

Mystic Stealer

TEKNİK ANALİZ RAPORU

ZAYOTEM

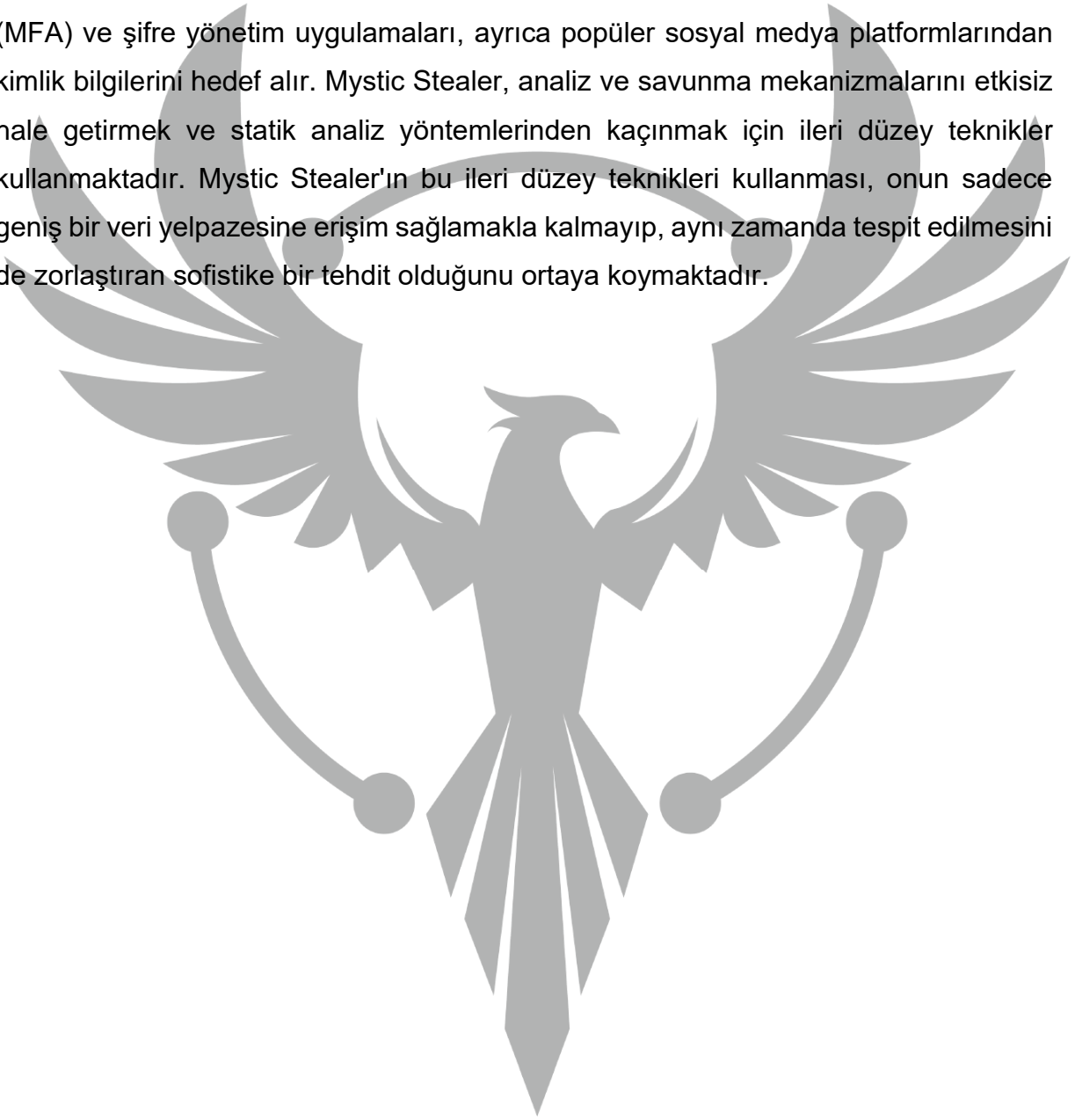
ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER.....	1
ÖN BAKIŞ	2
MYSTIC.EXE ANALİZİ	3
STATİK ANALİZ.....	4
DİNAMİK ANALİZ.....	5
DUMP.EXE ANALİZİ	12
NETWORK ANALİZİ	15
YARA KURALI	17
MITRE ATTACK TABLE	19
ÇÖZÜM ÖNERİLERİ.....	19
HAZIRLAYAN	20

Ön Bakış

Mystic Stealer, 2023 Nisan ayında ortaya çıkan ve kısa sürede siber suç dünyasında önemli bir yer edinen yeni bir bilgi çalma yazılımıdır. Bu zararlı yazılım, web tarayıcıları, tarayıcı uzantıları, kripto para uygulamaları, çok faktörlü kimlik doğrulama (MFA) ve şifre yönetim uygulamaları, ayrıca popüler sosyal medya platformlarından kimlik bilgilerini hedef alır. Mystic Stealer, analiz ve savunma mekanizmalarını etkisiz hale getirmek ve statik analiz yöntemlerinden kaçınmak için ileri düzey teknikler kullanmaktadır. Mystic Stealer'ın bu ileri düzey teknikleri kullanması, onun sadece geniş bir veri yelpazesine erişim sağlamakla kalmayıp, aynı zamanda tespit edilmesini de zorlaştıran sofistike bir tehdit olduğunu ortaya koymaktadır.

