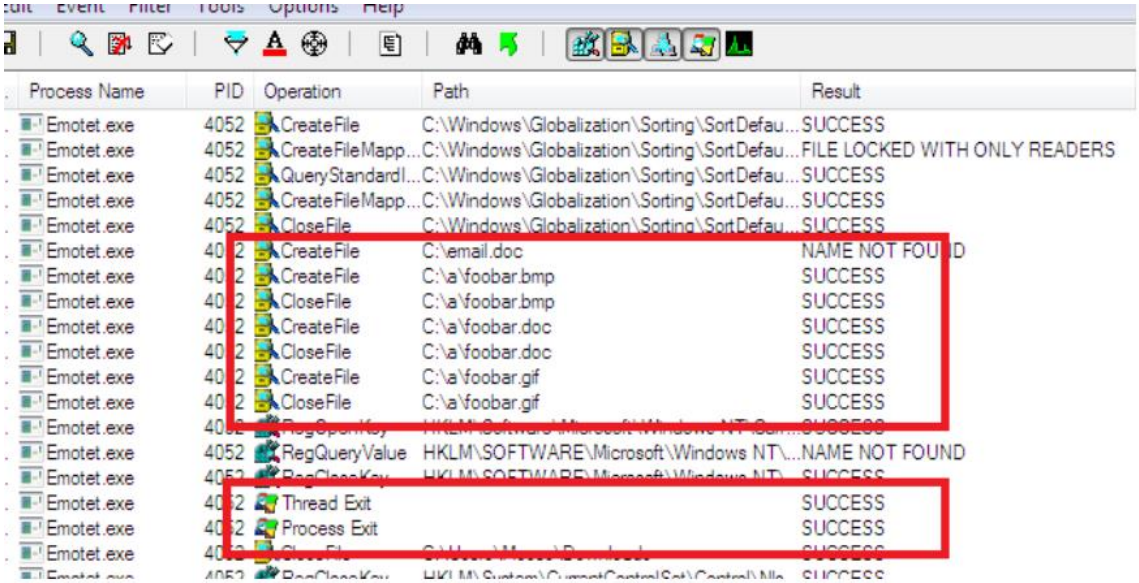
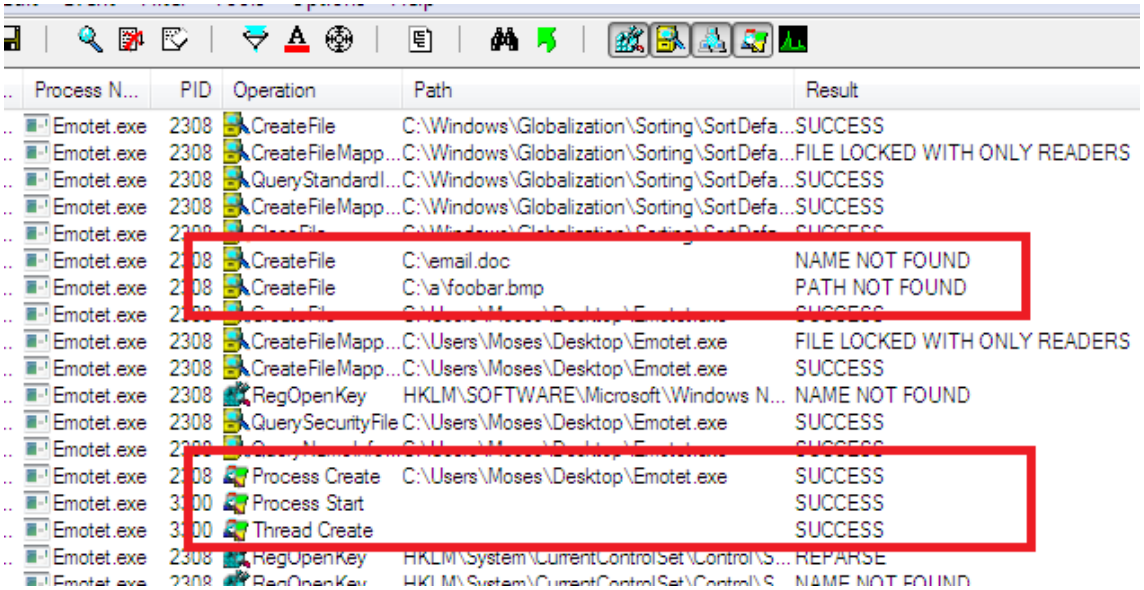


