の限定された対象である点と発症後にワイパー型マルウェア自身も削除される

ため、検体を回収することが難しく、その全容を解明できていないものも多いのが実態です。

発見された年	使用されたワイパー	主な攻撃対象国
2008年	Narliam	イラン
2012年	Shamoon	サウジアラビア
2013年	DarkSeoul	韓国
2016年	Industroyer	ウクライナ
2017年	NotPetya	ウクライナ
2018年	Olympic Destroyer	韓国
2019年	ZeroCleare	中東諸国
2019年	Dustman	バーレーン
2021年	MeteorWiper	イラン

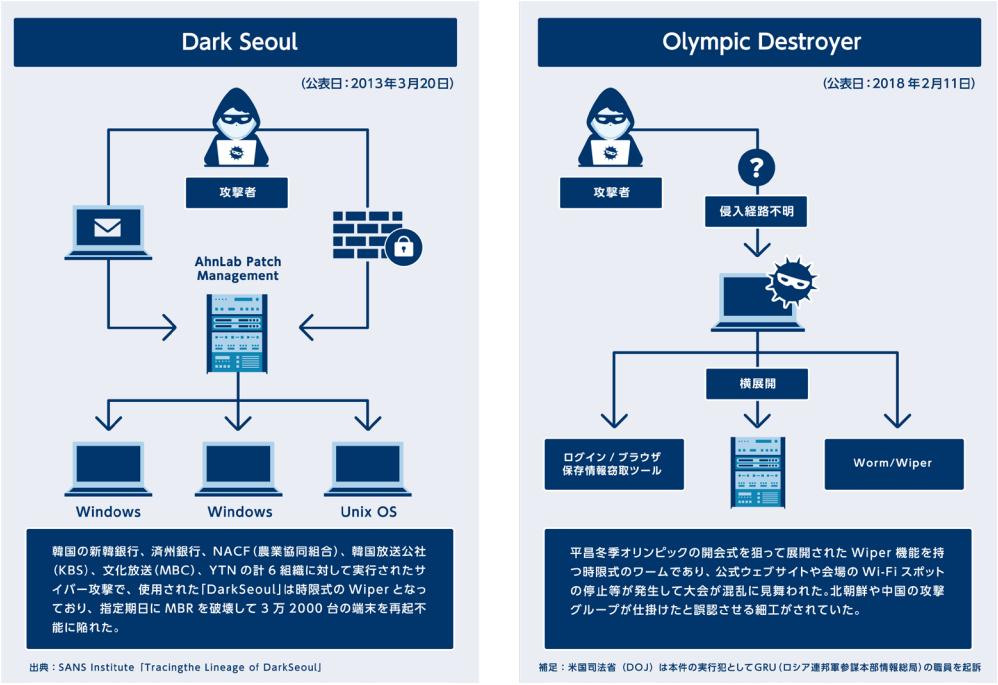


図　過去に発見されたワイパー型マルウェアの例

② ワイパー型マルウェア「HermeticWiper」の特徴

「HermeticWiper」の由来は「Hermetica Digital Ltd.,」によって発行された正規のコードサイニング証明書を利用していることが理由となっています。マルウェア自身が正規のコードサイニング証明書を保持していることから、起動に際して多くのアンチウイルス製品が信用できる実行ファイルとして扱ってしまいます。なお、この証明書は2022年4月15日付けで失効しています。