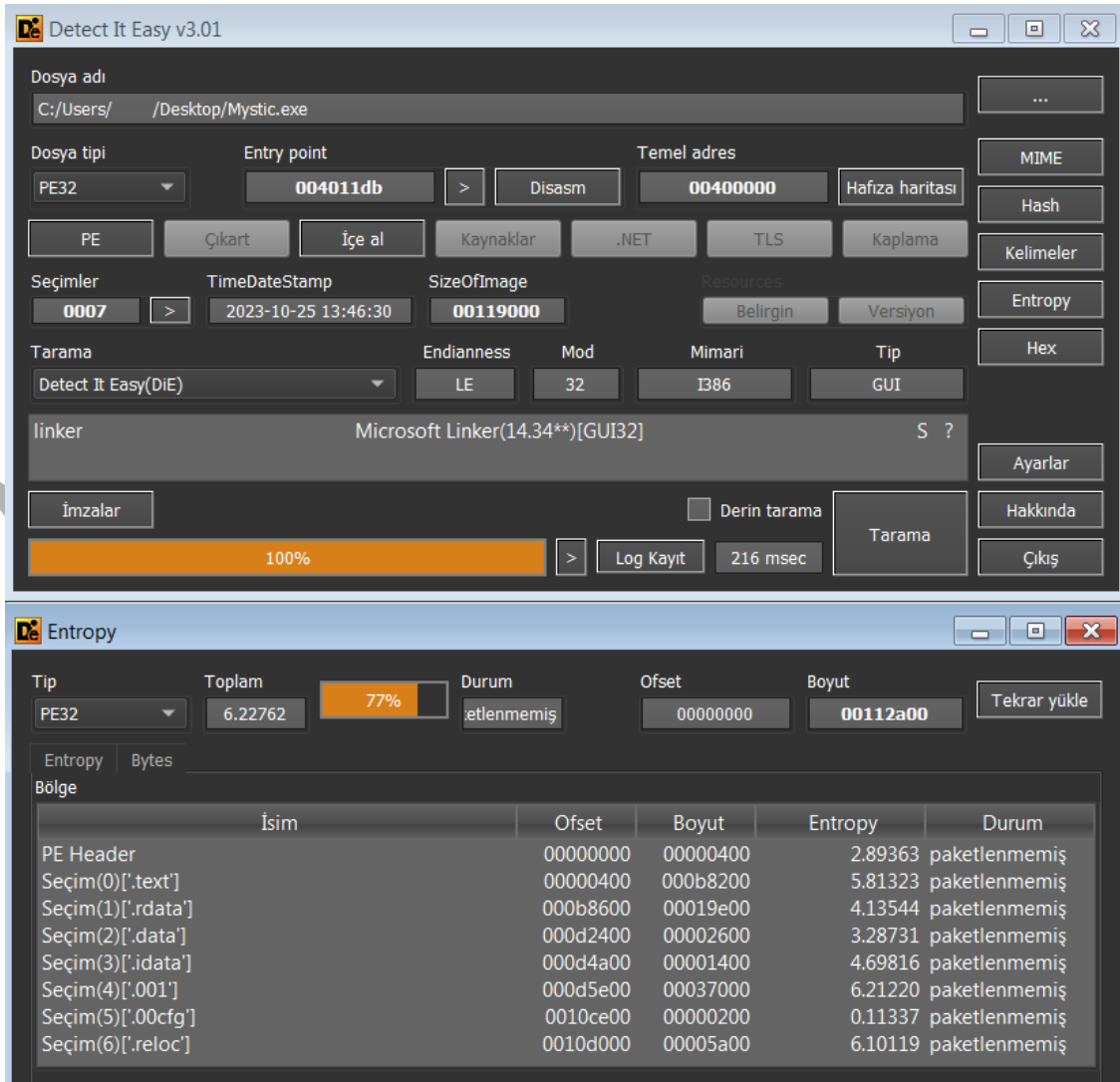


Mystic.exe Analizi

Adı	Mystic.exe
MD5	692a59e85b4c932049ab55cb372a9509
SHA256	dc094161dd0f8395e5363c61b3364191562edc470c785802d55d86f14bc40eaa
Dosya Türü	Portable Executable 32 (x86)

Zararlının MD5, SHA256 gibi bilgileri yukarıdaki tabloda verilmiştir. Orijinal ismi “dc094161dd0f8395e5363c61b3364191562edc470c785802d55d86f14bc40eaa.exe” olan zararlı, analiz sırasında kolaylık olması için “Mystic.exe” olarak adlandırılmıştır.

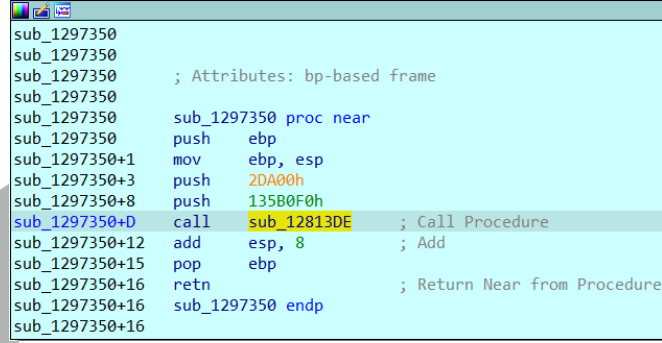
Statik Analiz



Görsel 1 – Zararlının statik olarak incelenmesi

Mystic.exe zararlısı incelendiğinde paketlenmemiş olduğu görülmektedir.

Dinamik Analiz



```
sub_1297350
sub_1297350
sub_1297350 ; Attributes: bp-based frame
sub_1297350
sub_1297350 sub_1297350 proc near
sub_1297350 push ebp
sub_1297350+1 mov ebp, esp
sub_1297350+3 push 2DA00h
sub_1297350+8 push 135B0F0h
sub_1297350+D call sub_12813DE ; Call Procedure
sub_1297350+12 add esp, 8 ; Add
sub_1297350+15 pop ebp
sub_1297350+16 retn ; Return Near from Procedure
sub_1297350+16 sub_1297350 endp
sub_1297350+16
```

Görsel 2 – Decryption Fonksiyonu

Dinamik analiz sırasında analiz edilen zararlı yazılımın bellek üzerinde şifreli şekilde saklanan baytlarını, çözümleme işlemine tabi tuttuğu görülmüştür. Bunu Görsel 2’ de de yer alan iki parametrelili fonksiyon aracılığıyla yapmaktadır. Birinci parametre, çözümlenecek bayt miktarını ve dolayısıyla döngünün kaç kez tekrarlanacağını belirleyen hexadecimal 2DA00h değeridir. İkinci parametre ise, çözümleme işleminin başlangıç noktası olan bellek adresini belirten hexadecimal 135B0F0h adresidir.

