サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2020 年 4 月～6 月] 《 付録 》 ～EKANS ランサムウェアの解析事例～

2020 年 7 月 30 日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

目次

1　はじめに

サイバー攻撃は、あらゆる企業・組織に対して試みられている。このような状況において、自組織（あるいはISAC[1]等の会員組織）に試みられた攻撃を分析し、その情報を蓄積し、他の組織と情報共有するといった活用を行っていくことは一定の意義があるものと考える。特に、攻撃者によって意図的に狙われて攻撃された場合（標的型攻撃）、分析・蓄積・共有を重ねた結果、自組織や関連業界が過去に受けた攻撃との関係性（連続性）の有無や攻撃手口の類似性等の点について、把握できる場合がある。こういった分析には様々な観点や方法があり、その一つとして、攻撃に用いられたウイルス等の不正ファイルの解析がある。

IPA セキュリティセンターでは、J-CSIP の運用をはじめとして、サイバー攻撃の情報を分析するため、必要に応じてウイルス等の解析を行っている。その中には、広く無差別にばら撒かれたウイルスと思われるものだけでなく、特定の業種・業界を狙った攻撃に使用されたと思われるウイルスもある。そして、これらの情報について、必要な範囲で情報共有を進めている。

この活動の中で、本四半期、複数の被害事例が報じられ注目された、「EKANS」（別名 SNAKE）ランサムウェアの検体についても、独自に解析を行っている。このウイルスは、標的型攻撃に準じた手口（人手によるランサムウェア攻撃、human-operated ransomware attacks）の中で使用されたと言われている。既に詳しい解析記事が三井物産セキュアディレクション社から公開されている[2]（以降、MBSD 解析記事）が、当機構では、過去、攻撃に使われた可能性のある複数の検体を公開情報から入手し、各検体の差分に注目することでいくつかの知見を得ることができた。

本書は、これら複数の EKANS 検体について解析し、検体間の比較を行った結果を、ひとつの事例として、解析におけるポイントの紹介と共に説明する。これは、あくまで特定のウイルスの解析結果を参考情報として示すものであり、今後のサイバー攻撃への直接的な対策となるものではない。一方、このようなウイルスの特徴や動作の仕組みを把握することは、ウイルス解析者のみならず、企業・組織のセキュリティ担当者においても、サイバー攻撃への対応・対策を検討する上で、役立つ可能性があるであろうと考え、報告するものである。

本書の対象読者

本書では、次の方々を主な対象読者と想定している。

- 企業の CSIRT[3]や ISAC 等、組織のセキュリティを扱う部門の方
- ウイルスの解析等を行う方、ウイルスの解析を外部専門組織へ依頼して業務を遂行する方

---

[1] Information Sharing and Analysis Center（ISAC、アイザック）。同じ業界の民間事業者同士でサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織。

[2] MBSD blog – SNAKE(EKANS)ランサムウェアの内部構造を紐解く
https://www.mbsd.jp/blog/20200616.html

[3] Computer Security Incident Response Team（CSIRT、シーサート）。組織内の情報セキュリティ問題を専門に扱う、インシデント対応チーム。

2 EKANS ランサムウェアの解析にあたって

本ウイルスは実行形式のファイルであり、GO 言語で作成されている。GO 言語で作成されたプログラムは、C#などで作成されたものと比較して、ファイルサイズが大きい（数 Mbyte 以上となる）という特徴があり、従ってコードの量も多くなるため、解析する上で 1 つの障害となりやすい。また、IDA Pro などのディスアセンブラに読み込ませて解析を試みても、そのままでは GO 言語が提供する各種ライブラリ（標準関数）を呼び出している箇所などが他と区別できないため、解析が難しい。

そのため、本書では、GO 言語で作成されたプログラムを解析する際に、IDA Pro と GoLangHelper というツールを組み合わせて解析を行っている。次の項では、GoLangHelper の紹介と、各検体の比較解析を行う際に利用した BinDiff というツールについても併せて紹介する。

2.1 GoLangHelper

GoLangHelper とは、IDA Pro で使用することができる Python で書かれたスクリプトで、Github 上に公開されており [4]、自由に利用できる。GoLangHelper を使用すると、GO 言語でビルドされたプログラムを解析し、標準関数の呼び出し箇所について、関数名へのリネームなどを自動的に行うことができる（図 1）。効率的な解析には欠かせないツールである。

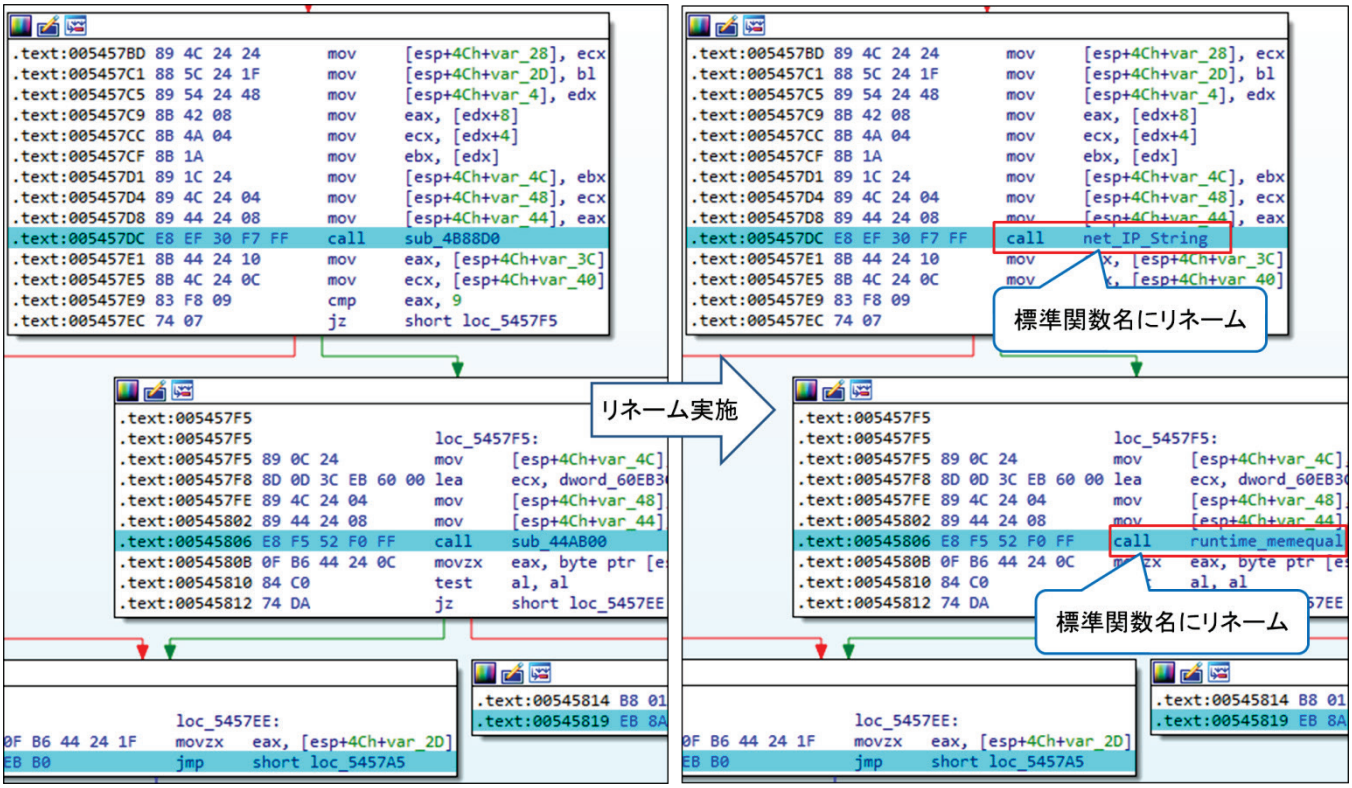

図 1：GoLangHelper を使用した標準関数名へのリネーム

[4] https://github.com/sibears/IDAGolangHelper

なお、GO 言語で作成されたプログラムは、コードの量が多くなると共に、プログラム内の関数（サブルーチン）の数が膨大な数となるため、解析対象としたい処理の関数を探し出すこと自体が困難となりうる。EKANS の場合、約 5,800 関数が存在する。GoLangHelper を使用して関数リネームを行うと、例えばメイン処理関数が「main_main」という名前にリネームされるため、IDA Pro の Functions window で「main_main」関数の検索を行うことにより、プログラムのメイン処理部分にすぐ行き着くことができる（図 2）。