Emotet の検知回避レベルが向上。どのように脅威攻撃を先制防御するか!?
2017 年 11 月 14 日 Minerva のブログから

Emotet はバンキングのトロイの木馬で銀行口座、オンラインバンキングなどの認証情報を詐取して口座のお金を狙います。また被害者のコンタクトリストや email アカウントも収集して感染がさらに蔓延していきます。

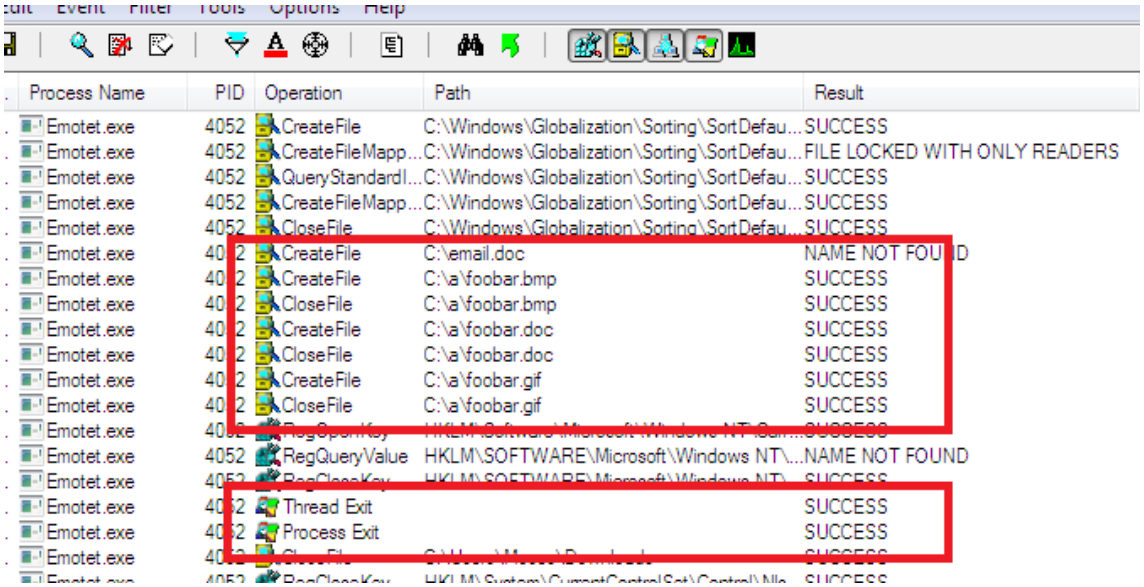
Emotet はとても脅威のあるマルウェアで、コアーボットには数十のペイロードが仕掛けられています。2017 年に多くのフィッシング攻撃で Emotet が仕込まれ、数百単位のドメインを利用して攻撃を仕掛けていました。

このブログでは Emotet がどのように進化向上していった経歴を説明していきます。初期の Emotet は単純なマルウェアでしたが、**長年にわたり Emotet 開発者は検知回避の向上に努めてきました。Minerva リサーチチームは Emotet 攻撃キャンペーンを追求し、最新のペイロード変種株などがどのようにアンチウィルスソフトから効果的に検知回避するのか調査を開始しました。3つの空ファイルを生成することで Emotet 攻撃から完全に防御することができると判明しました。**



Process N...	PID	Operation	Path	Result
Emotet.exe	2308	CreateFile	C:\Windows\Globalization\Sorting\SortDefa...	SUCCESS
Emotet.exe	2308	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefa...	FILE LOCKED WITH ONLY READERS
Emotet.exe	2308	QueryStandardI...	C:\Windows\Globalization\Sorting\SortDefa...	SUCCESS
Emotet.exe	2308	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefa...	SUCCESS
Emotet.exe	2308	CreateFile	C:\email.doc	NAME NOT FOUND
Emotet.exe	2308	CreateFile	C:\a\foobar.bmp	PATH NOT FOUND
Emotet.exe	2308	CreateFileMapp...	C:\Users\Moses\Desktop\Emotet.exe	FILE LOCKED WITH ONLY READERS
Emotet.exe	2308	CreateFileMapp...	C:\Users\Moses\Desktop\Emotet.exe	SUCCESS
Emotet.exe	2308	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows N...	NAME NOT FOUND
Emotet.exe	2308	QuerySecurityFile	C:\Users\Moses\Desktop\Emotet.exe	SUCCESS
Emotet.exe	2308	Process Create	C:\Users\Moses\Desktop\Emotet.exe	SUCCESS
Emotet.exe	3100	Process Start		SUCCESS
Emotet.exe	3100	Thread Create		SUCCESS