Belirtilen parametreler ile fonksiyon, 135B0F0 adresinden başlayarak 2DA00h uzunluğunda bir bellek bloğunu, yani 1388AF0h adresine kadar olan kısmı çözümlenmiştir. Sonuç olarak, şifrelenmiş verinin çözümlenmesi neticesinde, bu verinin aslında bir çalıştırılabilir dosya olduğu gözlemlenmiştir.

01297350	55	push ebp
01297351	8BEC	mov ebp,esp
01297353	68 00DA0200	push 2DA00
01297358	68 F0B03501	push mystic.135B0F0
0129735D	E8 7CA0FEFF	call mystic.12813DE
EIP → 01297362	83C4 08	add esp,8
01297365	5D	pop ebp
01297366	C3	ret
01297367	CC	int3
01297368	CC	int3
01297369	CC	int3

esp=002AFAFC

.text:01297362 mystic.exe:\$17362 #16762

Adres	Hex	ASCII
0135B0C0	25 64 20 31 20 4A 62 7A 61 55 68 73 38 71 31 00	%d 1 Jbzauhs8q1.
0135B0D0	25 64 20 31 20 4A 62 7A 61 55 68 73 38 71 31 00	%d 1 Jbzauhs8q1.
0135B0E0	25 64 20 31 20 4A 62 7A 61 55 68 73 38 71 31 00	%d 1 Jbzauhs8q1.
0135B0F0	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....yy.
0135B100	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00@.....
0135B110	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0135B120	00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00
0135B130	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..°..'.f!..L!Th
0135B140	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
0135B150	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
0135B160	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode...\$......

Görsel 4 – Çözümelen Çalıştırılabilir Dosya

Raporun bir önceki adımında bahsedilen ve byte byte çözümelen çalıştırılabilir dosya, Görsel 4'te görüldüğü gibidir.

.text:01293790	loc_1293790:	; CODE XREF: sub_1282FD6↑j
.text:01293790 55	push ebp	
.text:01293791 8B EC	mov ebp, esp	
.text:01293793 81 EC 9C 00 00 00	sub esp, 9Ch	; Integer Subtraction
.text:01293799 C7 45 F4 F0 B0 35 01	mov dword ptr [ebp-0Ch], offset unk_135B0F0	
.text:012937A0 F8	clc	; Clear Carry Flag
EIP → .text:012937A1 73 02	jnb short near ptr loc_12937A3+2	; Jump if Not Below (CF=0)
.text:012937A3	loc_12937A3:	; CODE XREF: .text:012937A1↑j
.text:012937A3 E8 8B 68 13 15	call near ptr 163CA033	; Call Procedure
.text:012937A8 C8 1D A1 00	enter 0FFFFA11Dh, 1	; "%d 1 Jbzauhs8q1"
.text:012937AC 8B 38 01	db 8Bh, 38h, 1	
.text:012937AC	db 8Bh ; <	
.text:012937AF	;	
.text:012937AF 50	push eax	
.text:012937B0 E8 20 30 FF FF	call sub_12867D5	; Call Procedure
.text:012937B5 83 C4 08	add esp, 8	; Add
.text:012937B8 89 45 E4	mov [ebp-1Ch], eax	
.text:012937BB 68 B6 73 94 E4	push 0E49473B6h	
.text:012937C0 8B 0D 00 8B 38 01	mov ecx, ds:dword_1388B00	
.text:012937C6 51	push ecx	
.text:012937C7 E8 09 30 FF FF	call sub_12867D5	; Call Procedure
.text:012937CC 83 C4 08	add esp, 8	; Add
.text:012937CF 89 45 C8	mov [ebp-38h], eax	
.text:012937D2 6A 44	push 44h ; 'D'	
.text:012937D4 6A 00	push 0	

Görsel 4 – Anti-disassembly Tekniği

Analiz sürecinde, zararlı yazılımın **Impossible Disassembly** adı verilen bir anti-disassembly tekniği kullandığı tespit edilmiştir. Bu teknik, koşullu atlama komutunun ardına veri baytları ekleyerek, ardından gelen gerçek komutun disassembler tarafından çözümlemesini engellemektedir. Disassembler'ın yanıltılmasıyla, gerçek komutların yanlış yorumlanmasına ve dolayısıyla hatalı çıktı üretilmesine neden olmaktadır.

.text:01293790		loc_1293790:		; CODE XREF: sub_1282FD61j
.text:01293790	55	push	ebp	
.text:01293791	8B EC	mov	ebp, esp	
.text:01293793	81 EC 9C 00 00 00	sub	esp, 9Ch	; Integer Subtraction
.text:01293799	C7 45 F4 F0 B0 35 01	mov	dword ptr [ebp-0Ch], offset unk_135B0F0	
.text:012937A0	F8	clic		; Clear Carry Flag
.text:012937A1	73 02	jnb	short loc_12937A5	; Jump if Not Below (CF=0)
.text:012937A1				
.text:012937A3	90	db	90h	
.text:012937A4	90	db	90h	
.text:012937A5				
.text:012937A5				
.text:012937A5		loc_12937A5:		; CODE XREF: .text:012937A11j
.text:012937A5	68 13 15 C8 1D	push	1DC81513h	
.text:012937AA	A1 00 8B 38 01	mov	eax, ds:dword_1388B00	
.text:012937AF	50	push	eax	
.text:012937B0	E8 20 30 FF FF	call	sub_12867D5	; Call Procedure
.text:012937B5	83 C4 08	add	esp, 8	; Add
.text:012937B8	89 45 E4	mov	[ebp-1Ch], eax	
.text:012937BB	68 B6 73 94 E4	push	0E49473B6h	
.text:012937C0	8B 0D 00 8B 38 01	mov	ecx, ds:dword_1388B00	
.text:012937C6	51	push	ecx	
.text:012937C7	E8 09 30 FF FF	call	sub_12867D5	; Call Procedure

Görsel 6 – Yamalanmış Kod

Zararlı yazılım tarafından kullanılan bu tekniği etkisiz hale getirmek amacıyla bir yamalama işlemi gerçekleştirilmiştir. İlgili yamalama işleminde, zararlı yazılımın kodundaki E8 ve 8B gibi spesifik opcode'lar, 90 (NOP) opcode'u ile değiştirilmiştir. NOP işlemi, işlemciye herhangi bir değişiklik yapmadan sonraki komuta geçmesini sağlar. Bu da disassembler programının kodun geri kalanını doğru bir şekilde okumasını sağlamıştır. Bu düzeltmeler sonucunda, zararlı yazılımın analizi doğru bir şekilde gerçekleştirilmiştir.

