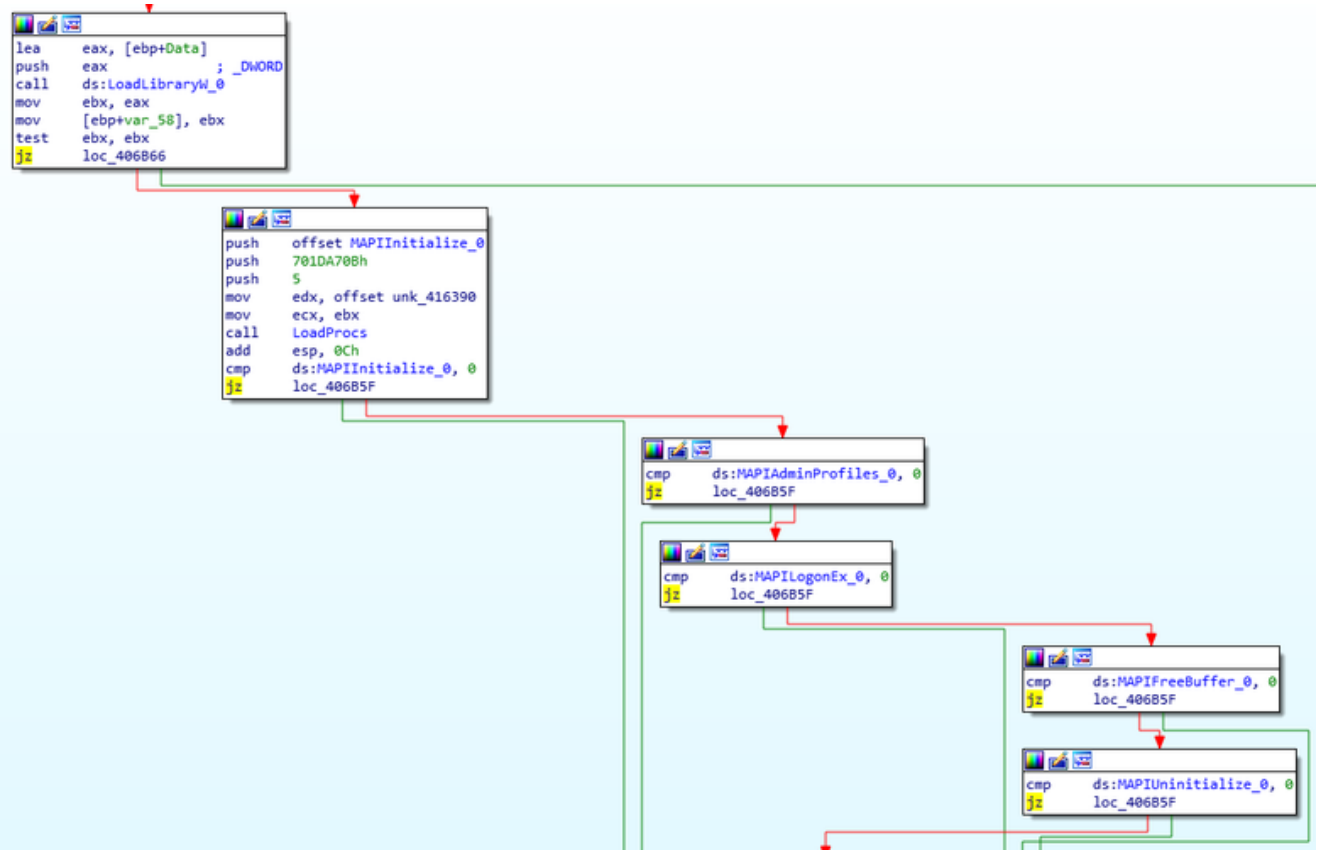
Emotet beutet Outlook aus

gdata.de/blog/2017/10/30110-emotet-beutet-outlook-aus

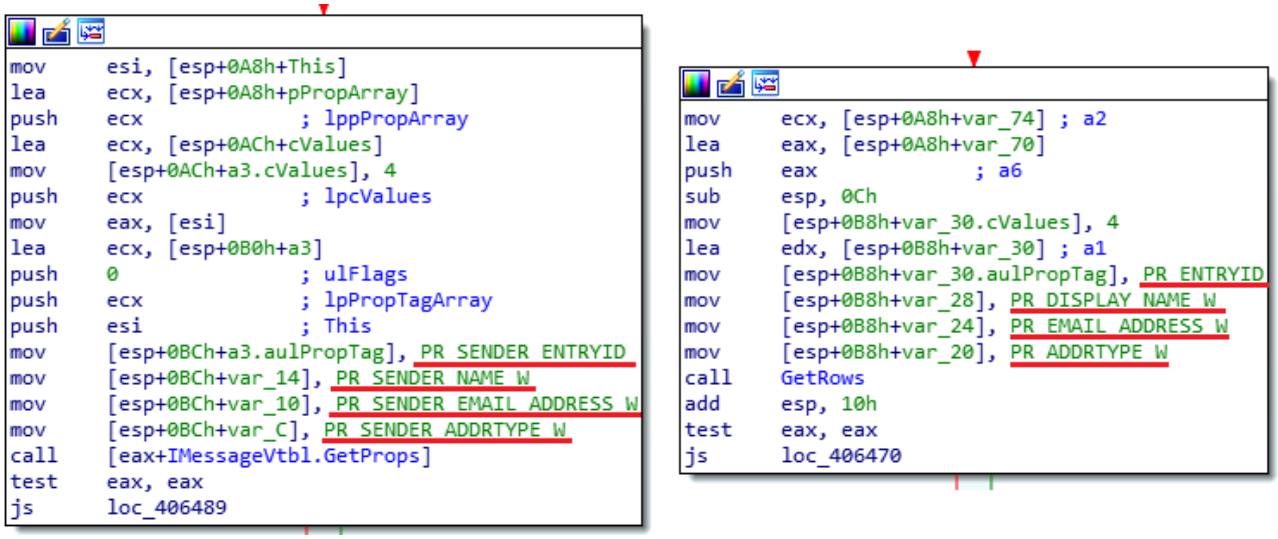
Emotet ist seit mehreren Jahren eine bekannte Trojaner-Gruppe. Lag der Fokus zuvor auf Internetbanking, so hat sich Emotet heute zu einem modularen Downloader und Infostealer entwickelt.

Erste Berichte der neusten Emotet-Version wurden von CERT Polska im April 2017 veröffentlicht. Bereits zur dieser Zeit wurde Emotet über per E-Mail versandte Links, die auf einen Dropper verweisen, verteilt.

Kürzlich warnte CERT-Bund erneut vor Spam-Emails, über die Emotet verbreitet wird. Auch bei diesen Mails scheint der Absender dem Empfänger bekannt zu sein - dies stärkt das Vetrauen in die E-Mail und erhöht die Wahrscheinlichkeit, dass der Empfänger eine genauere Überprüfung von Anhängen oder enthaltenen Links vernachlässigt. Um solche Beziehungen zwischen Personen herstellen zu können, liefert Emotet ein spezielles Modul aus, das alle E-Mails in den Outlook-Konten des aktuellen Benutzers analysiert und Relationen zwischen Sendern und Empfängern aufbaut.