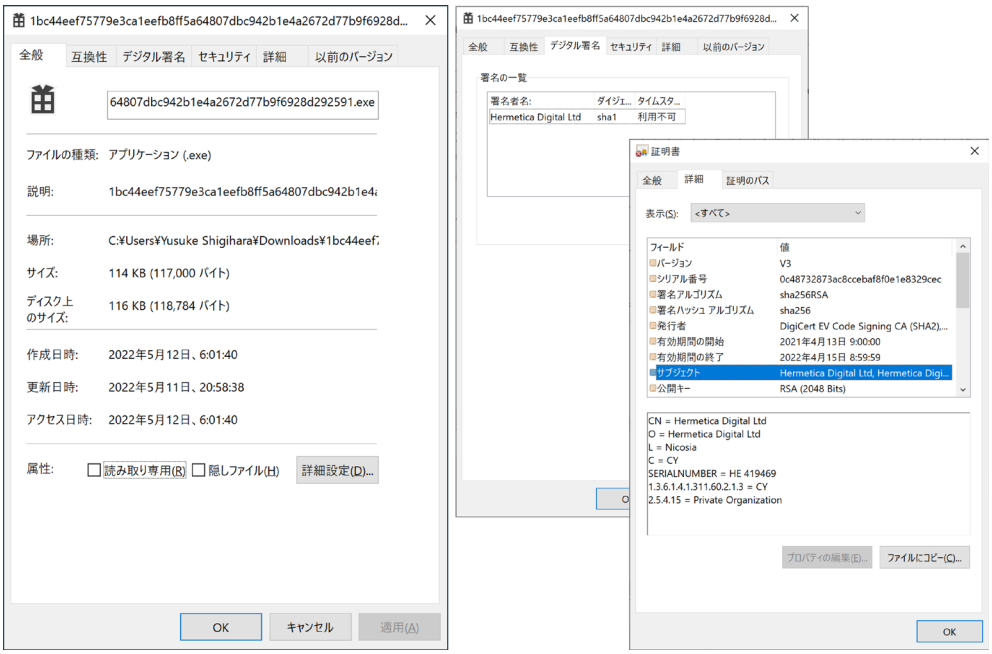


図　HermeticWiperが持つ正規のコードサイニング証明書

③ HermeticWiper が利用するドライバー

マルウェア自身が正規のコードサイニング証明書を保持していることも問題ですが、「HermeticWiper」は中国四川省に本社を置く「CHENGDU Yiwo Tech Development Co., Ltd.」が開発した「EaseUS Partition Master シリーズ」で利用されている正規のドライバーを利用していることがわかっています。正規のドライバーを利用することで、攻撃モジュール自体がアンチウイルス製品等に検知されにくくなります。

図　HermeticWiperのドライバーに悪用される正規のドライバー

このドライバーは VirusTotal に照会をかけると、ほとんどのアンチウイルス製品が危険性なしと判断します。解析を困難とする構造を持たせるだけではなく、安全だと認識された正規のドライバー等も攻撃に悪用するため、これまでの様な「悪いモノ」を見つける仕組みで検出していくことはより困難になっていくと想定されます。

以下に一例を示す通り、数としてはまだそれほど多くはありませんが、マルウェアの中には正規のドライバー又は正規のコードサイニング証明書を悪用するものが登場し、その存在感を強めています。

マルウェア	概要
Bankeiya	バッファロー社が提供するドライバーインストーラーがマルウェア「Bankeiya」に感染した状態で配布されており、インストール処理中に悪質なDLLファイルを実行するように細工されている。
RobbinHood	GIGA-BYTE　Technology社の正規ドライバーが持つ脆弱性 (CVE-2018-19320) を悪用することで、端末内の防御プロセスを強制終了させる。ランサムウェアを展開する前段階の処理として実行される。
AvosLocker	セーフモードを利用して検出を回避する従来型の特性に加えて、アンチウイルス製品「Avast」のルートキット対策ドライバーを悪用してアンチウイルス製品を無効化する亜種が存在する。ランサムウェアを展開する前段階の処理として実行される。

④ AppGuard による HermeticWiper への対処

「HermeticWiper」はプロセスメモリ空間にロードされた正規のドライバー（パーティション管理ツール）を使用して、システムに存在するすべての物理ドライブに対してランダムデータを用いて最初の 512 バイトを上書きすることで MBR（Master Boot Record：HDD などの記憶領域の先頭にあり、起動時に最初に読み込まれる特殊な領域）を破壊すると共にデータが復元できないように、ファイルに関するすべての情報を保持する MFT（Master File Table：パーティション内のどこにどのようなファイルが存在しているかを記録したデータ領域）も破壊します。

