

CoinMiner

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler Tablosu

ÖN BAKIŞ.....	1
GOLFSTİKATOR.EXE ANALİZİ.....	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
STAGE 2 ANALİZİ	6
STATİK ANALİZ	7
DİNAMİK ANALİZ	7
STAGE-3 ANALİZİ	8
STATİK ANALİZ	8
DİNAMİK ANALİZ	8
YARA KURALI.....	15
MITRE ATTACK TABLE.....	17
ÇÖZÜM ÖNERİLERİ.....	18
HAZIRLAYAN	19

Ön Bakış

Golfstikator.exe CoinMiner ailesinden bir zararlıdır. Coin Miner, kurbanın bilgisayarının donanım öğelerini madencilik yapmak için kullanan bir kötü amaçlı yazılım türüdür. Bulaşmış olduğu bilgisayarlarda yüksek CPU kullanarak madencilik işlemi yapmakta, bilgisayarda yavaşlamalara ve hatalara neden olmaktadır. Çoğu zaman, CoinMiner malware türünü kontrol eden saldırganlar Monero (XMR) veya Litecoin adlı coin'leri hedeflerler, çünkü bunlar mining için en kolay olanlardır. Golfstikator kötü amaçlı yazılımın virüs bulaş olduğu bilgisayarları;

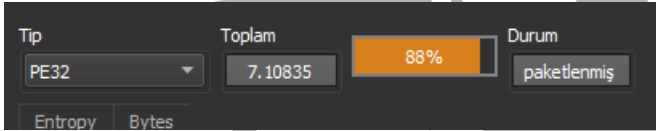
- Bilgisayar kaynaklarına,
- Bilgisayarda bulunan servislere, kayıtlara ve şifrelere,
- Bilgisayar ağına ve güvenlik yazılımlarına,
- Bilgisayar belgelerine erişim sağlamasına olanak sağlamaktadır.

Golfstikator.exe Analizi

Adı	golfstikator.exe
MD5	743fc0d22063e7ea97ca753280ff9f3e
SHA256	5c9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e74f86ba2
Dosya Türü	PE32/EXE

Statik Analiz

Golfstikator.exe zararlısı DIE aracı ile analiz edildiğinde paketlenmiş olduğu görülmektedir.



Şekil 1-Entropy değeri

Zararlının kodları statik olarak incelendiğinde şekil-2’de görüldüğü üzere işlevsiz, etkisiz API çağrıları ile karşılaşmaktadır. Bu API çağrıları ve anlamsız string’ler ile kodun analiz edilmesi zorlaştırılmaya çalışıldığı anlaşılmaktadır.

```
{
    GetNumberFormatA(
        0,
        0,
        "lediloporejefog guhewatazikisaniviho retubolozosoloru wetusevaligadubudiri",
        0,
        OutBuffer,
        0);
    GlobalFindAtomA("sageyi");
}
```

Şekil 2- İşlevsiz Api çağrıları

Dinamik Analiz

Golfstikator.exe zararlısının dinamik analiz kısmında, analizi zorlaştırmak için çeşitli teknikler kullanılmıştır. Zararlı incelenirken bu tekniklerden **Dynamic API Resolution** tekniğini kullanıldığı anlaşılmaktadır.

008F00F9	8D85 70FFFFFF	lea eax,dword ptr ss:[ebp-90]	
008F00FF	50	push eax	eax:"VirtualAlloc"
008F0100	FF75 C4	push dword ptr ss:[ebp-3C]	
008F0103	FF55 98	call dword ptr ss:[ebp-68]	
008F0106	8945 D8	mov dword ptr ss:[ebp-28],eax	
008F0109	C785 70FFFFFF 566972	mov dword ptr ss:[ebp-90],75CAF7F0 <kernel32.GetProcAddress>	
008F0113	C785 74FFFFFF 75616C	mov dword ptr ss:[ebp-8C],mov edi,edi	
008F011D	C785 78FFFFFF 726565	mov dword ptr ss:[ebp-88],push ebp	
008F0127	8D85 70FFFFFF	lea eax,dword ptr ss:[ebp-90]	
008F012D	50	push eax	
008F012E	FF75 C4	push dword ptr ss:[ebp-3C]	
008F0131	FF55 98	call dword ptr ss:[ebp-68]	
008F0134	8945 9C	mov dword ptr ss:[ebp-28],push dword ptr ss:[ebp-4]	
008F0137	C785 70FFFFFF 476574	mov dword ptr ss:[ebp-90],push dword ptr ss:[ebp-C]	
008F0141	C785 74FFFFFF 657273	mov dword ptr ss:[ebp-8C],call dword ptr ds:[<&GetProcAddressForCaller>]	

Şekil 3- GetProcAddress ile çözümlenmesi

Dinamik analiz sırasında zararlının self modifying tekniği ile yeni bir zararlı çıkarttığı farkedilmektedir. PE sectionları ayrı ayrı yazılarak oluşturulduğu anlaşılmaktadır.

