LAC

# サイバー救急センターレポート

- 脅威管理とインシデント対応をする人へ -

## プロキシサーバのすゝめ（ログの保管運用編）

## エクスプロイトキットの最新動向

白浜シンポジウムセキュリティ道場／DFRWS EU 2019 への参加

**第７号**

2019 夏

CYBER EMERGENCY CENTER

2019 年 7 月 31 日

サイバー救急センター

# サイバー救急センターレポート

## 第 7 号／2019 夏

### 目　　次

# はじめに

鷲尾　浩之

株式会社ラック
サイバー救急センター長

今年 4 月からセンター長に就任しました鷲尾です。引き続き本レポートで、皆様のセキュリティ運用に役立つ情報を発信していきたいと思いますので、よろしくお願いします。

セキュリティ事故が発生する原因は様々であり、サイバー救急センターには日々多くの相談を寄せていただいている状況ですが、事故原因で多いのはやはり運用管理上の不備です。本レポート内の「サイバー119 の出動傾向」でも触れていますが、発生した事故の原因としてはアカウント情報管理、アクセス制御、修正プログラムの適用不足・不備が多いという傾向があります。これらはセキュリティ運用において基本的な事項であるにも関わらず、事故原因として多くあげられることの真因の一つは、IT システムの利用者や運用者のなかにある「過信や油断」にあるのではないかと思います。

「セキュリティ対策は事故前提でリスクを評価する」というのはよく言われる話ですが、事故前提ということは、組織内の限られた人しか使わないようなシステムやクローズドなネットワークで使われる端末であっても、セキュリティ対策のレベルを下げてはいけないということです。

セキュリティ運用における PDCA サイクルのなかで、「過信や油断」によって管理が甘くなってしまっている部分がないか、今一度チェックしていただくことを推奨します。

想定外を想定内に。常に脅威の想定を見直して、想定外に備えていきましょう。

# サイバー119の出動傾向

## 2019年1月～6月の出動傾向

当該期間は、サーバを対象としたマルウェア感染、不正侵入のインシデントが発生した組織からの相談が多くありました。

攻撃の手口としては、悪用され続けている脆弱性の修正プログラムの適用漏れや通信のアクセス制御の不備、アカウント管理の不備といった運用管理上のミスとなります。構築時には適切な管理状況であったものの、運用中に管理が甘くなってしまったサーバがないか、改めて確認することを推奨します。

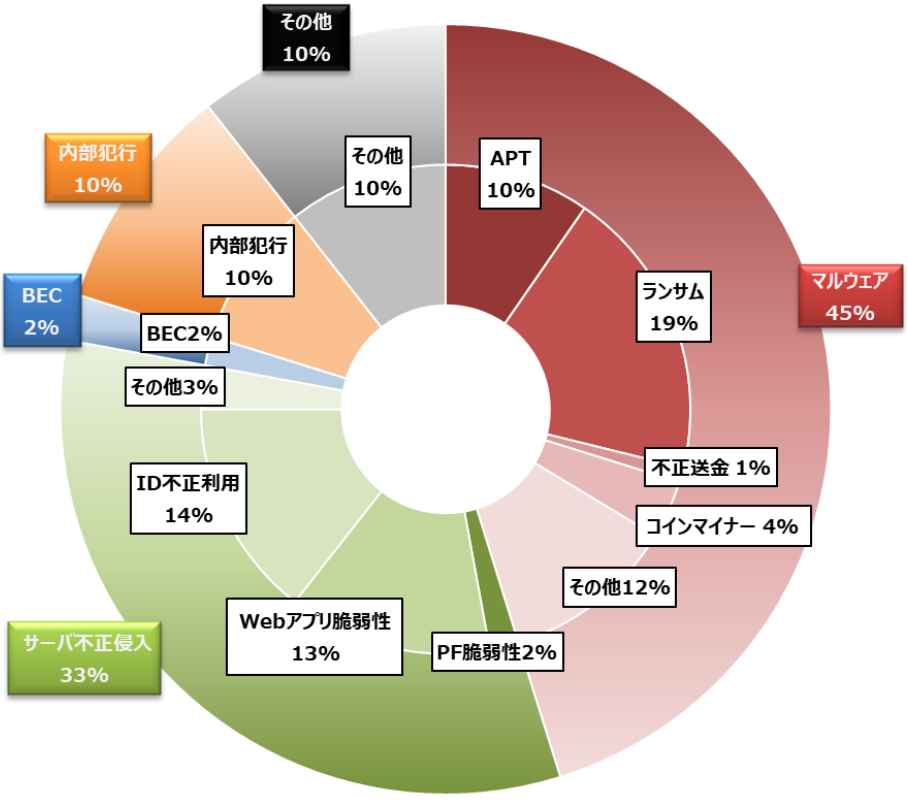



**図 1 2019年 1月～6月のインシデント傾向**

# 不正アクセスのインシデント傾向

クラウド環境上のデータベースを使用した Web システムが不正アクセスを受けたという相談を、複数の組織から受けています。いずれも、Web システムの開発時や運用保守を行う際に開放していた PostgreSQL のリモート接続ポート（5432/tcp）が、アクセス制限なしにインターネット上から接続可能になっており、かつ容易に推測可能なパスワードが設定されていたために、辞書攻撃などでパスワードが推測され、不正にログインされたというものです。

被害を受けた組織では、不正アクセスによって以下の事象が確認されています。このことから攻撃者は、金銭目的（データを人質に脅迫して身代金を得る）で不正アクセスを行っているものと推察されます。

- データベースがテーブルごと削除されている
- 残されたスキーマ名にハッキングしたことを示すメッセージと連絡先を示した痕跡が残されている

このような不正アクセスの被害に遭わないようにするため、ファイアウォールなどのネットワーク機器のアクセス制御ルールの再確認、脆弱性診断の実施など、これまで不備が無いと判断していた箇所について、改めてチェックすることを推奨します。

# マルウェアのインシデント傾向

2017 年 5 月に発生した WannaCry は、約 2 年経過しても未だに被害を受けた組織からの相談を受けています。初期の WannaCry は、Microsoft Windows の脆弱性「MS17-010」を標的とする EternalBlue と呼ばれる攻撃ツールと、DoublePulsar と呼ばれるバックドアプログラムを用いることで、感染した端末上でファイルの暗号化を行い身代金を要求するランサムウェアとしての機能と、自ら感染を広めるワーム機能を備えていました。

2019 年 1 月から 6 月の期間にあった弊社への相談内容は、この 2 つの機能のうちのワーム機能のみが備わった亜種に感染したというものでした。マルウェアに感染した対象端末は、WannaCry の感染拡大で悪用される脆弱性「MS17-010」の修正プログラムを未だに適用していなかったサーバ群であり、これらは他のネットワークと接続していないクローズドなネットワークに存在していました。しかしながら、メンテナンスなどで外部の PC をこのネットワークに接続する必要があり、接続したメンテナンス用 PC がランサムウェアに感染していたため、クローズドなネットワーク内に感染被害が拡大したと考えられます。

クローズドなネットワーク内のシステムであっても、メンテナンス等で外部の PC を接続する運用がある場合には、ネットワーク内のすべての端末、サーバに対して「MS17-010」の適用状況を改めて確認ください。

