二重脅迫型ランサムウェアに対するアンチウィルスソフトおよびEDRの振る舞い検知機能の評価

谷崎 俊介[1,a)]　Yin Minn Pa Pa[2,b)]　吉岡 克成[2,3,c)]　松本 勉[2,3,d)]

概要：二重脅迫型ランサムウェアは，感染者からファイルへのアクセスを奪うだけでなく，感染者の端末からファイルを盗み，身代金を支払わなければファイルを公開したり売ったりするといった脅しを行う．バックアップを取っていれば暗号化されたファイルや削除されたファイルは元に戻せるかもしれないが，データ流出はなかったことにできないという観点から考えると，組織や個人にとって二重脅迫型ランサムウェアは非常に脅威である．ランサムウェアへの対策の 1 つとして，アンチウィルスソフト (AV) や Endpoint Detection and Response (EDR) などのセキュリティ製品がある．これらのセキュリティ製品はパターンマッチによる既知のマルウェアの検知だけでなく，不審な振る舞いを検知する機能により未知のマルウェアも検知可能であると言われている．大量のファイルの暗号化や外部送信などの特徴的な振る舞いを示す二重脅迫型ランサムウェアに対してもこれらの振る舞い検知の機能が有効に働くことが期待される．本稿では，二重脅迫型ランサムウェアの特徴であるファイルの外部送信とファイルの暗号化，ファイルの削除に着目し，AV や EDR がこれらの振る舞いを検知し阻止できるのかを調査した．7 つの AV と 1 つの EDR を調査対象とし，製品をインストールした環境で，自作した 11 種類のランサムウェア (テスト検体) を実行した．その結果，ファイルの外部送信を検知，阻止できたセキュリティ製品は存在しなかった．また，ファイルの暗号化やファイルの削除を検知，阻止できたセキュリティ製品は多くても 1 つか 2 つ程度だった．以上のことから，AV や EDR はランサムウェアに対して十分な振る舞い検知の能力を有しているとは必ずしも言えないことがわかった．

キーワード：ランサムウェア, 二重脅迫, アンチウィルス, EDR, 検知

Evaluating the Behavior Detection Functionality of Antivirus and EDR against Double Extortion Ransomware

Shunsuke Tanizaki[1,a)]　Yin Minn Pa Pa[2,b)]　Katsunari Yoshioka[2,3,c)]　Tsutomu Matsumoto[2,3,d)]

Abstract: Double extortion ransomware is a type of ransomware that exfiltrates victim's files in addition to encrypting them or deleting them and threatens to release or sell them unless a ransom is paid. While backups may allow for file recovery, the fact that a data breach cannot be undone suggests that double extortion ransomware is a significant threat to organizations and individuals. Endpoint security products such as antivirus (AV) and endpoint detection and response (EDR) are countermeasures against ransomware. These security products are designed to detect not only known malware by pattern matching, but also unknown malware by detecting suspicious behavior. It is expected that these behavior detection features will be effective against double extortion ransomware. In this paper, we evaluate seven AVs and one EDR against double extortion ransomware's behavior such as file exfiltration, file encryption and file deletion. We developed custom ransomware (test samples) and executed them in the environments where AVs and EDR were installed. As a result, no products were able to detect or prevent file exfiltration and more than half of the products failed to detect or prevent file encryption and file deletion. From the above, it can be said that AV and EDR do not necessarily have sufficient behavior detection capability against ransomware.

Keywords: Ransomware, Exfiltration, Antivirus, EDR, Detection

1. はじめに

ランサムウェア攻撃は変化し続けており，ファイルの暗号化を行って身代金を要求する従来のランサムウェアに加え，二重，三重，四重の脅迫を行うランサムウェアが脅威となっている．二重脅迫型ランサムウェアは，ファイルを暗号化したり削除したりして感染者からファイルへのアクセスを奪うだけでなく，感染者の端末からファイルを盗み，身代金を支払わなければファイルを公開したり売ったりするといった脅しを行う．二重脅迫型ランサムウェアによる被害は 2019 年に始まったと言われている [1]．また，警察庁の資料 [2] によると，企業・団体等におけるランサムウェアの被害件数は 2020 年下半期から 2022 年下半期まで常に増加しており，2022 年のランサムウェア被害 230 件のうち二重脅迫型ランサムウェアによる被害は全体の 65% (119 件) を占めているという．バックアップを取っていれば暗号化されたファイルや削除されたファイルは元に戻せるかもしれないが，データ流出はなかったことにできないという観点から考えると，組織や個人にとって二重脅迫型ランサムウェアは非常に脅威である．さらに，二重脅迫型ランサムウェアの被害に遭うと，サービス妨害攻撃を行って身代金を要求する三重脅迫型ランサムウェアや，盗まれた情報の持ち主である顧客や患者，ビジネスパートナーなどの第三者にも身代金を要求する四重脅迫型ランサムウェアの被害に繋がる可能性がある [3]．三重，四重と被害を拡大させないためにも，二重脅迫型ランサムウェアの被害を防ぐことは重要である．