02190331	8D4401 18	lea eax,dword ptr ds:[ecx+eax+18]	
02190335	8945 A0	mov dword ptr ss:[ebp-60],eax	
02190338	8B45 C8	mov eax,dword ptr ss:[ebp-38]	
0219033B	0345 A0	add eax,dword ptr ss:[ebp-60]	
0219033E	8945 CC	mov dword ptr ss:[ebp-34],eax	
02190341	8B45 CC	mov eax,dword ptr ss:[ebp-34]	
02190344	8945 90	mov dword ptr ss:[ebp-70],eax	
02190347	8B45 90	mov eax,dword ptr ss:[ebp-70]	
0219034A	FF70 14	push dword ptr ds:[eax+14]	
0219034D	FF75 C8	push dword ptr ss:[ebp-38]	
02190350	FFB5 68FFFFFF	push dword ptr ss:[ebp-98]	
02190356	E8 8C090000	call 2190CE7	
0219035B	83C4 0C	add esp,C	
0219035E	8B85 68FFFFFF	mov eax,dword ptr ss:[ebp-98]	
02190364	8945 C8	mov dword ptr ss:[ebp-38],eax	
02190367	8B45 C8	mov eax,dword ptr ss:[ebp-38]	
0219036A	8B40 3C	mov eax,dword ptr ds:[eax+3C]	
0219036D	8B8D 68FFFFFF	mov ecx,dword ptr ss:[ebp-98]	
02190373	8D4401 04	lea eax,dword ptr ds:[ecx+eax+4]	
02190377	8945 E4	mov dword ptr ss:[ebp-1C],eax	
0219037A	8B85 68FFFFFF	mov eax,dword ptr ss:[ebp-98]	
02190380	0345 A0	add eax,dword ptr ss:[ebp-60]	
02190383	8945 CC	mov dword ptr ss:[ebp-34],eax	
02190386	8B85 58FFFFFF	mov eax,dword ptr ss:[ebp-A8]	
0219038C	8B40 0E	mov eax,dword ptr ds:[eax+E]	

=[0019F774]=5c9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e74f86ba2.00400000

00	03	00	00	00	04	00	00	00	FF	FF	00	00	ASCII
00	00	00	00	00	40	00	00	00	00	00	00	00	MZ.....yy..
00	00	00	00	00	00	00	00	00	00	00	00	00@.....
00	00	00	00	00	00	00	00	00	00	00	00	000.....
0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68I!..LI!TH
70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
93	B9	D6	2D	C0	B9	D6	2D	C0	B9	D6	2D	C0	y.C.'O-A'O-A'O-A
C0	28	D6	2D	C0	B0	AE	BE	C0	B6	D6	2D	C0	'O,A(O-A'0xA'0-A
C0	88	D6	2D	C0	D6	A0	B3	C0	B8	D6	2D	C0	O .A.O-AO *A.O-A
C0	A2	D6	2D	C0	D6	A0	B0	C0	B8	D6	2D	C0	O .A0-AO *A.O-A
68	B9	D6	2D	C0	00	00	00	00	00	00	00	00	Rich'O-A.....

Şekil 4- Yeni zararlı'nın section'larının yazılması

Section kısmı oluşturulduktan sonra [**jmp eax**] komutu ile yeni zararlının adresine yazılmaktadır.

006F08E7	8945 E8	mov dword ptr ss:[ebp-18],eax
006F08EA	8845 E8	mov eax,dword ptr ss:[ebp-18]
006F08ED	888D 4CFFFFFF	mov ecx,dword ptr ss:[ebp-B4]
006F08F3	8908	mov dword ptr ds:[eax],ecx
006F08F5	837D D0 00	cmp dword ptr ss:[ebp-30],0
006F08F9	74 07	je 6F0902
006F08FB	FF75 BC	push dword ptr ss:[ebp-44]
006F08FE	FF55 D0	call dword ptr ss:[ebp-30]
006F0901	59	pop ecx
006F0902	8885 58FFFFFF	mov eax,dword ptr ss:[ebp-A8]
006F0908	8840 0E	mov eax,dword ptr ds:[eax+E]
006F090B	8985 5CFFFFFF	mov dword ptr ss:[ebp-A4],eax
006F0911	8885 5CFFFFFF	mov eax,dword ptr ss:[ebp-A4]
006F0917	0385 68FFFFFF	add eax,dword ptr ss:[ebp-98]
006F091D	C9	leave
006F091E	FFEO	jmp eax
006F0920	6A 00	push 0
006F0922	6A FF	push FFFFFFFF
006F0924	B8 44444444	mov eax,44444444
006F0929	FFD0	call eax

Şekil 5- Oluşturulan zararlının adresine atlandığı kısım

Oluşturulacak olan zararlının kaydedilebilmesi için çevre değişkenleri ve path kontrolü yapılmaktadır.

00409E60	68 3C0A4100	push 5C9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e	esi: "USERPROFILE"
00409E65	56	push esi	
00409E66	E8 D986FFFF	call 5C9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e	
00409E68	83C4 14	add esp,14	
00409E6E	50	push eax	eax: "C:\\Users\\
00409E6F	FF15 EC004100	call dword ptr ds:[&GetEnvironmentVariableA]	eax: "C:\\Users\\
00409E75	85C0	test eax, eax	
00409E77	0F84 CD020000	je 5C9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e74	
00409E7D	FF75 F8	push dword ptr ss:[ebp-8]	
00409E80	8D85 44FDFFFF	lea eax,dword ptr ss:[ebp-28C]	
00409E86	FF75 FC	push dword ptr ss:[ebp-4]	
00409E89	50	push eax	eax: "C:\\Users\\
00409E8A	8D85 64FDFFFF	lea eax,dword ptr ss:[ebp-29C]	
00409E90	50	push eax	eax: "C:\\Users\\
00409E91	8D85 0CFBFFFF	lea eax,dword ptr ss:[ebp-4F4]	
00409E97	50	push eax	eax: "C:\\Users\\
00409E98	E8 35FBFFFF	call 5C9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e	

Şekil 6 - Path kontrolü

Kontrol sağlandıktan sonra zararlı "C:\\Users\\UserName" klasörü altına kaydedilmektedir.