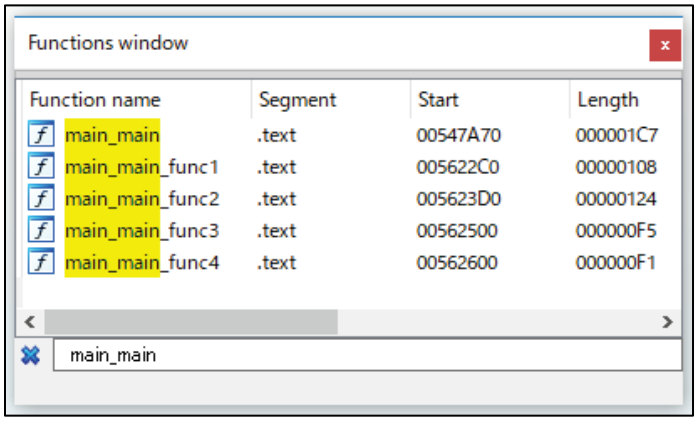

図 2：Functions window での main_main 関数の検索

2.2 BinDiff

BinDiff は、ディスアセンブルされた 2 つの検体のアセンブリコードの比較をグラフィカルに行うことができるツールで、IDA Pro のプラグインとして公開されている[5]。本件の解析のように、複数の同種のウイルスについて比較解析を行う場合、BinDiff を用いると効率的に実施することができる。

BinDiff を用いて実際にコードの比較を行った画面を図 3 に示す。図中の画面左側（primary）が比較元となる検体のコードで、画面右側（secondary）が比較先となる検体のコードである。コードの差分が無いエリアと、差分が有るエリアが色分けされるなど、視覚的に分かりやすく表示される。また、このグラフビューによるコード比較以外にも、関数自体が追加されていた場合は、その関数がリストアップされるなど、コードの比較を行う上で非常に有用なツールである。

コードの比較により差分を確認することで、例えば、次のような調査・推定の材料とすることができる。

- 攻撃者がウイルスをどのように更新したと思われるか
- ほぼ同時期に確認された／ほぼ同等と思われるウイルスの検体について、何が異なる点であるか（攻撃者が何を意図してウイルスの亜種を作成したと思われるか、等）

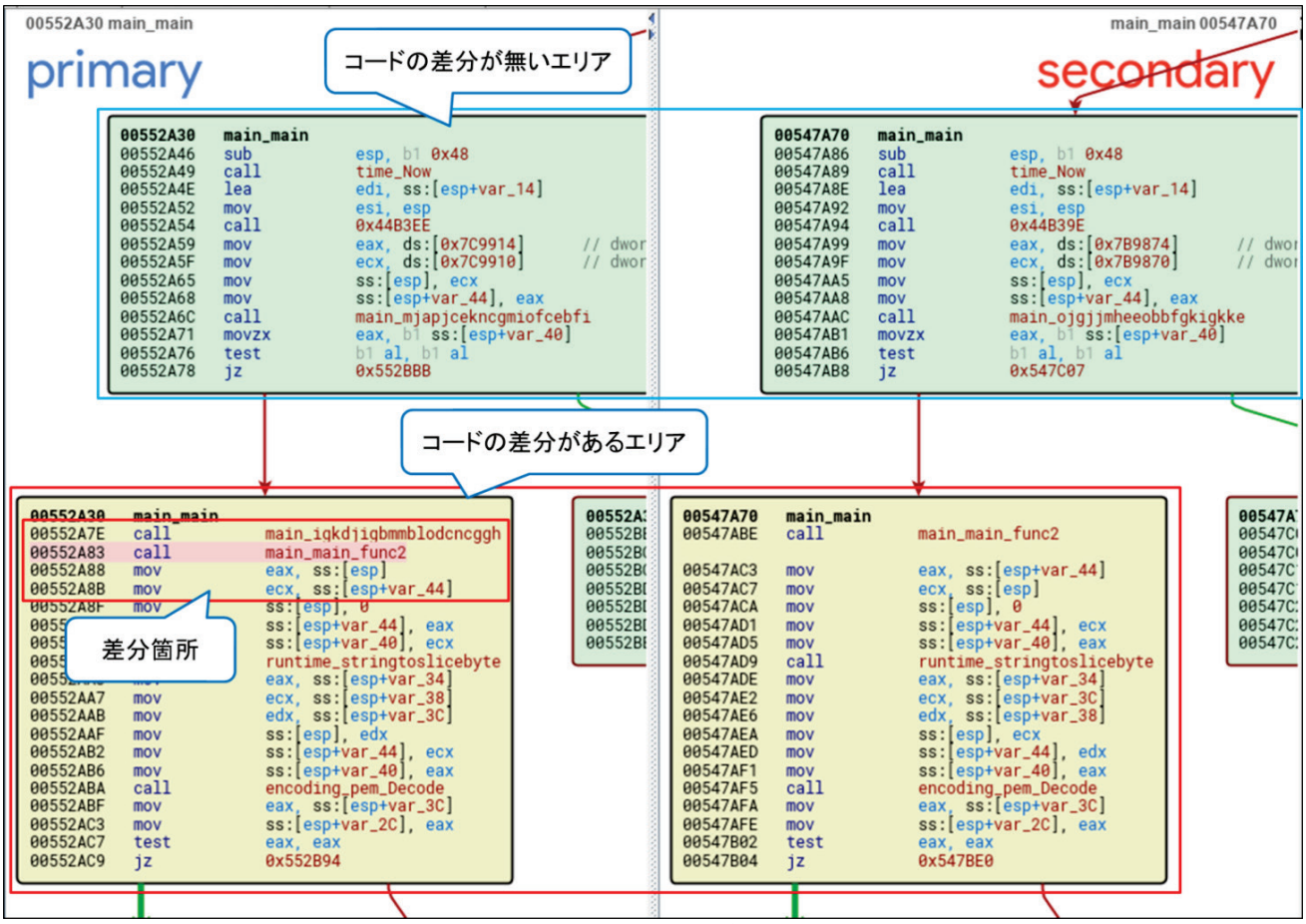

図 3：BinDiff でのコード比較画面

[5] https://www.zynamics.com/bindiff.html

3 EKANS ランサムウェアの動作解析と比較

本章では、EKANS の各検体の動作を解析し、比較した結果、判明した点を説明する。IPA が公開情報から入手した検体は 5 つあり、便宜上、A 検体、F 検体、F’検体、E 検体、H 検体と呼称する。それぞれの MD5 ハッシュ値と、検体が公開情報となった日時を表 1 に示す。MBSD 解析記事内で述べられている検体は、H 検体（公開情報となった日時が最も新しいもの）である。

なお、F’検体は F 検体と同等のものであったため、本章での比較解析の対象外としている（F’検体の詳細は後述する）。

表 1：EKANS 解析対象検体一覧

検体名	MD5 ハッシュ値	公開情報となった日時（UTC）
A 検体	3d1cc4ef33bad0e39c757fce317ef82a	2019-12-26 09:21:29
F 検体	47ebe9f8f5f73f07d456ec12bb49c75d	2020-05-04 05:32:35
F’検体	d659325ea3491708820a2beffe9362b8	2020-05-06 12:51:31
E 検体	7ddb09db3fb9b01fa931c2a1a41e13e1	2020-06-07 16:16:45
H 検体	ed3c05bde9f0ea0f1321355b03ac42d0	2020-06-08 01:36:39

