2019年
1·2月
JAN/FEB

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

日本を標的としたランサムウェア GandCrab 感染を狙う攻撃を観測

キヤノンマーケティングジャパン株式会社

はじめに

「マルウェアレポート」は、キヤノンマーケティングジャパンが運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

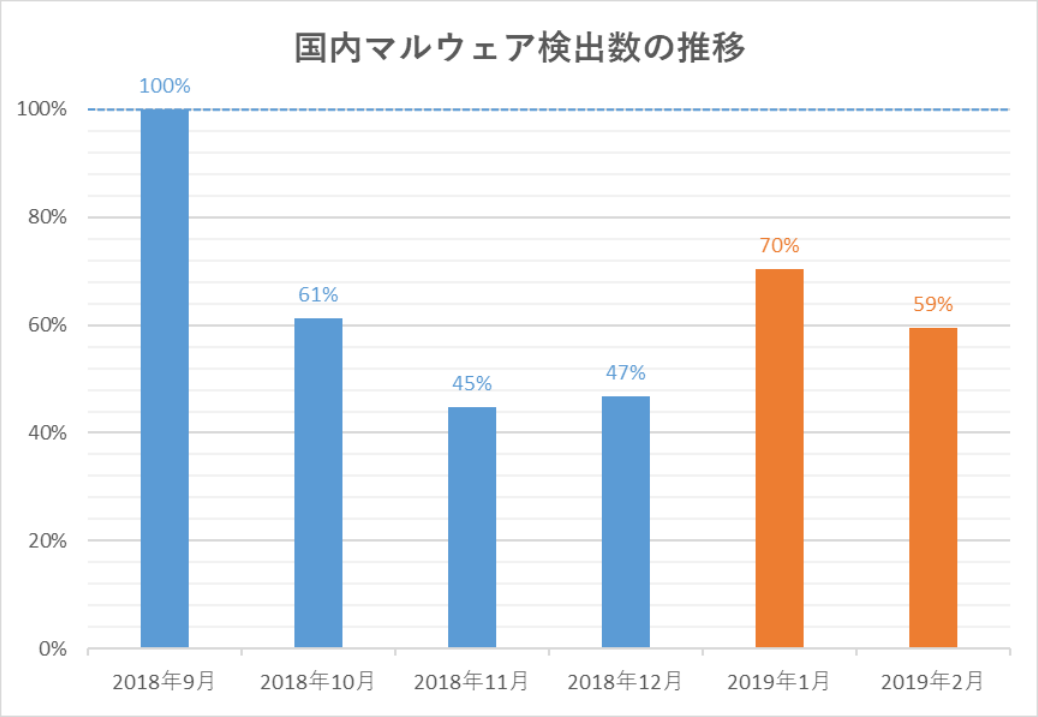
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2019 年 1 月･2 月マルウェア検出状況」

1. 1 月と 2 月の概況について
2. ランサムウェア GandCrab の感染を狙った malspam

1. 1 月と 2 月の概況について

2019 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 28 日）に ESET 製品が国内で検出したマルウェアの検出数は、以下のとおりです。



国内マルウェア検出数*1 の推移

（2018 年 9 月の全検出数を 100%として比較）

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2019 年 1 月と 2 月の国内マルウェア検出数は、2018 年 12 月と比較すると増加しました。

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数*2 上位（2019 年 1 月･2 月）

順位	マルウェア名	比率	種別
1	JS/Danger.ScriptAttachment	28.1%	ダウンローダー
2	HTML/ScrInject	8.3%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Agent	8.0%	アドウェア
4	VBA/TrojanDownloader.Agent	4.8%	ダウンローダー
5	JS/Mindspark	3.9%	アドウェア
6	HTML/Refresh	3.8%	別のページに遷移させるスクリプト
7	PDF/Phishing	1.8%	フィッシング目的の PDF ファイル
8	JS/Redirector	1.8%	リダイレクター
9	HTML/FakeAlert	1.7%	偽の警告文を表示するスクリプト
10	Win32/Exploit.CVE-2017-11882	0.7%	エクスプロイト

*2 本表には PUA を含めていません。

国内マルウェア検出数*2 上位（2019 年 1 月）

順位	マルウェア名	比率	種別
1	JS/Danger.ScriptAttachment	33.6%	ダウンローダー
2	HTML/ScrInject	7.8%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Agent	7.7%	アドウェア
4	HTML/Refresh	5.3%	別のページに遷移させるスクリプト
5	JS/Mindspark	3.5%	アドウェア
6	VBA/TrojanDownloader.Agent	3.3%	ダウンローダー
7	JS/Redirector	1.9%	リダイレクター
8	HTML/FakeAlert	1.8%	偽の警告文を表示するスクリプト
9	PDF/Phishing	1.6%	フィッシング目的の PDF ファイル
10	VBS/TrojanDownloader.Agent	0.6%	ダウンローダー