「HermeticWiper」が端末内のどこに配備されるのかによって AppGuard の反応は変わりますが、ユーザープロファイル配下（C:\Users）であれば正規のコードサイニング証明書を保持していても起動が許可されることはありません。AppGuard の仕組みとして信頼できない領域（例：ユーザープロファイル配下）から実行ファイルを起動させたい場合、自組織において信頼できる発行元のコードサイニング証明書をリスト化し、そこに登録されたものと同じ証明書を持つ場合のみ起動が許可されます。「HermeticWiper」に付与された証明書の発行元である「Hermetica Digital Ltd.」は IT ベンダーではありません。従って、ユーザーが意図的にこの証明書を信頼される発行元に登録することは現実的にあり得ません。

では、Active Directory のグループポリシー等を通じてシステムフォルダ配下(C:\Windows 等) へ配備された場合はどうでしょうか。AppGuard の制御ポリシーにおいてシステムフォルダ配下は信頼できる領域として扱われるため起動制御は行われません。しかし、破壊活動を始める際にはドライバーの追加処理が必要となります。AppGuard は攻撃者が悪用する可能性があるアプリケーションやツールをハイリスクアプリケーションとして定義し、3 つの制御（レジストリの改ざん不可、システムフォルダへの変更処理不可、他アプリのメモリ読み書き不可）を強制適用します。そのため、ドライバーの追加処理を試みても、ドライバーの書き込みが成立しなくなるため、「HermeticWiper」のプロセスが強制終了することになります。