ここでは、解析対象の検体が、上記の順（公開情報となった日時の順）に作成されたものであるとの仮定のもと、作成された順に、それぞれのウイルスがどのような動作を行うかをフローチャート形式で説明すると共に、処理の内容にどのような差分が有ったのか、比較した結果を解説していく。

3.1 A 検体(2019-12-26)の動作概要

A 検体の動作概要を、図 4 に示す。

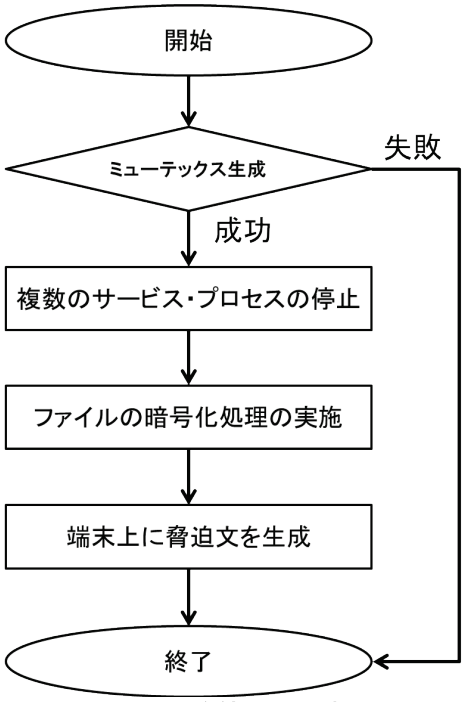

図 4:A 検体の動作概要

本検体は、起動すると、最初に「EKANS」という名称のミューテックスの生成を試みる。ミューテックスの生成に失敗すると動作を終了するが、このことによって、端末内で自身のプロセスが多重に起動することを防いでいる。このような多重起動の防止方法は、ランサムウェアに限らず、他のウイルスや一般的な正規のソフトウェアでも見られる動作である。

ミューテックスの生成に成功すると、続いてイベントログや特定のセキュリティ製品に関するサービスと、仮想化機能などのプロセスを停止させる処理を行う。これは、次に実施する暗号化処理や、ランサムウェアに感染した端末の調査を妨害するためと考えられる。

その後、ランサムウェアとしての主たる機能である、端末内のファイルの暗号化処理を実施する。暗号化処理の詳細な内容については、各種セキュリティベンダの解析記事に記載された通りのものであることを確認しており、本書では説明を省略する。

端末内のファイルの暗号化処理を終えると、最後に、感染端末内の「Public のデスクトップ」と「C ドライブの直下(C:¥)」に、テキスト形式の脅迫文ファイルを生成し、動作を終了する。

以上の通り、本検体の動作は、二重起動防止のためのミューテックスの生成箇所を除き、特段の分岐処理も無く、端末内のファイルの暗号化を行うのみの単純なものであった。

3.2 F 検体(2020-05-04)の動作概要

F 検体の動作概要を、図 5 に示す。

※ A 検体と比較し、F 検体で追加された処理については、赤色で示す。

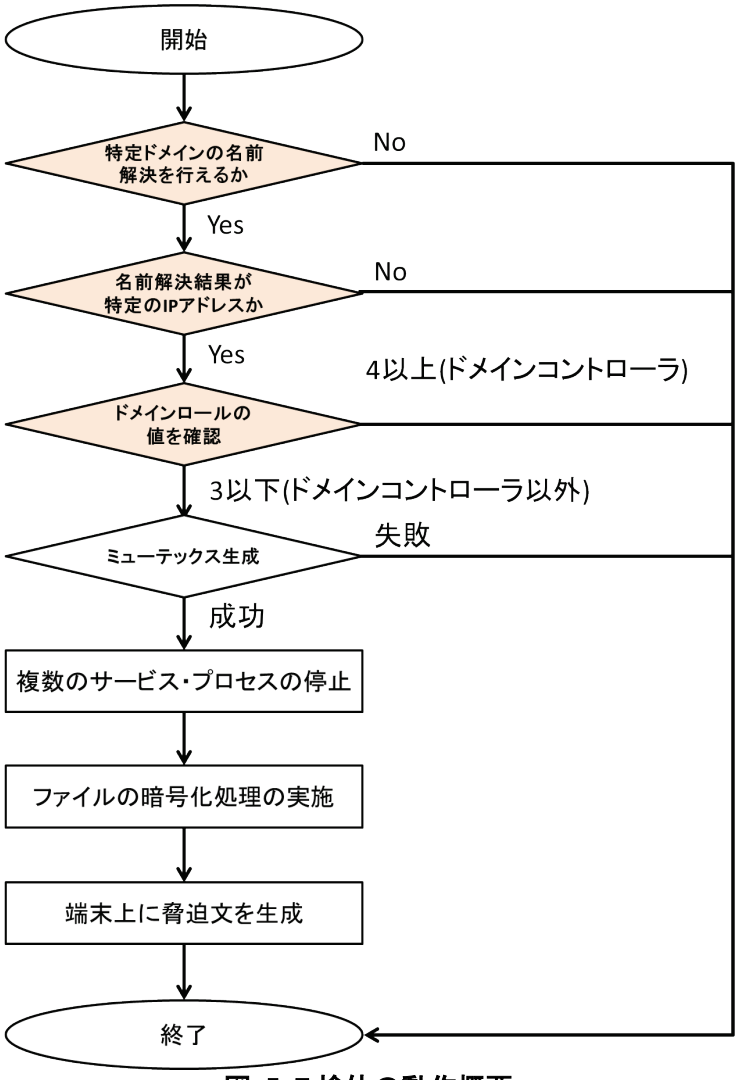

図 5:F 検体の動作概要

本検体では、ミューテックスの生成の前に複数の条件分岐が追加されていた。

本検体は、起動すると、まず特定ドメイン「ADS.FRESENIUS.COM」の名前解決が行えるかどうかをチェックする(名前解決が行えなかった場合は終了する)。名前解決に成功した場合、取得した IP アドレスが、ウイルス内部に固定値として保持している値(期待する結果)であるか確認し、期待する結果でなかった場合は動作を終了する。

期待する結果の IP アドレスの値は、「10.2.10.4」というローカルアドレスのものであった。このことから、本検体は、攻撃対象組織の内部ネットワーク環境下でのみ名前解決が可能なドメインのチェックを行うことで、被害を与える対象の端末を、対象組織内のものに限定しようとした可能性がある。あるいは、サンドボックス型のセキュリティ機器等の環境では動作しないようにすることで、ウイルスと検知されないようにした、といったことも考えられる。この特定ドメインが当該 IP アドレスであるという情報は、基本的には組織外からは知りえないため、(この IP アドレスが正しいならば)ウイルスの作成者は、攻撃対象組織の内部ネットワークへ侵入していた可能性がある。

期待する結果の IP アドレスが得られたことを確認できた場合（すなわち、おそらくは攻撃対象組織内の端末であることが確認できた場合）、更に端末のドメインロールの値を取得し、端末がドメインコントローラ（組織内の AD サーバ等）であるかをチェックする。端末がドメインコントローラであった場合は、暗号化処理は行わず、そのまま終了する。それ以外の場合は、A 検体と同様の処理（ファイルを暗号化して脅迫文ファイルを生成する）に進む。