Zur Extraktion der Informationen aus Outlook verwendet das Modul die standardisierte Schnittstelle MAPI (im Bild oben wird der Ladevorgang der MAPI-DLL und das Auflösen der vom Modul benötigten Funktionen dargestellt). Mit Hilfe dieser Schnittstelle iteriert das Modul über alle ihm zugänglichen Outlook-Profile des Computers. Aus jedem Profil werden aus allen vorhandenen E-Mail-Konten Name und E-Mail-Adresse extrahiert. Im Anschluss wird jeder Ordner des Profils rekursiv nach E-Mails durchsucht. Aus jeder gefundenen E-Mail werden der Absender (angezeigter Name und E-Mail-Adresse) sowie alle Empfänger (angezeigter Name und E-Mail-Adresse) inklusive der Empfänger in den CC- und BCC-Feldern extrahiert und in Relation zueinander gespeichert (im Bild unten sind die Felder zu sehen, welche aus den E-Mails extrahiert werden). Sollte in einem der extrahierten Felder ein Verweis auf das Adressbuch enthalten sein, wird aus dem entsprechenden Eintrag des Adressbuches Name und die E-Mail-Adresse der Person extrahiert. Allerdings werden nur die Header der E-Mail ausgewertet, der Inhalt wird nicht analysiert.



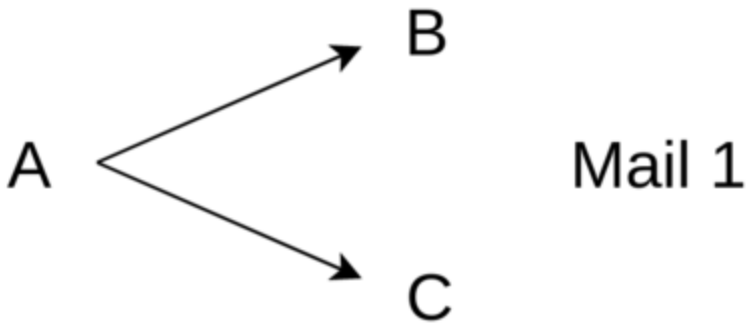
```
mov     esi, [esp+0A8h+This]
lea     ecx, [esp+0A8h+pPropArray]
push    ecx             ; lppPropArray
lea     ecx, [esp+0ACh+cValues]
mov     [esp+0ACh+a3.cValues], 4
push    ecx             ; lpcValues
mov     eax, [esi]
lea     ecx, [esp+0B0h+a3]
push    0               ; ulFlags
push    ecx             ; lpPropTagArray
push    esi             ; This
mov     [esp+0BCh+a3.aulPropTag], PR_SENDER_ENTRYID
mov     [esp+0BCh+var_14], PR_SENDER_NAME_W
mov     [esp+0BCh+var_10], PR_SENDER_EMAIL_ADDRESS_W
mov     [esp+0BCh+var_C], PR_SENDER_ADDRTYPE_W
call    [eax+IMessageVtbl.GetProps]
test    eax, eax
js      loc_406489
```

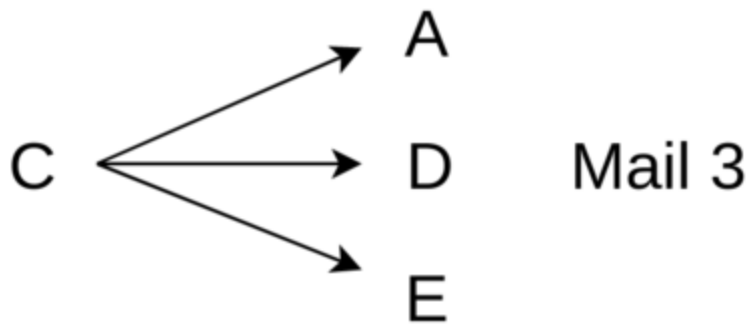
```
mov     ecx, [esp+0A8h+var_74] ; a2
lea     eax, [esp+0A8h+var_70]
push    eax             ; a6
sub     esp, 0Ch
mov     [esp+0B8h+var_30.cValues], 4
lea     edx, [esp+0B8h+var_30] ; a1
mov     [esp+0B8h+var_30.aulPropTag], PR_ENTRYID
mov     [esp+0B8h+var_28], PR_DISPLAY_NAME_W
mov     [esp+0B8h+var_24], PR_EMAIL_ADDRESS_W
mov     [esp+0B8h+var_20], PR_ADDRTYPE_W
call    GetRows
add     esp, 10h
test    eax, eax
js      loc_406470
```