ランサムウェアへの対策の 1 つとして，アンチウィルスソフト (AV) や Endpoint Detection and Response (EDR) などのセキュリティ製品がある．これらのセキュリティ製品はパターンマッチによる既知のマルウェアの検知だけでなく，不審な振る舞いを検知する機能により未知のマルウェアも検知可能であると言われている．大量のファイルの暗号化や外部送信などの特徴的な振る舞いを示す二重脅迫型ランサムウェアに対してもこれらの振る舞い検知の機能が有効に働くことが期待される．

本稿のリサーチクエスチョン (RQ) は以下である．

RQ： AV/EDR の振る舞い検知の機能は二重脅迫型ランサムウェアに対してどの程度有効か

上記の RQ に答えるために，二重脅迫型ランサムウェアの特徴であるファイルの外部送信とファイルの暗号化，ファイルの削除に着目し，AV や EDR がこれらの振る舞いを検知し阻止できるのかを調査した (実験 1)．7 つの AV と 1 つの EDR を調査対象し，製品をホスト 1 台にインストールした状態で，自作した 11 のランサムウェア (テスト検体) を実行した．その結果，ファイルの外部送信を検知，阻止できたセキュリティ製品は存在しなかった．また，ファイルの暗号化やファイルの削除を検知，阻止できたセキュリティ製品は多くても 1 つか 2 つ程度だった．

実験 1 の方法では性能評価できるセキュリティ製品の数に限りがあるため，作成した 11 のテスト検体を VirusTotal[4] へアップロードし，約 70 のベンダーによる検知率の変化を観測した (実験 2)．VirusTotal 上の検知率を 1 か月間観測した結果，検知率が大きく上昇した検体と，あまり上昇しなかった検体の存在を確認した．実験 2 の結果から，ファイルの暗号化や削除のみを行うランサムウェアより，ファイルの暗号化や削除に加えてファイルの外部送信を行う二重脅迫型ランサムウェアの方が検知されにくいのではないかという仮説が得られた．

以下，本稿による貢献である．

1) 自作したテスト検体 (未知の二重脅迫型ランサムウェア) を用いて AV/EDR の振る舞い検知能力を評価したのは本稿が初である．
2) 本稿の実験により AV や EDR はランサムウェアに対して十分な振る舞い検知の能力を有しているとは必ずしも言えないことがわかり，AV や EDR などのセキュリティ製品の弱点を把握することができた．
3) ファイルの暗号化のみを行う従来のランサムウェアよりも，二重脅迫型ランサムウェアの方が検知されにくいのではないかという仮説が得られた．

以下，本稿の構成である．2 章では，関連研究について述べる．3 章では，実験 1 と実験 2 の方法について述べる．4 章では，実験 1 と実験 2 の結果について述べる．5 章では，考察を行う．最後に 6 章でまとめを行う．

2. 関連研究

2.1 MITRE Engenuity ATT&CK Evaluations

MITRE Engenuity ATT&CK Evaluations[5] とは，MITRE 社が行っているセキュリティ製品の性能評価である．EDR などのセキュリティ製品がインストールされた環境に対して，実際のサイバー攻撃者グループを模倣した攻撃を行うことで，製品の性能評価を行う．今までに模倣された攻撃グループは，APT3，APT29，Carbanak，FIN7，Triton，Wizard Spider，Sandworm Team である．

[1] 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University
[2] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[3] 横浜国立大学大学院環境情報研究院
Faculty of Environment and Information Sciences, Yokohama National University
[a)] tanizaki-shunsuke-kg@ynu.jp
[b)] yinminn-papa-jp@ynu.ac.jp
[c)] yoshioka@ynu.ac.jp
[d)] tsutomu@ynu.ac.jp

性能評価のために模倣される攻撃の過程でファイルやデータを持ち出す Exfiltration が行われたこともあるが，テキストファイルや画像，ログファイルなどの Exfiltration を行うことが多く，どれも持ち出すデータを狙い撃ちした小規模な Exfiltration である．本稿で行う AV/EDR の性能評価の実験では，大量のファイルの Exfiltration を行うランサムウェアの振る舞いに焦点を合てており，ホストに存在する合計約 5GB のファイルを手当たり次第に外部送信するテスト検体を用いる．その点が，MITRE Engenuity ATT&CK Evaluations と本稿の実験の違いである．