いずれのシナリオにおいても AppGuard 保護下では「HermeticWiper」の攻撃が成立しないことを確認しています。

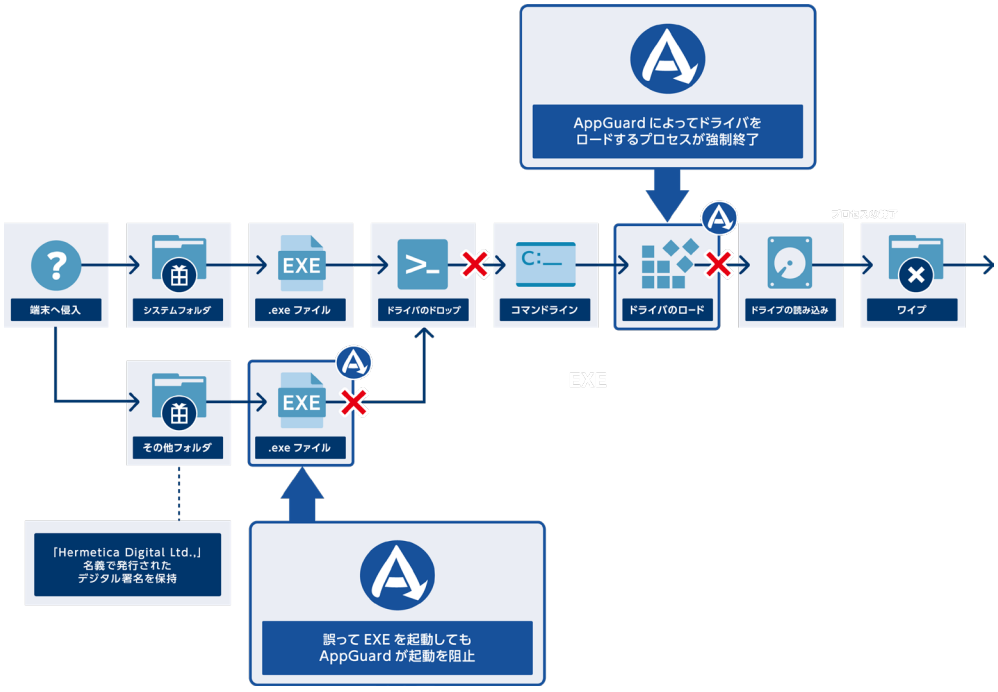


図　AppGuardがHermeticWiperを阻止するポイント

⑤ マルウェアにコードサイニング証明書を付与するサービスの存在
ハッカーフォーラム上では、マルウェアに有効なコードサイニング証明書を付与するサービス事業者が複数確認されています。このサービスを利用することで、攻撃者はマルウェアを「信頼できるファイル」として扱わせることができます。結果として、ブラウザに実装される SmartScreen やセーフブラウジング等をすり抜けたり、アンチウイルス製品等は実行しても問題ないと判断してしまう可能性があります。