

bomb_log セキュリティに関するbom

[トップ](#) > Emotetテイクダウン作戦 Operation LadyBird の成功への感謝

2021-02-01

Emotetテイクダウン作戦 Operation LadyBird の成功への感謝

2021/01/27、マルウェアEmotetのボットネットに対するテイクダウン作戦

「Operation LadyBird」が成功しました！

Emotetがどのようなものでどれだけ日本に被害を及ぼしていたかは周知の事実だと思いますが、詳しく知りたい方は[JSAC2021発表資料](#)を参照ください。

※テイクダウン作戦には直接的に関与していないため、公開されている情報や観測内容から記載しています。

「Operation LadyBird」

Emotetをテイクダウンするための作戦「Operation LadyBird」。

EuropolとEurojustが調整し、[アメリカ](#)、[ドイツ](#)、[イギリス](#)、[オランダ](#)、[カナダ](#)、[フランス](#)、[ウクライナ](#)、[リトアニア](#)の8カ国の法執行機関と司法当局が参加している。

Operation LadyBirdのロゴがこちら（左）。



ロゴから判断するに、Europolと6カ国が主導してリトアニアとウクライナは現地での捜査協力なのかと思われます。

作戦名がなぜLadyBirdなのか？公的には名言はされていませんが、答えは明白だと思います。

プロフィール



[bomccss](#)

セキュリティに関するbom

検索

最新記事

[Emotetテイクダウン作戦 Operation LadyBird の成功への感謝](#)

[Emotet - Epochとは](#)

[マルウェアEmotetの活動再開 \(2020/12/21-\) と変更点](#)

[返信型メールで感染する2つのマルウェア Emotet / IcedIDの区別](#)

[2020/10/16\(木\) 添付ファイル付不審メール「支払いの詳細 - 注文番号」「【2020年10月】請求額のご連絡」\(ZLoader\) の調査](#)

月別アーカイブ

- ▼ [2021 \(2\)](#)
[2021 / 2 \(2\)](#)
- ▶ [2020 \(11\)](#)
- ▶ [2019 \(64\)](#)

これまで対Emotetで活動していた、そしてこのLdayBirdにも深く協力していた、[2018 \(66\)](#)
Cryptolaemusへの敬意、だと思われます。

LadyBirdとはてんとう虫のことです。Cryptolaemusもてんとう虫の一種です。上記
ロゴの右の画像はCryptolaemusのアイコンです。

この作戦が実施されたということにも感動したのですが、この作戦名を見た時にも
また感動しました。

当然他にも理解している人もいて、Cryptolaemusも作戦に協力したと答えています。



ありがとう、Operation LadyBird、Cryptolaemus !

さて、本記事の主題のうち一つは上記ですが、もう一つ、この作戦の効果について。

”この作戦は成功したのか、今後Emotetの活動はなくなるのか？”