Emotet のプロセスがエンドポイント内へ侵入し実行前にチェック



Process Name	PID	Operation	Path	Result
Emotet.exe	4052	CreateFile	C:\Windows\Globalization\Sorting\SortDefau...	SUCCESS
Emotet.exe	4052	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefau...	FILE LOCKED WITH ONLY READERS
Emotet.exe	4052	QueryStandardI...	C:\Windows\Globalization\Sorting\SortDefau...	SUCCESS
Emotet.exe	4052	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefau...	SUCCESS
Emotet.exe	4052	CloseFile	C:\Windows\Globalization\Sorting\SortDefau...	SUCCESS
Emotet.exe	4052	CreateFile	C:\email.doc	NAME NOT FOUND
Emotet.exe	4052	CreateFile	C:\a\foobar.bmp	SUCCESS
Emotet.exe	4052	CloseFile	C:\a\foobar.bmp	SUCCESS
Emotet.exe	4052	CreateFile	C:\a\foobar.doc	SUCCESS
Emotet.exe	4052	CloseFile	C:\a\foobar.doc	SUCCESS
Emotet.exe	4052	CreateFile	C:\a\foobar.gif	SUCCESS
Emotet.exe	4052	CloseFile	C:\a\foobar.gif	SUCCESS
Emotet.exe	4052	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	NAME NOT FOUND
Emotet.exe	4052	Thread Exit		SUCCESS
Emotet.exe	4052	Process Exit		SUCCESS

エンドポイント内に作られた空のファイルは Emotet を防御

進化する脅威度

2014 年からの Emotet 攻撃以来このマルウェアは進化を遂げ高性能に変身しました。Emotet が他のバンキングトロイの木馬マルウェアと違うのは、攻撃実行時に悪意のある DLL ファイルを駆使して機密情報を詐取する能力が優れていることなどが挙げられます。

同年の後半期に Emotet の新バージョンが発見され、被害者の銀行口座からお金を詐取する

手法が自動振替サービスを利用している時に狙われ盗まれるようになりました。この Emotet 変種株は複合のモジュールを組み合わせることで脅威度がさらに高まりました。

この Emotet 変種株の開発者はロシアの公安組織からの監視を逃れるため、ロシア文化圏の国へは攻撃を敢えて仕掛けませんでした。

Emotet は 2015 年 1 月に再度登場しました。この時、開発者は複数にわたる検知回避技術を集結させ新たな Emotet 変種株が到来しました。

- 暗号化攻撃実行に必要なメモリを奪う能力。

- Emotet が仮想マシンで起動していたら、偽の C2 サーバーへ接続されます。これらの偽サーバーは実際に稼働せず、監視から逃れるために利用されます。同様の回避手法が同時に Andromeda¥Gamarue によって実行されます。カスペルスキーによると、いくつかのプロセス名は、“vboxservice.exe”, “vmacthlp.exe”, “vmtoolsd.exe”, and “vboxtray.exe”などであることが分かっています。

2017 年は Emotet にとって興味深い年でした。というのも、16 年の 4 月以来、多くの技術が組み込まれ、最新で脅威あるマルウェアとしてカムバックを果たしました。主要な技術は以下の内容です。

- **サンドボックスを回避:** サンドボックスを回避するため、URLs は暗号化リストに保管され、サンドボックスで検知されづらくなっていました。事実上サンドボックスは URL を検知することはできず、Emotet サンプルをダウンロードすることができないようになりました。

- **認証情報を狙うブルートゥース攻撃で感染:** Emotet 変種株はあらゆる手法で感染しようとします。Active Directory ドメインアカウントが辞書攻撃を利用するブルートフォース攻撃実行するなどが追加されています。