00409EA9	53	push ebx	
00409EAA	56	push esi	
00409EAB	E8 7A4F0000	call 5C9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07cd5e	
00409EB0	83C4 0C	add esp,C	
00409EB3	8D85 64FDFFFF	lea eax,dword ptr ss:[ebp-29C]	eax: "C:\\Users\\ \\z1bocbt.exe"
00409EB9	50	push eax	
00409EBA	8D85 0DFBFFFF	lea eax,dword ptr ss:[ebp-4F8]	eax: "C:\\Users\\ \\z1bocbt.exe"
00409EC0	50	push eax	
00409EC1	C685 0CFBFFFF 22	mov byte ptr ss:[ebp-4F4],22	22: " "

Şekil 7 - Zararlının oluşturulduğu klasör

Ayrıca, her defasında rastgele isimlerle aynı zararlıyı çıkarttığı gözlemlenmektedir. Başka bir örnek ekran resminde görüntülenmektedir.

Şekil 8- Zararlının başka isimlerle aynı klasöre oluşturulması

Yeni zararlı oluşturulduktan sonra, bilgisayar her yeniden başlatıldığında çalışabilmesi için

“Bilgisayar\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” yolundaki kayıt defteri adresine kaydedilmektedir. Registry kayıtlarını manipüle etmek için **RegOpenKeyExA**, **RegSetValueExA** ve **RegCloseKey** API'ları kullanılmaktadır.

Şekil 9- Kalıcılık için Run klasörüne kaydedilmesi

Run klasöründeki değerleri Şekil-10'da belirtilmektedir.

Bilgisayar\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
	Ad	Tür	Veri
	(Varsayılan)	REG_SZ	(değer atanmamış)
	evvmqsjr	REG_SZ	"C:\Users\ \zlbocbt.exe"
	MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
	OneDrive	REG_SZ	"C:\Users\tolga\AppData\Local\Microsoft\OneDri...

Şekil 10- Run klasöründeki görüntüsü

İşlemlerin sonunda yeni zararlı başarıyla oluşturulmaktadır. Yeni zararlı oluşturulduktan sonra Golfstikator zararlısının, yeni zararlıyı “/d” ve “/f” parametreleriyle çalıştırıp kendini silmekte ve kayıt defterine kaydederek kalıcılığı sağlamaktadır.

```
eax: "C:\\Users\\ \\bxmlhxf.exe" /d"C:\\Users\\ \\Desktop\\5c9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07c  
eax: "C:\\Users\\ \\bxmlhxf.exe" /d"C:\\Users\\ \\Desktop\\5c9051c7d3b4658cb635429f8644ed682bf23cf10f237b75dd07c
```

Şekil 11- Oluşturulan zararlının parametreler ile çalıştırılması

Zararlının Process Hacker ile incelendiğinde %47 CPU tüketimi yaptığı incelenmektedir.

explorer.exe	5348	0,08
ProcessHacker.exe	5900	0,43
vmtoolsd.exe	324	22,89
OneDrive.exe	7020	
5c9051c7d3b4658...	6776	47,54
SIHClient.exe	3052	0,04

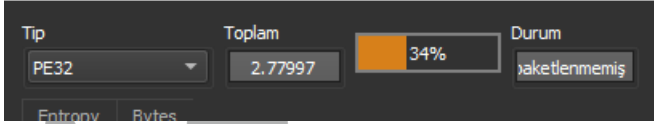
Şekil 12- Zararlının CPU tüketimi

Stage 2 Analizi

Adı	-
MD5	71d1f08703f6d940c3b2f88f811d792b
SHA256	e5d60c81a634c00c8c1861ef260d71810d1bca6294d8542598f664b260075fd8
Dosya Türü	PE32/EXE

Statik Analiz

Stage-2’de zararlı DIE aracına atılıp analiz edildiğinde paketlenmemiş olduğu görülmektedir. Statik analizin devamında Golfstikator zararlısıyla nerdeyse aynı olduğu ve bu zararlının da çeşitli dinamik çözümlemeler kullanılacağı anlaşılmaktadır.