2.2 初期侵入用マルウェアを用いた EDR の性能評価

関連研究 [6] では，初期侵入用のマルウェアを用いて 11 の EDR の性能評価を行っている．EDR を 1 台のホストにインストールし，Cobalt Strike のビーコンと呼ばれる初期侵入用のマルウェアの実行に成功するか否かをテストしている．CPL, HTA, EXE, DLL の 4 種類の初期侵入用マルウェアを用いて実験を行っており，4 つのマルウェアすべてを防ぐことができた EDR は存在しなかった．本稿は初期侵入用のマルウェアではなくランサムウェアのテスト検体を用いて実験を行う．また，本稿では企業向けの製品である EDR のテストも行うが，7 つの AV と 1 つの EDR を性能評価の対象としており，AV の性能評価が中心である．

2.3 ランサムウェアの振る舞い検知の性能評価

関連研究 [7] では，ファイルの暗号化を行うランサムウェアを用いて，5 つの商用 AV と 2 つの学術的なランサムウェア対策製品をテストしている．Farfel と呼ばれるランサムウェア対策製品のテストのためのフレームワークを開発しており，セキュリティ製品の性能評価に使用できるランサムウェアのサンプルを自動生成することができる．1536 のランサムウェアのテスト検体を用いて実験を行ったところ，CryptoDrop[8] と呼ばれる学術的なランサムウェア対策製品は 1536 のうち約 78%(1202 個) のテスト検体を検知できた．一方，すべてのテスト検体を検知することができなかった商用 AV が 3 つあった．本稿はファイルの暗号化を行うランサムウェアだけでなく，ファイルの暗号化とファイルの外部送信を行う二重脅迫型ランサムウェアのテスト検体を用いて実験を行う．

3. 実験手法

本稿のリサーチクエスチョン (RQ) は以下である．

RQ： AV/EDR の振る舞い検知の機能は二重脅迫型ランサムウェアに対してどの程度有効か

上記の RQ に答えるために，二重脅迫型ランサムウェアの特徴であるファイルの外部送信とファイルの暗号化，ファイルの削除に着目し，AV や EDR がこれらの振る舞いを検知し阻止できるのかを調査した (実験 1)．AV/EDR が未知のランサムウェアに対応できるのかを調査するために，実際の攻撃者が作成したランサムウェアを用いるのではなく，実験のために 11 のランサムウェアのテスト検体を作成した．また，静的解析の結果ではなくランサムウェアの実行を検知，阻止できるのかを確認するために，1 台の Windows のホストに AV/EDR をインストールした環境でテスト検体を実行し，実験 1 を行った．実験 1 では，7 つの AV と 1 つの EDR を調査対象した．

実験 1 の方法では性能評価できるセキュリティ製品の数に限りがあるため，作成した 11 のテスト検体を VirusTotal[4] へアップロードし，約 70 のベンダーによる検知率の変化を観測した (実験 2)．

本章では，テスト検体，性能評価対象の AV/EDR 製品，実験環境，外部送信・暗号化・削除対象のファイル，実験 1 と実験 2 の方法について述べる．

3.1 テスト検体

実験 1 と実験 2 に用いる 11 のランサムウェアのテスト検体を Python で作成した．表 1 はテスト検体の検体名と動作内容，ソースコードの行数である．ソースコードの行数は，コメントと空行を取り除いた値である．

ファイルの外部送信の方法は 3 種類あり, HTTPS, FTP, Dropbox[9] を用いてファイルを流出させる方法を実装した．HTTPS を用いたファイルの外部送信では，HTTPS サーバーに POST メソッドでファイルをアップロードする．HTTPS サーバーを用意する際，取得したドメインを Amazon Lightsail[10] の Ubuntu 22.04 LTS に割り当て，SSL 証明書については Let's Encrypt[11] を利用した．FTP を用いたファイルの外部送信では，FTP サーバーにログインし，ファイルをアップロードする．HTTPS サーバーと同様に，取得したドメインを Amazon Lightsail の Ubuntu 22.04 LTS に割り当て，FTP サーバーを用意した．FTP サーバーへのログインに必要なユーザー名とパスワードはソースコードに含まれている．Dropbox を用いたファイルの外部送信では，Dropbox の API を使用し，Dropbox のストレージにファイルをアップロードする．

ファイルの暗号化は AES (Advanced Encryption Standard) 暗号で行う．また，AES 鍵を攻撃者の RSA (Rivest–Shamir–Adleman) 暗号の公開鍵で暗号化することにより，RSA 秘密鍵を持つ攻撃者のみがファイルを復号化できるような仕組みにしている．ファイル暗号化のアルゴリズムは以下の通りである．

1. ランダムな AES 鍵を生成
2. AES 鍵でファイルを暗号化
3. AES 鍵を攻撃者の RSA 公開鍵で暗号化
4. 暗号化した AES 鍵をファイルの末尾に追加