01293790	55	push	ebp	
01293791	8BEC	mov	ebp,esp	
01293793	81EC 9C000000	sub	esp,9C	
01293799	C745 F4 F0B03501	mov	dword ptr ss:[ebp-C],mystic.135B0F0	
012937A0	F8	clic		
012937A1	73 02	jae	mystic.12937A5	
012937A3	90	nop		
012937A4	90	nop		
012937A5	68 1315C81D	push	1DC81513	
012937AA	A1 008B3801	mov	eax,dword ptr ds:[1388B00]	
012937AF	50	push	eax	
012937B0	E8 2030FFFF	call	mystic.12867D5	
012937B5	83C4 08	add	esp,8	
012937B8	8945 E4	mov	dword ptr ss:[ebp-1C],eax	
012937BB	68 B67394E4	push	E49473B6	
012937C0	8B0D 008B3801	mov	ecx,dword ptr ds:[1388B00]	
012937C6	51	push	ecx	
012937C7	E8 0930FFFF	call	mystic.12867D5	
012937CC	83C4 08	add	esp,8	
012937CE	8945 C8	mov	dword ptr ss:[ebp-38],eax	

dword ptr [ebp-1C]=[002AFAF0 <&writeProcessMemory>]=<kernel32.writeProcessMemory>
eax=<kernel32.CreateProcessW> (7692103D)
.text:012937B8 mystic.exe:\$137B8 #12BB8

Görsel 7 – API Hashing

Analiz sürecü boyunca, “**mystic.12867D5**” isimli fonksiyonun API hashing tekniğini kullanarak kritik API'lerin adreslerini çözdüğü belirlenmiştir.


```

012938CB 90 nop
012938CC 68 32ABF0AE push AEF0AB32
012938D1 A1 008B3801 mov eax,dword ptr ds:[1388B00]
012938D6 50 push eax
012938D7 E8 F92EFFFF call mystic.12867D5
012938DC 83C4 08 add esp,8
012938DF 8945 C0 mov dword ptr ss:[ebp-40],eax
012938E2 6A 00 push 0
012938E4 6A 04 push 4
012938E6 8D4D A8 lea ecx,dword ptr ss:[ebp-58]
012938E9 51 push ecx
012938EA 8B55 F8 mov edx,dword ptr ss:[ebp-8]
012938ED 8B82 A4000000 mov eax,dword ptr ds:[edx+A4]
012938F3 83C0 08 add eax,8
012938F6 50 push eax
012938F7 8B4D CC mov ecx,dword ptr ss:[ebp-34]
012938FA 51 push ecx
012938FB FF55 C0 call dword ptr ss:[ebp-40]
012938FE 6A 40 push 40
01293900 68 00300000 push 3000
01293905 8B55 FC mov edx,dword ptr ss:[ebp-4]

```

ReadProcessMemory

[ebp-58]: "%d 1 jbzauh8q1"

[ebp-4]: "PE"

dword ptr [ebp-40]=[002AFAC <ReadProcessMemory>]=<kernel32.ReadProcessMemory>

.text:012938FB mystic.exe:\$138FB #12CFB

Görsel 10 - ReadProcessMemory Kullanımı

Ardından zararlı yazılım ReadProcessMemory API'sini çağırmıştır.

Process Hacker (WIN-...)

Processes

Name	PID	CF
winlogon.exe	484	
explorer.exe	1668	0
vmtoolsd.exe	844	0
x32dbg.exe	1600	0
Mystic.exe	2244	0
AppLaunch.exe	2672	0
ida.exe		

AppLaunch.exe (2672) Özellikleri

Base address	Type	Size	Protection
0x400000	Image	4 kB	WCX
0x500000	Mapped	16 kB	R
0x600000	Mapped	4 kB	R
0x700000	Private	4 kB	RW
0x800000	Private	4 kB	RW
0xA00000	Private	256 kB	RW
0x2A0000	Private	1,024 kB	RW
0x400000	Private	208 kB	RWX
0x930000	Image	112 kB	WCX
0x76E0000	Image	1,660 kB	WCX
0x76F0000	Image	1,536 kB	WCX
0x76F0000	Image	16,384 kB	R
0x76F0000	Private	64 kB	R

VirtualAllocEx

TerminateProcess

[ebp-4]: "PE"

[ebp-4]: "PE"

[ebp-4]: "PE"

[ebp-4]: "PE"

dword ptr [ebp-40]=[002AFAC <ReadProcessMemory>]=<kernel32.ReadProcessMemory>

.text:0129391A mystic.exe:\$1391A #12D1A

Görsel 11 - VirtualAllocEx ile Bellek Alanı Ayırma

Zararlının, daha önce askıya alma modunda başlatmış olduğu AppLaunch isimli uygulamanın bellek alanında VirtualAllocEx API'sini kullanarak yer tahsis etmektedir.

```

01293934 8D55 BC lea edx,dword ptr ss:[ebp-44]
01293937 52 push edx
01293938 8B45 FC mov eax,dword ptr ss:[ebp-4]
0129393B 8B48 54 mov ecx,dword ptr ds:[eax+54]
0129393E 51 push ecx
0129393F 8B55 F4 mov edx,dword ptr ss:[ebp-C]
01293942 8B45 EC mov eax,dword ptr ss:[ebp-14]
01293946 50 push eax
01293947 8B4D CC mov ecx,dword ptr ss:[ebp-34]
0129394A 51 push ecx
0129394B FF55 E4 call dword ptr ss:[ebp-1C]
0129394E 837D EC 00 cmp dword ptr ss:[ebp-14],0
01293952 75 0E jne mystic.1293962
01293954 6A 05 push 5
01293956 8B55 CC mov edx,dword ptr ss:[ebp-34]
01293959 52 push edx
0129395A FF55 B8 call dword ptr ss:[ebp-48]
0129395D E9 AFFEFFFF jmp mystic.1293811
01293962 74 55 jz mystic.1293962