作戦が実施・公表されてから、私も既に幾度となく聞かれています。

私は冒頭に記載したように、「Operation LadyBirdは成功した！Emotetはテイクダウンされた！」と考えています。

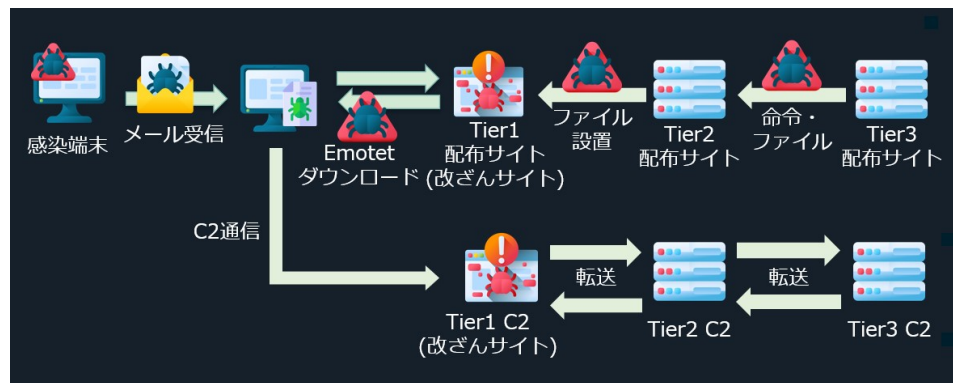
その成功について、考えていきます。

Emotet インフラの仕組み

まずは、Emotetインフラの仕組みについて、今回の各国の捜査機関等の発表により分かっていることをまとめます。

特にアメリカ司法省の[宣誓供述書](#)にはインフラの構成について記述があります。そ

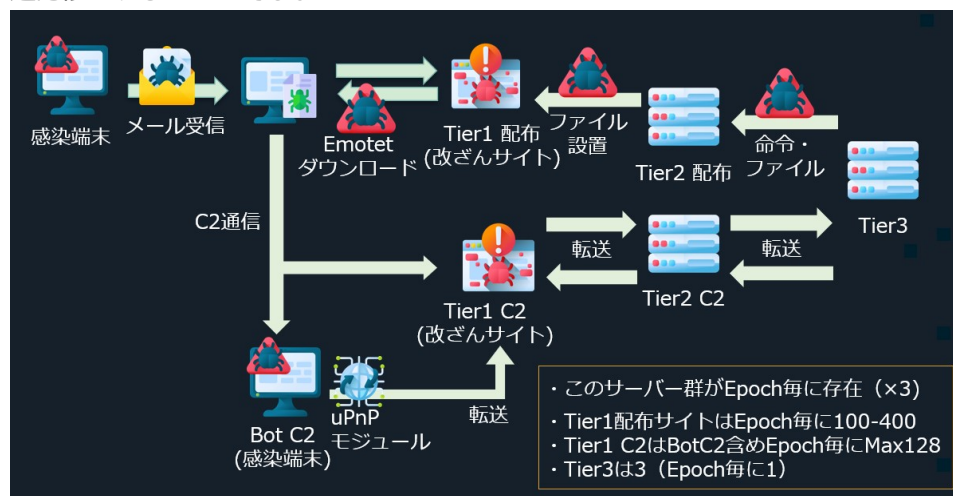
れを表すと以下のようになります。



Emotetのインフラは、数百台のサーバーで大規模で複雑なネットワークで構築されています。マルウェアの配布サーバやC2サーバ、防弾用の正規サイトの改ざんサイトなどです。Tier1は正規サイトを改ざんしたもので、Tier2,3を隠すための層として使われています。

発表により用語が統一されていないため憶測も含まれますが、オランダ警察の発表ではメインサーバーが3つあり、うち2つはオランダにあったとなっています。恐らくはこのメインサーバーがTier3のことかと思われます。3つというのはEpochごとに1つずつと考えられ、配布用のTier3とC2のTier3も同じサーバーが使われているということかと思われます。

追記修正するのでしょうか。



配布サイトやC2などのサーバー（恐らくはTier2）がドイツで最初に特定され、その分析により、更にヨーロッパの幾つかの国でサーバーが特定されました。その後、オランダ警察がEmotetインフラに対してハッキングで侵入して調査しインフラの全体像が把握されました。（日本では法的に実行不可。）

Emotetoインフラのテイクダウン

この作戦で世界中で63台のC2サーバが押収され、うちアメリカは3台のTier2配布サーバー、ドイツは17台、カナダは13台。オランダは2つのメインサーバー。他にリトアニア、ウクライナにあったものも押収しているようです。

これらの停止されたサーバーはTier1-3が含まれると思われますが、全てのサーバーを

押収したわけではないようです。

押収していないTier1 C2に対しては、TeamCymruの調整によって、ネットワーク事業者が協力してTier1 C2宛の通信を遮断することで、無効化しました。

