

AveMariaRAT

TEKNİK ANALİZ RAPORU

ZAYOTEM

ZARARLI YAZILIM ÖNLEME VE TERSİNE MÜHENDİSLİK

İçindekiler

İÇİNDEKİLER	i
ÖN BAKIŞ.....	1
AVEMARİARAT.EXE ANALİZİ.....	2
STATİK ANALİZ	2
DİNAMİK ANALİZ	3
ALAIW.EXE ANALİZİ.....	5
STATİK ANALİZ	5
DİNAMİK ANALİZ	6
WARZONE160.EXE ANALİZİ	14
STATİK ANALİZ	14
DİNAMİK ANALİZ	15
YARA KURALI.....	20
MITRE ATTACK TABLE.....	25
ÇÖZÜM ÖNERİLERİ	25
HAZIRLAYANLAR	26

Ön Bakış

AveMariaRAT, kötü niyetli bir yazılım türüdür ve Warzone RAT olarak da bilinir. Sistemlere bulaşarak genellikle uzaktan erişim yetenekleri kazanmak için kullanılır. Bu Truva atı ilk olarak 2018 yılında kötü amaçlı kimlik avı kampanyaları aracılığıyla yayılmıştır ve o zamandan bu yana daha fazla görünür hale gelmiştir. Kullanıcıları enfekte etmek için sosyal mühendislik, e-posta ekleri, kötü amaçlı web siteleri gibi yöntemler kullanılır. AveMariaRAT gibi Uzaktan Erişim Araçları (RAT), siber suçlular tarafından casusluk, veri hırsızlığı ve diğer zararlı faaliyetlerde kullanılarak kullanıcıların bilgisayar sistemlerine ciddi riskler oluşturabilir.

Bu kötü amaçlı yazılım virüs bulaşmış bilgisayarlarda;

- Uzaktan kontrol sağlama,
- Dosya indirme ve silme,
- Klavye tuş vuruşlarını kaydetme,
- Sistem bilgilerini kontrol etme,
- Tarayıcılar üzerindeki verilere erişim sağlama gibi davranışlar göstermektedir.

AveMariaRAT.exe Analizi

Adı	AveMariaRAT.exe
MD5	d802bc50f7321efb13358d27280910ca
SHA256	45c59e6d1a36e978effba98230fe70262b68748ff190562d2f2b8cca d7c43c7
Dosya Türü	Portable Executable 32 (x86)

Zararlının MD5, SHA256 gibi bilgileri yukarıdaki tabloda yer almaktadır. Orijinal ismi “45c59e6d1a36e978effba98230fe70262b68748ff190562d2f2b8ccad7c43c7.exe” olan zararlı analiz sırasında kolaylık olması açısından “**AveMariaRAT.exe**” olarak adlandırılmıştır.

Statik Analiz

Tip	Toplam	Durum	Ofset	Boyut	
PE32	7.81694	97% paketlenmiş	00000000	0004fbf8	Tekrar yükle
Entropy	Bytes				
Bölge	İsim	Ofset	Boyut	Entropy	Durum
	PE Header	00000000	00000400	2.18835	paketlenmemiş
	Seçim(0)['.text']	00000400	00006800	6.41751	paketlenmemiş
	Seçim(1)['.rdata']	00006c00	00001400	5.14135	paketlenmemiş
	Seçim(2)['.data']	00008000	00000600	4.11152	paketlenmemiş
	Seçim(4)['.rsrc']	00008600	0000d200	6.89180	paketlenmiş
	Kaplama	00015800	0003a3f8	7.99919	paketlenmiş

Görsel 1 Zararlının DIE Aracında İncelenmesi

AveMariaRAT.exe zararlısı DIE aracına atıldığında **paketlenmiş** olduğu görülmektedir.

Advapi32.dll	Shell32.dll	Ole32.dll
Comctl32.dll	User32.dll	Gdi32.dll
Kernel32.dll		

Tablo 1 Zararlının Kullandığı Bazı DLL'ler

Zararlının kullandığı bazı DLL'ler tablo 1'de gösterilmektedir.

Dinamik Analiz

Uxtheme.dll	Userenv.dll	Setupapi.dll
Apphelp.dll	PropSys.dll	Dwmapi.dll
Cryptbase.dll	Oleacc.dll	Clbcatq.dll
Ntmarta.dll		

Tablo 2 Dinamik Olarak Çıkarılan DLL'ler

Dinamik olarak yüklenen dll'lerin bazıları tablo 2'deki gibidir.

<pre> mov ecx, eax push 0 inc ecx neg ecx sbb ecx, ecx and ecx, eax push ecx push dword ptr ss:[esp+14] push 0 push 1 push dword ptr ss:[esp+1C] push dword ptr ss:[esp+1C] call dword ptr ds:[&CreateFileW] ret C push ebp mov ebp, esp push ecx </pre>	<pre> [esp+1C]:L"C:\\Users\\ [esp+1C]:L"C:\\Users\\ \\AppData\\Local\\Temp\\qqscag.po" \\AppData\\Local\\Temp\\qqscag.po" </pre>
--	--

Görsel 2 CreateFileW API'si Kullanılarak "qqscag.po" Dosyasının Oluşturulması

Zararlı, "C:\\Users\\%username%\\AppData\\Local\\Temp" konumuna **CreateFileW** API'sini kullanarak "qqscag.po" isimli bir dosya oluşturmaktadır.

