MRLAB

Sənədlərin elektron sorğusu – yerli dövlət orqanlarını hədəf alan zərərvericinin analizi

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti – Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi - Malware Research Lab – F. Cəfərov - 10 iyun 2022

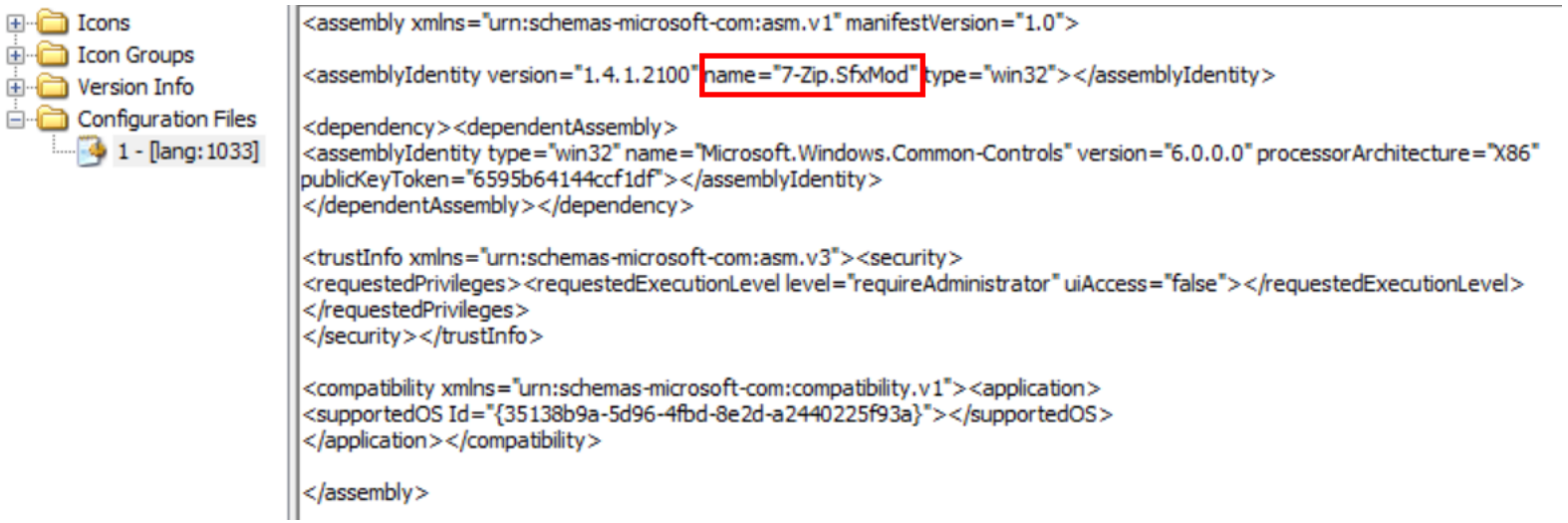
Bu məqalədə dövlət qurumlarına göndərilən "Sənədlərin elektron sorğusu" adlı icra olunan faylın analizini aparılacaq. İlk öncə faylın statik analizi aparılacaq.

File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	8.54 MB (8950370 bytes)
PE Size	298.00 KB (305152 bytes)
Created	Tuesday 07 June 2022, 15.54.06
Modified	Friday 29 January 2021, 02.31.32
Accessed	Wednesday 08 June 2022, 09.47.02
MD5	187C5C50CD81FDF336C527DA62375531
SHA-1	2BF61DBFF3E4FB8D4317A27C312824C18C52C5AC

Property	Value
CompanyName	TektonIT
FileDescription	RMS Component
FileVersion	6.3
InternalName	
LegalCopyright	Copyright © 2015 TektonIT. All rights reserved.
OriginalFilename	RMS Module
PrivateBuild	
ProductName	RMS

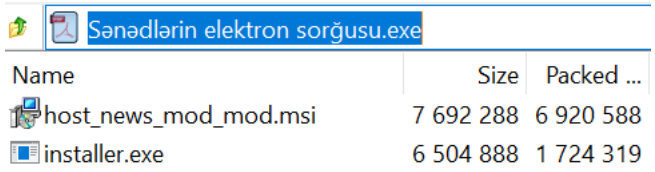
Şəkil 1.