また、自組織の管理対象ではないPCやサーバをネットワークに接続する場合には、その対象端末が自組織のセキュリティポリシーに相当する管理がされているものかどうかを確認し、無許可で管理対象外の端末がネットワークに接続できない仕組みや運用の徹底を推奨します。また、WannaCry のような広く流行しているマルウェアはクローズドな環境でもウイルス対策ソフトで検知できる場合もあるため、ウイルス対策ソフトの導入、定義ファイルのアップデート、リアルタイムスキャンや定期スキャンの有効化も検討ください。

なお、クローズドな環境にあるシステムにおける定義ファイルアップデートは、インターネット通信可能な管理サーバを構築するか、インターネット通信可能な別端末で定義ファイルをダウンロードし外部記憶媒体経由でアップデートする仕組みを検討ください。その際、インターネットの通信先は限定、もしくは外部記憶媒体を経由してアップデートする際は、許可された外部記憶媒体のみ利用可能な仕組みも併せて検討ください。

# 攻撃者の残した痕跡に学ぶ

## プロキシサーバのすゝめ（ログの保管運用編）

皆様はログをどのように保管されているでしょうか？セキュリティインシデントにおいて、ログは重要な手がかりとなります。

一口にログといっても、Windows のイベントログ、Linux の Syslog、そしてファイアウォールや Web プロキシサーバ（以降、プロキシサーバと記載します。）、IPS や IDS[1]などのネットワーク機器のログなど多くの種類があります。このうち、マルウェアに感染した端末を特定できる可能性があるのが、ネットワーク機器のログです。今回はプロキシサーバのログについて、取得する際の注意点をお伝えします。

セキュリティ対策でログというと、真っ先に検討対象に上がるのが「ログの保管期間」です。これは 2018 年に公開したサイバー救急センターレポート第 2 号[2]でも「プロキシサーバのすゝめ」と題して紹介しましたが、少なくとも 1 年以上保管することを推奨しています。一方で、ただ保管しておくだけでなく、すぐに取り出し、調査できる状態にしておくことも重要です。

多くの組織では、直近のログはサーバ上に置いておき、古いログは別媒体に保管する運用かと思います。この古いログの保管場所や取り出し方などを確認し、インシデント調査の際に迅速に参照できるかテストしておくことを推奨します。

### (1)まずはログ出力設定の見直しから

さて、今回は、サイバー救急センターで対応した様々な事例をもとに、第 2 号では紹介しきれなかったプロキシサーバーログの適切な保管方法や運用上の注意点について解説します。

ログの保管期間について先述しましたが、単にログの保管期間が長ければよいというものではありません。ログに記録される情報が不足していると、せっかく保管したログが役に立たないということもあります。例えば著名なプロキシサーバである Squid のデフォルト設定で記録されたログを図 2 に示します。

[1] ネットワーク通信を監視し、攻撃を検知するシステム。IDS は攻撃を検知するのみで、IPS は攻撃を遮断する。

[2] https://www.lac.co.jp/lacwatch/report/20180302_001587.html

```
1560475304.218     122 192.168.0.1 TCP_MISS/200 31091 GET http://www.example.jp
/ - HIER_DIRECT/192.168.0.2 text/html
```

**図 2 デフォルト設定で記録されたログの例**

このログには、時刻（UNIX 時間[3]）、接続先 URL、接続元 IP アドレス、接続先 IP アドレスといった基本的な情報は記録されています。しかし、HTTP リファラ（以降、リファラと記載します。）や、ユーザエージェントが記録されていません。また、UNIX 時間は人間には理解しづらい時刻フォーマットです。そこで、以下のような設定を行うことで、ログに記録される項目を追加、修正します。

```
strip_query_terms off
logformat combined %>a %>p %[un [%tl] %<a %<p %<A "%rm %ru HTTP/%rv" %>Hs %>st
 %<st "%mt" "%{Referer}>h" "%{User-Agent}>h" %Ss:%Sh
access_log daemon:/var/log/squid3/access.log combined
```

**図 3 Squid 3.5 の推奨設定[4]**

上記の設定を行った後に記録されたログを以下に示します。

```
192.168.0.1 58250 - [14/Jun/2019:10:24:18 +0900] 192.168.0.2 80 "GET
http://www.example.jp/ HTTP/1.1" 200 389 31090 "text/html" "
http://www.example.jp/" "Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101
Firefox/60.0" TCP_CLIENT_REFRESH_MISS:HIER_DIRECT
```

**図 4 推奨設定を行ったログの例**

図 2 で示したログと図 4 で示したログを比較すると、主に以下の点が改善されています。

・時刻が見やすく、日本時間で記録されるようになった
・リファラが記録されるようになった
・ユーザエージェントが記録されるようになった
・URL のクエリが記録されるようになった

[3] UTC で 1970 年 1 月 1 日午前 0 時 0 分 0 秒から数えた秒数。システム内部で使われている時刻。

[4] 記載している設定は、弊社の検証環境で動作することを確認していますが、すべての環境で問題なく動作するとは限りません。設定を反映する際は、問題なく動作するか検証の上、反映してください。

リファラやユーザエージェントは、通常のブラウザによる通信とマルウェアによる通信とでは、異なる文字列が記録される傾向[5]があります。そのため、リファラやユーザエージェントがログに記録されることによって、マルウェアによる通信を発見しやすくなります。

## (2)ログが不足している例

また、ネットワーク環境によっては、ログを保管してもマルウェアに感染した端末を特定できない場合があります。よくある事例としては DHCP 環境であるため、各種ログに記録されたクライアント IP アドレスから端末が特定できないというケースです。