「ドメインコントローラではウイルスが動作を停止する」という条件分岐が追加された理由は、想像の域を出ないが、次のような可能性が考えられる。攻撃者は、乗っ取ったドメインコントローラ経由で、本検体を攻撃対象組織内の多数の端末へ配布し感染させることを計画した。この時、何らかの原因で、ウイルスの配布元として悪用するためのドメインコントローラ上のファイルを暗号化してしまうと、攻撃が継続できなくなる可能性がある。そのような状況を避けるため、この条件分岐を追加した、というものである。

3.3 E 検体（2020-06-07）の動作概要

E 検体の動作概要を、図 6 に示す。

※ F 検体に対し、E 検体で追加された処理については、赤色で示す。

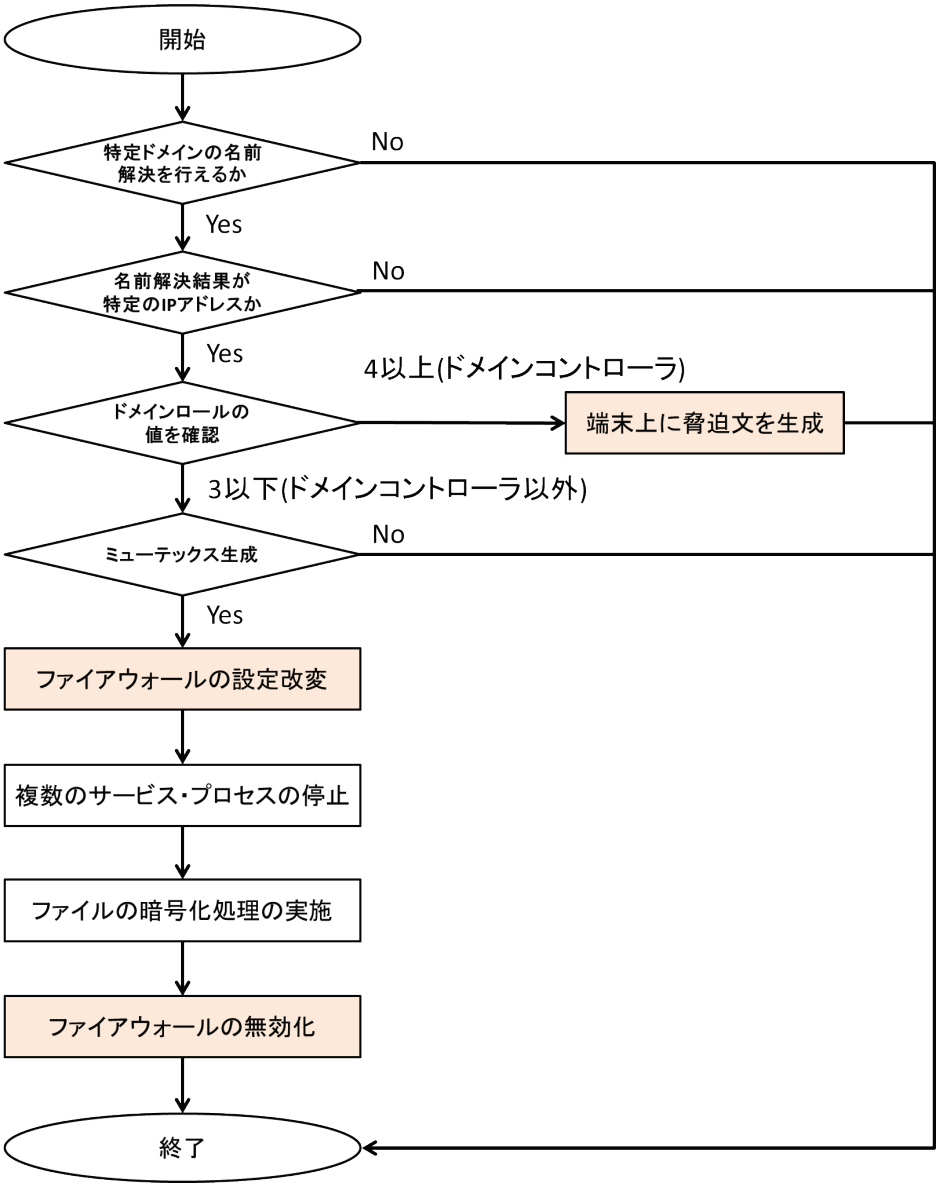

図 6:E 検体の動作概要

本検体は、F 検体とは脅迫文ファイルを生成する対象端末が異なる。端末がドメインコントローラであった場合にのみ脅迫文ファイルを生成し、ファイルの暗号化を行った（被害を与えた）端末には、脅迫文ファイルを生成しないよう変更された。これは、ドメインコントローラを乗っ取っていることが前提の機能であり、身代金の交渉相手が、明確にシステム管理者（および経営層）であるという攻撃者からのメッセージのように思える。

また、本検体では、暗号化処理を行う前にファイアウォールの設定改変を行い、端末のネットワーク通信を妨害する処理が追加されていた。暗号化処理中にネットワーク経由の監視を遮断することで、攻撃の検知や中断を避けるようにした可能性が考えられる。なお、暗号化処理が完了した後は、ファイアウォールを無効にする処理も追加されていることを確認している。

3.4 H 検体(2020-06-08)の動作概要

E 検体とほぼ同時期に公開情報となった H 検体について、BinDiff による検体比較を行ったところ、E 検体とほとんど差分が無いことが分かった。具体的には、約 5,800 関数のうち、差分が有ったのは 6 関数のみであった。E 検体と H 検体の BinDiff での比較結果を図 7 に示す。