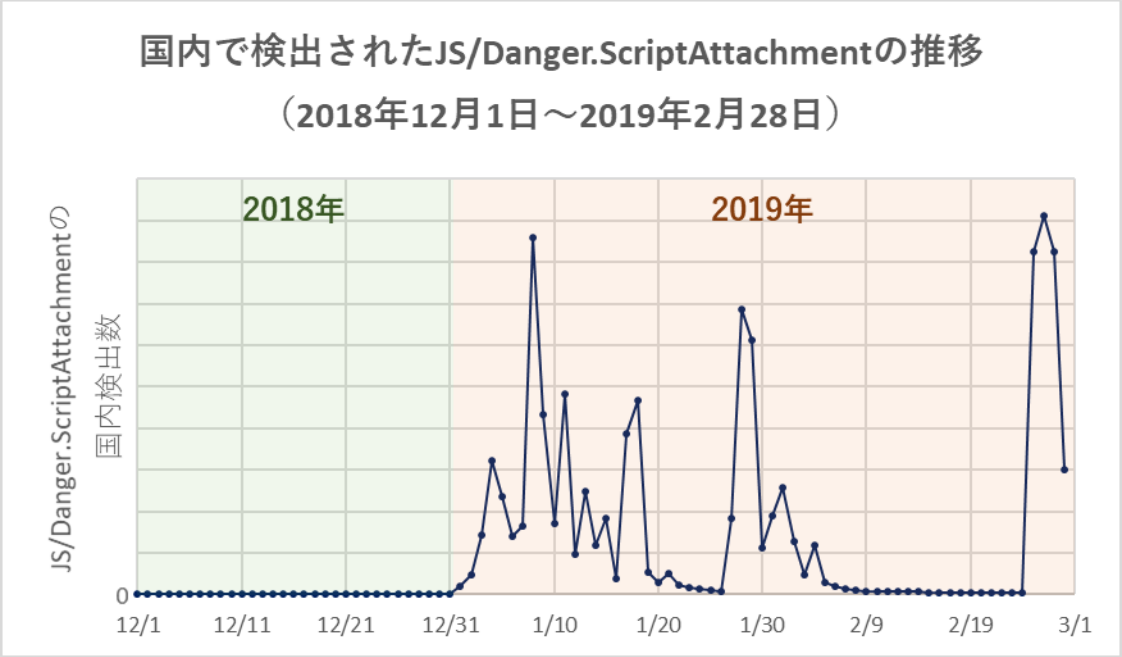
国内マルウェア検出数*2 上位（2019 年 2 月）

順位	マルウェア名	比率	種別
1	JS/Danger.ScriptAttachment	21.6%	ダウンローダー
2	HTML/ScrInject	8.9%	HTML に埋め込まれた不正スクリプト
3	JS/Adware.Agent	8.4%	アドウェア
4	VBA/TrojanDownloader.Agent	6.6%	ダウンローダー
5	JS/Mindspark	4.4%	アドウェア
6	PDF/Phishing	2.1%	フィッシング目的の PDF ファイル
7	HTML/Refresh	2.1%	別のページに遷移させるスクリプト
8	JS/Redirector	1.7%	リダイレクター
9	HTML/FakeAlert	1.5%	偽の警告文を表示するスクリプト
10	JS/Agent.OAY	1.5%	トロイの木馬

*2 本表には PUA を含めていません。

1 月と 2 月に国内で最も多く検出されたマルウェアは、JS/Danger.ScriptAttachment でした。加えて、JS/Danger.ScriptAttachment の割合は、2 番目に多く検出された HTML/ScrInject の割合に対して大きく差をつけていることがわかります。

JS/Danger.ScriptAttachment は、電子メールに添付された悪意のある JavaScript ファイルの汎用検出名です。 国内で検出された JS/Danger.ScriptAttachment の推移は以下のとおりです。