以下のようなネットワークがあったとします。

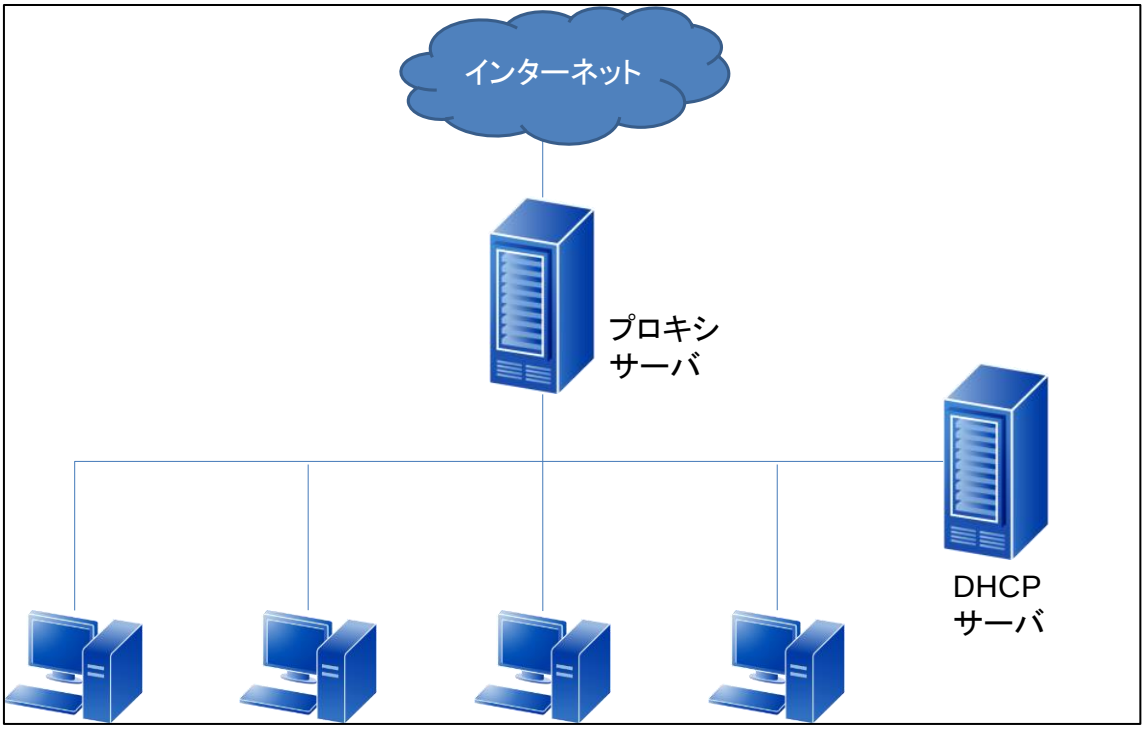



**図 5 ネットワークの一例**

上記のネットワーク図内にあるプロキシサーバのログに、以下の不審な通信が記録されていたとします。さて、このログから端末が特定できるでしょうか？

[5] リファラとユーザエージェントは偽装することができるため、リファラとユーザエージェントだけでマルウェアによる通信と判断するのは通常困難ですが、他の情報と合わせて検討することで判断の精度を上げることができます。

```
192.168.0.1 876 - [14/Jun/2019:15:34:24 +0900] 192.168.0.3 80 malware.evil "GE
T http://malware.evil/malware.exe HTTP/1.1" 200 389 31090 "text/html" "" "" TC
P_CLIENT_REFRESH_MISS:HIER_DIRECT
```

**図 6 プロキシサーバのログの例**

残念ながら、この場合は、このネットワークから不審な通信が発生していることはわかりますが、DHCPサーバにより動的に IP アドレスが割り当てられているため、端末の特定はできません。端末を特定する場合は、DHCP ログが必要になります。

このように、せっかくログが保管されていても、ネットワーク構成によってはログが不足していて十分な調査ができないこともあります。なお、認証が必要なプロキシサーバを利用している場合には、ユーザ名をログに記録する設定とすることで、ユーザ（＝端末）の特定が可能となります。

## (3)まとめ

プロキシサーバのログに限らず、様々なログはセキュリティインシデント発生時の調査において重要な手がかりになるため、できるだけ長期間保管することを推奨します。また、ログを保管する際には、どのようなログを保管するか、どのような情報をログに記録するか、ログは迅速に参照できるかについても考慮する必要があります。

マルウェアに感染したという想定で、現在取得しているログから感染端末の特定が本当にできるのか、事前にシミュレーションしておくと、実際にインシデントが発生した際にスムーズな対応が可能になりますので、インシデント対応訓練の一環として平時に練習しておくことを推奨します。

# 脅威分析報告

## エクスプロイトキットの最新動向

エクスプロイトキットは、Web ブラウザや Adobe Flash Player などの Web サイトを閲覧する際に利用するソフトウェアの脆弱性などを悪用して、閲覧者の PC をマルウェアに感染させるために攻撃者が用いる攻撃ツールです。エクスプロイトキットで有名な Angler Exploit Kit[6]が流行していた 2015 年と比較すると、エクスプロイトキットを使用した攻撃活動は減少傾向であると見られます。一方で、一部の攻撃者は複数のエクスプロイトキットを併用し、現在も攻撃活動を継続しています。

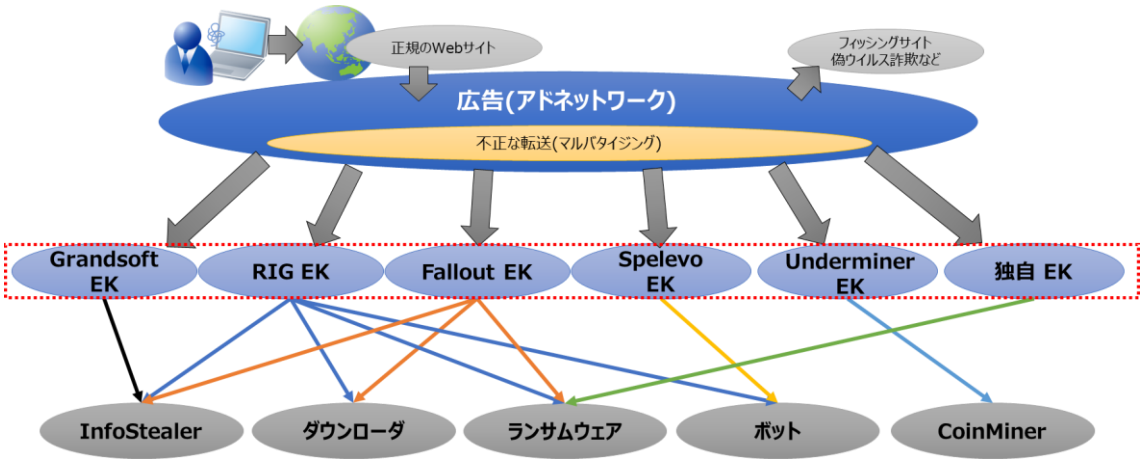



**図 7 広告経由によるエクスプロイトキットへの誘導事例**

エクスプロイトキットへの誘導は、図 7 のように閲覧者が正規の Web サイトを閲覧している際に、サイト内に表示されている広告などから意図せずに別のサイトへ転送させる方法で行われます。このように不正な広告からの誘導先には、エクスプロイトキットによる攻撃サイトを含め以下のようなサイトへの転送を確認しています。

- エクスプロイトキットが仕掛けられた攻撃サイト
- マルウェアをダウンロードさせるサイト
- ソフトウェアのアップデートを促す偽サイト
- マイクロソフトを騙るサポートサイト

[6] Exploit Kit を表内および攻撃ツール名を表記する際に、EK と記載します。

ここではサイバー救急センターの脅威分析チームが、2019 年 1 月から 2019 年 6 月までの半年間、広告からマルウェアに感染する恐れのあるエクスプロイトキットへの誘導に焦点をあて、エクスプロイトキットの動向を分析した結果を報告します。

今回の調査期間では、6 種類のエクスプロイトキットを利用する攻撃活動を確認できました（図 7 内の赤枠）。脅威分析チームが個別の名称を把握していない一部のエクスプロイトキットは、以降、独自 EK と記載します。

## (1)エクスプロイトキットへの誘導について

2017 年以前は改ざんされた正規サイトが、エクスプロイトキットへ誘導する温床となっていました。しかし、現在のエクスプロイトキットへの誘導方法の多くは、正規サイトに表示される広告の仕組みを悪用する方法になっています（図 8）。