現時点では、このような非合法なサービスがどの程度活用されているのか等、定量的なデータがなく影響度合いは不明ですが、引き続き注視する必要があります。

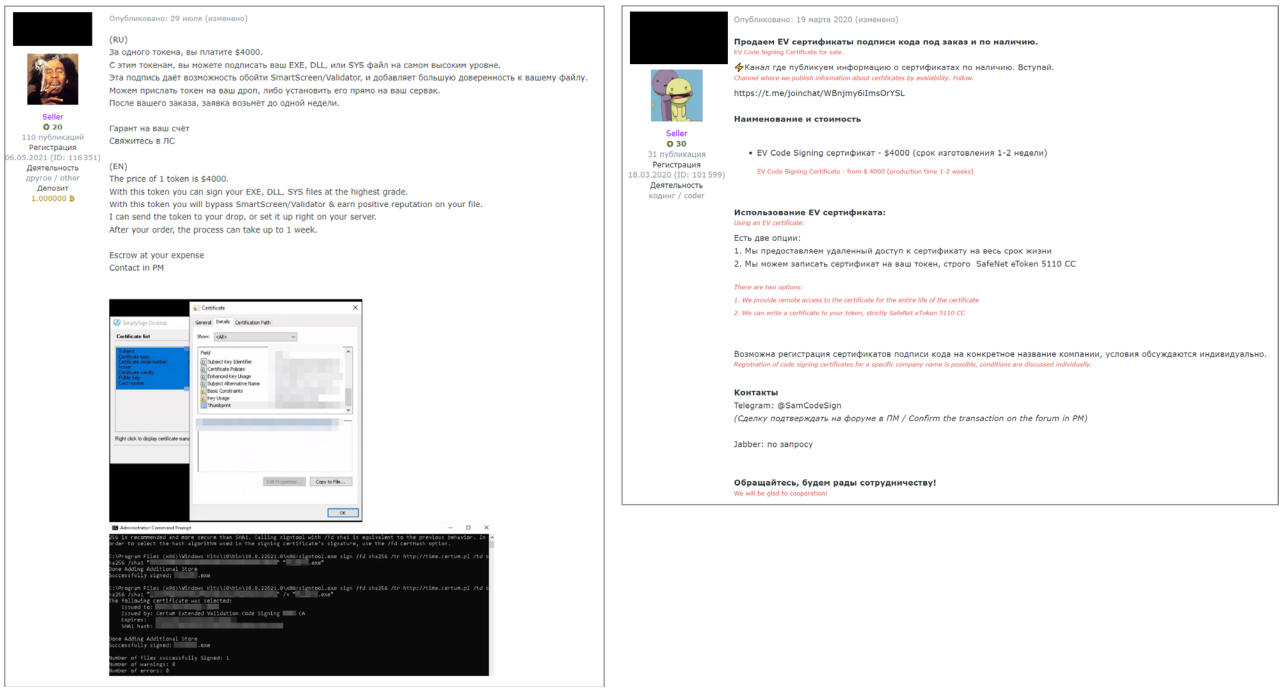


図　マルウェアにコードサイニング証明書を付与するサービスの宣伝

2 ソフトウェアサプライチェーン攻撃によるリスクの増大

アンチウイルス製品等、サイバー攻撃へ対抗するために様々な領域で AI 技術が使われ始めています。セキュリティ対策において AI 技術の活用は我々にとって脅威を退ける頼もしい存在ではあるものの、使い方次第では大きな脅威となり得ることを理解しておく必要があります。その 1 つに AI 技術を利用したファジング（Fuzzing）が挙げられます。