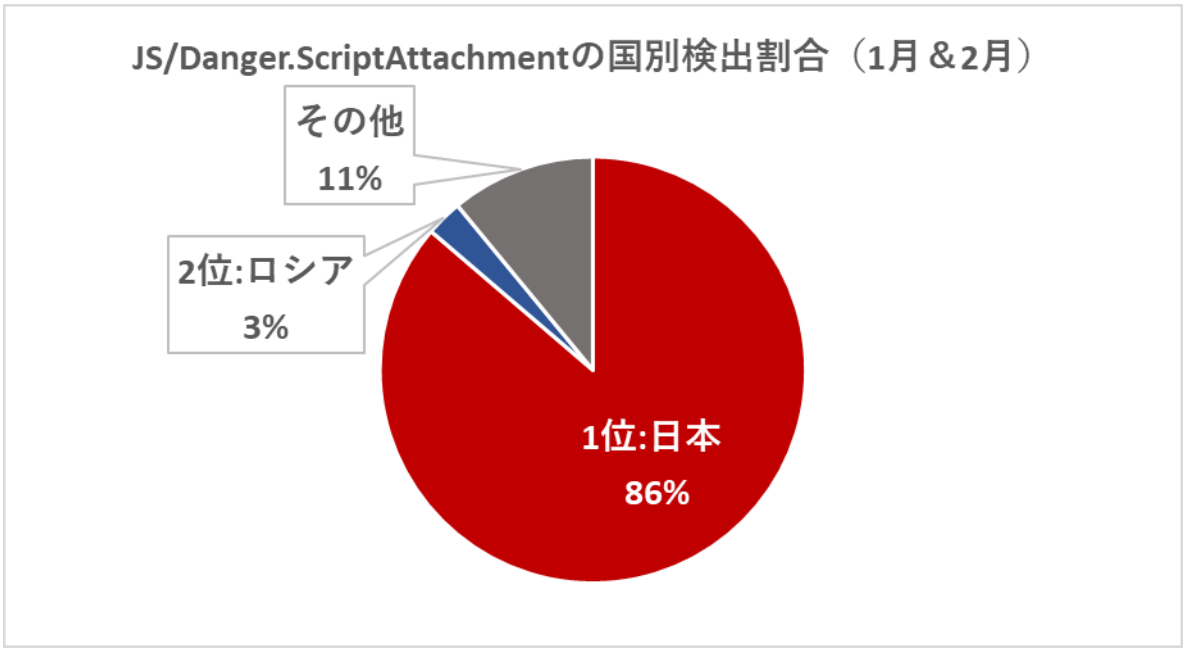


国内で検出された JS/Danger.ScriptAttachment の推移

JS/Danger.ScriptAttachment は、昨年の 12 月はほとんど検出されていませんでしたが、年明けとともに検出数が急増しています。これは、1 月以降に悪意のある JavaScript を含む zip ファイルを添付したメール攻撃が多数確認されたためです。

メールに添付された JavaScript のファイル名が、Love_you_<数字>となっていたことから、ESET ではこの攻撃を“Love You” malspam campaign と呼んでいます。

1 月と 2 月に検出された JS/Danger.ScriptAttachment の国別割合は、以下のとおりです。



JS/Danger.ScriptAttachment の国別検出割合（1 月&2 月）

世界全体において 1 月と 2 月に検出された JS/Danger.ScriptAttachment のうち、86%は日本で確認されました。そのため、“Love You” malspam campaign は、日本を主なターゲットとした攻撃であったことが推測されます。

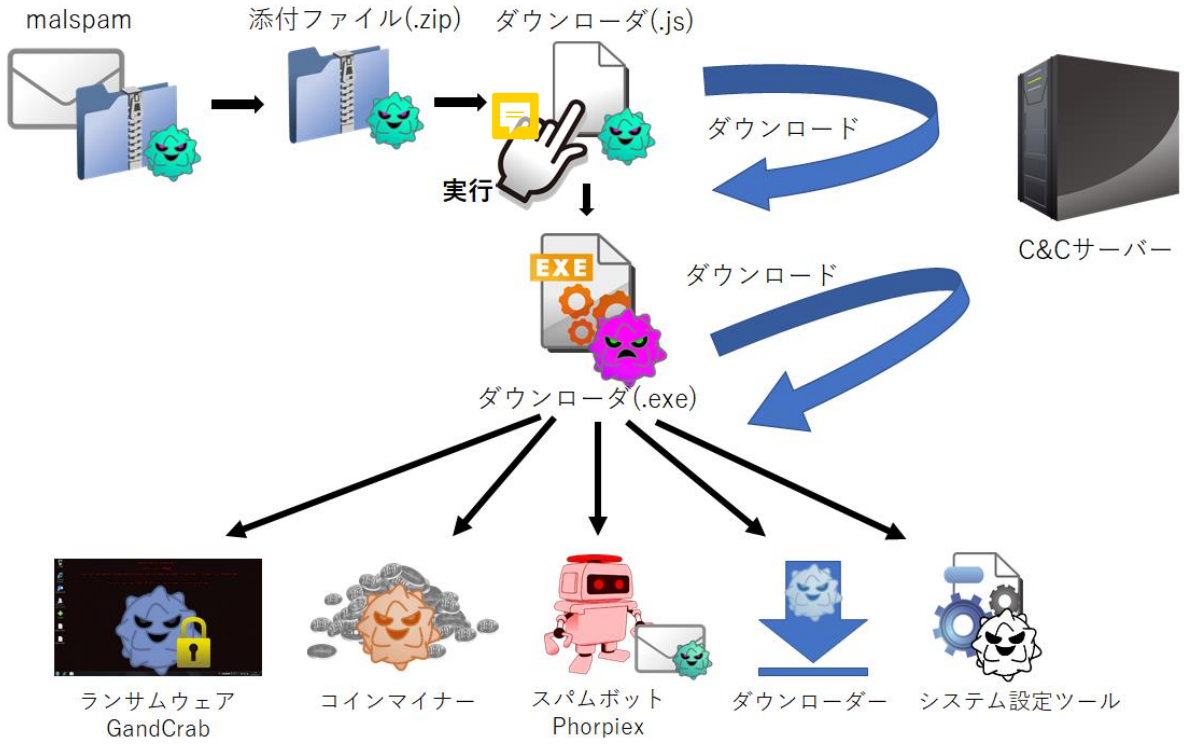
“Love You” malspam campaign については、次章で紹介いたします。