攻撃者が広告を利用するようになった背景の一つとして、2017 年 2 月に民間企業と法執行機関の協力によって、国内外で改ざんサイトの無害化が進んだため、別の手法を使い始めたと考えられます。[7]

| Time | Host | URL | Body | Content-Type | Comments |
|---|---|---|---|---|---|
| 2019/05/28 22:21:56 | [redacted] | /ad/ad?p=38636&w=42... | 1,661 | text/html; charset=utf-8 | Malvertising |
| 2019/05/28 22:21:57 | | /aS/feedclick?s=rI4dICd... | 0 | | Malvertising |
| 2019/05/28 22:21:57 | | /adServe/adClick?ai=oV... | 0 | | Malvertising |
| 2019/05/28 22:21:58 | | /?utm_trc=Worldwidepo... | 0 | text/html; charset=utf-8 | Malvertising |
| 2019/05/28 22:21:59 | 92.63.102.1 | /?MjM0Mzkz&XOCWAEU... | 16,663 | text/html;charset=UTF-8 | RIG EK |
| 2019/05/28 22:22:00 | 92.63.102.1 | /?MjUyMTQ0&amfZmAe... | 9,364 | application/x-shockwave-flash | RIG EK |
| 2019/05/28 22:22:01 | 92.63.102.1 | /?NTExNzIz&msXCETQa&... | 160,256 | application/x-msdownload | RIG EK |

**図 8 広告経由によるエクスプロイトキットへの誘導事例（RIG EK）**

[7] RIG-EK 改ざんサイト無害化の取組
https://www.jc3.or.jp/topics/op_rigek.html

## (2)エクスプロイトキットが悪用している脆弱性

今回の調査期間において、各々のエクスプロイトキットと、それらが悪用する脆弱性との対応は、表 1 の通りです[8]。

| EK／脆弱性 | VBScript EngineのRCE | | | Adobe Flash PlayerのRCE | |
|---|---|---|---|---|---|
| | CVE-2016-0189 | CVE-2018-8174 | CVE-2018-8373 | CVE-2018-4878 | CVE-2018-15982 |
| Grandsoft EK | ● | ● | – | – | – |
| RIG EK | ● | ● | – | ● | – |
| Fallout EK | – | ● | ● | ● | ● |
| Spelevo EK | – | – | – | – | ● |
| Underminer EK | – | ● | – | ● | ● |
| 独自EK | – | ● | – | – | – |

**表 1 エクスプロイトキットが悪用する脆弱性について**

これらの脆弱性がエクスプロイトキットに誘導された端末に存在していた場合、その端末はマルウェアに感染することになります。なかでも「CVE-2018-8174」については、Grandsoft EK や RIG EK だけでなく独自 EK も含む、ほとんどのエクスプロイトキットが悪用しており、未対策の場合にはマルウェア感染のリスクが高まります（図 9）。

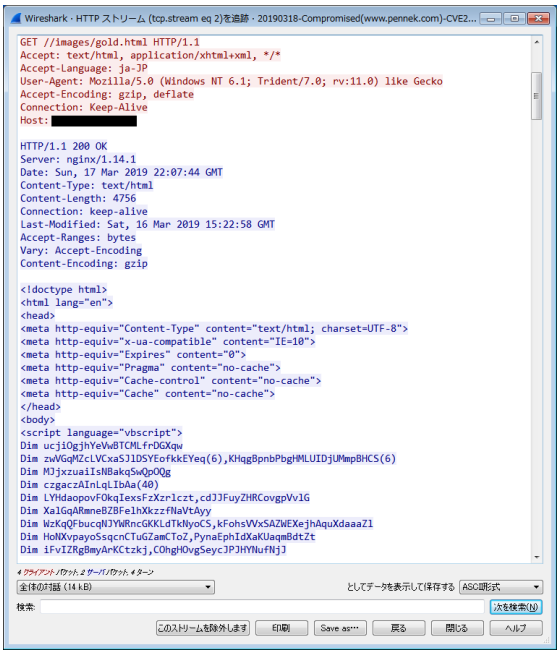



**図 9 独自 EK による CVE-2018-8174 の悪用事例**

[8] 週末なにしてますか？ 忙しいですか？ DbD を解析してもらっていいですか？
https://jsac.jpcert.or.jp/archive/2019/pdf/JSAC2019_1_koike-nakajima_jp.pdf

次からは、エクスプロイトキットの種類ごとにその活動状況を紹介します。

## (3)Grandsoft EK

Grandsoft EK の特徴は以下のとおりです。

- 2018 年 2 月頃から活発なエクスプロイトキット
- オンラインバンキングの情報や Web の閲覧履歴などの情報を窃取する「Ramnit」を継続的に配布

  時期によっては、「AZORult」や「Vidar」、「Pony」と呼ばれる InfoStealer[9]と合わせて配布（表 2）
- 2019 年 6 月上旬に新たに「IceID」と呼ばれる InfoStealer を単体で配布（図 10）

| Time | Host | URL | Body | Content-Type | Comments |
|---|---|---|---|---|---|
| 2019/06/04 14:50:05 | warming.simbaooshi.space | /purists_allies.html | 542 | text/html; charset=utf-8 | Grandsoft EK |
| 2019/06/04 14:50:06 | warming.simbaooshi.space | /getversoinpd/1/2/3/4 | 21,214 | text/html; charset=utf-8 | Grandsoft EK |
| 2019/06/04 14:50:07 | warming.simbaooshi.space | /9/80790640 | 436,8... | application/octet-stream | Grandsoft EK |
| 2019/06/04 14:55:16 | 95.213.217.139 | /Tini_Projectx86.exe | 3,911,... | application/octet-stream | |
| 2019/06/04 14:55:16 | 95.213.217.139 | /SWKLPDVX.exe | 151,5... | application/octet-stream | |
| 2019/06/04 14:55:16 | 54.36.218.96 | /tin.exe | 342,5... | application/octet-stream | |
| 2019/06/04 14:55:16 | Tunnel to | 195.69.187.86:443 | 473 | | |
| 2019/06/04 14:55:20 | wagenstead.xyz | /data2.php?CBBD537FA0... | 0 | | |
| 2019/06/04 15:00:44 | thracial.pw | /data2.php?CBBD537FA0... | 0 | | |

IceID

**図 10 Grandsoft EK から IceID 感染事例**

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| InfoStealer | AZORult | → | | | | | |
| | IceID | | | | | | → |
| | Vidar | | | → | | | |
| | Pony | → | | | | | |
| | Ramnit | → | → | → | → | → | → |

**表 2 Grandsoft EK にて配布されていたマルウェア**

なお、2019 年 6 月中旬から 7 月下旬まで、Grandsoft EK を利用した攻撃の観測が途絶えています。6 月上旬ごろから、セキュリティ研究者の調査を妨げるために、IP アドレスまたは位置情報などから Grandsoft EK の観測ができないことがありました。今後も Grandsoft EK の攻撃活動を注視していきます。

[9] 侵入先のコンピュータから機密情報を収集する類いのマルウェアを指します。

## (4) RIG EK

RIG EK の特徴は以下のとおりです。

- 2016 年 9 月頃から最も活発なエクスプロイトキット[10]
  活動を停止する時期もありますが、執筆時点の 2019 年 7 月下旬も観測
- RIG EK に利用される通信先の多くがロシアの IP アドレス
- InfoStealer やランサムウェアの他にボットなど様々なマルウェアを配布（表 3）