これにより、Emotet感染端末は押収されたC2とのみ通信を行います。

Emotet感染端末の隔離

更に、オランダ警察はメインサーバーを押収し、Emotetの更新ファイルを隔離用ファイルへと置き換えました。

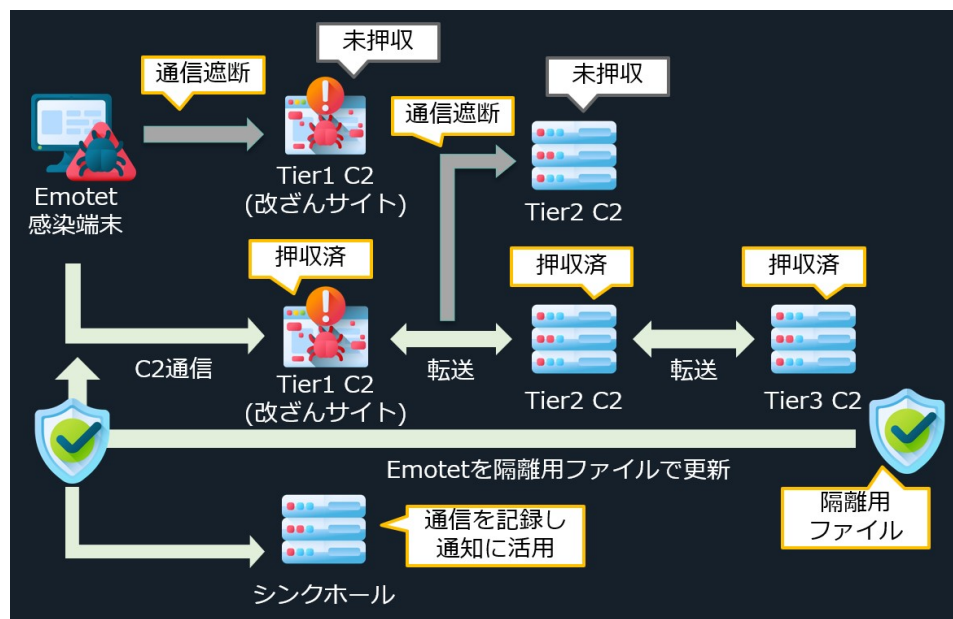
Emotetに感染している端末はEmotetが持っている更新の仕組みに乗っ取り、押収されたC2を経由してオランダ警察が管理するメインサーバーへ接続することで、Emotetが隔離用ファイルへと自動的に置き換えられます。

この隔離用ファイルは既存のEmotetのC2とは通信をせず、ドイツが管理するシンクホールサーバーのみと通信を行います。

Emotetの感染端末は既存のC2と通信を隔離され、攻撃者は感染端末を操作できなくなります。

感染端末がシンクホールサーバーへ接続したログは保存され、被害者への通知のために使用されます。

テイクダウンの対応をまとめると図のようになります。



隔離用ファイル (law enforcement file)

隔離用ファイルは日本時間で2021/2/26 18:00以降に更新されるようになっているのを確認しています。

これらはEpoch1-3全てで同じものが与えられます。

DLL版

MD5: 9a062ead5b2d55af0a5a4b39c5b5eadc

SHA256: a9c68d527223db40014d067cf4fdae5be46cca67387e9cfdff118276085f23ef

<https://tria.ge/210126-13k64pez2a>

EXE版

MD5: 13b9d586bb973ac14bfa24e4ae7b24f1

SHA256: 90e4f02ab9157f389d785c3dcddfa432085b237f2a4c3befb4a093d0f2711b5b

<https://tria.ge/210126-avsn5j8x5a>

隔離用ファイルは12月以降に使用されるようになったDLL版だけでなく、10月まで使用されていたEXE版にも対応しており、それぞれ以前に動いていたものに応じて更新版が与えられます。

隔離用ファイルは既存のEmotetを流用し設定を書き換えて作られています。追加機能として、感染端末の設定時刻が2021/4/25 12:00になると永続化を削除し、プロセスを消去します。なお、隔離用ファイル自体は残存します（挙動は実際に確認済）

これにより、感染端末はEmotetからクリーンになります。

様々な環境で確認を行いました。全てでこの隔離用ファイルが与えられており、全てのEmotet感染端末はこの隔離用ファイルを与えられると結論付けて良さそうです。

Operation LadyBirdの成功

まとめると、以下をもって、成功したと考えています。

- ・ 全てのEmotetのインフラが押収されたか通信がブロックされたこと
- ・ 全てのEmotetの感染端末のEmotetは隔離用ファイルに更新されているであろうということ
- ・ Emotetのインフラを運営していた攻撃者グループの一部が実際に逮捕されていること。

逮捕者については中枢の人物ではないのではないかと思います。逮捕に伴う捜査により、Emotetの攻撃グループだけでなく、Emotetを利用していた他の攻撃グループも特定されていると発表されていますので、更なる関係者の逮捕者が出るであろうと考えられます。

また、Emotetは他の多くのマルウェアと異なり、単一の攻撃グループが運用するマルウェアです。そのため、今回のテイクダウンでは全てのEmotetが対象となっており、一部の攻撃グループが使うEmotetはテイクダウンされていない、という事象は発生しません。