表 1 テスト検体の検体名と動作内容，ソースコードの行数

検体名	検体の動作	ソースコードの行数
mal-https	HTTPS サーバーにファイルを送信する	56
mal-https-enc	HTTPS サーバーにファイルを送信したのち，ファイルを暗号化する	107
mal-https-del	HTTPS サーバーにファイルを送信したのち，ファイルを削除する	80
mal-ftp	FTP サーバーにファイルを送信する	94
mal-ftp-enc	FTP サーバーにファイルを送信したのち，ファイルを暗号化する	149
mal-ftp-del	FTP サーバーにファイルを送信したのち，ファイルを削除する	122
mal-dbx	Dropbox のストレージにファイルを送信する	76
mal-dbx-enc	Dropbox のストレージにファイルを送信したのち，ファイルを暗号化する	133
mal-dbx-del	Dropbox のストレージにファイルを送信したのち，ファイルを削除する	95
mal-enc	ファイルを暗号化する	75
mal-del	ファイルを削除する	48

ファイルの削除については，ファイルの中身をすべて空バイトで埋めてからファイルを削除する．ただ単にファイルを削除すると，ハードウェアにファイルの中身が残ったままとなりファイルが復元可能な場合がある．ファイルの削除前にファイルの中身をすべて空バイトで埋めるのは，ファイルの復元を防ぐためである．

ランサムウェア攻撃では，バックアップの削除やインストールなどの管理者権限が必要な処理が行われることがあるが，本稿の実験で用いるテスト検体はそのような処理は行わない．管理者権限が必要な処理は行わないため，テスト検体は Medium Integrity で実行されることを想定している．Windows の Integrity とは，プロセスやオブジェクトのアクセス制御に用いられるもので，Low，Medium，High，System などのレベルが存在する．標準ユーザーやローカル管理者が EXE ファイルを実行すると，通常 Medium Integrity でプロセスが実行される．ソフトウェアをインストールする際などは，プロセスは High Integrity で実行される必要があり，管理者権限を要求するプロンプトが画面に出てくる．

完成した Python スクリプトは，Pyarmor[12] を用いて難読化を施し，PyInstaller[13] で実行ファイルに変換した．今回の実験ではコード署名は行わなかった．

3.2 AV/EDR 製品

性能評価の対象として AV/EDR を選んだ方法について述べる．実験 1 に用いた AV/EDR 製品はすべて商用のセキュリティ製品であり，Web 上の製品の説明に「ランサムウェアからエンドポイントを保護する」などの記述があることを前提に実験対象の製品を選んだ．さらに，インターネットで情報収集を行い，マーケットシェアが高い製品や，性能が高いと評判の製品に絞り込み，最終的に 7 つの AV と 1 つの EDR を実験対象として選んだ．なお，本稿ではセキュリティ製品の名前やベンダーの名前は公表しない．

3.3 実験環境

1 台のノートパソコンで実験を行った．OS は Windows 10 Pro 64bit である．ローカル管理者の権限を持つユーザー Bob を作成し，Medium Integrity のレベルでランサムウェアの実行を行った．このマシンはインターネットに接続されており，攻撃者が管理する HTTPS サーバーや FTP サーバー，Dropbox のクラウドストレージにアクセス可能となっている．

3.4 外部送信・暗号化・削除対象のファイル

以下のユーザーフォルダ内にあるすべてのファイルを外部送信の対象とした．合計 1555 ファイル，228 フォルダ，5.04GB である．PDF や画像や音声，動画などの一般ユーザーが使用するようなファイルをインターネットから集めた．また，GitHub[14] の public リポジトリをいくつかダウンロードした．表 2 は拡張子別のファイル数，ファイルサイズの合計，全体に対して占める割合 (ファイルサイズ) である．ファイル数が上位 15 位の拡張子のみを表示している．表 2 を見ると，PDF，mp3，mp4 が 5.04GB のファイルのうち，約 95%を占めていることがわかる．

約 5GB のファイルの外部送信にかかる時間は，HTTPS で 2〜3 分，FTP で 6〜7 分，Dropbox で 11〜12 分である．

- C:\Users\Bob\Desktop
- C:\Users\Bob\Documents
- C:\Users\Bob\Downloads
- C:\Users\Bob\Music
- C:\Users\Bob\Pictures
- C:\Users\Bob\Videos

上記に加え，Outlook と Thunderbird のメールを盗む目的で，以下のフォルダ内にあるすべてのファイルも外部送信の対象とした．これらのファイルを盗まれた場合，メールの中身も全て見られてしまう．

- C:\Users\Bob\AppData\Local\Microsoft\Outlook

表 2 外部送信・暗号化・削除対象のファイル
(ファイル数が上位 15 位の拡張子のみ表示)