① AI ファジングとは
ファジング（Fuzzing）とは、対象となるシステムやアプリケーションに対して想定しない値（不正、無効、ランダム）を挿入することで意図的に例外を発生させることで潜在的なバグや脆弱性を見つけ出すテスト手法の 1 つです。AI ファジングはこの作業を自動化することによってテストの高速化や効率化を図っています。

② サイバー攻撃における人的要因の排除
AI ファジングは視点を変えれば特定のアプリケーションのゼロデイ脆弱性を発見する仕組みとして利用することも可能です。豊富な資金力を持つサイバー犯罪者であれば、HPC (High Performance Computing) による高性能な解析環境と AI ファジングを組み合わせることで攻撃に転用可能なゼロデイ脆弱性の発見を効率的に実現していくことができます。特にソフトウェアサプライチェーン攻撃に転用できるゼロデイ脆弱性が発見された場合、より大規模なインシデントが各所で引き起こされることが想定されます。

サイバー犯罪における収益性を高めていくことを考えるのであれば、高コストな人的リソースの消費を極力抑える必要があります。今後、サイバー犯罪者が AI 技術を積極的に活用する様になってくると、サイバー攻撃における人的要因の多くが排除され、より洗練された攻撃のフレームワークが構築される可能性があります。

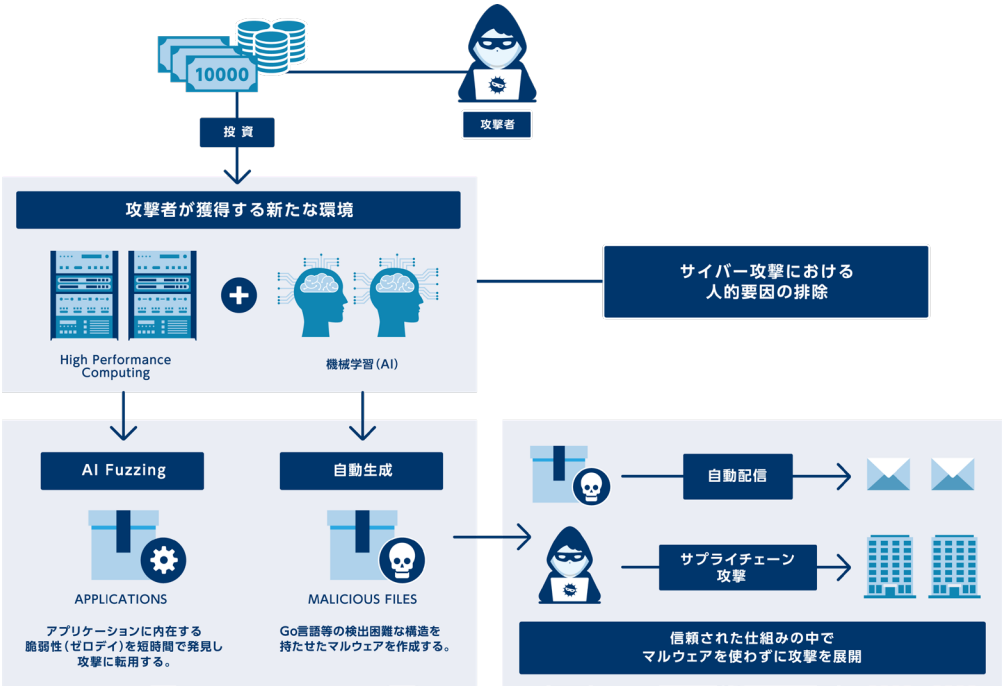


図　AI Fuzzingを利用したゼロデイ脆弱性の特定

③ ソフトウェアサプライチェーン攻撃とは
ソフトウェアサプライチェーン攻撃とはソフトウェアで利用されるコード、ライブラリ、サービス及び依存関係にあるサードパーティにおいて、悪意あるコードや処理を混入させることで当該ソフトウェアを利用するユーザーに対して合法的な処理プロセス上で攻撃を仕掛ける仕組みです。開発、配布、アップデートといったソフトウェアにおける一連の動作工程において展開されるため対処が困難であり、攻撃者にとって標的を直接攻撃するよりも容易に攻略が可能となります。

サイバー攻撃者は前述の AI ファジング等を利用して発見したゼロデイ脆弱性を悪用することで、ソフトウェアのサプライチェーンに脅威を忍ばせることが想定され

ます。その結果、ユーザーは当該ソフトウェアによってつながったサプライチェーンを通じた侵害リスクに晒されます。ソフトウェアサプライチェーン攻撃が脅威となるのは、利用ユーザーから見ると検出や対処が困難なこと以外に、それがインターネットに接続されているか否か関係なく攻撃を成立させられる可能性があることです。

まず、ソフトウェアサプライチェーン攻撃とは厳密には言えませんが、インターネットから隔絶された環境で動作する産業制御システム(ICS) におけるサプライチェーンを通じた攻撃事例として「Stuxnet」を紹介します。イランの原子力関連施設を破壊する目的で作成されたとされる「Stuxnet」は、攻撃対象施設で利用される制御システムに係わる事業者を通じてインターネットから隔絶されたネットワークへ侵入したことが 2010 年に発覚しています。攻撃者は攻撃対象施設と何らかの形で接続性を持つ事業者を入念に調べ上げて攻撃を仕掛けています。当初、リムーバルメディアを通じて侵入されたと指摘されていましたがシマンテックやカスペルスキーの調査によって、「Stuxnet」がコンパイルされた時間が関連事業者内で最初の感染が発生してから数時間前であることから物理的にリムーバルメディアを運ぶことが難しく、関連事業者と攻撃対象施設を結ぶ専用回線等を利用している可能性が高いことが推察されています。

また、2020 年に発生した「SolorWinds」、2021 年に発生した「Kaseya」といった構成管理やリモート管理を目的としたソフトウェアを悪用したソフトウェアサプライチェーン攻撃は世界中で大規模なインシデントを引き起こしたことは記憶に新しいところです。