Şekil 13-Entropy değeri

Dinamik Analiz

Stage-2’nin analizinde Golfstikator zararlısından farklı bir bulguya rastlanmamaktadır. Herhangi bir bulguya rastlanmadığından, Şekil-14’te belirtilen bölgeden “dump” alınmış ve analize alınan “dump” üzerinden devam edilmesi uygun görülmüştür.

```
007F0268 FF75 F0 push dword ptr ss:[ebp-10]
007F026E 8885 58FFFFFF mov eax,dword ptr ss:[ebp-A8]
007F0274 FF70 02 push dword ptr ds:[eax+2]
007F0277 8885 58FFFFFF mov eax,dword ptr ss:[ebp-A8]
007F027D 83C0 3A add eax,3A
007F0280 50 push eax
007F0281 E8 E3070000 call 7F0A69
007F0286 83C4 14 add esp,14
007F0289 EB 43 jmp 7F02CE
007F028B 83A5 48FFFFFF and dword ptr ss:[ebp-B8],0
007F0292 EB 0D jmp 7F02A1
007F0294 8885 48FFFFFF mov eax,dword ptr ss:[ebp-B8]
007F029A 40 inc eax
007F029B 8985 48FFFFFF mov dword ptr ss:[ebp-B8],eax
007F02A1 8885 58FFFFFF mov eax,dword ptr ss:[ebp-A8]
007F02A7 8880 48FFFFFF mov ecx,dword ptr ss:[ebp-B8]
007F02AD 3848 02 cmp ecx,dword ptr ds:[eax+2]
007F02B0 73 1C jae 7F02CE
007F02B2 8845 F0 mov eax,dword ptr ss:[ebp-10]
007F02B5 0385 48FFFFFF add eax,dword ptr ss:[ebp-B8]
007F02B8 8880 58FFFFFF mov ecx,dword ptr ss:[ebp-A8]
007F02C1 0380 48FFFFFF add ecx,dword ptr ss:[ebp-B8]
007F02C7 8A49 3A mov cl,byte ptr ds:[ecx+3A]
007F02CA 8808 mov byte ptr ds:[eax+3A],cl
007F02CC EB C6 jmp 7F0294
007F02CE 8D45 E0 lea eax,dword ptr ss:[ebp-20]
007F02D1 50 push eax
007F02D2 6A 40 push 40
007F02D4 8885 58FFFFFF mov eax,dword ptr ss:[ebp-A8]
007F02DA FF70 0A push dword ptr ds:[eax+A]
007F02DD FF85 50FFFFFF push dword ptr ss:[ebp-B0]
007F02E3 FF55 D8 call dword ptr ss:[ebp-28]
007F02E6 8945 F4 mov dword ptr ss:[ebp-C],eax
007F02E9 8885 50FFFFFF mov eax,dword ptr ss:[ebp-B0]
```

tr [ebp-B0]=[0019F75C]=nqngxztj.00400000

D

Hex	ASCII
0 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....yy..
0 88 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 0E 1F 8A 0E 00 84 09 CD 21 88 01 4C CD 21 54 68!..L!Th
0 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
0 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
0 6D 6F 64 65 2E 0D 00 0A 24 00 00 00 00 00 00 00	mode...\$.

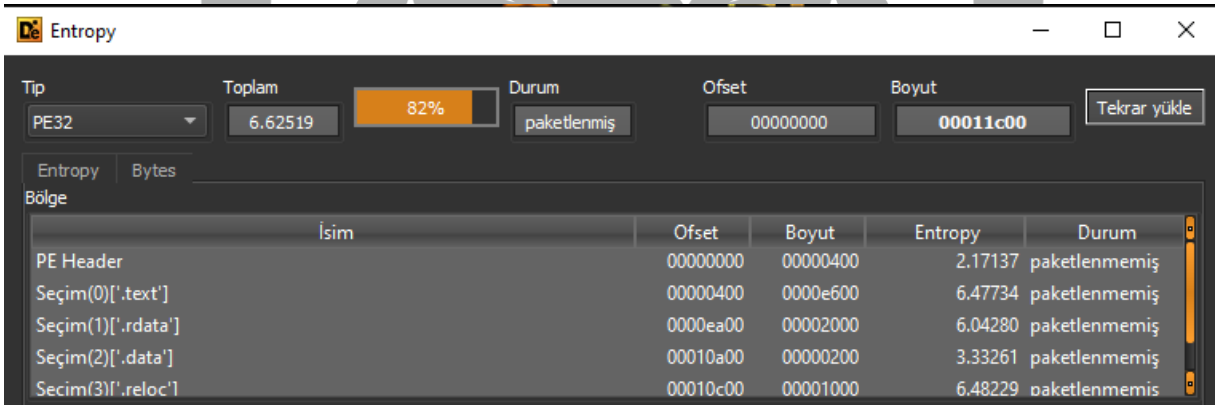
Şekil 14- Section'ların yazıldığı döngü

Stage-3 Analizi

Adı	-
MD5	a050f3c88055b70ddf52d04747d4f527
SHA256	ca07ed841c430fedf79b2696148963cc5c5c989641e40aa34c022d4685e8ba3e
Dosya Türü	PE32/EXE

Statik Analiz

Alınan “dump” DIE aracı ile incelendiğinde entropy değerinden dolayı paketlenmiş olduğu görülmektedir fakat section'ları incelendiğinde paketlenmemiş olduğu anlaşılmaktadır.



Şekil 15-Entropy değeri

Dinamik Analiz

Stage-3 zararlı (dump) incelendiğinde öncelikle kayıt defterinde çeşitli manipülasyonlar yapıldığı ve sistem servislerinin bilgisine ulaşıldığı görülmektedir.