```

[ebp-4]: "PE"

dword ptr [ebp-1C]=[002AFAC <WriteProcessMemory>]=<kernel32.WriteProcessMemory>

.text:0129394B mystic.exe:\$1394B #12D4B

Varsayılan (stdcall)

Index	Address	Value
1:	[esp]	0000005C
2:	[esp+4]	00400000
3:	[esp+8]	013580F0 mystic.013580F0
4:	[esp+C]	00000400
5:	[esp+10]	002AFAC8

Görsel 12 - WriteProcessMemory Kullanımı

Daha sonra **WriteProcessMemory** API'sinin çağırması üzerine yapılan incelemede, zararlı yazılımın suspend (askıya alma) modunda başlatılan "**AppLaunch**" isimli meşru yazılıma müdahale ettiğini ortaya koymuştur. Zararlı yazılımın, **VirtualAllocEx** API'sini kullanarak bu uygulamanın bellek alanında 0x0400000 adresinde özel olarak tahsis ettiği alana, daha önce çözümlenen ve başlangıç adresi 0x0135B0F0 olan çalıştırılabilir dosyayı yazmıştır.

012939F7	51	push ecx	
012939F8	8B55 D0	mov edx,dword ptr ss:[ebp-30]	
012939FB	52	push edx	
012939FC	FF55 B0	call dword ptr ss:[ebp-50]	SetThreadContext
012939FF	68 B42ED605	push 5D62EB4	
01293A04	A1 008B3801	mov eax,dword ptr ds:[1388800]	
01293A09	50	push eax	
01293A0A	E8 C62DFFFF	call mystic.12867D5	eax = ResumeThread
01293A0F	83C4 08	add esp,8	
01293A12	8945 AC	mov dword ptr ss:[ebp-54],eax	
01293A15	8B4D D0	mov ecx,dword ptr ss:[ebp-30]	
01293A18	51	push ecx	
01293A19	FF55 AC	call dword ptr ss:[ebp-54]	ResumeThread
01293A1C	8BE5	mov esp,ebp	
01293A1E	5D	pop ebp	
01293A1F	C3	ret	

dword ptr [ebp-54]=[002AFAB8 <&ResumeThread>]=<kernel32.ResumeThread>

.text:01293A19 mystic.exe:\$13A19 #12E19

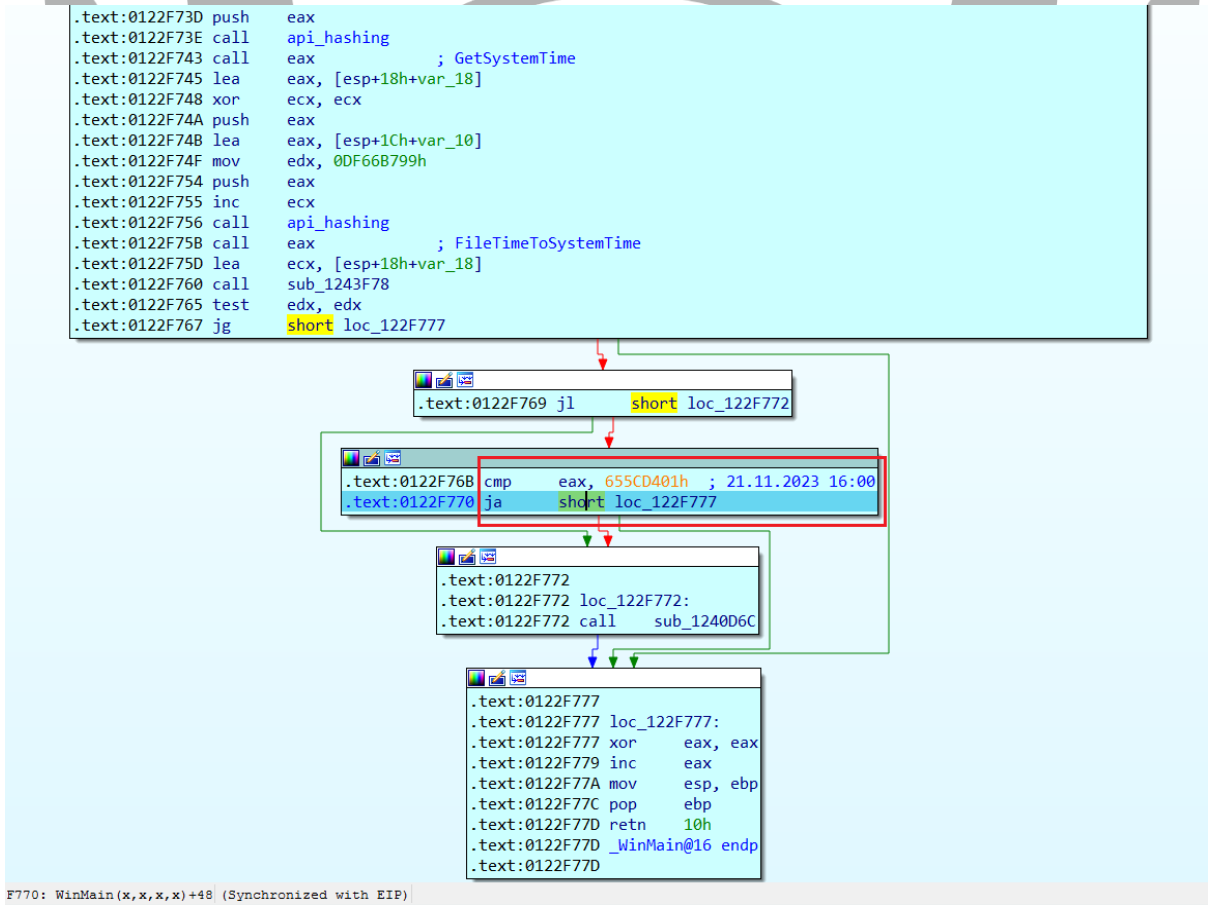
Görsel 13 – SetThreadContext Kullanım ve ResumeThread Kullanımı

Analizin devamında, zararlı yazılım **SetThreadContext** API'sini kullandığı ve ardından **ResumeThread** API'sini kullanarak askıya alınmış işlemi devam ettirme işlemini başarıyla gerçekleştirdiği belirlenmiştir. Bu durum, zararlı yazılımın **Process Hollowing** tekniğinin son aşamasını, yani meşru görünen ancak zararlı kod ile doldurulmuş bu sürecin devam ettirilmesi aşamasının tamamlandığı göstermektedir.