Daxil olan fayl Microsoft Visual c++ 6.0 verisyasında hazırlanmış 32 bitlik portable executable-dır. Faylın həcmi 8.54 MB-dır. Faylın resurs bölməsinə nəzər yetirək. Burada “Configuration files” bölməsində “7-Zip.SfxMod” yazısı diqqətimizi cəkir (Şəkil 2).



Şəkil 2.

Bu yazı icra olunan faylın SFX modulu ilə sıxışdırılmış olduğun göstərir. SFX modulu quraşdırma (installation) proqramı yaratmağa imkan verir. Modul istifadəçinin müvəqqəti qovluğuna arxivi çıxarır və müəyyən edilmiş proqramı işə salır və proqram başa çatdıqdan sonra müvəqqəti faylları silir. 7-zip vasitəsi ilə icra olunan faylı açaq (şəkil 3). Faylın host_news_mod_mod.msi və installer.exe faylların görürük.



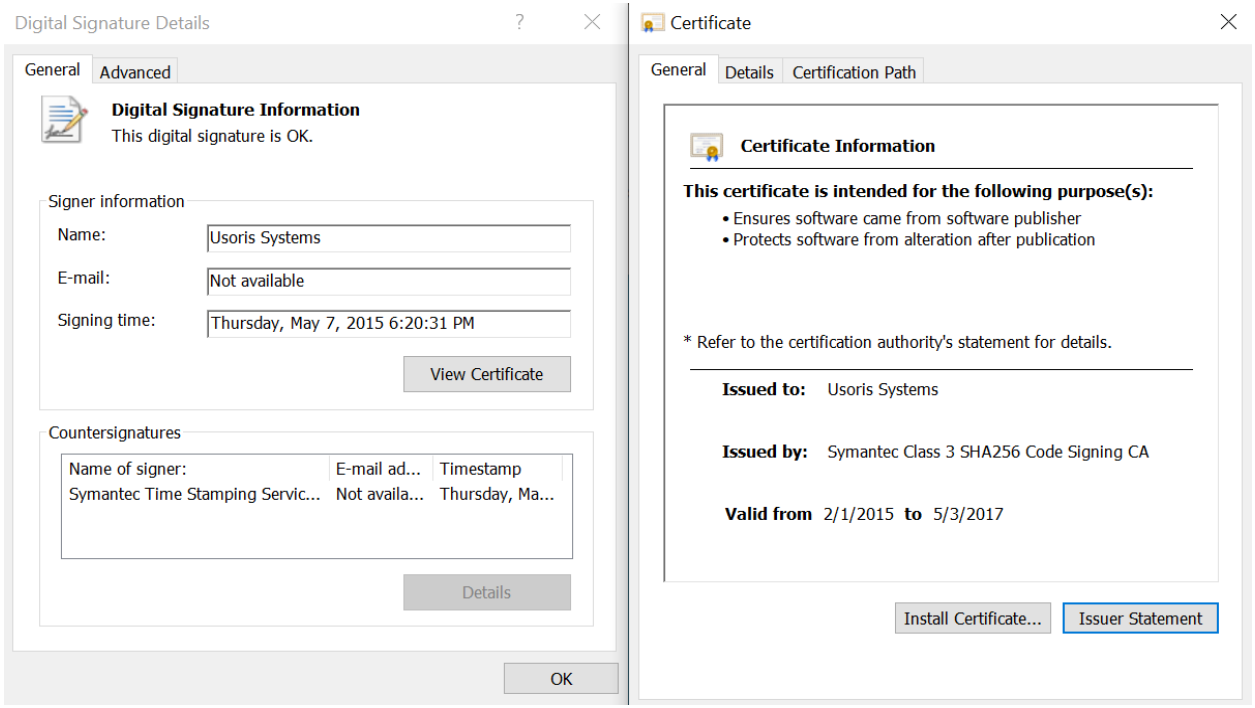
Şəkil 3.