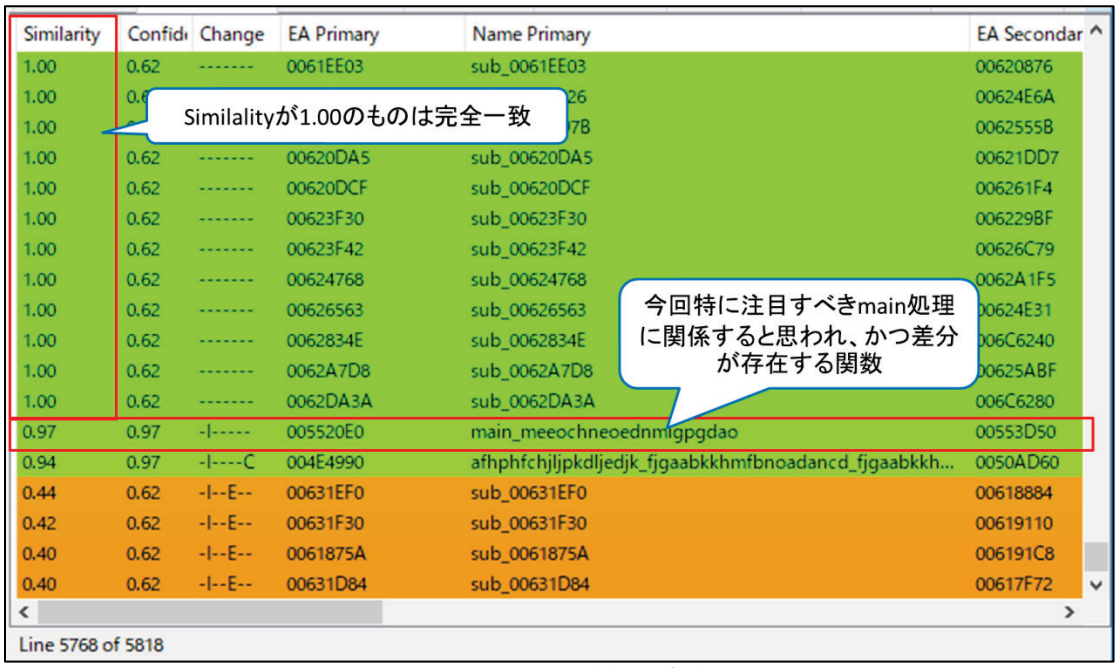

図 7:BinDiff での検体比較結果

また、差分が有った関数についてグラフビューによる比較を行ったところ、差分が存在するのは関数内のごく限られた箇所であることも判明した(図 8)。

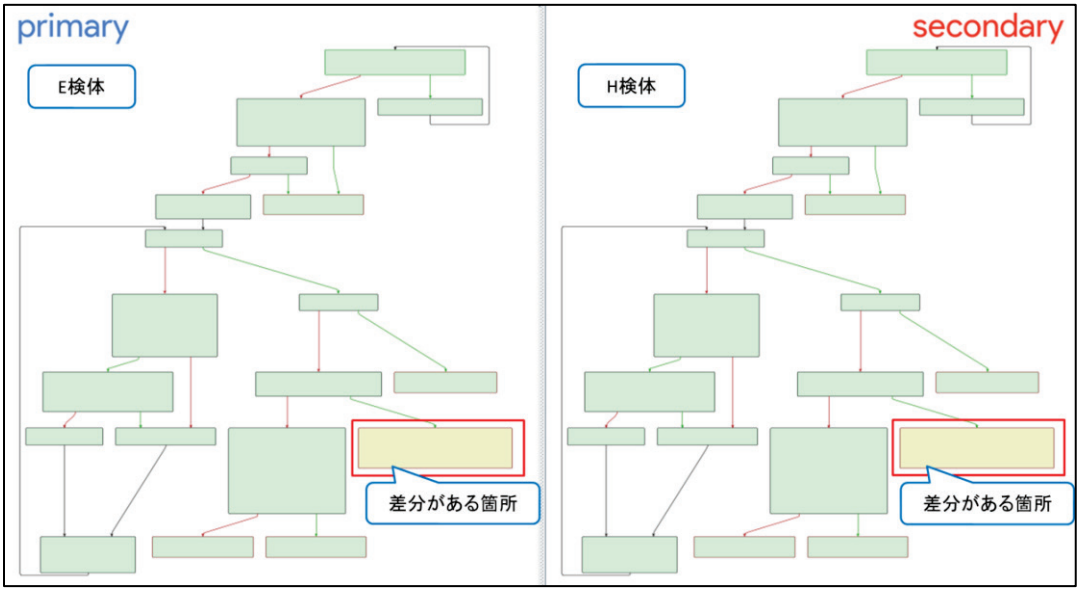

図 8:差分のあった関数を比較表示した結果

更に詳細に確認すると、コードの差分は脅迫文ファイルを生成する関数の直前の箇所であった（該当箇所を図 9 に示す）。この箇所は、脅迫文ファイルに記載する連絡先メールアドレス（CarrolBidell@～）の文字列を、脅迫文ファイルに反映するため、ファイルを生成する関数に渡す処理である。E 検体は検体内に平文で保持しているメールアドレスの文字列を使用するが、H 検体では、メールアドレスの文字列が暗号化されて格納されており、それを復号して使用するという違いがあることが判明した。

E 検体と H 検体の脅迫文ファイルへ最終的に記載される連絡先メールアドレスは同じものであった。この改変は、メールアドレスの文字列を対象としたシグネチャマッチング等による検知を防ぐための細工であった可能性が考えられる。

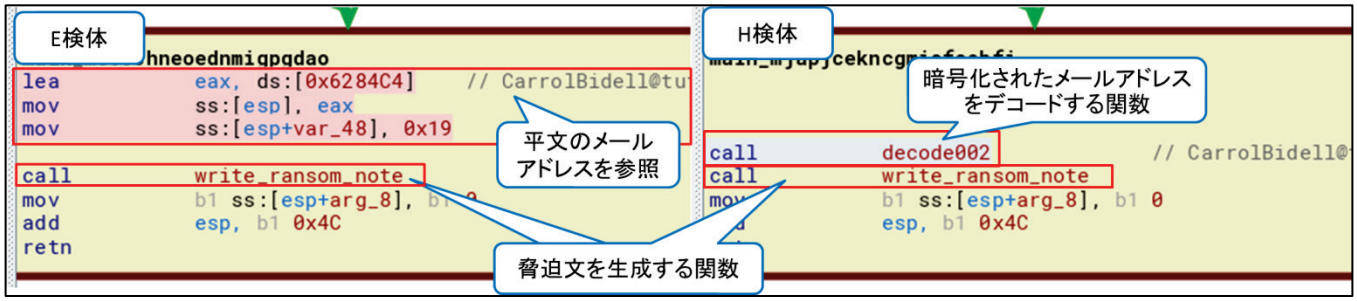

図 9:H 検体で改変された箇所

このほか、E 検体と H 検体では、名前解決するドメイン名や、その結果として期待する IP アドレスについても差分があったが、コードとしては同等のものであった。

3.1～3.4 章で説明した、各検体の処理内容の一覧を表 2 に示す。各検体の動作概要（フローチャート）と同様、その検体から新しく追加された処理については赤色で示している。

表 2:各検体の処理内容の一覧

検体名	A 検体	F 検体	E 検体	H 検体
公開情報となった日時（UTC）	2019-12-26 09:21:29	2020-05-04 05:32:35	2020-06-07 16:16:45	2020-06-08 01:36:39
特定ドメインの名前解決	-	○	○	○
取得した IP アドレスの確認	-	○	○	○
ドメインロールの値の確認（ドメインコントローラを暗号化の対象外とする条件分岐）	-	○	○	○
脅迫文ファイルの設置対象	感染端末	感染端末	ドメインコントローラ	ドメインコントローラ
ミューテックス生成	○	○	○	○
ファイアウォールの設定改変	-	-	○	○
複数のサービス・プロセスの停止	○	○	○	○
ファイルの暗号化処理	○	○	○	○
ファイアウォールの無効化	-	-	○	○
連絡先メールアドレスの暗号化	-	-	-	○

※ 表中、「-」は該当する処理が無いことを示す。

※ 各処理において、例えば「プロセスの停止」の対象となるプロセス名など、細かい点で差分が存在する箇所があるが、本書では説明を省略する。

3.5 各検体の文字列復号処理の差分

EKANS は、連絡先メールアドレスの他に、脅迫文などの文字列を暗号化して保持している。復号する処理は、同じサイズのデータ①とデータ②から 1 バイトずつ値を取得し、それらを XOR 演算していくという方式（図 10）となっているが、この処理について着目したところ、検体によって微妙な差分があることが判明した。

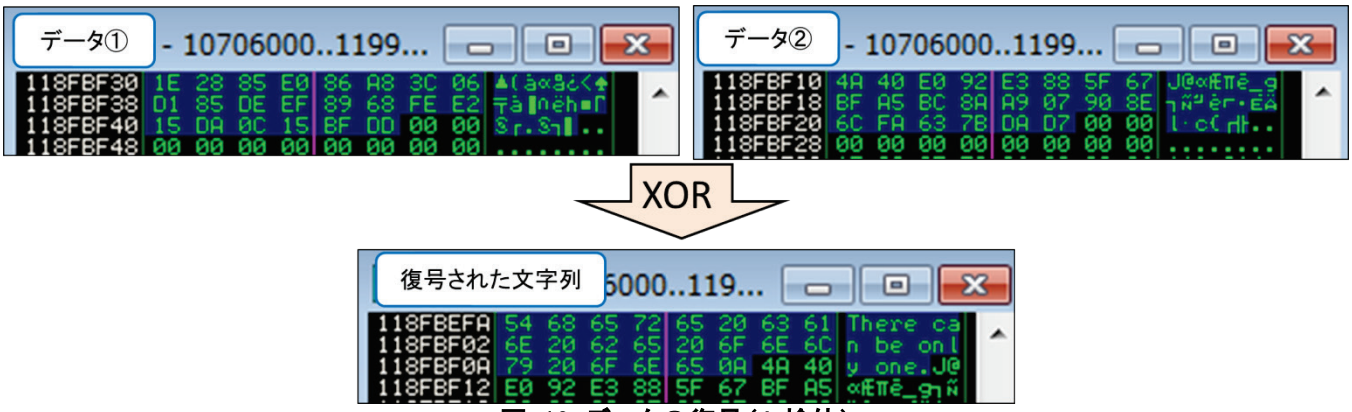

図 10:データの復号（A 検体）

A 検体では、単純に取得した値をそのまま XOR 演算していたが、F 検体ではデータ①から取得した値に固定値（2Ah）を加算する処理が加わっていた。更に E・H 検体では、固定値の代わりに、変数値を加算（1 文字目には 0 を加算し、2 文字目以降は 2、4、6・・・と 2 の倍数を順に加算）する処理に変更されており、徐々にではあるが複雑化する変化が見られた（表 3）。