Bundan sonraki aşamada, enjekte edilen kodların detaylı bir analizi için **dump**'ı alınmış ve incelenmeye devam edilmiştir.

Dump.exe Analizi

Adı	Dump.exe
MD5	e561df80d8920ae9b152ddddefd13c7c
SHA256	5484ca53027230772ae149e3d7684b7e322432ceb013b6bc2440bd3c269192ea
Dosya Türü	Portable Executable 32 (x86)



Görsel 14 – Tarih Kontrolü

Zararlı yazılımın dump'ının detaylı incelenmesine başlandığında, ilk olarak dinamik API çözümlemesi yapıldığı ve **GetSystemTime** ile **FileTimeToSystemTime** API'lerinin sırasıyla kullanıldığı tespit edilmiştir. Bu API'ler ile zararlı yazılım, sistem üzerindeki mevcut zaman bilgisini almaktadır. Yapılan analize göre, zararlı yazılımın temel bir zaman kontrol mekanizmasına sahip olduğu ve sistem zamanının 21 Kasım 2023, saat 16:00'dan önce olup olmadığını kontrol ettiği belirlenmiştir. Eğer sistem zamanı bu tarihi geçmişse, zararlı yazılım kendini kapatmaktadır.

01242A9E	50	push eax
01242A9F	53	push ebx
01242AA0	53	push ebx
01242AA1	E8 8D28FFFF	call <dump.api_hashing>
EIP → 01242AA6	FFD0	call eax
01242AA8	0FB615 10CC2401	movzx edx,byte ptr ds:[124cc10]
01242AAF	8BF0	mov esi,eax
01242AB1	8A0D 94CC2401	mov cl,byte ptr ds:[124cc94]
01242AB7	B8 15DC0000	mov eax,BC15

eax=<kernel32.CreateMutexA> (76924B6B)

.text:01242AA6 dump.exe:\$22AA6 #21EA6

Görsel 15 – Mutex Oluşturma

Zararlı yazılım **CreateMutexA** API'sini kullanarak mutex oluşturmaya çalışmaktadır, eğer bu başarısız olur veya ilgili mutex zaten varsa kendini kapatmaktadır.

01240FD3	8B4424 3C	mov eax,dword ptr ss:[esp+3c]	
01240FD7	04 24	add al,24	
01240FD9	C1EA 18	shr edx,18	
01240FDC	0FB6C0	movzx eax,al	
01240FDF	8855 05	mov byte ptr ss:[ebp+5],dl	
01240FE2	83C5 08	add ebp,8	
01240FE5	69D8 6A0721FF	imul ebx,eax,FF21076A	
01240FEB	836C24 2C 01	sub dword ptr ss:[esp+2c],1	
01240FF0	8B4424 40	mov eax,dword ptr ss:[esp+40]	
01240FF4	893D 98CB2401	mov dword ptr ds:[124CB98],edi	
01240FFA	896C24 28	mov dword ptr ss:[esp+28],ebp	
01240FFE	0F85 84FEFFFF	jne dump.1240E88	
01241004	8B7424 44	mov esi,dword ptr ss:[esp+44]	[esp+44]: "http://193.233.255.73/"
01241008	81E7 560F9E6A	and edi,6A9E0F56	
0124100E	890D C4CB2401	mov dword ptr ds:[124CBC4],ecx	
01241014	80C9 C0	or cl,C0	
01241017	0FB6C1	movzx eax,cl	

Görsel 16 – IP Adresi Çözümleme

mov byte ptr ss:[esp+89],b1		
mov dword ptr ds:[124CB00],eax		
lea eax,dword ptr ss:[esp+7c]		
push eax		
lea eax,dword ptr ss:[esp+24]		
push eax		
push esi		
push 104		
push dump.124DFF8		
mov edx,534FBFB6		
xor ecx,ecx		
call <dump.api_hashing>		
call eax		
mov eax,dword ptr ds:[124CB10]		
lea edi,dword ptr ss:[esp+34]		
mov edx,dword ptr ds:[124CADc]		
add eax,16748B3F		

esi: "http://193.233.255.73/"

124DFF8: "http://193.233.255.73/loghub/master"

_snprintf

Varsayılan (stdcall)			
1:	[esp+4]	00000104	"%s%s"
2:	[esp+8]	0022F7D4	"%s%s"
3:	[esp+c]	0060BFE8	"http://193.233.255.73/"
4:	[esp+10]	0022F814	"loghub/master"
5:	[esp+14]	0060BFE8	"http://193.233.255.73/"

Görsel 17 – Adres Bilgisi

Zararlı yazılım, şifrelenmiş IP adresini ve yol bilgisini çözerek, **_snprintf** fonksiyonu ile "193[.]233[.]255[.]73/master/login" adresini oluşturmaktadır.

The screenshot shows a debugger window with the following components:

- Assembly Window:** Displays assembly instructions. The instruction at address 0123AF37 is highlighted. The EIP register points to this address. The instruction is `call <dump.api_hashing>`.
- Register Window:** Shows the value of the `eax` register as `<wininet.InternetReadFile> (75511C80)`.
- Hex Dump Window:** Shows the data being read. The data is a multipart/form-data boundary string: `Content-Type: multipart/form-data; boundary=Zu2Cpvtim7RzwjX2CXFM..Content-Length: 213.üvd(..%?..P#...üvd(..!ç05`.