İlk öncə host_news_mod_mod.msi faylının analizini aparaq. Faylı dekompress edirik. Dekompress olunandan sonra “Data1.cab” faylının analizi ilə davam edirik. “CAB” – Microsoft tərəfindən hazırlanmış məlumatların sıxılma fayl növüdür. LZX, Quantum və

ZIP kimi sıxılmış məlumat alqoritmlərini dəstəkləyir. Data1.cab faylını dekompress edirik.
Aşağıda göstərilən fayllar diqqətimizi çəkir:

Faylın adı	MD5	SHA1	SHA256
rfusclient.exe	477bd1ce48510c988c41011ca8195b49	8dd2fc30218e13e23bdcbdf6a5402bd3495323e1	a5033cc383c699a39fa314491592be448e4821fa25611d6833f364238de2d5b0
rutserv.exe	90e027b39d2786d5b465a9dc53bf040e	5a9d6b1fcdaf4b2818a6eeca4f1c16a5c24dd9cf	99de2f7653107a227a79993aeb03b1bb443b66376c49ec590cf3a91d6cf184c8

rfusclient.exe - Borland Delphi 4.0 versiyasında hazırlanmış, 32 bitlik icra olunan fayldır. Faylın “Usoris Systems LLC” tərəfindən hazırlandığını və “File Description” bölməsində proqramın “Remote utilities” (uzaqdan idarəetmə) təsnifatına aid olduğu qeyd edilib. Proqram təminatı sertifikatla təmin edilib (şəkil 4).



Şəkil 4.

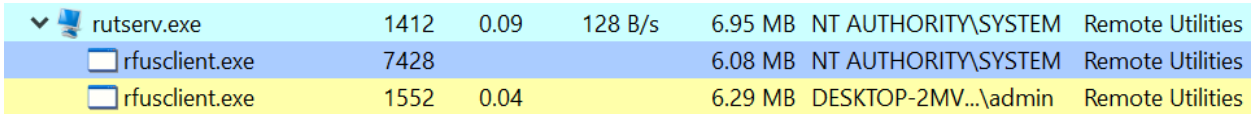
"**Remote Utilities**" haqqında daha ətraflı məlumat verək. "Remote Utilities" istifadəçiyə (viewer) başqa bir kompüteri uzaqdan idarə (host) etməyə imkan verən proqramıdır. Proqram təminatı uzaq kompüter üzərində tam nəzarəti təmin edir. Istifadəçi həmçinin internet üzərindən əlaqə yarada və İnternet ID bağlantısı vasitəsilə tələb olunan yorucu konfiqurasiyalardan yan keçə bilər. İnternet ID bağlantısı, istifadəçi və uzaq kompüter arasında əlaqə yaratmaq üçün vebdəki vasitəçi serverdən ("İnternet ID serveri") istifadə edir.

Qoşulma vasitçi serverə ehtiyac olmadan, IP ünvanı və ya DNS adı vasitəsilə host və uzaq kompüter arasında sürətli və birbaşa əlaqə yaratmağa imkan verir. Birbaşa əlaqə host kopüter birbaşa uzaq kompüterə görünən zaman yaradıla bilər, yəni host öz IP ünvanı və ya DNS ilə ünvanlana bilər. İnternet ID bağlantısından fərqli olaraq, birbaşa əlaqə host və uzaq kompüter arasında aralıq serverdən istifadə etmir. Əlaqə LAN və ya VPN kimi şəxsi şəbəkə üzərindən birbaşa əlaqə yaradıla bilər, yəni İnternetə çıxış olmadan təcrid olunmuş şəbəkələr üçün uyğundur.