拡張子	ファイル数	ファイルサイズの合計 (Bytes)	全体に対して占める割合
pdf	345	961,497,433	17.7 %
js	268	494,877	0.0 %
mp3	217	1,135,212,134	20.9 %
md	80	720,698	0.0 %
mp4	75	3,053,566,556	56.3 %
py	67	966,534	0.0 %
png	65	41,389,736	0.8 %
docx	63	18,120,448	0.3 %
jpg	57	42,047,946	0.8 %
xlsx	55	15,247,208	0.3 %
json	43	2,111,089	0.0 %
yaml	37	101,630	0.0 %
pptx	14	51,967,442	1.0 %
css	12	4,768	0.0 %
sh	12	40,459	0.0 %

- C:\Users\Bob\AppData\Roaming\Thunderbird

ファイルの暗号化と削除に関しては，ユーザーフォルダ内のファイルのみを対象とした．

3.5 AV/EDR の性能評価実験 (実験 1) の方法

図 1 の方法で AV/EDR の性能評価の実験 (実験 1) を行った．AV/EDR を 1 つずつインストールし，性能評価を行う．AV/EDR のインストール後，特に製品の設定は行わず，デフォルトの設定のまま実験を行った．次に，製品をインストールした環境に 11 のテスト検体を 1 つずつダウンロードし実行する．テスト検体の実行が終わるまで，あるいは AV/EDR がテスト検体の実行を検知し阻止するまで待機する．ファイルの暗号化や削除を行うテスト検体を実行した場合，次のテスト検体へ進む前にファイルを元に戻す．すべてのテスト検体を実行し終えたら，インストールしていた製品をアンインストールし，次の製品の性能評価を行う．

実験 1 は 2023 年 7 月 23 日に行った．長期間に渡って実験を行った場合，実験期間中にテスト検体がセキュリティベンダー間で共有されて実験結果に影響を及ぼす可能性があるため，すべての AV/EDR の性能評価を一日以内に済ませた．

3.6 VirusTotal 上の検知率の観測実験 (実験 2) の方法

表 1 の 11 のランサムウェアのテスト検体を 2023 年 7 月 23 日に VirusTotal へアップロードし，2023 年 8 月 22 日までの 1 か月間，検知率の変化を観測した (実験 2)．毎日テスト検体の再解析を行い，値を更新した．

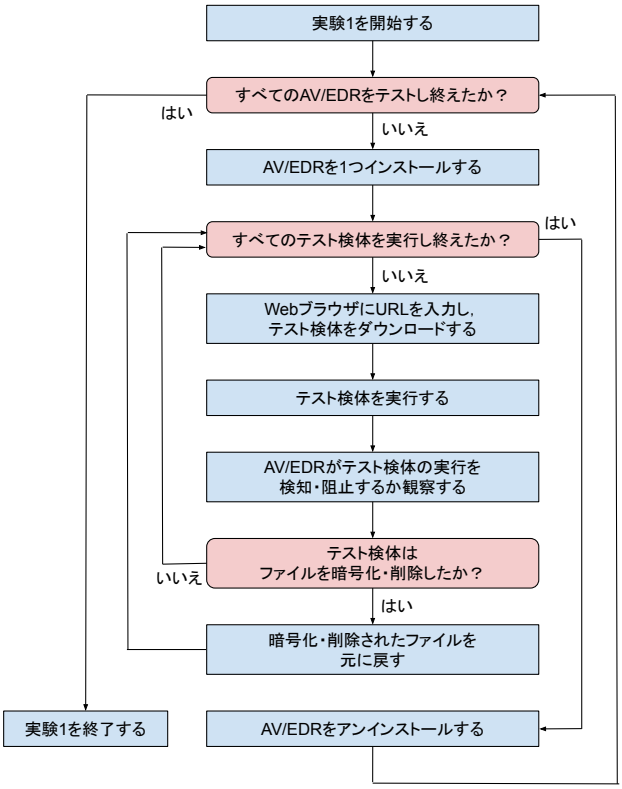

図 1 実験 1 のフローチャート

4. 実験結果

4.1 AV/EDR の性能評価実験 (実験 1) の結果

3.5 節で述べた方法で実験を行い，AV/EDR の性能評価の実験 (実験 1) を行った．表 3 は実験 1 の結果である．AV1〜AV7 はアンチウイルスソフトを意味している．○はテスト検体の実行を検知し，阻止できたことを意味する．× は検知も阻止もできなかったことを意味する．SD は Signature Detection (シグネチャ検知) の略で，テスト検体のダウンロード直後に検知され，実行ができなかったことを意味する．表 3 の 1 つのセル内に ○ や × が 2 つあるものについては，左側の ○ や × はファイルの外部送信を，右側の ○ や × はファイルの暗号化あるいは削除を検知，阻止できたかを表している．

すべての AV と EDR のうち，ファイルの外部送信を行う段階でテスト検体の実行を検知し阻止することはできたものは存在しなかった．

7 つのうち 3 つの AV（AV1〜AV3）と EDR はどのテスト検体に対しても検知，阻止できなかった．

7 つのうち 2 つの AV（AV4 と AV5）は，一部のテスト検体のシグネチャ検知に成功しているが，振る舞い検知によって検知，阻止できたテスト検体は一つも存在しなかった．