00CD7456	53	push ebx	
00CD7457	6A 22	push 22	
00CD7459	68 E806CE00	push dump.CE06E8	
00CD745E	8E F822CE00	mov esi,dump.CE22F8	
00CD7463	56	push esi	esi:"SYSTEM\\CurrentControlSet\\services", esi:"SYSTEM\\CurrentControlSet\\services"
00CD7464	E8 DB80FFFF	call dump.CD2544	
00CD7469	83C4 14	add esp,14	
00CD746C	50	push eax	
00CD746D	68 02000080	push 80000002	eax:"SYSTEM\\CurrentControlSet\\services"
00CD7472	FF15 6000CE00	call dword ptr ds:[<&RegOpenKeyExA>]	
00CD7478	68 00010000	push 100	

Şekil 16- Kayıt defteri adreslerinden servis kontrolü

İncelemeler devam ettiğinde kayıt defterindeki .NET servisinin çeşitli kayıtlarına erişebildiği görüntülenmektedir.

00027700	FF75 EC	push dword ptr ss:[ebp-14]	eax:".NET CLR Data"
00027703	FF75 F0	push dword ptr ss:[ebp-10]	
00027706	FF15 5C000300	call dword ptr ds:[<&RegEnumKeyA>]	
0002770C	85C0	test eax,eax	eax:".NET CLR Data"
0002770E	0F84 8EFDFFFF	je dump.274A2	
00027714	FF75 F0	push dword ptr ss:[ebp-10]	
00027717	FF15 78000300	call dword ptr ds:[<&RegCloseKey>]	
0002771D	E9 DF000000	jmp dump.27801	
00027722	C607 2E	mov byte ptr ds:[edi],2E	2E:'. '
00027725	EB B6	jmp dump.276DD	
00027727	83F8 05	cmp eax,5	eax:".NET CLR Data"
0002772A	75 29	jne dump.27755	
0002772C	8D85 D8FDFFFF	lea eax,dword ptr ss:[ebp-228]	eax:".NET CLR Data"
00027732	50	push eax	
00027733	FF75 14	push dword ptr ss:[ebp+14]	
00027700	FF75 EC	push dword ptr ss:[ebp-14]	
00027703	FF75 F0	push dword ptr ss:[ebp-10]	
00027706	FF15 5C000300	call dword ptr ds:[<&RegEnumKeyA>]	eax:".NET CLR Networking"
0002770C	85C0	test eax,eax	
0002770E	0F84 8EFDFFFF	je dump.274A2	
00027714	FF75 F0	push dword ptr ss:[ebp-10]	
00027717	FF15 78000300	call dword ptr ds:[<&RegCloseKey>]	
0002771D	E9 DF000000	jmp dump.27801	
00027722	C607 2E	mov byte ptr ds:[edi],2E	2E:'. '
00027725	EB B6	jmp dump.276DD	
00027727	83F8 05	cmp eax,5	eax:".NET CLR Networking"
0002772A	75 29	jne dump.27755	

Şekil 17- .NET servislerinin kayıtları

Daha sonrasında, başlangıç servislerini barındıran “**Current Version\Run**” kayıtlarına eriştiğini gözlemlenmektedir.

00CD7083	56	push esi	esi:"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
00CD7084	E8 8B84FFFF	call dump.CD2544	
00CD7089	83C4 14	add esp,14	
00CD708C	50	push eax	eax:"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
00CD708D	68 01000080	push 80000001	
00CD70C2	FF15 6000CE00	call dword ptr ds:[<&RegOpenKeyExA>]	
00CD70C8	85C0	test eax,eax	eax:"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run"
00CD70CA	0F85 E8000000	jne dump.CD71B8	
00CD70D0	E8 EDFCFFFF	call dump.CD6DC2	
00CD70D5	8D4D F4	lea ecx,dword ptr ss:[ebp-C]	
00CD70D8	51	push ecx	

Şekil 18- Kayıt defterinden Run klasörüne erişilmesi

İncelemeye devam edildiğinde OneDrive ve Microsoft Edge gibi Windows uygulamalarını araştırdığı gözlemlenmektedir.

Şekil 19- Microsoft Edge klasör kontrolü

“ **Control Panel\Buses** ” kayıtlarında yeni bir değer oluşturulduğu ve içine anlamsız string atamaları yapıldığı görülmektedir.

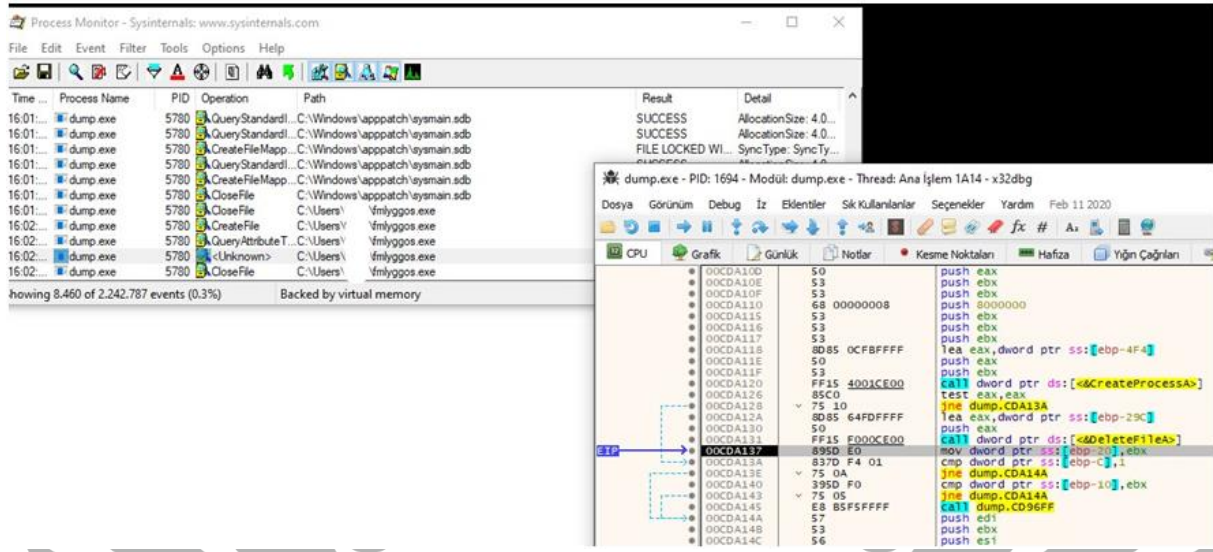
Şekil 20- Kayıt defterinde yeni bir kayıt oluşturma