テイクダウン後の対応

ただし、Emotetはテイクダウンされましたが、これで終わりではありません。

世界中に存在する感染端末があります。

今は無害化されましたが、EmotetはEmotetの対処をしてお終いではありません。

Emotetにより二次感染した別のマルウェアへの対応が必要になります。

この二次感染に対処しなければいけない、というのがこのOperation LadyBirdでの特徴だと思います。

他のマルウェアであれば、C2からマルウェアをアンインストールするコマンドを送って終わり、ということもあります。

しかし、それでは他のマルウェアの感染には対処出来ません。

そのため、隔離用ファイルを作ってシンクホールへの通信を続けられる、という特殊な対応が行われたのだと考えられます。

(こういった無害なマルウェアに感染させてその後の対処に活用する、というのは世界的にも実施が難しいケースで、一部の国であれば法執行機関でのみ実施可能、というもののようです。)

Emotetは、カナダの6,000台、米国45,000台を含む226か国で170万台以上のコンピューターに感染したと報告されています。

Emotetボットネットから押収したデータからはパスワード付きのメールアドレスが60万件見つかっています。

隔離用ファイルによりシンクホールへ通信があったIPや押収されたデータから見つかったメールアドレスについてはISPや各国CERTへと情報が送られ、通知に使われることになります。

通知をして、感染端末を二次感染したマルウェア含めて対処を行う、そのための期間が4/25までの約3ヶ月間ということだと思われます。

通知が中々届かない、などのケースも多分に考えられます。3ヶ月実施して通知が届かない、対応されない、というのはその先待っても難しいでしょう。

そのため、3ヶ月という区切りを付けて、最後は自動的に消去するのだと考えられます。

今後の攻撃グループの動向

ここは何も根拠となるものはありません。

しばらくは、EmotetやEmotetを利用していた攻撃グループは逮捕に怯えておとなしくなるのではないのでしょうか。

しかし、しばらくすれば他の攻撃グループがEmotetの代わりとなるマルウェアを探して様々な他のマルウェアの使用率が上がるのではないかと考えられます。

Emotetの攻撃グループはEmotetのインフラを再構築しようとすると考えられます。しかし、例えばバックアップファイル等があったとしても、インフラは1からの再構築になると考えられます。同じ手法で構築したら、すぐにオランダ警察にハックバックされるでしょう。

その手間をしてまで構築したとしても、それは再び出てくるまで、長い時間がかかるのではないのでしょうか。その場合はまた別のマルウェアと呼んでも良い気がします。

それよりは、他のマルウェアを利用するグループへ合流するのではないかと考えられます。

攻撃グループ同士が近いと言われているTrickbotを使っている攻撃グループなどに。

その場合考えられるのは、Emotetが使用していたモジュールを他のモジュール型マルウェア、例えばTrickbotの後継と言われるBazaarマルウェアに移植される可能性などが考えられます。これは嫌なケースです。

また、Emotetを真似て同様にメールを送信するQbotなどのマルウェアも既に出ています。

これからもマルウェア付きメールには注意する必要があります。

しかし、過去最高に危険度の高い、被害を出してきたEmotetはテイクダウンされました。

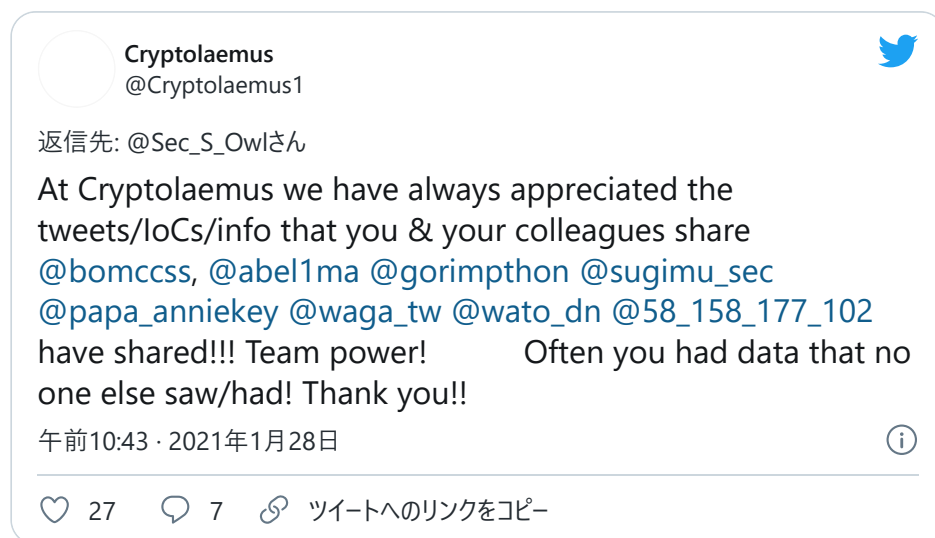
世界が今回の経験を活かし、イタチごっこではありますが、新たな脅威が出たとしても、今後もテイクダウンに向けて動いていくのではないかと思います。