Uzaqdan idarədə heç kimin olmadığı kompüterə 24/7/365 məhdudiyyətsiz giriş imkanı yaradır. Uzaq kompüterdə admin səlahiyyətə malik olub, hostu quraşdırıb və nəzarətsiz girişi əldə etmək mümkündür. Tam idarəetmə rejimi uzaqdan ekrana baxmaq, siçan göstəricisini hərəkət etdirmək və klaviatura idarə etmək imkanı verir. Proqram təminatı vasitəsilə ekran görüntüsü almaq, səs yazılarına qulaq asmaq, fayl ötürmə kimi imkanlar yaradır. Fayl ötürmə rejimi hər iki kopüterdən (host və uzaq kompüter) faylları kopyalamağa imkan verir.

installer.exe faylı təhlükəsizlik sertifikatı ilə təmin edilib. Statik analizi burada yekunlaşdırıb dinamik analizə keçid edirik.

Faylı işə salırıq. Proqram təminatı kompüterə quraşdırılır və “rutserv.exe” adı ilə dərhal işə düşür. “rutserv.exe” öz növbəsində 2 eyni “rfusclient.exe” adlı proses yaradır (şəkil 5).



Şəkil 5.

Proqramın qoşulduğu IP ünvanları tapmaq üçün trafik analizinə keçirik. Burada diqqətimizi bir IP ünvan cəkir (şəkil 6). Bütün sorğular TCP protokolu ilə gedir.

Source	Destination	Protocol	Length	Info
192.168.188.130	198.147.28.34	TCP	1514	49371 → 5655 [ACK] Seq=9 Ack=1 Win=64240 Len=1460
192.168.188.130	198.147.28.34	TCP	115	49371 → 5655 [PSH, ACK] Seq=1469 Ack=1 Win=64240 Len=61
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [ACK] Seq=1 Ack=9 Win=64240 Len=0
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [ACK] Seq=1 Ack=1469 Win=64240 Len=0
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [ACK] Seq=1 Ack=1530 Win=64240 Len=0
198.147.28.34	192.168.188.130	TCP	1514	5655 → 49371 [ACK] Seq=1 Ack=1530 Win=64240 Len=1460
198.147.28.34	192.168.188.130	TCP	149	5655 → 49371 [PSH, ACK] Seq=1461 Ack=1530 Win=64240 Len=95
192.168.188.130	198.147.28.34	TCP	60	49371 → 5655 [ACK] Seq=1530 Ack=1556 Win=64240 Len=0
192.168.188.130	198.147.28.34	TCP	60	49371 → 5655 [PSH, ACK] Seq=1530 Ack=1556 Win=64240 Len=4
192.168.188.130	198.147.28.34	TCP	94	49371 → 5655 [PSH, ACK] Seq=1534 Ack=1556 Win=64240 Len=40
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [ACK] Seq=1556 Ack=1534 Win=64240 Len=0
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [ACK] Seq=1556 Ack=1574 Win=64240 Len=0
198.147.28.34	192.168.188.130	TCP	60	5655 → 49371 [PSH, ACK] Seq=1556 Ack=1574 Win=64240 Len=4

Şəkil 6.

Bu sorğularda hansı məlumatların ötürüldüyünə baxaq (Şəkil 7). Xml formatda göndərilən məlumatda ilk öncə, <string_param> atributunda istifadəçinin (zərərçəkənin) proqram təminatının istifadə etdiyi ID göndərilir, <data> atributunda isə base64 şifrələnmiş məlumat göndərilir.

Şəkil 7.

Base64 məlumatı deşifrə etdikdə kompüter adı, ölkə, admin səlahiyyətinə sahib olma, əməliyyat sistemi və s. haqqında məlumatın xml formada göndərildiyini görürük (şəkil 8).

Proqram təminatı quraşdırıldıqdan sonra xaker zərərçəkənin kompüterinə tam nəzarəti əldə edir. Bu üsul rəsmi proqram təminatlarının zərərverənlər tərəfindən necə istifadə edildiyinin nümunəsidir.

İstinadlar

https://www.remoteutilities.com/product/
https://en.wikipedia.org/wiki/Self-extracting_archive