Kayıt defterinde oluşturulan değerler Şekil-23’de görülmektedir.

Bilgisayar\HKEY_CURRENT_USER\Control Panel\Buses	Tür	Veri
HKEY_CLASSES_ROOT	REG_SZ	(değer atanmamış)
HKEY_CURRENT_USER	REG_BINARY	cc a0 22 3d 18 da dc 03 24 ed b4 7d 45 0d d4 9d 13 ...
AppEvents	REG_BINARY	49 79 13 8e d0 6f 69 02 86 42 5e 38 eb 91 6b be f8 89...

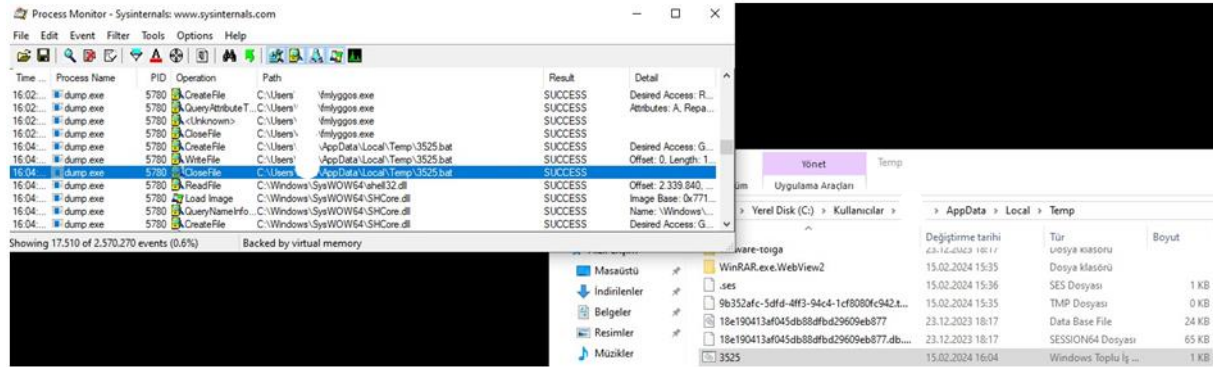
Şekil 21-Oluşturulan kayıt değerleri

Zararlıının, dinamik olarak kodları incelenmeye devam edildiğinde **CreateProcessA** API’ı ile yeni bir process oluşturup “ **C:\Users\UserName** ” dizinine kaydettiğini daha sonrasında bu işlemi **DeleteFileA** kullanarak sildiğini ancak bu işlemin Process Monitor’de bilinmeyen işlem olarak bildirildiği incelenmektedir.

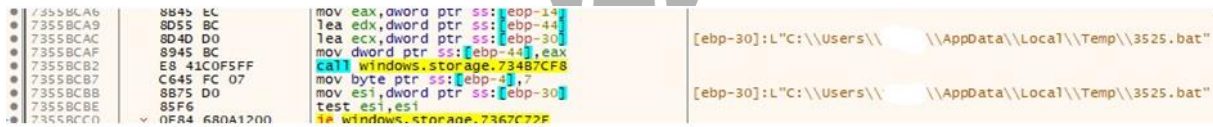


Şekil 22- Zararlıının silme işleminin Procmon ve Debugger araçındaki işlem görüntüsü

İncelemeler devam ettiğinde **\Temp** dizininde 3525 adında bat uzantılı bir dosya oluşturduğu ardından dump dosyasını sildiği anlaşılmaktadır.