終わりに

この記事は多分に感情的です。

私はCryptolaemusのファンであり、彼らの協力者です。

Cryptolaemusに言われたこの言葉はとても嬉しかったです。



今回のテイクダウンに、日本の公的機関の協力はありませんでした。私達日本のコミュニティはCryptolaemusに協力することで、間接的にテイクダウンに貢献できていた、と信じています。



TEAM POWER!
Cryptolaemus with
Japanese community

Kill all the Mealybugs!

なお、冒頭にも記載しましたが、マルウェアEmotetの詳細と日本への影響 については以下のJSAC2021資料を参照ください。[宣伝]

とあるEmotetの観測結果

[日本語] https://jsac.jpCERT.or.jp/archive/2021/pdf/JSAC2021_104_sajo-sasada_jp.pdf

[English] https://jsac.jpCERT.or.jp/archive/2021/pdf/JSAC2021_104_sajo-sasada_en.pdf

参考文献

World's most dangerous malware EMOTET disrupted through global action

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an in...



www.europol.europa.eu **9 users**

www.europol.europa.eu

Internationale politieoperatie LadyBird: wereldwijd botnet Emotet ontmanteld

Met het uit de lucht halen van servers achter de agressieve malware Emotet is een belangrijke slag geslagen in de strijd tegen cybercriminaliteit: de Emotet-besmetting is niet langer actief op de...



www.politie.nl

www.politie.nl

BKA - Listenseite für Pressemitteilungen - Infrastruktur der Emotet-Schadsoftware zerschlagen

Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main -ZIT- und des Bundeskriminalamtes

www.bka.de

www.bka.de

Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі ко...

Хакери за допомоги вірусного програмного забезпечення здійснювали масові втручання в роботу серверів приватних та державних установ країн Європи та Сполучених Штатів Америки. У результаті такої «діяльності» іноземним банкам та фінустанова...

www.npu.gov.ua

www.npu.gov.ua

NCA in international takedown of notorious malware Emotet

A malware botnet that was used by cybercriminals to infiltrate thousands of companies and millions of computers worldwide has been taken down in an international operation.

www.nationalcrimeagency.gov.uk



www.nationalcrimeagency.gov.uk

Emotet Botnet Disrupted in International Cyber Operation

The Justice Department today announced its participation in a multi-national operation involving actions in the United States, Canada, France, Germany, the Netherlands, and the United Kingdom to disrupt...

 www.justice.gov



www.justice.gov

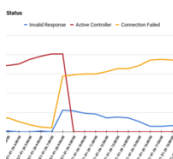
The RCMP takes part in an international operation to neutralize Emotet | Royal Canadian Mounted Police


 www.rcmp-grc.gc.ca

www.rcmp-grc.gc.ca

Taking Down Emotet

The Emotet botnet takedown was a coordinated effort among law enforcement cyber threat researchers and cyber security vendors. Team Cymru helped to map the botnet infrastructure and recruited th...

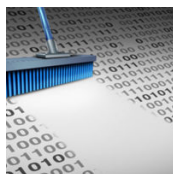


 team-cymru.com

team-cymru.com

Cleaning up after Emotet: the law enforcement file

Following global law enforcement action to take over the Emotet botnet, a special update is being sent to clean up infected machines.



 blog.malwarebytes.com

blog.malwarebytes.com

Cryptolaemus Pastedump

This is where we store information

 paste.cryptolaemus.com **3 users**

paste.cryptolaemus.com

bomccss 9時間前



0

19

シェア


ツイート



4

送る

[Emotet - Epochとは »](#)

 [bomb_log](#)

Powered by [Hatena Blog](#) | [ブログを報告する](#)