AV6 については，ファイルの暗号化機能を持つテスト検体 (mal-https-enc, mal-ftp-enc, mal-dbx_enc, mal-enc) の

検知，阻止を行うことができた．ファイルの外部送信を行う段階では何も検知しなかったが，ファイルの外部送信が終わりファイルが暗号化され始めるとテスト検体のプロセスが終了させられた．

AV7 については，ファイルの暗号化機能を持つテスト検体 (mal-https-enc, mal-ftp-enc, mal-dbx-enc, mal-enc) に加え，ファイルの削除を行うテスト検体（mal-https-del, mal-dbx-del）の検知，阻止に一部成功していることがわかる．

以上の結果から，ランサムウェアのテスト検体を検知，阻止できた AV はいくつかあったものの，AV や EDR はランサムウェアに対して十分な振る舞い検知の能力を有しているとは必ずしも言えないことがわかった．

4.2 VirusTotal 上の検知率の観測実験 (実験 2) の結果

表 1 の 11 のランサムウェアのテスト検体を 2023 年 7 月 23 日に VirusTotal へアップロードし，2023 年 8 月 22 日までの 1 か月間，約 70 種類のベンダーによる検知率の変化を観測した．毎日テスト検体の再解析を行って値を更新した結果，図 2 のように検知率が変化した．図 2 を見ると，どの検体もアップロードしてから約 2 週間の期間に検知率が上昇し，それ以降の検知率の変化は小さくなっていることがわかる．また，検知率の上昇の仕方にはばらつきがあり，検知率が大きく上昇した検体とあまり上昇しなかった検体が存在することがわかる．FTP によるファイルの外部送信を行うテスト検体 (mal-ftp, mal-ftp-enc, mal-ftp-del) と，ファイルの暗号化のみを行うテスト検体 (mal-enc)，ファイルの削除のみを行うテスト検体 (mal-del) については，検知率の大きな上昇が見られた．それ以外のテスト検体に関しては，検知率に大きな変化は見られなかった．FTP によるファイルの外部送信を行うテスト検体の検知率が上昇したのは，FTPS ではなく FTP を使用した通信を行っていることが原因の可能性があり，テスト検体に含まれるランサムウェアの振る舞いが原因ではないかもしれない．しかし，ファイルの暗号化のみを行うテスト検体 (mal-enc) とファイルの削除のみを行うテスト検体 (mal-del) の検知率が上昇したのは，検知すべき対象だとセキュリティベンダーが判断したからだと考える．検知率があまり上昇しなかった検体は，HTTPS によるファイルの外部送信を行うテスト検体 (mal-http, mal-http_enc, mal-http_del) と Dropbox によるファイルの外部送信を行うテスト検体 (mal-dbx, mal-dbx_enc, mal-dbx_del) である．これらの検体は mal-enc や mal-del と同様にファイルの暗号化やファイルの削除を行うにも関わらず，検知率は上昇しなかった．もしこれらの結果が偶然ではないのであれば，ファイルの暗号化や削除のみを行うランサムウェアより，ファイルの暗号化や削除に加えてファイルの外部送信を行うランサムウェアの方が検知されにくいと言える．つまり，通常のランサムウェアよりも二重脅迫型ランサムウェアの方が検知されにくいのではないかという仮説が得られる．しかし，サンプル数が少なく断定はできない．仮説を裏付けるためには，テスト検体の数を増やし，長期間に渡って検体のアップロードと検知率の観測を行う必要があると考える．

5. 考察

本稿の実験 1 で 7 つの AV と 1 つの EDR の性能評価を行った結果，ファイルの暗号化やファイルの削除の検知，阻止ができたセキュリティ製品は多くても 1 つか 2 つ程度だった．検知できている製品が存在するため，ファイルの暗号化やファイルの削除の検知は不可能ではないはずである．今回の実験で検知できなかった半数以上の製品の改善に期待したい．