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| InfoStealer | Amadey | | | → | | | |
| | AZORult | → | → | → | → | → | → |
| | Baldr | | | | | → | |
| | Kpot | | | → | | | |
| | Vidar | → | → | | | | |
| ダウンローダ | Smokeloader | → | | | → | | |
| ランサムウェア | Buran | | | | | | → |
| | GandCrab | → | → | | → | | |
| | GetCrypt | | | | | → | |
| | Paradise | | | → | | | |
| | Maze | | | | | | → |
| | Sodinokibi | | | | | | → |
| | Unknown | | | | | → | |
| ボット | Electrum DoS Miner | | | | → | → | |
| | Phorpiex | | | | | → | |
| | Pitou | | | | | | → |
| | Tofsee | | | | | | → |

**表 3 RIG EK にて配布されていたマルウェア**

[10] CYBER GRID VIEW Vol.3「猛威を振るう RIG Exploit Kit の全貌と対策」
https://www.lac.co.jp/lacwatch/report/20170202_001203.html

RIG EK を利用する攻撃者は、2019 年 5 月下旬から 6 月下旬までの間に 3 種類のスパムメールの拡散に利用されるスパムボットを配布していました。各々のスパムボットが、下記のようなスパムメールの拡散を試みていました。

- Phorpiex：セクストーションメール[11]
- Tofsee：アダルトサイトの会員登録を促すスパムメール
- Pitou：ドラッグやギャンブルの宣伝目的としたスパムメール

「Phorpiex」は、2019 年 1 月から顔文字や芸能人の名前（図 11）を用いて、ランサムウェア「GandCrab」やオンラインバンキングの情報を窃取するマルウェア「Ursnif」を拡散していました。RIG EK から配布されていた「Phorpiex」は、図 12 のような仮想通貨を要求するセクストーション[12]と呼ばれるスパムメールの拡散のみでした。今後、マルウェア等を拡散する可能性もあるため、引続き注視していきます。

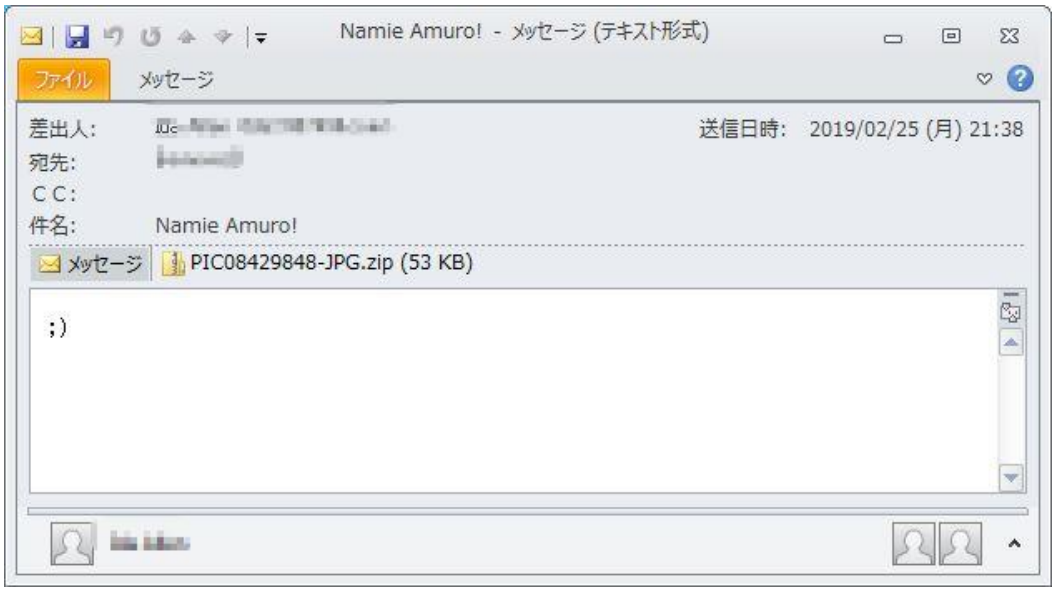



**図 11 女性芸能人の名前を含むマルウェアスパムの例**

[11] 性的な内容で根拠なく脅し、仮想通貨を要求する脅迫メール
「セクストーション」とは、「sex（性的な）」と「extortion（ゆすり、恐喝）」という言葉を足し合わせた造語です。

[12] 仮想通貨を要求するセクストーション詐欺スパム
https://blog.kaspersky.co.jp/sextortion-scam/22706/

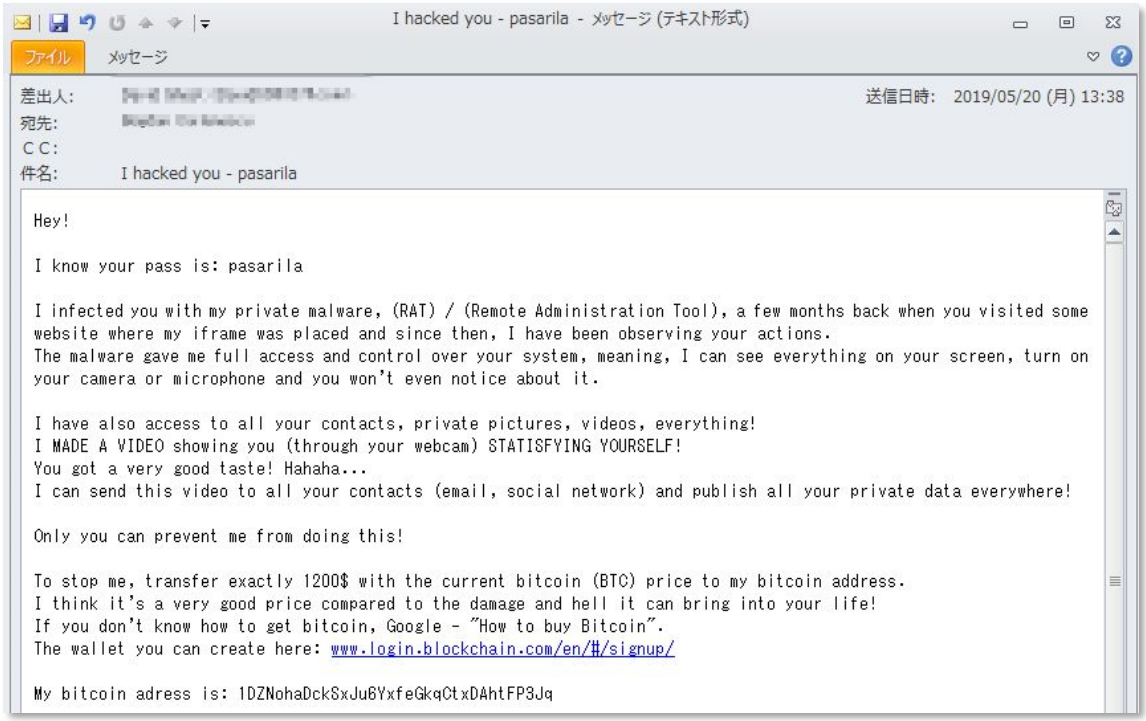



**図 12 「Phorpiex」から配布を試みていたメールのサンプル**

## (5) Fallout EK

Fallout EK の特徴は以下のとおりです。

- 2018 年 8 月頃から悪用されているエクスプロイトキット
- 誘導時に RIG EK と同一のインフラを度々利用（図 13）
- InfoStealer やランサムウェアなどのマルウェアを配布（表 4）