Nachdem alle Profile, Ordner und E-Mails durchsucht wurden, schreibt das Modul die gesammelten Daten in eine temporäre Datei im Verzeichnis %PROGRAMDATA%. Die E-Mail-Adressen werden zusätzlich noch nach der Häufigkeit ihres Vorkommens absteigend sortiert. Jede E-Mail wird um alle Kontakte erweitert, zu denen sie in Relation steht. Es werden dabei jedoch zwei Fälle unterschieden:

- ist der referenzierte Kontakt der Absender einer E-Mail, werden alle Empfänger dem Kontakt zugeordnet
- ist der referenzierte Kontakt ein Empfänger der E-Mail, wird nur der Absender dem Kontakt zugeordnet.

Beispiel:





Postfach von A:

Mail 1: A sendet an B und C

Mail 2: D sendet an A

Mail 3: C sendet an A , D und E

A wird 3-mal referenziert und steht in der Liste ganz oben. A hat durch Mail 1 eine Verbindung zu B und C, diese werden also mit A verknüpft. Mail 2 zeigt eine Verbindung von D zu A, deshalb wird D ebenfalls mit A verknüpft. In Mail 3 ist eine Relation von C nach A vorhanden. Diese wird allerdings ignoriert, da sie bereits zu Beginn mit A→C erfasst wurde. In Mail 3 gibt es allerdings noch die Relationen C↔D und C↔E. Da weder die Relation C↔D noch C↔E in der Liste vorhanden sind, werden C die Kontakte D und E zugeordnet und ebenfalls in die Liste aufgenommen.

Die vollständige Liste, die dem Angreifer übermittelt wird, sieht nun wie folgt aus:

A<A@mail.com>; B<B@mail.com>; C<C@mail.net>; D<D@mail.com>

C<C@mail.net>; D<D@mail.com>; E<E@mail.com>

Anschließend wird die Datei verschlüsselt, an den Server der Angreifer übermittelt und von der Festplatte des Computers gelöscht.

Durch dieses Modul erhalten die Angreifer einen umfassenden Überblick, ob und in welcher Relation die Sender und Empfänger der Mails stehen. Unter Zuhilfenahme einer solchen Liste ist es für einen Angreifer mit keinem großen Aufwand verbunden, die Beziehungen von Personen zueinander zu erkennen und Spam-Mails mit passenden Absendern zu schicken. Zusätzlich gewinnt ein Angreifer Informationen über Relationen von Personen, deren Rechner nicht befallen sind.

Um die Spam E-Mails später an die passenden Adressaten verteilen zu können, benötigen die Angreifer E-Mail Accounts. Um dies zu erreichen, setzen sie ein zusätzliches Modul mit der Aufgabe, die Zugangsdaten aus E-Mail Programmen zu extrahieren und an die Angreifer zu übermitteln, ein. Das Modul greift dazu auf eine mitgeführte Kopie der Anwendung *Mail PassView* der Firma NirSoft zurück. Diese extrahiert die Zugangsdaten aus allen geläufigen E-Mail Programmen (Microsoft Outlook, Mozilla Thunderbird, Windows Mail, ...) und schreibt diese ebenfalls in eine temporäre Datei. Diese Datei wird dann wieder verschlüsselt, an den Server der Angreifer übermittelt und anschließend gelöscht.

Update: Emotet nimmt Bankkunden ins Visier - vollständige Analysen verfügbar

Weitere Informationen finden Sie auch auf dem Blog der G DATA Advanced Analytics. (Quelle in englischer Sprache)

- Malware
- CyberCrime
- Mails

Sollten Sie in Ihrem Posteingang keine E-Mail von uns vorfinden, kontrollieren Sie bitte auch Ihren Spamordner.

zurück zum Formular