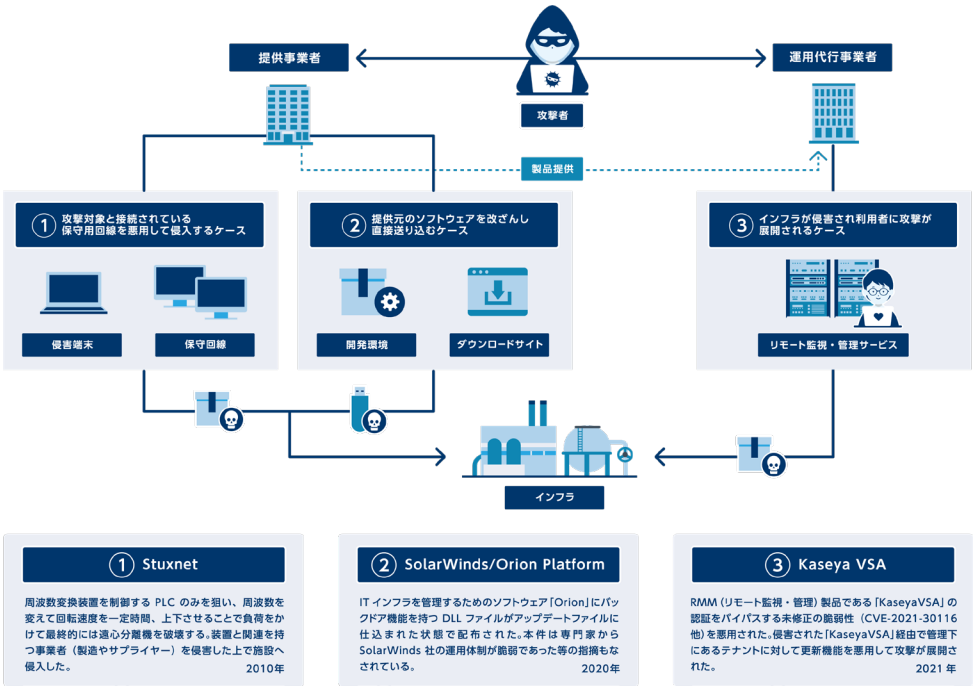


図　ソフトウェアサプライチェーン攻撃

自治体のネットワーク
三層分離構造とは
自治体では利用用途ごとにPCやネットワークを物理的(仮想的な構築ケースもある)に三つの層に分離しそれぞれが影響を与えない形でシステムを構成しています。この三層は以下で構成されます。
①インターネット接続系
自治体職員がインターネットに接続し日常業務を行うためのシステム群
② LG-WAN 接続系
各自治体の庁内 LAN を相互接続する LG-WAN に接続するためのシステム群
③個人番号(マイナンバー)利用系
個人番号にて管理する住民情報を取り扱うためのシステム群

前者においては、提供元である SolorWinds 社が持つ正規のアップロード認証資格が窃取され、同社の「Orion Platform」に係るマルウェアが仕込まれた不正なアップデートファイルが利用ユーザーに対して公開されています。後者においては、顧客の IT インフラをリモートで管理することができる「Kaseya VSA」の脆弱性を悪用しています。その特性上、利用ユーザーに対する管理者レベルのアクセス権限を持ち、配下の利用ユーザーにアップデート処理を装ってランサムウェアを配布されています。

前述の通り、ソフトウェアサプライチェーン攻撃を用いれば、外部から攻略が不可能と思われる様なネットワークであっても侵害できる可能性があります。例えば、日本の自治体が採用している三層分離の構造を持った堅牢なネットワークであっても、ソフトウェアの提供事業者や保守事業者を介することで閉域環境へ侵入することも理論上は可能となります。