| Time | Host | URL | Body | Content-Type | Comments |
|---|---|---|---|---|---|
| 2019/06/13 7:10:48 | [redacted] | /ad/ad?p=38636&w=42411... | 69 | text/html; charset=utf-8 | Malvertising |
| 2019/06/13 7:10:50 | | /BD9mJN?cost=0.00110 | 179,366 | text/html; charset=utf-8 | Compromised |
| 2019/06/13 7:10:57 | traffstats.info | /PKXjnL?cost=0.00110 | 598 | text/javascript;charset=UTF-8 | Redirector |
| 2019/06/13 7:11:01 | butthurtrain.com | /7845_Splitters_Anaphora/... | 4,497 | text/html;charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:05 | butthurtrain.com | /sundered-Finery/calderon... | 28,883 | text/javascript;charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:06 | butthurtrain.com | /15993/Redroot | 7,704 | text/html; charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:07 | butthurtrain.com | /iKQm/Gangion/forded-dian... | 28,716 | text/html; charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:07 | butthurtrain.com | /favicon.ico | 0 | text/html; charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:08 | butthurtrain.com | /Longbeard_potentate/Rep... | 35,149 | application/x-shockwave-flash | Fallout EK |
| 2019/06/13 7:11:08 | butthurtrain.com | /1962_05_25/1995-03-02.a... | 0 | text/html; charset=UTF-8 | Fallout EK |
| 2019/06/13 7:11:11 | butthurtrain.com | /7845_Splitters_Anaphora/... | 0 | text/html; charset=UTF-8 | Fallout EK |

**図 13 広告経由による Fallout EK への誘導事例**

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| InfoStealer | Amadey | | → | | | | |
| | AZORult | → | | | | → | |
| | Kpot | | | | | → | |
| | Raccon | | | | | | → |
| | Vidar | | → | | | | |
| ダウンローダ | Smokeloader | → | | | | | |
| ランサムウェア | GandCrab | → | → | | → | | |
| | Maze | | | | | | → |

**表 4 Fallout EK にて配布されていたマルウェア**

Fallout EK が利用され始めた 2018 年 8 月頃のドメインは、セキュリティ研究者を揶揄したドメイン名をつけていた時期がありましたが、最近のドメインにはそのような傾向はなく特定しづらい状況です。さらに、Fallout EK の通信は、HTTPS で暗号化されているため、フィルタリングや検知をするためには暗号化通信を復号する必要があります。

また、Fallout EK へ誘導する転送サイトを定期的に変更するなど、活動も活発なため注意が必要です。

## (6)Spelevo EK

Spelevo EK の特徴は以下のとおりです。

- 2019 年 3 月頃に確認された新しいエクスプロイトキット
- 誘導時に RIG EK と同一のインフラを度々利用
- 「PsiXBot」と呼ばれるボットを配布(図 14、表 5)

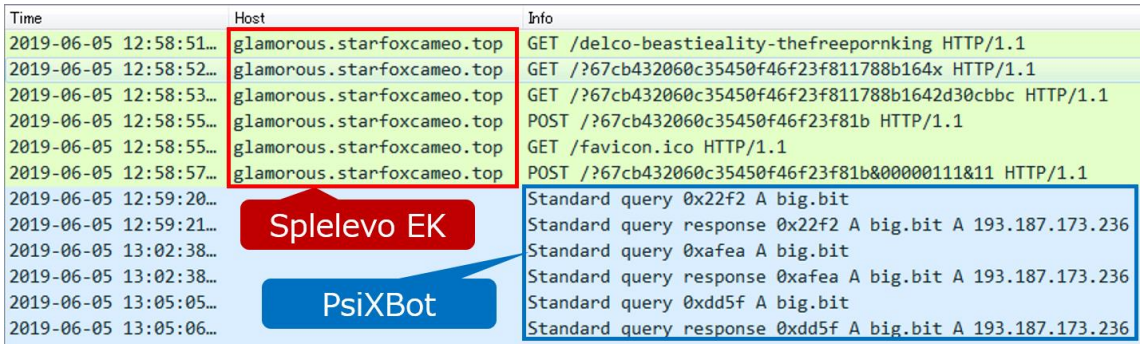



**図 14 Spelevo EK から PsiXBot 感染事例**

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| ボット | PsiXBot | | | → | | | → |

**表 5 Spelevo EK にて配布されていたマルウェア**

Spelevo EK は、2019 年 3 月に確認された比較的新しいエクスプロイトキットです。今回の調査では「PsiXBot」と呼ばれるボットの配布を確認しましたが、「IceID」と呼ばれる InfoStealer や「Shade」と呼ばれるランサムウェアを配布していたとの報告があります[13]。そのため、Spelevo EK を利用する攻撃者が他のマルウェアを配布する可能性が考えられるため、引続き注意が必要です。

## (7) Underminer EK

Underminer EK の特徴は以下のとおりです。

- 2018 年 7 月頃から活動しているエクスプロイトキット
- 2019 年 4 月ごろから長期にわたり広告経由で誘導（図 15）
- 仮想通貨の採掘に用いられる「Hidden Bee」と呼ばれる CoinMiner を配布（表 6）

| Time | Host | URL | Body | Content-Type | Comments |
|---|---|---|---|---|---|
| 2019/06/12 7:15:20 | [redacted] | /ad/ad?p=38636&w=424119&d=8f3342... | 50 | text/html; charset=utf-8 | Malvertising |
| 2019/06/12 7:15:22 | | /OUvuF | 0 | text/html; charset=UTF-8 | Malvertising |
| 2019/06/12 7:15:22 | 174.139.17.164 | /XKIOEEEEE.KDJDD.php | 0 | text/html; charset=UTF-8 | Redirector |
| 2019/06/12 7:15:23 | 174.139.17.164 | /9B2MlV3hJrXeoCulSq8PJUIG3w3AFY8c.... | 4,271 | text/html; charset=UTF-8 | Redirector |
| 2019/06/12 7:15:24 | 38.75.136.186:9081 | /index.php?ad_id=Nqt0zi5kdKZiBlRMPTy... | 2,988 | text/html; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:24 | 38.75.136.186:9081 | /js/rbl8ki1o9tsif4h7hn4tb4faa8.js | 9,441 | text/javascript; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:25 | 38.75.136.186:9081 | /logo.swf | 638 | application/x-shockwave-flash | Underminer EK |
| 2019/06/12 7:15:28 | 38.75.136.186:9081 | /pubs/servlet.php?fp=aebfc920ba81f91... | 0 | | Underminer EK |
| 2019/06/12 7:15:28 | 38.75.136.186:9081 | /views/3rfrdinb8mul8hi5r614nur8k4.html | 3,411 | text/html; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:28 | 38.75.136.186:9081 | /static/encrypt.min.js | 51,822 | text/javascript | Underminer EK |
| 2019/06/12 7:15:28 | 38.75.136.186:9081 | /static/tinyjs.min.js | 11,536 | text/javascript | Underminer EK |
| 2019/06/12 7:15:28 | 38.75.136.186:9081 | /js/3d5sujieraoh3uubnfcg78ls1g.js | 27 | text/javascript; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:29 | 38.75.136.186:9081 | /views/lp13dl02ihdfbcnj0a2nc2t9nc.html | 9,079 | text/javascript; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:29 | 38.75.136.186:9081 | /pubs/article.php?id=4fab5344e3432796... | 572 | text/html; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:29 | 38.75.136.186:9081 | /views/sgm10id0itf4pcdaiio7h026fg.html | 746 | text/html; charset=utf-8 | Underminer EK |
| 2019/06/12 7:15:30 | 38.75.136.186:9081 | /views/ssf8ud842qtshglh3u241gojmk.swf | 102,501 | application/x-shockwave-flash | Underminer EK |
| 2019/06/12 7:15:31 | 38.75.136.186:9081 | /views/h9vhqj4m9rtdk0nl7g4emunlpk.wav | 48,860 | audio/wav | Underminer EK |