Görsel 18 – InternetReadFile API

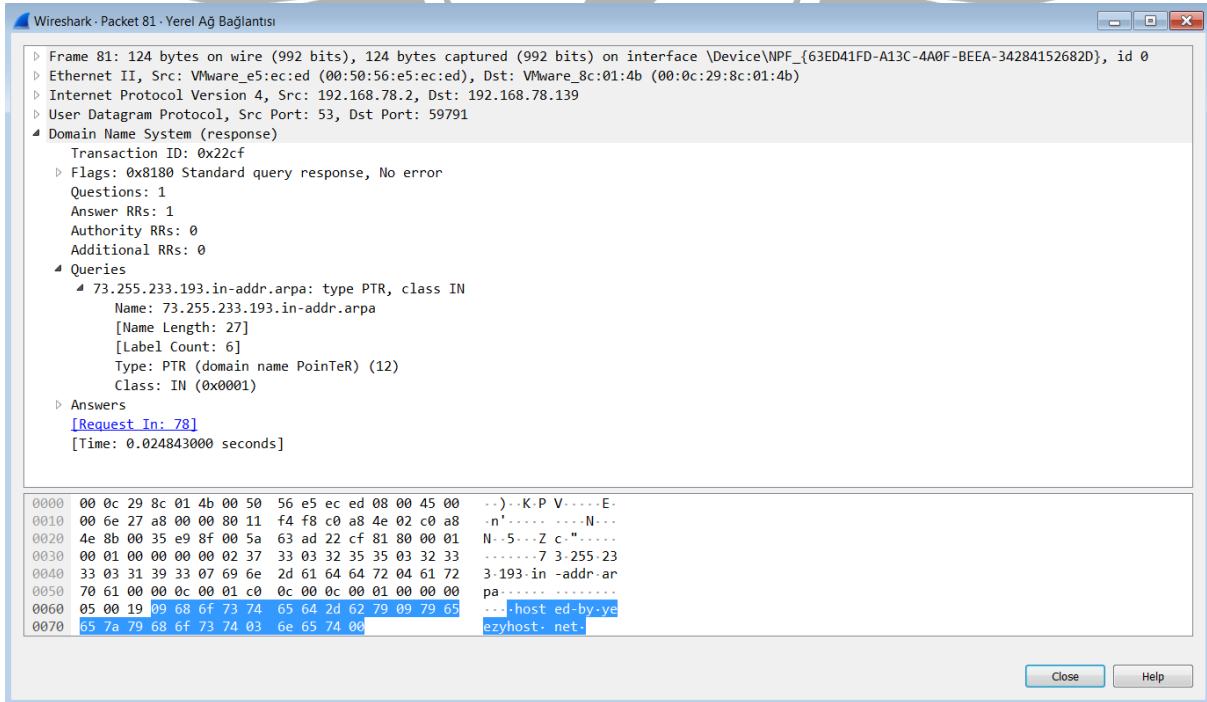
Zararlı yazılım, internet üzerinden iletişim kurma sürecinde belirli bir API zinciri kullanmaktadır. İlk adım olarak, **InternetOpenA** ile genel bir internet bağlantısı başlatmaktadır. Daha sonra, URL ayrıştırma için **InternetCrackUrlA** kullanılmakta ve **InternetConnectA** ile belirli bir sunucuya bağlantı kurulmaktadır. Bağlantı kurulduktan sonra, **HttpOpenRequestA** ile bir HTTP isteği oluşturulmaktadır. İsteğin özelliklerini ayarlamak için ardışık olarak üç kez **InternetSetOptionA** çağrısı yapılmaktadır. Bu ayarlamaların ardından, hazırlanan HTTP isteği **HttpSendRequestA** ile gönderilmektedir. İstek gönderildikten sonra, **HttpQueryInfoA** kullanılarak sunucudan gelen yanıt bilgileri sorgulanmakta ve **InternetReadFile** ile yanıt içeriği okunmaktadır. Ancak, sunucu kapalı olduğundan, **HttpSendRequestA** çağrısı başarısız olmakta ve bu durum, zararlı yazılımın etkinleşememesine ve operasyonlarını sürdürememesine dolayısıyla kendini kapatmasına neden olmaktadır. Bu davranış, zararlı yazılımın etkinleşmesi ve operasyonlarını sürdürmesi için dış sunucularla başarılı bir iletişim kurmasının gerekliliğini göstermektedir.

Network Analizi

98	60.104444	192.168.78.139	192.168.78.2	NBNS	92 Name query NB WPAD<00>
99	60.416766	192.168.78.139	193.233.255.73	TCP	62 [TCP Retransmission] 49440 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
100	61.401787	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0xfac1b79
101	61.401787	192.168.78.254	192.168.78.136	DHCP	342 DHCP Offer - Transaction ID 0xfac1b79
102	61.617796	192.168.78.139	192.168.78.2	NBNS	92 Name query NB WPAD<00>
103	63.162266	192.168.78.139	192.168.78.255	NBNS	92 Name query NB WPAD<00>
104	63.926766	192.168.78.139	192.168.78.255	NBNS	92 Name query NB WPAD<00>
105	64.691014	192.168.78.139	192.168.78.255	NBNS	92 Name query NB WPAD<00>
106	71.259672	192.168.78.139	192.168.78.2	DNS	76 Standard query 0x7781 A dns.msftncsi.com
107	71.291880	192.168.78.2	192.168.78.139	DNS	92 Standard query response 0x7781 A dns.msftncsi.com A 131.107.255.255
108	72.430326	192.168.78.139	193.233.255.73	TCP	66 49441 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	72.433537	193.233.255.73	192.168.78.139	TCP	60 80 → 49440 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
110	75.439422	192.168.78.139	193.233.255.73	TCP	66 [TCP Retransmission] 49441 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
111	75.953939	VMware_8c:01:4b	VMware_e5:ec:ed	ARP	42 Who has 192.168.78.2? Tell 192.168.78.139
112	75.954046	VMware_e5:ec:ed	VMware_8c:01:4b	ARP	60 192.168.78.2 is at 00:50:56:e5:ec:ed
113	77.407633	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0xfac1b79
114	77.407633	192.168.78.254	192.168.78.136	DHCP	342 DHCP Offer - Transaction ID 0xfac1b79
115	81.445213	192.168.78.139	193.233.255.73	TCP	62 [TCP Retransmission] 49441 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
116	93.473876	193.233.255.73	192.168.78.139	TCP	60 80 → 49441 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
117	105.748245	192.168.78.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
118	105.779509	192.168.78.1	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1

Görsel 19 – Wireshark Görüntüsü

Zararlıının internet ile etkileşimi Görsel 19'da Wireshark aracından alınan ekran görüntüsündeki gibidir.