- **エクスプロイト攻撃:** Emotet は初めて ETERNALBLUE¥DOUBLEPULSAR エクスプロイトコンボを採用することで組織的なサイバー犯罪キャンペーンの一部として広がり始めました。このコンボエクスプロイトを組み合わせることで Emotet は寄生虫の如く、ネットワークに感染していき、最終的に全組織のネットワークへ蔓延してしまいます。

- **C2 と密な連携:**攻撃対象者の情報をサーバーで POST リクエストする代わりに、ベース 64 エンコードクッキー内に暗号化された情報が送り込まれます。暗号化された内容が含まれていて、“404: page not found”などを返答することで検知回避から免れようとします。

- **新たなモジュール:** 変種株はブラウザーとメールクライアント認証情報を詐取できるようになりました。

- **難読コード:**コードの難読化レベルは向上し、ジャンクコードを挿入して分析者からの追跡を困難にしています。更にハッシュ値配列上にロードしたい機能を隠蔽することでランタイムのみで利用されます。

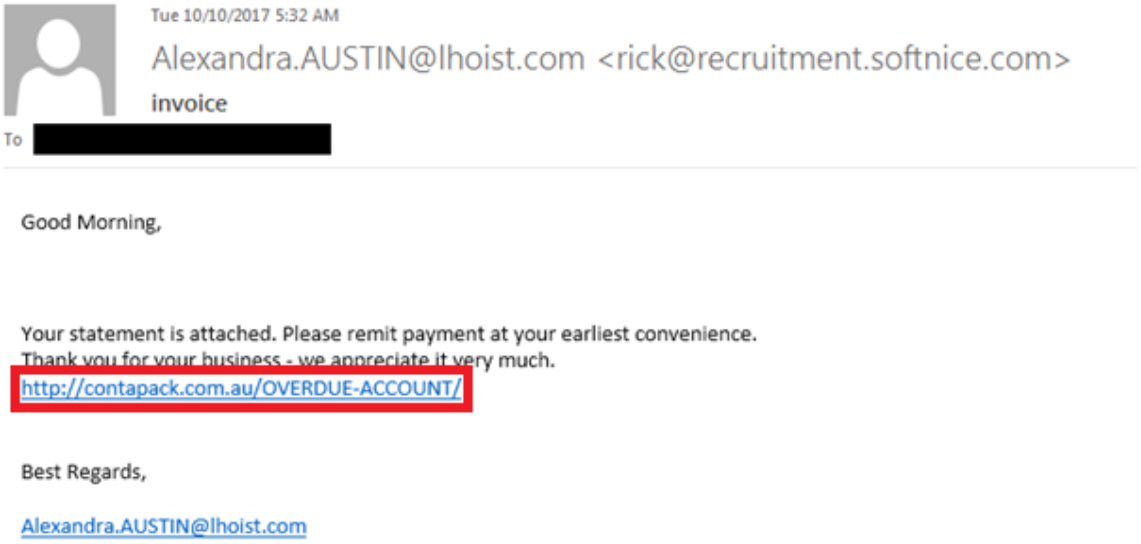
- **攻撃対象者の情報収集:**このマルウェアはプロセス名などのマシンに関する情報を収集することで攻撃方法を決定します。

- **暗号化:** 最新の Emotet は異なる暗号アルゴリズムを採用してきています。前バージョンでは、RC4 を利用した暗号化で、第 4 バージョンでは CBC モードでさらに強い 128-bit AES へ移行しています。

- **C2 プロトコール:**Emotet はプロトコールバッファーを使用しています。Google によるコミュニケーションプロトコールでエンコーディングタイプを追加することでデフォルトの解析手法では不可能です。