**図 15 広告経由による Underminer EK への誘導事例**

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| CoinMiner | Hidden Bee | | | | → | → | → |

**表 6 Underminer EK にて配布されていたマルウェア**

[13] 新たな厄介者：Shade ランサムウェアを配信する Spelevo EK
https://www.cybereason.co.jp/blog/cyberattack/3417/

Underminer EK は、利用され始めた当時はあまり継続的な活動を確認できませんでしたが、2019 年 4 月以降は継続的な活動を確認しています。Underminer EK を利用する攻撃者は、一貫して「Hidden Bee」と呼ばれる CoinMiner を配布していることから、金銭目的の攻撃者グループと推察されます。

## (8)独自 EK

独自 EK の特徴は以下のとおりです。

- 2019 年 3 月中旬に活動
- 広告経由で改ざんされた正規サイトへ誘導（図 16）
  コンテンツ内に「CVE-2018-8174」を悪用するコードが挿入（図 9）
- ランサムウェア「GoledenAxe」を配布（図 17）

| Time | Host | URL | Body | Content-Type | Comments |
|---|---|---|---|---|---|
| 2019/03/17 13:23:58 | [redacted] | /go/224663/5070/98 | 283 | text/html | Malvertising |
| 2019/03/17 13:23:58 | | /ad/ad?p=224663&w=507... | 49 | text/html; charset=utf-8 | Malvertising |
| 2019/03/17 13:23:59 | | / | 20 | text/html; charset=UTF-8 | Compromised |
| 2019/03/17 13:23:59 | | /images/gold.html | 4,769 | text/html | CVE-2018-8174 |
| 2019/03/17 13:24:00 | | /images/Flash_Player.exe | 1,685,520 | application/octet-stream | GoldenAxe Payload |

**図 16 広告経由による独自 EK への誘導事例**

| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| ランサムウェア | GoledenAxe | | | → | | | |

**表 7 独自 EK にて配布されていたマルウェア**

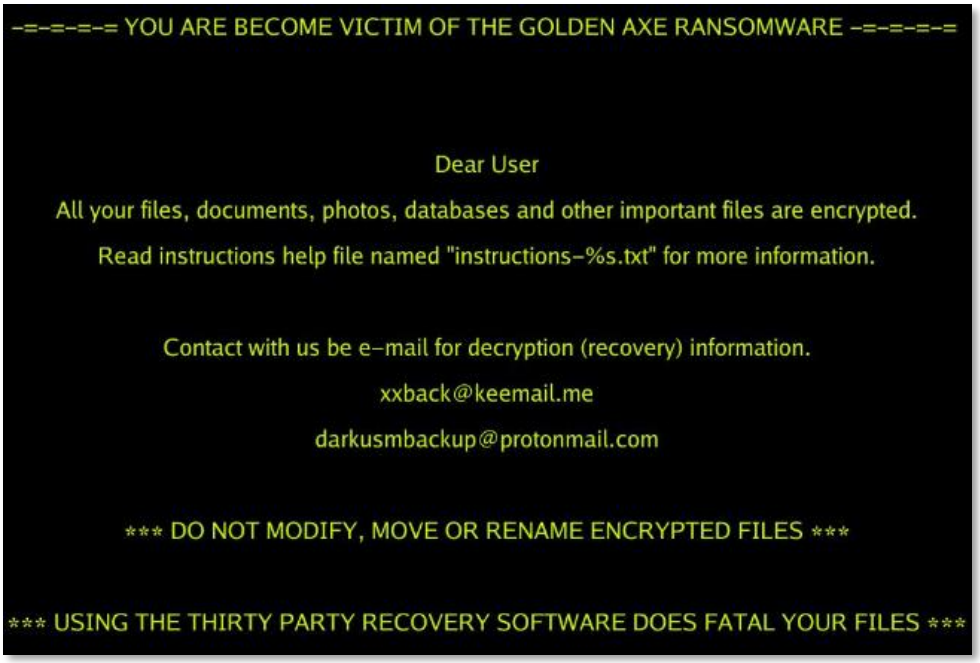



**図 17 ランサムウェア「GoledenAxe」**

なお、2019 年 7 月上旬から中旬にかけて、CVE-2018-8174 と CVE-2016-0189 の脆弱性を悪用し、AZORult や Netwire などの InfoStealer を配布していることを確認しています。

端末の脆弱性を悪用する攻撃以外の事例として、広告経由で不正なファイルのダウンロードを促し、ユーザが誤って実行した場合に、CoinMiner に感染する事例を確認しています。今後も独自にカスタマイズされたエクスプロイトキットや新たなエクスプロイトキットの出現の動向にも注視していきます。

## (9)おわりに

正規の Web サイトに表示される広告を経由したエクスプロイトキットなどへの不正な誘導は、日々観測されています。万が一に備え、OS やアプリケーション・ソフトウェア、およびウイルス対策ソフトの定義ファイルを最新の状態に保つことが、被害を減少させる重要な対策の一つです。端末の運用状況を改めて確認していただくことを推奨いたします。

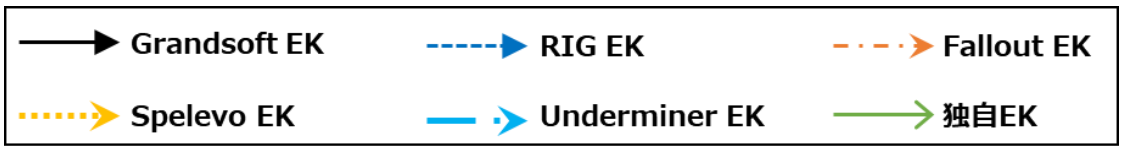
また、巧妙化するサイバー攻撃に備えるには、ゲートウェイ、エンドポイント、ネットワーク、サーバなどの各階層でセキュリティ対策を実施し、複数の階層で防御・検知する多層防御の考え方が重要です。