Görsel 20 – DNS İsteği

Time	Process Name	PID	Operation	Path	Result
00:04:43	Dump.exe	2680	TCP Reconnect	49418 -> hosted-by.yeezyhost.nethttp	SUCCESS
00:04:49	Dump.exe	2680	TCP Reconnect	49418 -> hosted-by.yeezyhost.nethttp	SUCCESS
00:05:04	Dump.exe	2680	TCP Reconnect	49419 -> hosted-by.yeezyhost.nethttp	SUCCESS
00:05:10	Dump.exe	2680	TCP Reconnect	49419 -> hosted-by.yeezyhost.nethttp	SUCCESS

Görsel 21 – Process Monitor Görüntüsü

TCPView - Sysinternals: www.sysinternals.com											
File Options Process View Help											
A →											
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Recv	
Dump.exe	2312	TCP	localhost	43378	hosted-by.yeszyhost.net	http	SYN_SENT				
lsass.exe	496	TCP		49156		0	LISTENING				
lsass.exe	496	TCPv6		49156		0	LISTENING				
services.e...	460	TCP		49155		0	LISTENING				
services.e...	460	TCPv6		49155		0	LISTENING				
svchost.exe	700	TCP		epmap		0	LISTENING				
svchost.exe	784	TCP		49153		0	LISTENING				
svchost.exe	900	TCP		49154		0	LISTENING				
svchost.exe	784	UDP		bootpc		*		6	1.800		
svchost.exe	872	UDP		nlp		*					
svchost.exe	324	UDP		ssdp		*					
svchost.exe	324	UDP		ssdp		*					
svchost.exe	324	UDP		64349		*		12	1.596		
svchost.exe	700	TCPv6		epmap		0	LISTENING				
svchost.exe	784	TCPv6		49153		0	LISTENING				
svchost.exe	900	TCPv6		49154		0	LISTENING				
svchost.exe	872	UDPv6		123		*					
svchost.exe	784	UDPv6		546		*					
svchost.exe	324	UDPv6		1900		*					
svchost.exe	324	UDPv6		1900		*					
svchost.exe	324	UDPv6		64348		*					
svchost.exe	592	UDP		llmnr		*					
svchost.exe	592	UDPv6		5355		*					
System	4	TCP		netbios-ssn		0	LISTENING				
System	4	TCP		microsoft-...		0	LISTENING				
System	4	UDP		netbios-ns		*		43	2.474		
System	4	UDP		netbios-dgm		*					
System	4	TCPv6		microsoft-...		0	LISTENING				
wininit.exe	400	TCP		49152		0	LISTENING				
wininit.exe	400	TCPv6		49152		0	LISTENING				

Görsel 22 – TCPView Görüntüsü



YARA Kuralı

```
import "hash"

rule MysticStealer_s
{
    meta:
        author = " Barış Tural"
        description = "MysticStealer"

    strings:
        $str1 = "%d 1 JbzaUhs8q1"

        $str2 =
"C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\AppLaunch.exe"
wide

        $str3 = "GYAUs87atedyuw3"

        $str4 = "A8791hbx78iUA"

        $hashing_alg = {D1 E2 8B 45 E8 0F BE 0C 10 C1 E1 10 33 4D F8
89 4D F8}

        $anti_disass1 = {F8 73 02 E8 8B 68 13 15 C8 1D A1 ?? ?? ?? ?? 50
E8 20 30 FF FF}

        $anti_disass2 = {73 04 72 02 E8 A0 68 27 26 65 7B A1}

        $anti_disass3 = {E0 72 04 73 02 E9 9F 6A 04}

    condition:
        all of them or hash.md5(0,filesize) ==
"692a59e85b4c932049ab55cb372a9509" or 3 of ($str*) and 2 of
($anti_disass*) or $hashing_alg
```

```

import "hash"

rule MysticStealer_d

{
    meta:

        author = " Barış Tural"

        description = "MysticStealer"

    strings:

        $str1 = "HH:mm:ss" wide

        $str2 = "morda"

        $str3 =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz012
3456789+/"

        $alg = {33 C8 2B D9 8B CB 8B C3 C1 E1 04 C1 E8 05}

        $ip_resolv = {80 C9 18 89 74 24 44 88 0D ?? ?? ?? ?? B8 F5 2A 00
00 0F B6 C9 66 33 C8 B8 D1 52 00 00 66 2B C8}

    condition:

        hash.md5(0,filesize) == "e561df80d8920ae9b152ddddefd13c7c" or
(2 of ($str*) and ($alg or $ip_resolv))

}

```

MITRE ATTACK TABLE

Reconnaissance	Execution	Discovery	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
		System Information Discovery (T1082)	Process Injection (T1055)	Obfuscated Files or Information (T1027)		Application Layer Protocol (T1071)	
				Process Injection (T1055)			
				Deobfuscate /Decode Files or Information			

Çözüm Önerileri

1. Mystic Stealer'ın iletişim kurduğu bilinen IP adresleri ve etki alanlarını sürekli olarak izleyin ve bu adreslere erişimi engelleyin.
2. Kullanıcıları Mystic Stealer gibi zararlı yazılımların yayılma yöntemleri hakkında bilgilendirin. Kimlik avı saldırılarına ve zararlı e-posta eklerine karşı dikkatli olmaları konusunda uyarın.
3. Mümkün olduğunca iki faktörlü kimlik doğrulama (2FA) özelliğini etkinleştirin.
4. Kullanılan antivirüs ve zararlı yazılım tespit araçlarını sürekli güncel tutun.
5. Sistemlere erişimi kısıtlayın ve kullanıcı hesapları için gereksiz yüksek izinleri kaldırın. Kripto para cüzdanları gibi hassas uygulamalara erişim için ek güvenlik katmanları ekleyin.

HAZIRLAYAN

Bariş TURAL

<https://www.linkedin.com/in/baristural/>