表 3:各検体の復号処理一覧

検体名	復号処理の内容
A 検体	（データ①）XOR（データ②）
F 検体	（データ①＋2Ah）XOR（データ②）
E・H 検体	（データ①＋変数値 [6]）XOR（データ②）

なお、E 検体・H 検体の復号処理のロジックは同じであったが、それぞれの暗号データ①と②の値は、復号後に同じ結果の文字列となる、異なる組み合わせの値となっていた。一例として、実際に検体内に存在する「EKANS」という文字列の場合、それぞれの検体のデータ①とデータ②は表 4 のように異なるが、この値を上述の XOR 演算で復号すると、両検体とも同じ文字列が得られる。復号処理のロジックの変更と合わせて、これらはシグネチャマッチングによる検知を回避することが目的であると考えられる。

表 4:「EKANS」文字列の場合のデータ

	E 検体	H 検体
データ①	67h 0Bh 1Eh D1h 7Fh	42h C8h 49h 28h B4h
データ②	22h 46h 63h 99h D4h	07h 81h 0Ch 60h EFh
復号結果	45h 4Bh 41h 4Eh 53h （'E' 'K' 'A' 'N' 'S'）	

[6] 0, 2, 4, 6, 8 … と変化していく値

3.6 名前解決するドメインおよび期待する IP アドレス

各検体が名前解決を試みるドメインと、結果として期待する IP アドレスの一覧を表 5 に示す。

表 5:ドメインと IP アドレス

検体名	名前解決を試みるドメイン	期待する IP アドレス
A 検体	（処理無し）	（処理無し）
F 検体	ADS.FRESENIUS .COM	10.2.10.4
E 検体	ENELINT.GLOBAL	10.16.173.233
H 検体	MDS.HONDA.COM	170.108.71.15

4　動作面以外の差異

本章では、ウイルスの動作面以外の点について比較を行い、判明した点を説明する。

4.1 GO 言語のバージョンとビルド時のアカウント名

検体内に残留していた文字列から、開発に使われた GO 言語のバージョンと、ビルドを実行した際のアカウント名が推定できる（表 6）。これらの 4 検体では、GO 言語のバージョンは共通していたが、アカウント名に違いが見られた。攻撃者がアカウント名を変えている理由は不明だが、公開情報となった日時に数時間しか差がない E 検体と H 検体ではアカウント名が変わっていないことから、ビルド毎に変えているわけではなく、定期か不定期かは不明なものの、ある程度期間が空いた時にアカウント名やビルド環境に変化があるものと思われる。

表 6：GO 言語のバージョンと、ビルド時のアカウント名

検体名	GO 言語のバージョン	アカウント名
A 検体	go1.10.8	WIN1
F 検体	go1.10.8	Admin
E・H 検体	go1.10.8	Admin3

4.2 脅迫文ファイルの差異

生成される脅迫文ファイルについて比較を行ったところ、各検体とも、脅迫文ファイルの生成場所は共通していたが、A 検体のみ脅迫文のファイル名に違いが見られた（表 7）。

表 7：脅迫文のファイル名と生成場所

検体名	脅迫文ファイル生成場所	脅迫文ファイル名
A 検体	C ドライブの直下（C:¥）、Public の Desktop	Fix-Your-Files.txt
F・E・H 検体	C ドライブの直下（C:¥）、Public の Desktop	Decrypt-Your-Files.txt

次に、脅迫の文面について比較を行ったものを、図 11～図 13 に示す（差分がある行を黄色で着色している）。なお、E 検体と H 検体の脅迫文の文面は同一である。

```
-----------------------------------------------
| What happened to your files?
-----------------------------------------------
We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -
all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!
You can still get those files back and be up and running again in no time.

-----------------------------------------------
| How to contact us to get your files back?
-----------------------------------------------
The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.
Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with
better cyber security in mind. If you are interested in purchasing the decryption tool contact us at bapcocrypt@[redacted]

-------------------------------------------------------
| How can you be certain we have the decryption tool?
-------------------------------------------------------
In your mail to us attach up to 3 files (up to 3MB, no databases or spreadsheets).
We will send them back to you decrypted.
```

図 11:A 検体の脅迫文

```
-----------------------------------------------
| What happened to your files?
-----------------------------------------------
We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -
all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!
You can still get those files back and be up and running again in no time.

-----------------------------------------------
| How to contact us to get your files back?
-----------------------------------------------
The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.
Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with
better cyber security in mind. If you are interested in purchasing the decryption tool contact us at alfredmir@[redacted]

-------------------------------------------------------
| How can you be certain we have the [redacted]
-----------------------------------
In your mail to us attach up to 3 non critical files (up to 3MB, no databases or spreadsheets).
We will send them back to you decrypted.

-------------------------------------------------------
| What happens if you dont contact us within 48 hours or refuse payment?
-------------------------------------------------------
We publish sensitve databases and documents we collected from your network.
-------------------------------------------------------
```