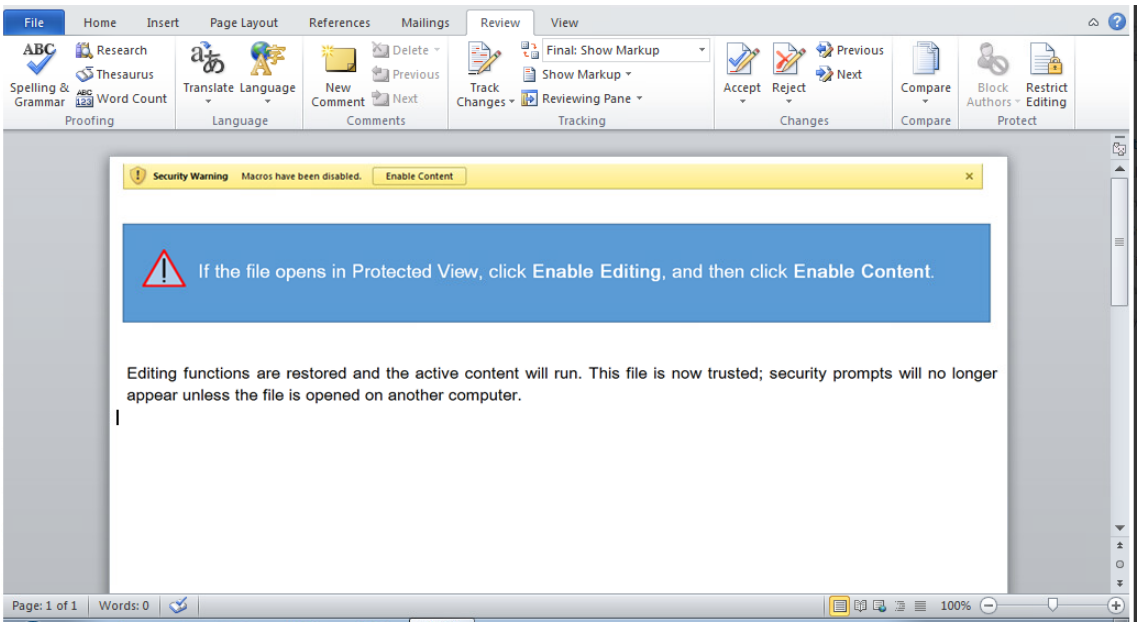
2017 年後半は Emotet の荒波

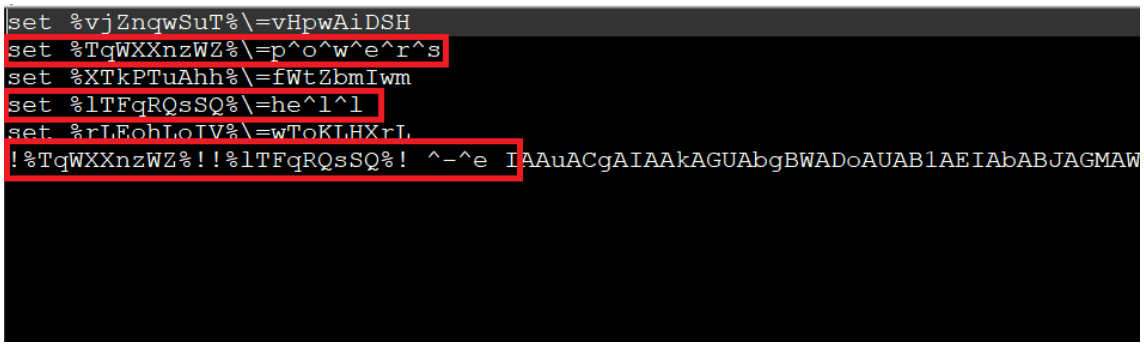
2017 年の後半に最新 Emotet 変種株が悪意のメールメッセージを利用してリンク先のクリックを促し、ワードなどのドキュメントを実行させる感染経路が席巻しました。



他の攻撃キャンペーンとは異なり、ドキュメントは email へ添付せず、代わりにリモートウェブサーバー上でホーストされていることが分かります。この仕組みは、メール添付物が悪意コンテンツを検知するセキュリティソリューションを素通させるための意図的な狙いです。

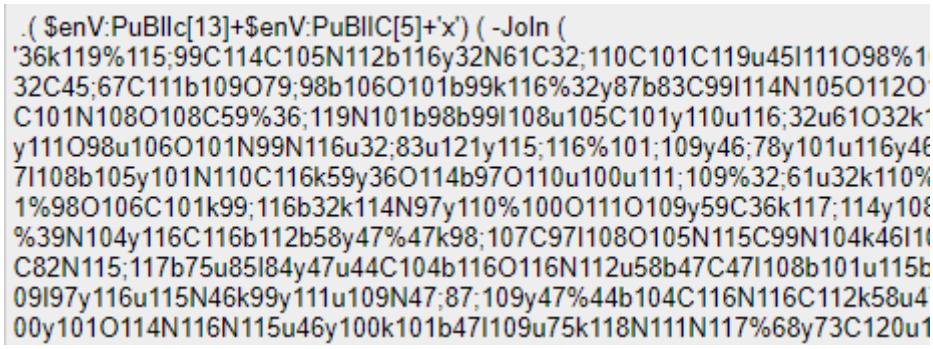
ユーザーがダウンロードするように仕掛けた悪意のドキュメントは多くのケースで見受けられ、何も知らないユーザーがマクロを実行すると、ドキュメントはバッチスクリプトが実行されます。