2. ランサムウェア GandCrab の感染を狙った malspam

1 月、2 月は GandCrab の感染を狙った malspam *3 を数多く観測しています。
【速報】ランサムスパム「Love you」がさらに進化をとげ、日本をターゲットとした大規模キャンペーンを展開中でもご紹介したように、1 月初旬から Love you malspam が確認されました。
メールには、zip ファイルが添付されており 、中には JS(JavaScript)形式のダウンローダーが含まれています。JS 形式ダウンローダーを実行すると、別のダウンローダーがダウンロードされ、別のダウンローダーにより複数のマルウェアがダウンロードされます。

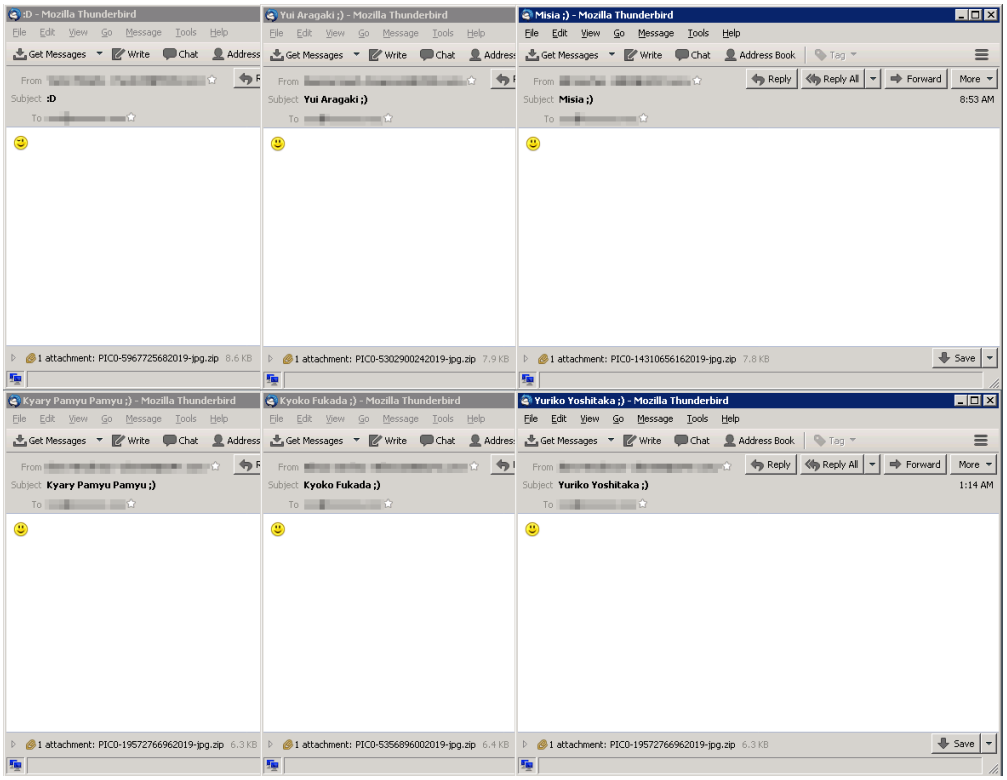
*3 malware spam または malicious spam の略です。ここでは、マルウェア感染を狙ったスパムメールを指します。

ダウンロードされるマルウェアは、実行されるタイミングにより異なり、ランサムウェア GandCrab、スパムボット Phorpiex、コインマイナー、ダウンローダー、システム設定ツールなど様々なマルウェアが存在します。



Love you malspam の感染フロー

この malspam は、日本をターゲットにした攻撃と考えられ、件名が日本の芸能人の名前になっているメールがばらまかれています。しかし現段階ではメールの件名や本文、GandCrab の脅迫画面が日本語にはなっていないため、完成度はそこまで高くありません。