本稿の実験 1 で性能評価を行った AV/EDR の中には，ファイルの外部送信を振る舞い検知によって阻止できた製品は存在しなかった．これは悪い結果のように見えるが，ファイルの外部送信が阻止すべき振る舞いかどうかは状況によって異なり，常に阻止すべきというわけではない．例えば，Google Drive[15] や Dropbox などのクラウドストレージにファイルをアップロードしたり，GitHub にファイルをプッシュしたりなど，ユーザーは日々のタスクにおいてもファイルの外部送信を行う．ファイルの外部送信を検知しようとすると誤検知が増え，ユーザーの利便性を大きく損なう可能性があるため，そもそもセキュリティベンダーはファイルの外部送信を検知すべき対象と認識していない可能性がある．本稿の実験で VirusTotal における検知率があまり上昇しなかったテスト検体は，セキュリティベンダーによって検知すべき対象として認識されなかった可能性がある．しかし，ファイルの外部送信を行う二重脅迫型ランサムウェアが脅威であることに変わりはなく，何らかの方法でファイルの流出を防ぐ必要がある．ファイルの暗号化や削除，外部送信を行うランサムウェアへの根本的な対策として，ランサムウェアがファイルにアクセスできないようにするという方法がある．例えば，Qubes OS[16] などの Isolation 技術を使用すれば，攻撃者やマルウェアがファイルにアクセスできる機会は少なくなる．Isolation などの根本的な対策を行いつつ，AV/EDR などのセキュリティ製品も使用する，といった対策が良いのではないかと考える．

VirusTotal 上の検知率の観測を行った実験 2 の結果については，懸念事項がある．VirusTotal 上における検知率があまり上昇しないテスト検体があったが，それはセキュリティベンダーがテスト検体に注目しておらず，テスト検体の解析すらしていなかったことが原因なのではないかという懸念である．セキュリティベンダーによるインシデントレポートで紹介されるようなマルウェアは優先的に解析すべき検体であり，セキュリティベンダーによっては，解析

表 3　テスト検体に対する AV/EDR の性能評価実験の結果

	mal-https	mal-https-enc	mal-https-del	mal-ftp	mal-ftp-enc	mal-ftp-del	mal-dbx	mal-dbx-enc	mal-dbx-del	mal-enc	mal-del
AV1	×	×, ×	×, ×	×	×, ×	×, ×	×	×, ×	×, ×	×	×
AV2	×	×, ×	×, ×	×	×, ×	×, ×	×	×, ×	×, ×	×	×
AV3	×	×, ×	×, ×	×	×, ×	×, ×	×	×, ×	×, ×	×	×
AV4	×	×, ×	×, ×	×	×, ×	×, ×	SD	×, ×	×, ×	×	×
AV5	×	×, ×	×, ×	SD	×, ×	SD	×	×, ×	×, ×	×	SD
AV6	×	×, ○	×, ×	×	×, ○	×, ×	×	×, ○	×, ×	○	×
AV7	×	×, ○	×, ○	×	×, ○	×, ×	×	×, ○	×, ○	○	×
EDR	×	×, ×	×, ×	×	×, ×	×, ×	×	×, ×	×, ×	×	×

○：テスト検体の実行を検知し阻止できた，×：テスト検体の実行に対して何もしなかった
SD：Signature Detection (ダウンロード直後に検知され，テスト検体を実行できなかった)