連絡先メールアドレスが異なる

「non critical」が追記されている

脅迫の文言が追加されている

図 12:F 検体の脅迫文

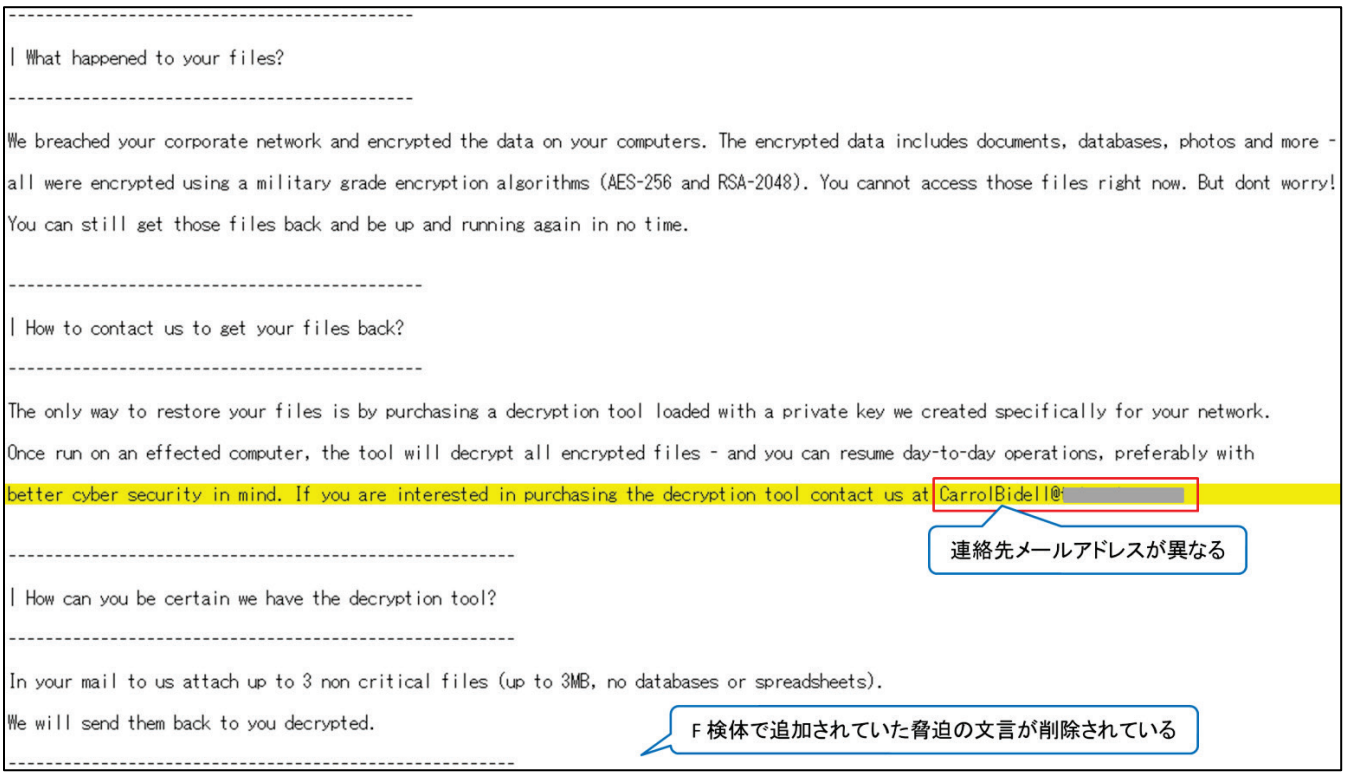

図 13:E 検体と H 検体の脅迫文

以上の通り、EKANS は、脅迫の文面についても更新が行われていることが分かったが、F 検体で追加された「奪ったデータを公開する」と脅す、被害組織に対してより効果的に作用すると思われる脅迫の文言が、E 検体と H 検体では削除されているなど、変更理由が不可解な点も見られた。

「奪ったデータを公開する」と脅す文言が存在しない点については、可能性として、暗号化された脅迫文の復号処理にバグがあり（復号するデータサイズの指定誤りなど）、脅迫文面が途中までしか復号されていないことが原因かとも考えたが、暗号データの解析を詳細に行い、結果として、E 検体と H 検体の内部には、当該文言のデータが存在しないことを確認している（図 14）。

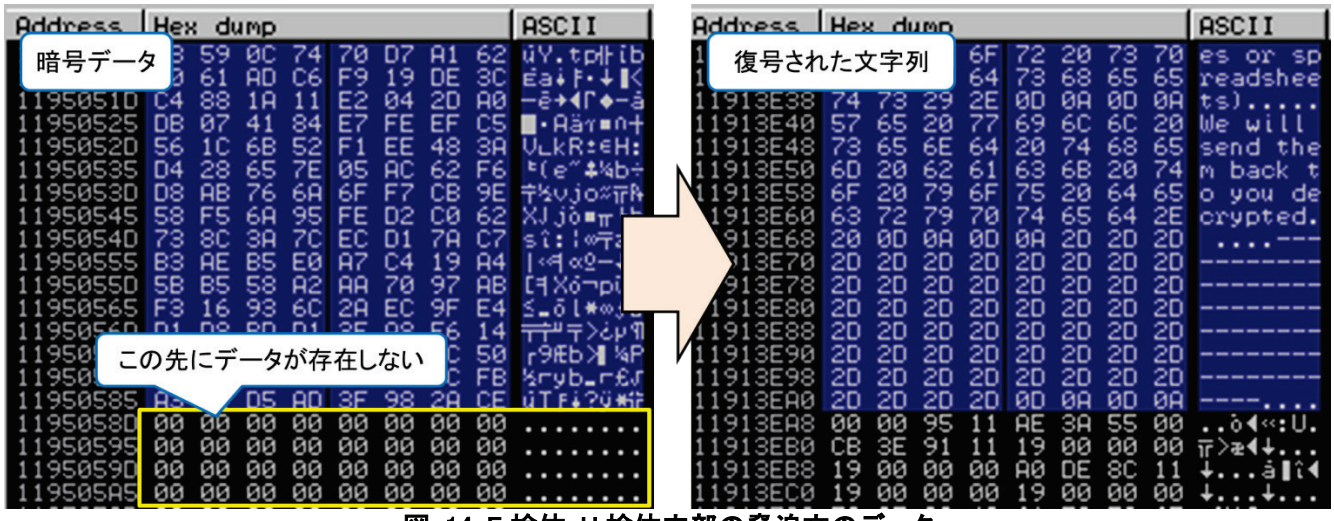

図 14:E 検体・H 検体内部の脅迫文のデータ

4.3 RSA 公開鍵

各検体の、ファイルの暗号化の際に使用される RSA 公開鍵の一覧を表 8 に示す。

ファイルを暗号化して人質に取るというランサムウェアの特性上、当然のことながら、公開鍵は各検体で全て異なっており、攻撃者からどれか 1 つの秘密鍵を得られたとしても、鍵を流用して他の検体で暗号化されたファイルを復号することはできない仕組みとなっていた。

表 8:各検体の RSA 公開鍵

検体名	RSA 公開鍵
A 検体	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAyQ+M5ve829umuy9+BSsUX/krgdF83L3m8/uxRvKX5EZbSh1+buON ZYr5MjfhrdiOGnrbB1j0Fy31U/uzvWcy7VvK/zcsO/5aAhujhHB/qMAVpZ8zT5BB ujT1Bvsith/BXgtM99MixD8oZ67VDZaRM9TPE89WuAjnaBZORrk48wFcn1DOAAHD Z9z9komtqIH1fm3Y0Q6P76nUscLsYOme082L217Th/lTMoqqs4cF2rn9O9Vp4V9U aCs4XVxGSpcuqbIscfpf0cm44P2eOEk+sbZdah09C6fezt7YF4OCJ4Vz3qqMD6z4 +6d7FRxUu6k3Te2T2bWBZnsDO30pYFi/gwIDAQAB -----END RSA PUBLIC KEY-----
F 検体	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAuMBx+hZWQFjyOGwHtb13JhGJS6FohQRzg4ouAuFPC59VydRSfcWp 0YCwSMR4NbJw38/527eGeG3vPeSg1aqz4fFEISm3GR9i2bLWxI7r7gQx2iuwQbZJ jzSm7ymwc7P9rOERdgTHFltz+x1JIa/pUEUdjpSgJMrcEYeix4TDVUjKMPFZbvAo wU/wTRJmb6/Cv0ibyEfyDNUazP+jdqojgI9egCmRTX56LmH41Q1Y3pQQFLFxOpge MOizcr4c0HAqUJw9lu2/a4ATQ/DS/nk3J2DF+1RPhDXWrYJY3iIK6NIdZTa2ZWx4 ZDfceIe2t/4GcgpBdSTU9Q+fBmbcyY3qvQIDAQAB -----END RSA PUBLIC KEY-----
E 検体	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAnqjO7EYoSfxESLO7yAoCLOXxdR9N8wVkgRuKM84ie1MAEkBONIsy eLhEMoAeUEDyVAML4gtwjKDX3eVs7nrmk3wRcq8nU803fq9fYu57EYAXZpb40srq FpiVnDZ1vB47MMhn7oHepbQ/pHhItU7evgmyB5s8J80hnDg5eQfnAdPmLPO/S3fs DT5KLOY0x2S14q0jBKgUiLOZhdqqHUTchFPSVid0U8AKOidJwhpz+j9J2jUZ2M2t njdXbOU06R8NFAoJSxY7T9nY7FA0SNqL9N/V9sThDIoLpCn8RanUb0jZzoEFqWrf Hsr1l/5F2350MmIr+YuWnMI5kSNILO551QIDAQAB -----END RSA PUBLIC KEY-----
H 検体	-----BEGIN RSA PUBLIC KEY----- MIIBCgKCAQEAt1GCKUHXITsiWc1d8V0vo1Y9Jm18RDZEmMS60kHI7pZT0RHAThIR BFITZY9bXrI6RFdUwmIX0WYn5ZqIlhLAEe1cqd8RpJ/KK20eiTn0CJ1CGmO0JvfM 5rFa8whVAU9cnh/iVCcf+aEHJVcHhzB5tTtiT3lBIdfzaLL6GR5EmytbQ3V3O1Uk Y4FCKxYOMVoPzPtRG3vo3688uUWpZIKBV7e6dht/mAhuCEIlRGcdpAEf6f4zUUYf dtHcDafMVEA4Sy/DDsd76wAyBIMOXKLv1+vH476TN1K1tIRBrR98QFI5mlXkgqz6 h+Wpb/5KYWWvG0ZLZcu6eWOCGmLEmorvWQIDAQAB -----END RSA PUBLIC KEY-----