Love you malspam におけるメール例
（※本文の顔文字は Thunderbird の機能により自動的に絵文字に変換されています。）

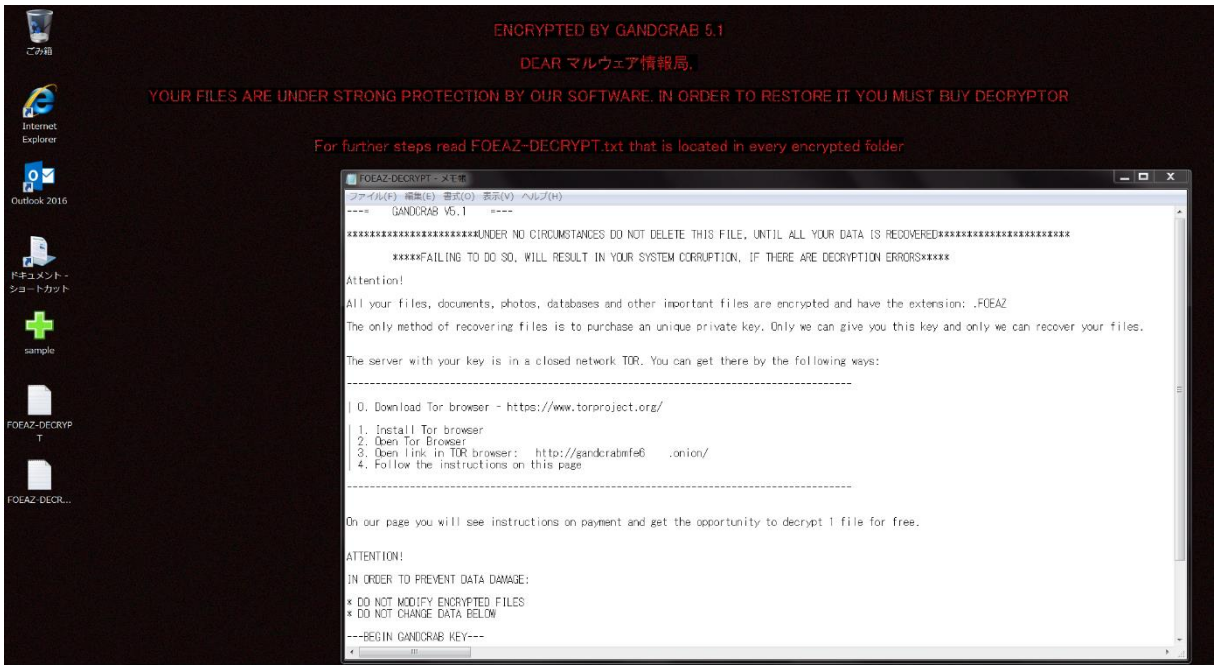
上記のメールは、最終的にダウンロードされるマルウェアの一つであるスパムボット Phorpiex により送信されます。

2 月に確認した Phorpiex の検体では、下記の件名リストがハードコードされていました。この検体には、日本の芸能人の名前が 89 件含まれ、大半が女性芸能人(83 件)の名前でした。また、別の検体では、男性芸能人の名前を多く含む検体も確認しています。