# IOC情報（マルウェア検体情報）

| マルウェア分類 | マルウェア名称 | MD5 |
|---|---|---|
| InfoStealer | Amadey | 4a22417395b241a18528591ef56a07be |
| | AZORult | 3d9f67b49cddc531ee5bc81c3c7efbec |
| | Baldr | 236ac57f988be74d9170d80fd3592ab9 |
| | Kpot | 70ce22275834c1e34e6ee52ac8e5df31 |
| | Pony | 0eb8eacc5157cafad7dc0915b4e8ff3f |
| | Raccon | bcd942808a6e52f62a104804fde15691 |
| | Ramnit | 63a117eb811b54caae613574e871add4 |
| ダウンローダ | Smokeloader | bfd998484e38fbd29162f171ac0ae016 |
| ランサムウェア | Buran | e60e767e33acf49c02568a79d9cbdadd |
| | GandCrab | 6819c92a781b04ce8e2e00ccd9de64d6 |
| | GetCrypt | 6d21c5c3bcff6076179bccd9ea6d1464 |
| | GoledenAxe | 3520dec68c0a8b28e7cf7b49e90a706e |
| | Maze | c35a15f340ed724b1e6b78f4c935643a |
| | Paradise | 475d5a08ff779bc5e1fbd2ed146f7704 |
| | Sodinokibi | F0728A11B184E4A021275723AA2D29EB |
| | Unknown | c07cc32ef42f5d98faf09d13c70f89e1 |
| ボット | Electrum DoS Miner | c4ded2bda86c82672411f1cf583c6650 |
| | Phorpiex | d9e59a4295926df49c8d6484aa6b8305 |
| | Pitou | 1e493d19e6c46ab8a4fe8f7362767590 |
| | PsiXBot | 73b768ccc69f26e555f94d48a4acb4cb |
| | Tofsee | 4f4d72a1be1093b4ec55507a0b2deb9b |
| CoinMiner | Hidden Bee | 831d0b55ebeb5e9ae19732e18041aa54 |

※今回分析から特定した一部のマルウェアに紐づくMD5を記載しています。

# EKとマルウェアの変遷




| マルウェア | | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 |
|---|---|---|---|---|---|---|---|
| InfoStealer | Amadey | | | | | | |
| | AZORult | | | | | | |
| | Baldr | | | | | | |
| | IceID ※ | | | | | | |
| | Kpot | | | | | | |
| | Pony | | | | | | |
| | Raccon | | | | | | |
| | Ramnit ※ | | | | | | |
| | Vidar | | | | | | |
| ダウンローダ | Smokeloader | | | | | | |
| ランサムウェア | Buran | | | | | | |
| | GandCrab | | | | | | |
| | GetCrypt | | | | | | |
| | GoldenAxe | | | | | | |
| | Paradise | | | | | | |
| | Maze | | | | | | |
| | Sodinokibi | | | | | | |
| | Unknown | | | | | | |
| ボット | Electrum DoS Miner | | | | | | |
| | Phorpiex | | | | | | |
| | Pitou | | | | | | |
| | PsiXBot | | | | | | |
| | Tofsee | | | | | | |
| CoinMiner | Hidden Bee | | | | | | |

※オンラインバンキング情報を窃取するバンキングマルウェア

# コラム：セキュリティ百景　＃13

## 白浜シンポジウム
## セキュリティ道場

2019年5月23日～25日、白浜シンポジウムにて警察向けのトレーニング（セキュリティ道場）を実施しました。今回は前編でデジタルフォレンジックの基礎知識を学び、後編で実際に調査を演習で行う構成としました。

参考:http://www.riis.or.jp/symposium23/dojo/


写真1 当日の風景

演習は、転職した社員が機密情報をUSBメモリで持ち出した疑いがあるとの事案想定で実施し、受講者には転職した社員がUSBメモリを使用して機密情報を持ち出した痕跡があるかとの観点で調査をしてもらいました。

この演習では、デジタルフォレンジックを使用した調査のほかに近年セキュリティ業界で注目を集めている、EDR（Endpoint Detection and Response）のログ調査機能を用いた調査手法も取り入れました。

警察が企業に対し捜査を行う場合、ただその場にあるPCやメディアを押収するだけではなく、資産管理ソフトやEDRログなど他に有益な証拠がないかを確認することが重要です。

しかし、企業内にどのようなログが存在する可能性があり、そこから何が分かるのか、事前に把握しておかなければ、敵対した状態の企業からそのような証拠を入手することはできません。

今回の演習では、「デジタルフォレンジックでは得ることができない証拠があること」、「その証拠が事件立証に極めて有益となる場合があること」の2点を認識してもらうことを主な目的として実施しました。

受講後のアンケートで「EDRを初めて触ることができ大変参考になった」などの感想を多くいただきました。今後も受講者に気付きを得てもらうことができるようなトレーニングを継続していく予定です。

写真2 白浜の思い出

佐藤　敦

# コラム：セキュリティ百景　＃14

## DFRWS EU 2019 への参加

2019年4月24日（水）から4月26日（金）に、ノルウェーのオスロで開催されたDFRWS EU 2019[14]に参加しました。ラックからの参加は初と聞いています。

DFRWSは、2001年8月から開催されているデジタルフォレンジックに関するカンファレンスです。論文発表の他にも、ワークショップやプレゼンテーションがあります。参加者層は、警察や軍隊所属、大学関係者が多く、私たちのように企業に所属するエンジニアは見かけませんでした。

参加したワークショップは、マルウェア解析、WhatsApp解析に特化したフォレンジック製品の紹介、aff4 イメージに対応したフォレンジック製品の紹介です。短い時間ながらも実践的で、大変有意義な内容でした。

論文発表のセクションは、macOS、スマートフォン、タブレットのフォレンジックに関する発表が多く、基礎研究寄りの内容のため、すぐに日頃の調査に役立てられるわけではありませんが、フォレンジックツールを開発するためにデータ構造を明らかにする発表や、調査のための新たなフレームワークを提案する発表など、知見が広がりました。

なお、発表に関する資料は、DFRWS のプログラムのページからアクセスできます[15]。

余談ではありますが、カンファレンスで出張していた期間がちょうどRUSSと呼ばれる祝典の期間で、赤いつなぎを着た高校生たちが街中を歩いていたのが非常に印象的でした。

写真1　宿泊先の近くで食べた肉料理

高橋 勇介

[14] http://www.dfrws.org/conferences/dfrws-eu-2019

[15] http://www.dfrws.org/conferences/dfrws-eu-2019/schedule/program-0

# 編集後記

特別編集号に続き、通常構成のレポートとなりましたがいかがだったでしょうか。サイバー攻撃やサイバー犯罪が巧妙になってきていることはよく言われる話ですが、守る側のセキュリティ運用も常に進化していかなければなりません。これからも旬な脅威情報をお伝えすることで、皆様のセキュリティ運用の進化に寄与できるよう尽力してまいります。（鷲尾）

## アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/7YRHV7J

編集長　鷲尾 浩之

編集者・執筆者　遠藤 裕樹、扇沢 健也、髙源 武彦、佐藤 敦、髙橋 勇介


**株式会社ラック**

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

E-MAIL: sales@lac.co.jp

https://www.lac.co.jp/


**緊急対応窓口：サイバー救急センター**

24時間365日 緊急対応コール
0120-362-119
CYBER EMERGENCY CENTER

**ご相談は予約不要、24時間対応。すぐにご連絡ください。**