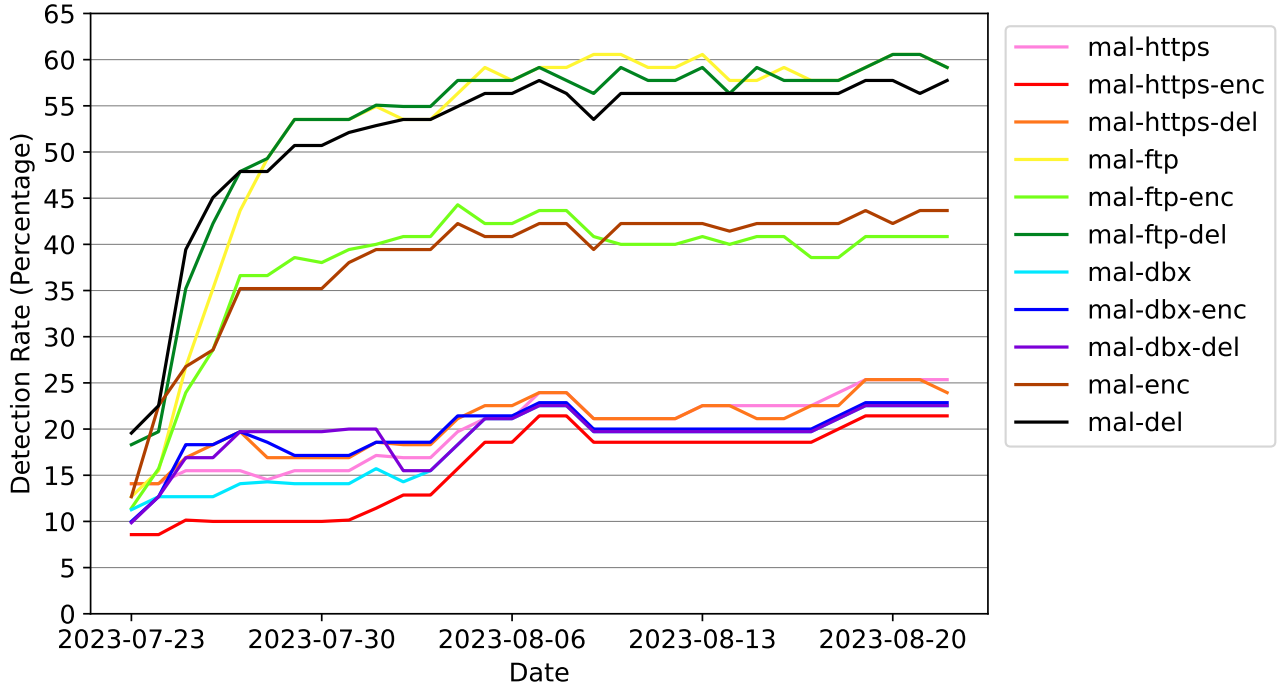

図 2　VirusTotal 上におけるテスト検体の検知率の変化 (実験 2 の結果)

すべきマルウェアが山積みとなっている可能性がある．本稿の実験で使用したテスト検体は，VirusTotal に毎日アップロードされる多数の検体のうちのほんの一部に過ぎず，埋もれてしまった可能性がある．実際のサイバー攻撃に用いられるランサムウェアをセキュリティ製品が検知するのかを観測するのが望ましいため，本稿の実験 2 の結果は適切でない可能性がある．

6. おわりに

本稿では，二重脅迫型ランサムウェアの特徴であるファイルの外部送信とファイルの暗号化，ファイルの削除に着目し，AV や EDR がこれらの振る舞いを検知し阻止できるのかを調査した．7 つの AV と 1 つの EDR を調査対象とし，製品を 1 台の Windows のホストにインストールした環境で，自作した 11 のランサムウェアのテスト検体を実行した．その結果，ファイルの外部送信を検知，阻止できたセキュリティ製品は存在しなかった．また，ファイルの暗号化やファイルの削除を検知，阻止できたセキュリティ製品は多くても 1 つか 2 つ程度だった．以上のことから，AV や EDR はランサムウェアに対して十分な振る舞い検知の能力を有しているとは必ずしも言えないことがわかった．また，作成したテスト検体を VirusTotal にアップロードしたところ，検知率が大きく上昇した検体とあまり上昇しない検体が存在した．ファイルの暗号化や削除のみを行うテスト検体より，ファイルの暗号化や削除に加えてファイルの外部送信を行うテスト検体の方が検知されにくい結果となった．このことから，通常のランサムウェアよりも二重脅迫型ランサムウェアの方が検知されにくいのではないかという仮説が得られた．しかし，実験に用いたテスト検体の数は 11 と少なく仮説の立証はできない．また，5 章で述

べたように，セキュリティベンダーがテスト検体に注目しておらず，テスト検体が解析されなかった可能性がある．今後の調査では，テスト検体の数を増やしたり，テスト検体を実行する際に実際のインシデントに見せかけてセキュリティベンダーの注目を集めたりするなどの工夫が必要だと考えている．本稿の実験を通して AV や EDR の弱点を指摘することができた．これらの指摘は AV/EDR をはじめとしたセキュリティ製品の性能向上に繋がると考える．

謝辞 本研究の一部は JSPS 科研費 JP21H03444 と JP21KK0178 の助成を受けて行われた．

参考文献

[1] Zscaler. “What Is Double Extortion Ransomware?”. Zpedia. 2023. https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware, (accessed 2023-08-22).

[2] 警察庁. “令和４年におけるサイバー空間をめぐる脅威の情勢等について”. 2023. https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf, (accessed 2023-08-22).

[3] paloalto. “What is Multi-Extortion Ransomware?”. Cyberpedia. 2023. https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware, (accessed 2023-08-22).

[4] VirusTotal. https://www.virustotal.com.

[5] MITRE Engenuity ATT&CK Evaluations. https://attackevals.mitre-engenuity.org/.

[6] Karantzas, George, and Constantinos Patsakis. “An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors.” Journal of Cybersecurity and Privacy 1.3 (2021): 387-421.

[7] Gupta, Abhinav, Aditi Prakash, and Nolen Scaife. “Prognosis negative: Evaluating real-time behavioral ransomware detectors.” 2021 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2021.

[8] Scaife, Nolen, et al. “Cryptolock (and drop it): stopping ransomware attacks on user data.” 2016 IEEE 36th international conference on distributed computing systems (ICDCS). IEEE, 2016.

[9] Dropbox. https://www.dropbox.com.

[10] Amazon Lightsail. https://aws.amazon.com/lightsail/.

[11] Let’s Encrypt. https://letsencrypt.org/.

[12] Pyarmor. https://pypi.org/project/pyarmor/.

[13] PyInstaller. https://pypi.org/project/pyinstaller/.

[14] GitHub. https://github.com.

[15] PyInstaller. https://www.google.com/drive/.

[16] Qubes OS. https://www.qubes-os.org.