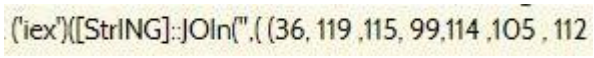
ランタイムで最終列がエンコードされたペイロードで PowerShell コマンドが実行されます。

ペイロードは以下の文字列でデコードされます。

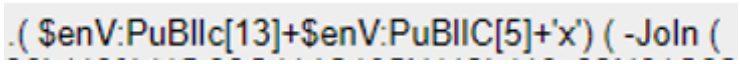


最新バージョンでは、Emotet は 1 週間単位でクオリティーが進歩しており、どのような回避手法で検知を免れているか説明します。初期の変種株は PowerShell スクリプトを利用し、明確に”iex”コードを書いて、暗号化スクリプトを起動させようとしておりましたが、最近の変種株は難読なコードで書かれています。

以下は初期の変種株で“iex”が明確に書かれています。



最近の変種株は以下のようにプログラムを書くことにより検知回避をしています。



env.public は文字列で以下の内容となります。
C:¥Useres¥Public
この変種株では、アルファベット 14 番目の’I’と 6 番目の’e’を結合し、スクリプトで’iex’と記載しなくてもいいようにハードコーディングされた’x’を挿入して組み込んでいます。以前はセキュリティー製品で検知されていましたが、このシンプルな回避手法はとても賢い方法で Emotet がこの回避手法で行った典型的な例となります。

感染最終ステージにおいて Emotet ドロッパーデクリプトの文字列は難読化されプログラムが起動されます。

悪意のあるスクリプトは5つのウエブサイトへ攻撃を仕掛け、ある1つのウエブサイトからペイロードをダウンロードさせるように侵入に成功しました。

3つのファイルで Emotet を防御
Emotet(10 月-11 月 2017 年)バージョンではさらに回避能力が高度になりました。マルウェア新技術としてサンドボックスやアンチウィルスソフトから回避できるようになったのです。例えば以下に記載のサンドボックス関連ファイルが存在するという状況でテストを行いました。

- “C:¥a”下のファイル
  - C:¥a¥foobar.bmp
  - C:¥a¥foobar.gif
  - C:¥a¥foobar.doc
- “C:¥123” と“C:¥”下のファイル
  - C:¥email.doc
  - C:¥email.htm
  - C:¥123¥email.doc
  - C:¥123¥email.docx

Emotet が初めの 3 つのファイル又は 2 回目の 4 つのファイルを認識する場合、サンドボックス内で検知されるのを回避するために攻撃実行を止めてしまうことが分かりました。

更に Emotet は、サンドボックスに関連しているユーザーとホースト名のリストを注視しています。以下に記載された Windows のユーザー名又はコンピューター名を見つけると、攻撃実行を止めてしまいます。

- TEQUILABOOMBOOM
- Wilbert
- admin
- SystemIT
- KLONE_X64-PC
- John Doe
- BEA-CHI
- John