5　F’検体の解析

F’検体は、F検体とほぼ同一の検体であるが、特定ドメインの名前解決などのチェックは行うものの、チェック結果に関わらず、必ず端末内のファイルの暗号化を行う動作となっていた。内部処理を確認すると、ファイルにコードの改変（バイナリデータの書き換え）が行われており、必要最小限の改変でありながら、必ず暗号化処理に進むよう、人為的と思われる改造がなされていることが確認できた（図 15）。

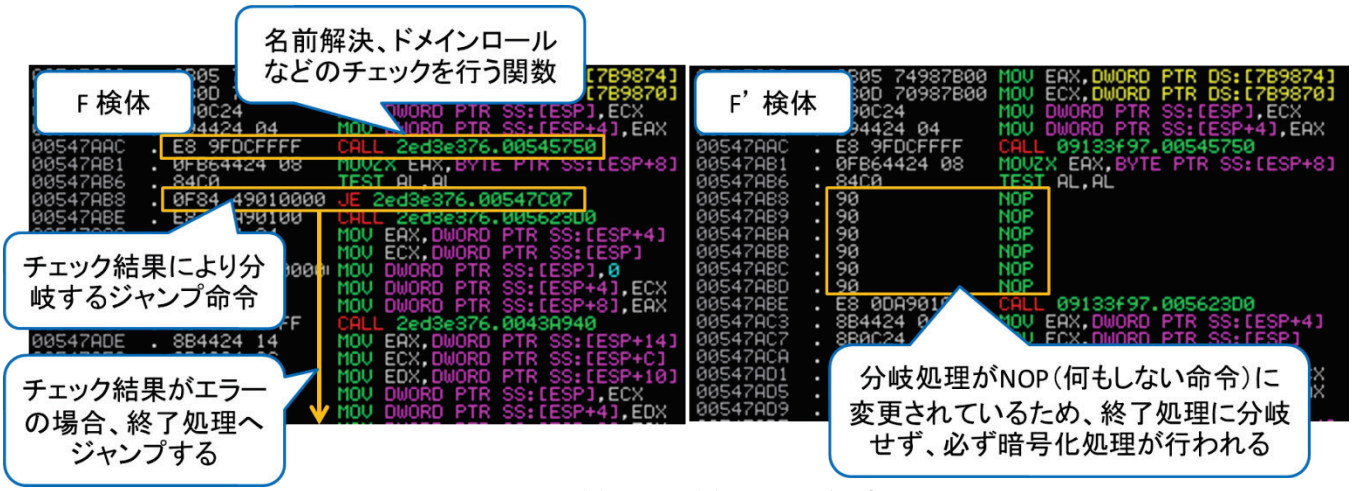

図 15:F 検体と F’検体のコード比較

改変が行われた範囲や、改変元が F 検体であることを厳密に確認するため、コードの改変が行われた部分（「NOP」命令に置き換えられた 6 バイト分）をバイナリエディタで修正したところ、F 検体と F’検体（修正済み）のハッシュ値が一致したため、F’検体は、F 検体を改造したものであろうことが確認できた（図 16）。

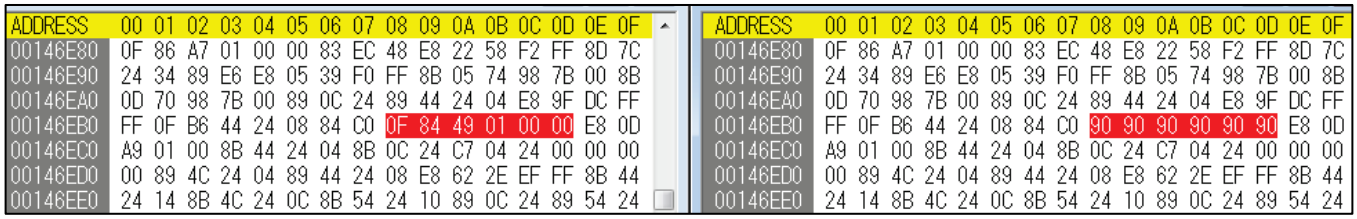

図 16:F 検体と F’検体のバイナリエディタでの比較

F’検体は、実行するとどの環境下でもファイルの暗号化が行われてしまうため、ランサムウェアとしての危険性は増しているとも言えるが、この改造を行った人物は元のウイルス開発者とは別人であった可能性が考えられ、かつ、必ずしも悪意があったとは限らない。例えばセキュリティのリサーチャーなどが、サンドボックス上で本検体を動作させるため改造を行った、といった研究目的である可能性も考えられる（F’検体は、F 検体の約 2 日後に公開情報となっている）。

6 おわりに

IPA で入手した 5 つの EKANS について比較解析を行ったことで、短い期間でウイルスが意図的にアップデートされていたであろう痕跡を確認することができた。特に、E 検体から追加されたファイアウォールの設定変更処理については、約 1 か月の間の変更点であり、作成者は高いモチベーションを持って開発を行っていることがうかがえるものであった。

各処理の追加については、単純にランサムウェアとしての性能の向上を図ったものである可能性もあるが、組織内に侵入した攻撃者が、組織内の構成を調べた上で、ランサムウェアが効果的に組織内へ被害を与えるために作り変えた、といった可能性も考えられる。または、過去、別の組織への攻撃を行った際に、何らかの失敗があり、その教訓を活かしたものであった可能性もある。

これを考慮すると、F 検体で追加され、後の E 検体では何故か削除されていた、「支払いを拒んだ場合、収集した機微なデータを公開する」という脅し文句については、攻撃者がミスをしたということは考えにくく（プログラムの一部が巻き戻ったわけではない。F 検体で追加された「non critical」の文言は残っている）、一つの推論を示す。

〈 F 検体による攻撃自体は成功したが、攻撃者は、身代金を得ることができなかったと仮定する。この脅し文句があることによって、被害を受けた組織が、「例え身代金を払っても、データが窃取されているのならば、事態は悪くなるのではないか（再び脅迫されたり、結局公開されてしまうのではないか）」といった、自分たち攻撃者側への不信感を抱かせてしまった可能性はないだろうか。身代金の交渉に乗せるためには、単純に、データを元に戻すことだけを脅迫の材料とすべきなのではないか。そう考えた攻撃者が、次の犯行からは文言を削除した。 〉　…と、全くの想像とはなるが、このような可能性が考えられる。

本件のように、検体の比較解析を行うことによって得られた知見を元に、様々な推論を行うことが、ただちに企業や組織のセキュリティ対策に繋がるわけではないが、攻撃者の意図を把握しようとする試みは、長期的な観点では必要なことであると思われる。ウイルス解析を通じ、このような知見を積み重ねていくことが、被害を未然に防ぐための対策を考慮する上でも、意義があるものと考えている。

本書執筆：君島 知也

以上