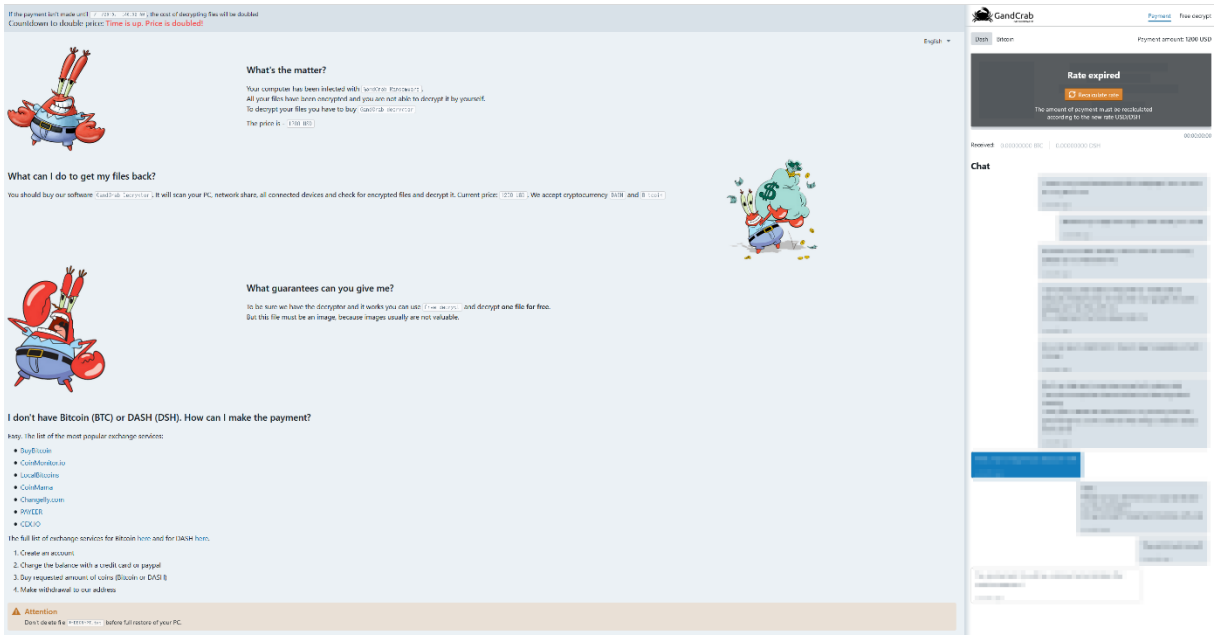
```
87654321  0011 2233 4455 6677 8899 aabb ccdd eeff  0123456789abcdef
0013c160: 0000 3a29 0000 3b29 0000 3a44 0000 3b44  ..:)..;)..:D..;D
0013c170: 0000 3a2d 2900 3a2d 4400 3b2a 0000 4973  ..:-).:-D.;*..Is
0013c180: 2074 6869 7320 796f 753f 3f00 0000 5261   this you??...Ra
0013c190: 7465 206d 7920 6e65 7720 7068 6f74 6f20  te my new photo
0013c1a0: 706c 6561 7365 2100 0000 4f75 7220 7068  please!...Our ph
0013c1b0: 6f74 6f00 0000 4b65 6570 2074 6869 7320  oto...Keep this
0013c1c0: 7072 6976 6174 6500 0000 446f 6e27 7420  private...Don't
0013c1d0: 7368 6f77 2061 6e79 6f6e 6521 0000 4973  show anyone!..Is
0013c1e0: 2074 6869 7320 796f 7572 2070 686f 746f   this your photo
0013c1f0: 3f00 5068 6f74 6f20 6f66 206c 6173 7420  ?.Photo of last
0013c200: 7061 7274 7900 5068 6f74 6f20 6a75 7374  party.Photo just
0013c210: 2066 6f72 2079 6f75 0000 4920 6c6f 7665   for you..I love
0013c220: 2079 6f75 2100 596f 7520 6172 6520 6d79   you!.You are my
0013c230: 206c 6f76 6521 0000 0000 596f 7520 6c6f   love!....You lo
0013c240: 6f6b 2073 6f20 7567 6c79 2068 6572 6500  ok so ugly here.
0013c250: 0000 596f 7520 7769 6c6c 2062 6520 7368  ..You will be sh
0013c260: 6f63 6b65 6421 0000 0000 4169 2048 6173  ocked!....Ai Has
0013c270: 6869 6d6f 746f 2100 0000 4169 204f 7473  himoto!...Ai Ots
0013c280: 756b 6121 0000 4169 7269 204d 6174 7375  uka!..Airi Matsu
0013c290: 6921 0000 0000 416b 696e 6120 4e61 6b61  i!....Akina Naka
0013c2a0: 6d6f 7269 2100 416c 6963 6520 4869 726f  mori!.Alice Hiro
0013c2b0: 7365 2100 0000 416e 6765 6c61 2041 6b69  se!...Angela Aki
0013c2c0: 2100 416f 6920 4d69 7961 7a61 6b69 2100  !.Aoi Miyazaki!.
0013c2d0: 0000 4179 6120 5565 746f 2100 0000 4179  ..Aya Ueto!...Ay
0013c2e0: 616d 6520 476f 7269 6b69 2100 0000 4179  ame Goriki!...Ay
0013c2f0: 756d 6920 4861 6d61 7361 6b69 2100 4368  umi Hamasaki!.Ch
0013c300: 6968 6972 6f20 4f6e 6974 7375 6b61 2100  ihiro Onitsuka!.
0013c310: 0000 4372 7973 7461 6c20 4b61 7921 0000  ..Crystal Kay!..
0013c320: 0000 4569 7220 416f 6921 0000 0000 456d  ..Eir Aoi!....Em
0013c330: 6920 5461 6b65 6921 0000 4572 696b 6120  i Takei!..Erika
0013c340: 5361 7761 6a69 7269 2100 4572 696b 6120  Sawajiri!.Erika
0013c350: 546f 6461 2100 4861 7275 6b61 2041 7961  Toda!.Haruka Aya
0013c360: 7365 2100 0000 4861 7275 6e61 204b 6177  se!...Haruna Kaw
0013c370: 6167 7563 6869 2100 0000 4861 7275 6e61  aguchi!...Haruna
```

メール送信に用いる件名リスト(一部)