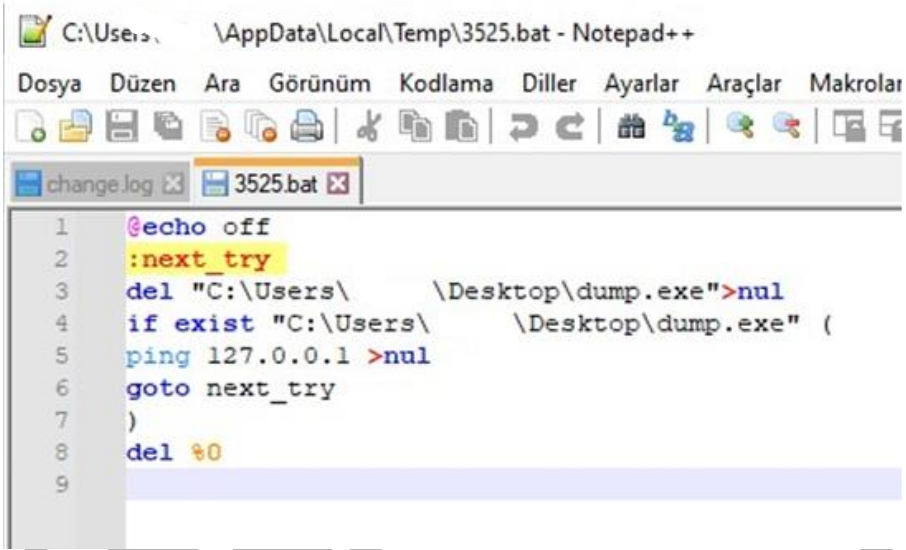


Şekil 23- Silmek için oluşturulan .bat uzantılı dosya



Şekil 24- İlgili dosyanın Debugger'daki kontrolü

İlgili dosya incelendiğinde silmek için kullanılan script aşağıdaki şekilde görüntülenmektedir.



```
1 @echo off
2 :next_try
3 del "C:\Users\      \Desktop\dump.exe">nul
4 if exist "C:\Users\      \Desktop\dump.exe" (
5 ping 127.0.0.1 >nul
6 goto next_try
7 )
8 del %0
9
```

Şekil 25- .bat uzantılı dosyanın içeriği

Debugger'dan incelendiğinde .bat uzantılı dosyanın **ShellExecuteA** API'ı ile çalıştırıldığı görüntülenmektedir.

00CD91C8	50	push eax	
00CD91C9	E8 96FEFFFF	call dump.CD9064	
00CD91CE	83C4 24	add esp,24	
00CD91D1	85C0	test eax,eax	
00CD91D3	74 12	je dump.CD91E7	
00CD91D5	57	push edi	
00CD91D6	57	push edi	
00CD91D7	57	push edi	
00CD91D8	8D85 FCFEFFFF	lea eax,dword ptr ss:[ebp-104]	
00CD91DE	50	push eax	
00CD91DF	57	push edi	
00CD91E0	57	push edi	
00CD91E1	FF15 D801CE00	call dword ptr ds:[<&ShellExecuteA>]	
00CD91E7	5F	pop edi	
00CD91E8	5E	pop esi	
00CD91E9	C9	leave	
00CD91EA	C3	ret	
00CD91EB	55	push ebp	
00CD91EC	8BEC	mov ebp,esp	
00CD91EE	81EC 08020000	sub esp,208	
00CD91F4	8365 F8 00	and dword ptr ss:[ebp-8],0	
00CD91F8	53	push ebx	
00CD91F9	56	push esi	
00CD91FA	57	push edi	
00CD91FB	8B7D 0C	mov edi,dword ptr ss:[ebp+C]	[ebp+C]:EntryPoint
00CD91FE	803F 00	cmp byte ptr ds:[edi],0	
00CD9201	C745 FC 10000000	mov dword ptr ss:[ebp-4],10	
00CD9208	0F84 FA000000	je dump.CD9308	
00CD920E	6A 0D	push 0	
00CD9210	57	push edi	
00CD9211	E8 ED5A0000	call dump.CDED03	

exe: \$91E0 #85E0

Döküm3		Döküm4		Döküm5		İzle 1		[x=] Yerel Değişkenler		Yapı	
ASCII											
6F 20 6F 66	66 0D 0A 3A	6E 65 78 74	@echo off..:next								
0D 0A 64 65	6C 20 22 43	3A 5C 55 73	_try..del "C:\Us								
74 6F 6C 67	61 5C 44 65	73 6B 74 6F	ers\ \Deskto								
6D 70 2E 65	78 65 22 3E	6E 75 6C 0D	p\dump.exe">nul.								
65 78 69 73	74 20 22 43	3A 5C 55 73	.if exist "C:\Us								
74 6F 6C 67	61 5C 44 65	73 6B 74 6F	ers\ \Deskto								
6D 70 2E 65	78 65 22 20	28 0D 0A 70	p\dump.exe" (..p								
31 32 37 2E	30 2E 30 2E	31 20 3E 6E	ing 127.0.0.1 >n								
67 6F 74 6F	20 6E 65 78	74 5F 74 72	ul..goto next_tr								
0D 0A 64 65	6C 20 25 30	0D 0A 00 01	y..).del %0....								
01 00 00 00	50 70 12 01	04 00 00 00	uMiW....Pp.....								
8A 2A 51 8D	48 70 12 01	00 00 12 01	zPiW.*Q.Hp.....								
00 00 00 00	00 00 00 00	30 AE D1 770 Nw								
FE FF FF FF	80 ED 0F 01	7C 6E CE 77	Z..üpyyy.i.. niW								
20 00 00 00	00 00 00 00	18 00 07 1F	...								
00 00 12 01	01 00 00 00	D7 00 00 00	c..P.....x...								
BF 86 14 01	7F 00 00 00	70 00 00 00	...Z.....P...								

Şekil 26- .bat uzantılı dosyanın Debugger'da oluşturulması

Dinamik analizin devamında “vanheim.cn”, “jotunheim.name” ve “free.serv-tech.ru” adında dns adresleri ile iletişim kurduğu tespit edilmektedir.