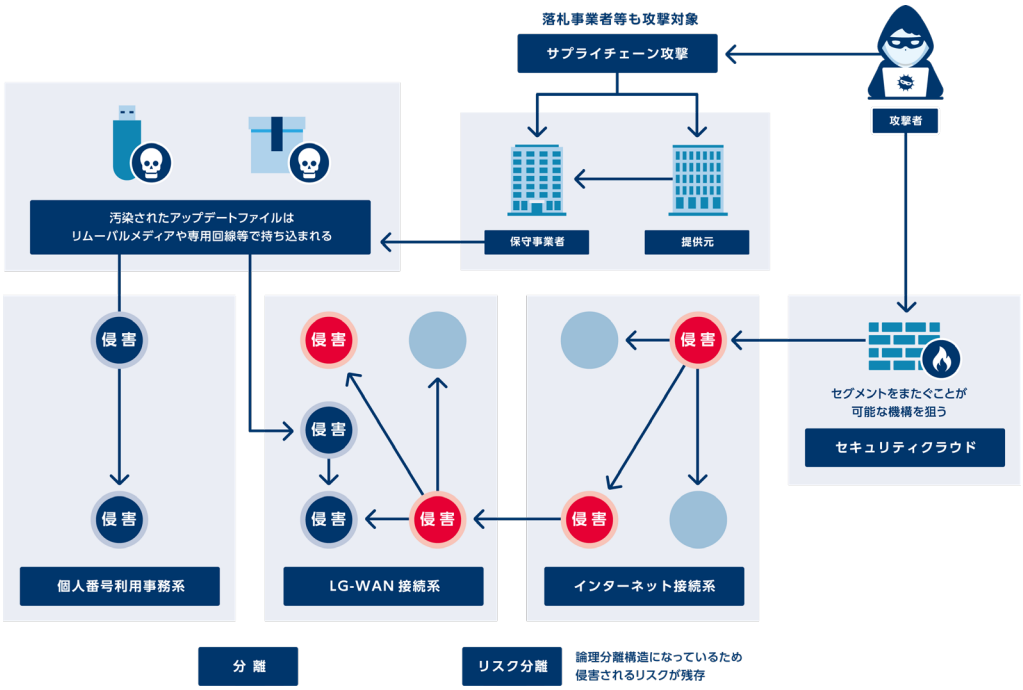


図　自治体の三層分離構造を持つネットワークを侵害する方法

これらの脅威に対して耐性を高めるためには、ソフトウェアの提供事業者やその運用代行事業者に対して、過去の惨事を踏まえて適切なセキュリティ対策や運用体制が構築され、適切に履行されていることに責任を持たせる必要があります。

また、現実的に脆弱性をゼロにする方法がない以上は、この様なリスクを受け入れた上で自組織においてソフトウェアサプライチェーン攻撃における活動の初期段階で検知・阻止できる環境を構築しなければならなくなります。

06.

エピローグ

06. エピローグ

サイバー犯罪において攻撃する側と攻撃される側には情報の非対称性があるため、攻撃される側は圧倒的に不利な状況にあります。しかし、デジタル空間においては攻撃を仕掛けるための予備調査はデジタル空間上で得られる情報を基に調査が行われます。つまり、ユーザーは圧倒的に不利な状況にはあるものの、攻撃者と同じ様にデジタル空間上で「自分たちは外からどのように見えているのか?どこが狙われるのか?」という情報を得ることが可能です。この特性を有効活用することが攻撃者と対峙する上では重要になると考えられます。

現在、サイバーセキュリティ市場で注目・推奨されている「有事」を意識した取り組みは「治療」にあたります。確かに自組織のサイバーセキュリティ戦略において必要な取り組みではありますが、それは起こった事象に対する対症療法でしかありません。根本的な解決を目的としていないため、「いたちごっこ」から抜けることは困難です。

医療の世界には疾患に対して対症療法と原因療法が存在し、状況に応じた適切な療法が選択されます。しかし、サイバーセキュリティの世界においては医療の世界と違って、その発生原因が明確です。また、それを攻撃者と同じ視点で見つけることが可能です。だからこそ、我々は平時の状態から IT インフラ環境の衛生状態を維持し、侵害の原因となる要因を取り除くことにまずは目を向けるべきだと考えます。

これまで見てきたようにサイバー攻撃が成立する多くの要因は、ユーザー側の小さな見落としや怠惰です。IT 化やデジタルトランスフォーメーションの推進を加速させるために、自組織のサイバーセキュリティ戦略を改めて見直し、より現実的かつ効果の上がるものとするために攻撃対象領域の管理（サイバー攻撃を受ける可能性のあるところの管理）を徹底して受動的なセキュリティ対策から能動的なセキュリティ対策へと変革していくことが推奨されます。

Author:
Yusuke Shigihara

Editor:
Kenta Okumura
Kiyomi Sakai
Toshiro Arahata
Yujiro Natsume

Director:
Hirotaka Sakajiri

Designer:
Ai Yamanashi

Sponsor:
Blue Planet-works

Special Thanks to...
Stonebeat Security, Inc.
IT Guard Corporation

テクノロジーの力で、
すべての人をセキュリティリスクから解放し、
安心してつながれる世界をつくる。

株式会社Blue Planet-works

〒141-0032
東京都品川区大崎4-1-2 ウィン第２五反田ビル三階

P. 03-6825-1891
E. tmc@blueplanet-works.com
www.blueplanet-works.com