別のダウンローダーのダウンロード先のサーバには、GandCrab が置かれている場合が多く、GandCrab に感染するとファイルが暗号化されます。



GandCrab v5.1 の暗号化後の脅迫画面



GandCrab の支払いページ

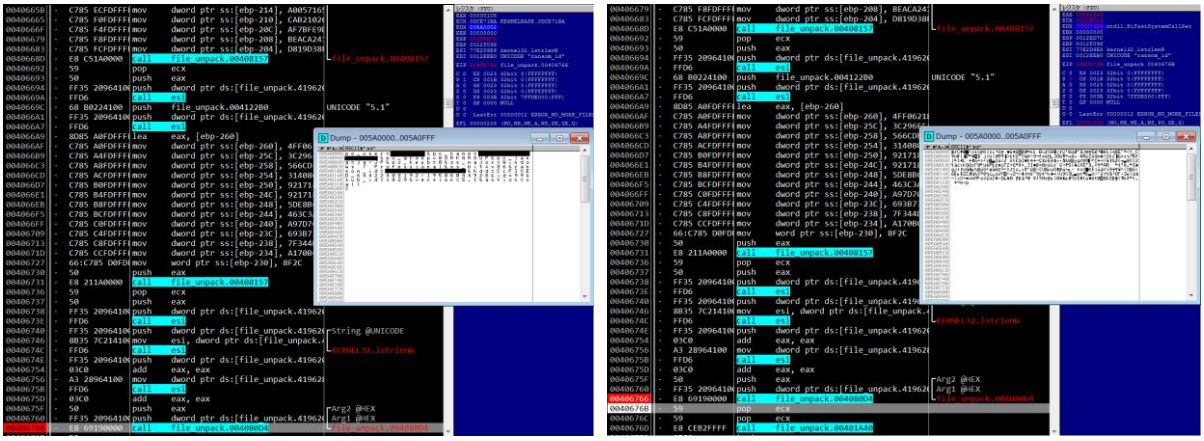
また、下記の情報を収集します（一部の情報は取得しない場合があります）。

収集する情報

pc_user	ユーザ名	
pc_name	コンピューター名	
pc_group	ドメイン	
av	セキュリティソフトの情報	
pc_lang	言語設定	
pc_keyb	キーボードの言語設定のフラグ	
os_major	OS バージョン	
os_bit	プロセッサアーキテクチャ	
ransom_id	ランサムウェア ID（ボリュームシリアルナンバー、プロセッサー名、プロセッサーファミリから作成）	
hdd	ハードディスク情報（ドライブ種類、総容量、使用容量）	
GandCrab の情報	id	99
	sub_id	1029
	version	5.1