00088851	59	pop ecx	ecx:"free.serv-tech.ru"
00088852	59	pop ecx	ecx:"free.serv-tech.ru"
00088853	85C0	test eax,eax	
00088855	74 15	je dump.B886C	
0008256D	4F	dec edi	
0008256E	75 EA	jne dump.B255A	
00082570	5E	pop esi	esi:"jotunheim.name"
00082571	8B45 08	mov eax,dword ptr ss:[ebp+8]	[ebp+8]:"jotunheim.name"
00082574	5F	pop edi	
00082575	5D	pop ebp	
00082576	C3	ret	
00082577	8B41 0C	mov eax,dword ptr ds:[ecx+C]	eax:"jotunheim.name"
0008257A	8D50 FF	lea edx,dword ptr ds:[eax-1]	

Şekil 27- İletişim kurulan DNS adresleri

Zararlıının yaptığı diğer bağlantılar ProcMon aracı ile incelendiğinde rastgele ip adresleriyle bağlantı kurduğu anlaşılmaktadır.

dump.exe	1104	TCP Disconnect	DESKTOP-GI7IRKR.localdomain:49833 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Disconnect	DESKTOP-GI7IRKR.localdomain:49836 -> 80.66.75.4:416	SUCCESS
dump.exe	1104	TCP Disconnect	DESKTOP-GI7IRKR.localdomain:49837 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Disconnect	DESKTOP-GI7IRKR.localdomain:49838 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Disconnect	DESKTOP-GI7IRKR.localdomain:49839 -> 83.97.73.44:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49851 -> 83.97.73.44:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49848 -> 80.66.75.4:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49851 -> 83.97.73.44:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49848 -> 80.66.75.4:416	SUCCESS
dump.exe	1104	TCP Send	DESKTOP-GI7IRKR.localdomain:49851 -> 83.97.73.44:416	SUCCESS
dump.exe	1104	TCP Send	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Send	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Send	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Send	DESKTOP-GI7IRKR.localdomain:49848 -> 80.66.75.4:416	SUCCESS
dump.exe	1104	TCP Connect	DESKTOP-GI7IRKR.localdomain:49852 -> free.serv-tech.ru/https	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49852 -> free.serv-tech.ru/https	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49851 -> 83.97.73.44:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49848 -> 80.66.75.4:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49849 -> 176.113.115.135:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49847 -> 62.122.184.92:416	SUCCESS
dump.exe	1104	TCP Receive	DESKTOP-GI7IRKR.localdomain:49850 -> 176.113.115.136:416	SUCCESS

Şekil 28- Procmon aracı ile bağlantı kurulan adreslerin görüntülenmesi

YARA Kuralı

```
import "hash"

rule golfstikator

{

    meta:

        author = "Tolga Yılmaz"

    strings:

        $a1 = "C:\\jupivulehu.pdb"

        $a2 = "sageyi"

        $a3 = "puduvikajicezodezofut"

        $b = { 6C 65 64 69 6C 6F 70 6F 72 65 6A 65 66 6F 67 20 67 75 68
65 77 61 74 61 7A 69 6B 69 73 61 6E 69 76 69 68 6F }

    condition:

        hash.md5(0, filesize) == "743fc0d22063e7ea97ca753280ff9f3e" or

        2 ($a*) or $b

}
```

```
import "hash"

rule tofsee

{

    meta:

        author = "Tolga Yılmaz"

    strings:

        $a1 = "\\.\pipe\\"

        $a2 = "smtp_herr"

        $a3 = "lid_file_upd"

        $a4 = "loader_id"

        $a5 = "12:08:32"

        $b = { 77 74 6D 5F }

    condition:

        hash.md5(0, filesize) == "a050f3c88055b70ddf52d04747d4f527" or

        3 of ($a*) and $b

}
```

MITRE ATTACK TABLE

Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	C&C
Command and Scripting Interpreter (T1059)	Windows Service (T1543.003)	Windows Service (T1543.003)	Software Packing (T1027.002)	Security Software Discovery (T1518.001)	Application Layer Protocols (T1071)
Native API (T1106)	Registry Run Keys / Startup Folder (T1547.001)	Process Injection (T1055)	File Deletion (T1070.0040)	System Time Discovery (T1124)	Non-Application Layer Protocol (T1095)
	Create or Modify System Process (T1543)		Virtualization/Sandbox Evasion (T1497)	File and Directory Discovery (T1083)	
			Process Injection (T1055)	System Owner/User Discovery (T1033)	
				Modify Registry (T1112)	

Çözüm Önerileri

1. Güncel bir antivirüs yazılımı kullanarak sistem güvenliği artırılmalıdır.
2. Güvenlik yazılımınızı ve işletim sisteminizi düzenli olarak güncelleyerek, bilinen saldırılara karşı savunması güçlendirilmelidir.
3. Kötü niyetli web sitelerine ve indirmelere maruz kalmamak için güvenilir web sitelerini kullanılmalı ve indirmeler güvenilir kaynaklardan yapılmalıdır.
4. Önemli verilerinizi yedekleyerek, kötü amaçlı yazılımların neden olabileceği veri kaybı riski azaltılmalıdır.
5. Hesaplarınız için iki faktörlü kimlik doğrulama (2FA) veya çoklu aşamalı doğrulama (MFA) gibi ikinci katman güvenlik önlemleri etkinleştirilmelidir.

Hazırlayan

Tolga Yılmaz

<https://www.linkedin.com/in/tolga-ylmz/>