回避手法を逆コンパイルすることで Joe-sandbox の分析レポートで報告されています。

```
0x004e1bb6    _t84 =  *__imp__GetComputerNameExA(1, _v828,  &_v800); // executed
0x004e1bc8    _v860 = _t84;
0x004e1bcc    _t85 = lstrcmpA(_v844, "TEQUILABOOMBOOM");
0x004e1bd6    _v872 = 1;
0x004e1bda    if(_t85 != 0) {
0x004e1be0        _v824 = 0;
0x004e1bf3        _v824 = _v560;
0x004e1c10        if(lstrcmpA(_v856, "Wilbert") != 0 || lstrcmpA(_v852, "SC") != 0 && lstrcmpA(_v860, "CW") != 0) {
0x004e1c60            if(lstrcmpA(_v864, "admin") != 0 || lstrcmpA(_v864, "SystemIT") != 0) {
0x004e1cbe                L8:
0x004e1cd2                if(lstrcmpA(_v872, "admin") != 0) {
0x004e1cf7                    L10:
0x004e1cfb                    _v856 = 0;
0x004e1d03                    _v860 = 0;
0x004e1d1b                    _v908 =  &_v860;
0x004e1d24                    if(lstrcmpA(_v880, "John Doe") != 0 || lstrcmpA(_v916, "BEA-CHI") != 0) {
0x004e1d5e                        if(lstrcmpA(_v888, "John") != 0) {
0x004e1ddf                            L16:
0x004e1df8                            _t98 = CreateFileA("C:\\email.doc", 0x80000000, 0, 0, 3, 0, 0); // executed
0x004e1e01                            _v944 = _t98;
0x004e1e12                            _v952 = CloseHandle(_t98);
0x004e1e16                            if(_v948 == 0xffffffff) {
0x004e1ed4                                L20:
0x004e1eed                                _t101 = CreateFileA("C:\\a\\foobar.bmp", 0x80000000, 0, 0, 3, 0, 0); // executed
0x004e1ef6                                _v980 = _t101;
0x004e1f07                                _v988 = CloseHandle(_t101);
0x004e1f0b                                if(_v984 == 0xffffffff) {
0x004e1f87                                    L23:
0x004e1f89                                    _v920 = 0;
0x004e1f0d                                } else {
0x004e1f2f                                    _v1020 = CreateFileA("C:\\a\\foobar.doc", 0x80000000, 0, 0, 3, 0, 0);
0x004e1f40                                    _v1028 = CloseHandle(CreateFileA);
0x004e1f44                                    if(_v1024 == 0xffffffff) {
0x00000000                                        goto L23;
0x004e1f46                                    } else {
0x004e1f68                                        _v1060 = CreateFileA("C:\\a\\foobar.gif", 0x80000000, 0, 0, 3, 0, 0);
0x004e1f7e                                        _v1068 = CloseHandle(CreateFileA);
0x004e1f81                                        _v984 = 1;
0x004e1f85                                        if(_v1064 == 0xffffffff) {
0x00000000                                            goto L23;
0x00000000                                        }
0x004e1f85                                    }
0x004e1f44                                }
```

脅威トレンドと規模

最新の Emotet アクティビティに関連する約 700 のドメインリストが侵害の痕跡（IOC＝Indicators of Compromise）後に収集取得できました。

- **ドロッパーが仕組まれた Office ドキュメント**
  - ユーザーがフィッシングメールのリンクをクリックする際に、悪意のサイトがマルウェア感染のドキュメントをダウンロードさせる。
  - 脆弱性があるワードプレスのウエブサイト。

- **Emotet のペイロード攻撃**
  - サーバーにはマルウェアが保管され、ドロッパーによってダウンロードされる。
  - 悪意のあるウエブサイト上で稼働する。

- **C2 Servers**
  - Emotet 感染後に情報収集し C2 サーバーと連携する。

ドメインに関する全リストを参照したい場合は以下のURLへアクセス：https://github.com/MinervaLabsResearch/BlogPosts/blob/master/Emotet/Domains.txt

まとめ
Emotet の進化について開発者がどのようにサンドボックスやアンチウィルスソフトからの検知を逃れてきたか分かります。

従来はローカル設定ファイルと事前に決められたマルウェアロジックで攻撃試行して、非常網に引っかかっていたのが、最近はアンチウィルスソフト、サンドボックスなどからの検知を回避し、また詐取したエンドポイント情報は、暗号化で C2 サーバーへ通信され、ディスク上には痕跡を残さず、ファイルレスで正当なツールを使用しての攻撃へと進化しています。

年々マルウェアは高度化し、
回避能力も優れてきていることがお分かりになられたことでしょう。

Emotet からの攻撃から Goodbye したいですか？ それでは以下のファイルを作成しましょう。

- C:¥a¥foobar.bmp
- C:¥a¥foobar.gif
- C:¥a¥foobar.doc
- C:¥email.doc
- C:¥email.htm
- C:¥123¥email.doc
- C:¥123¥email.docx

これらのファイルを生成することで、Emotet からの攻撃を防御することが可能ですが、手間がかかったりするかもしれません。Minerva Labs の製品 Minerva Armor は Emotet などのマルウェアを先制防御するだけでなくあらゆる未知のマルウェアからあなたの企業組織である IT セキュリティーを保持することでしょう。

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。