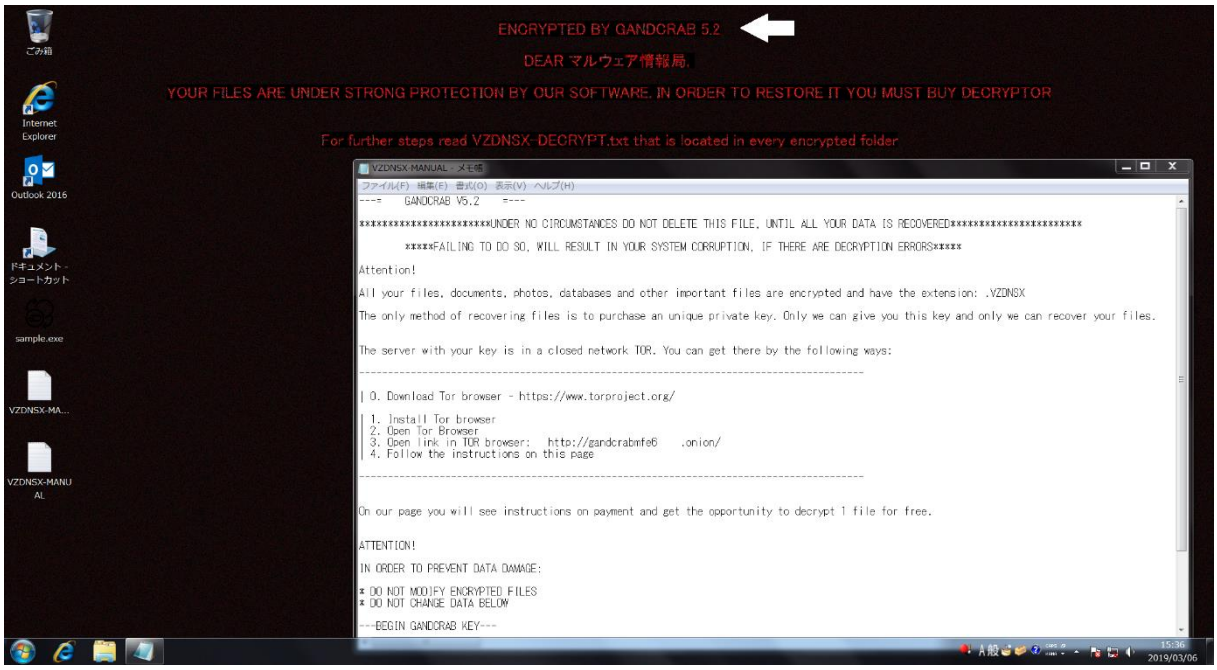
	action	call

収集したデータは下図のように暗号化されます。



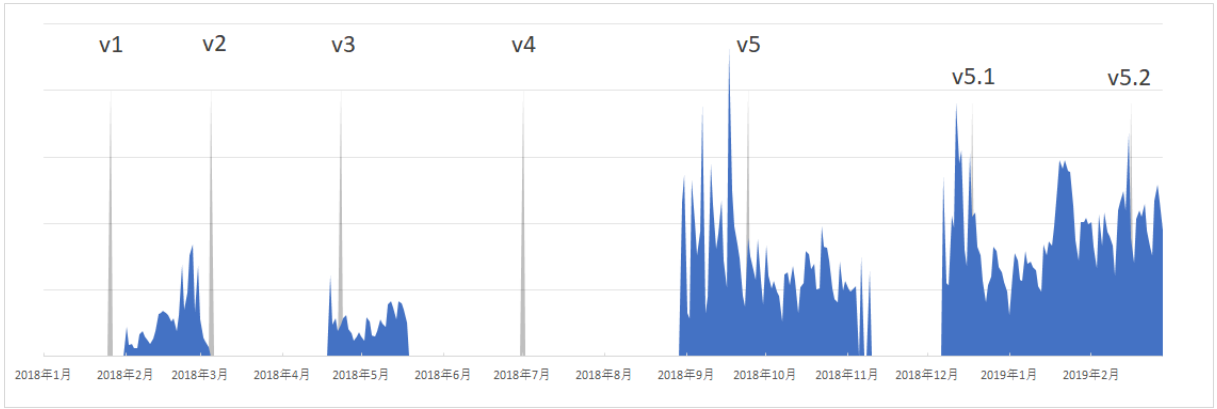
収集したデータ(左)、暗号化のデータ(右)

1 月に観測された GandCrab v5.1 は、「No More Ransom」からダウンロードできる復号ツールに対応しています。しかし、2 月中旬に観測された GandCrab は v5.2 にバージョンアップされています。3 月上旬現在の段階では復号ツールは対応していません。



GandCrab v5.2 の暗号化後の脅迫画面

2018 年 4 月 マルウェアレポートの Adobe Flash Player の脆弱性を悪用しランサムウェアに感染させる攻撃でもご紹介したように、GandCrab は 2018 年 1 月末にバージョン 1 が確認されて以来、頻繁にバージョンアップが行われています。



世界の GandCrab の検出数と GandCrab のバージョン*4

*4 GandCrab として検出した検出数のみを表示しています。Kryptik などとして検出した場合は含みません。

2018 年、2019 年と継続的に検出していることが確認できます。特に 2018 年後半から検出数が増えていますので、今後も注意が必要です。

Love you malspam では、メールに添付された JS 形式のダウンローダーを実行すると様々なマルウェアに感染する可能性があります。
このようなマルウェアに感染しないためにも、侵入の初期段階であるメールにおいて下記のような基本的な対策を行うことが重要です。

- 不審なメールの添付ファイルは開かない
- 不審なメールに記載された URL にはアクセスしない
- 不審メールの注意喚起情報を確認し共有・周知する
- .js の拡張子の関連付けをメモ帳などに変更する（日常的に JavaScript を使用していない場合）
- メールアドレスの変更を検討する（既に不審メールを受信している場合）

また、Phorpiex などに感染し、自身の PC から感染を拡大していないか、ネットワークログなどから不審なメールを送信していないことを確認してください。

ESET 製品では、JS 形式のダウンローダーが含まれた zip ファイルを添付したメールを「JS/Danger.ScriptAttachment」、GandCrab を「Win32/Filecoder.GandCrab」、Phorpiex を「Win32/Phorpiex」などの検出名で検出します。

ESET Endpoint Security V6.6 における JS/Danger.ScriptAttachment の検出画面

ESET Endpoint Security V6.6 における Win32/Filecoder.GandCrab の検出画面

ESET Endpoint Security V6.6 における Win32/Phorpiex の検出画面

ご紹介したように、1 月･2 月はランサムウェア GandCrab の感染を狙った malspam が数多く観測されました。この malspam では複数のマルウェアに感染する可能性があります。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ 常日頃からリスク軽減するための対策について

各記事でご案内しているようなリスク軽減の対策をご案内いたします。
下記の対策を実施してください。

1. ESET 製品プログラムのウイルス定義データベースを最新にアップデートする
ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しております。
最新の脅威に対応できるよう、ウイルス定義データベースを最新にアップデートしてください。

2. OS のアップデートを行い、セキュリティパッチを適用する
ウイルスの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。
「Windows Update」などの OS のアップデートを行い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する
ウイルスの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく
万が一ウイルスに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。 念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る
「知らない人」よりも「知っている人」の方がウイルスに感染するリスクは低いと考えられます。ウイルスという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

Canon

キヤノンマーケティングジャパン株式会社