<pre> mov ecx,eax push 0 inc ecx neg ecx sbb ecx,ecx and ecx,eax push ecx push dword ptr ss:[esp+14] push 0 push 1 push dword ptr ss:[esp+1C] push dword ptr ss:[esp+1C] call dword ptr ds:[<&CreateFileW>] ret C push ebp mov ebp,esp push ecx </pre>	<pre> [esp+1C]:L"C:\\Users\\ [esp+1C]:L"C:\\Users\\ \\AppData\\Local\\Temp\\alaiw.exe" \\AppData\\Local\\Temp\\alaiw.exe" </pre>
--	--

Görsel 3 CreateFileW API'si Kullanılarak "alaiw.exe" Dosyasının Oluşturulması

Daha sonra zararlı CreateFileW API'sini tekrar kullanarak “C:\Users\%username%\AppData\Local\Temp” konumuna “alaiw.exe” isimli bir çalıştırılabilir dosya (PE) oluşturmaktadır.

<pre> 00403F8C 57 00403F8D 83C0 69 00403F90 68 C5404000 00403F95 0FB7C0 00403F98 57 00403F99 50 00403F9A FF35 60A24200 00403FA0 FF15 2C824000 00403FA6 6A 05 00403FA8 88F0 00403FAA E8 5CD4FFFF 00403FAF 6A 01 00403FB1 E8 B1FCFFFF 00403FB6 8BC6 </pre>	<pre> push edi add eax,69 push avemariarat.4040C5 movzx eax,ax push edi push eax push dword ptr ds:[42A260] call dword ptr ds:[<&DialogBoxParamW>] push 5 mov esi,eax call avemariarat.401408 push 1 call avemariarat.403C67 mov eax,esi </pre>
--	---

Görsel 4 DialogBoxParamW API'si ile Shellcode'un Çalıştırılması

Zararlı, görsel 4'teki **DialogBoxParamW** WinAPI çağrısını kullanarak bellekte saklanan **shellcode**'u çalıştırmaktadır.

<pre> push eax xor eax,eax push avemariarat.426750 push eax push eax push 4000000 push eax push eax push eax push dword ptr ss:[ebp+8] push eax call dword ptr ds:[<&CreateProcessW>] test eax,eax je avemariarat.405C8A push dword ptr ss:[ebp-C] call dword ptr ds:[<&CloseHandle>] mov eax,dword ptr ss:[ebp-10] </pre>	<pre> [ebp+8]:L"C:\\Users\\ [ebp-C]:L"C:\\Users\\ \\AppData\\Local\\Temp\\alaiw.exe\" " \\AppData\\Local\\Temp\\alaiw.exe\" " </pre>
--	--

Görsel 5 CreateProcessW API'si ile "alaiw.exe"nin Çalıştırılması

Ardından **CreateProcessW** API'si ile daha önce oluşturmuş olduğu “alaiw.exe”yi çalıştırmaktadır.

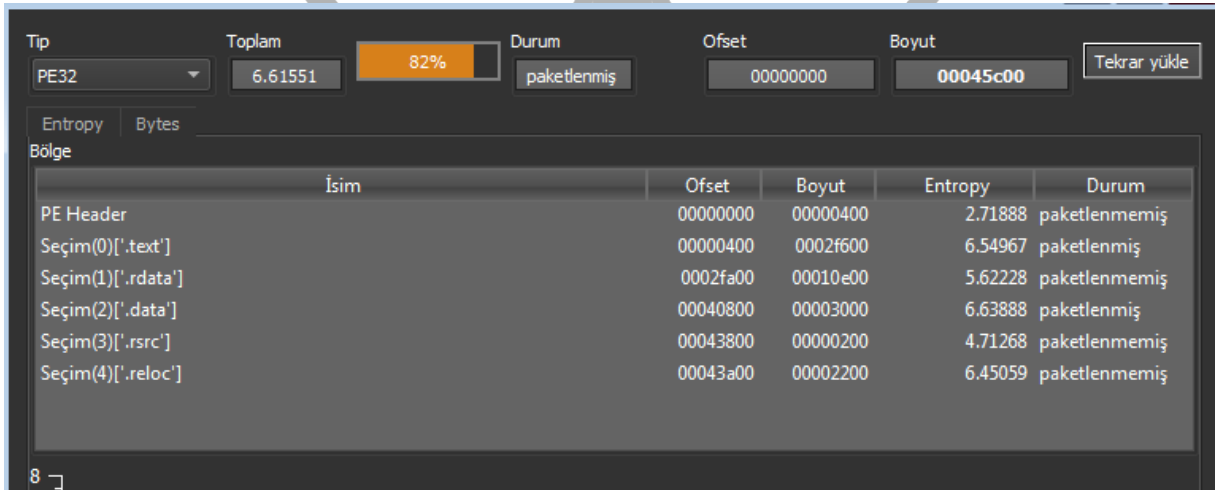
alaiw.exe Analizi

Adı	alaiw.exe
MD5	fa0be3eb24b13d060a0ae4e25c22ef1c
SHA256	54152ed7b7386c7a7bef26fafcc72fe3d51ddfbb677292bd9d1261b2c6199ebd
Dosya Türü	Portable Executable 32 (x86)

AveMariaRAT.exe içerisinde “C:\Users\%username%\AppData\Local\Temp” dosya yolunda oluşturulan alaiw.exe dosyasının MD5, SHA256 gibi bilgileri yukarıdaki tabloda yer almaktadır.

Statik Analiz

DIE aracı ile alaiw.exe incelendiğinde **paketlenmiş** olduğu görülmektedir.



Tip	Toplam	Durum	Ofset	Boyut	
PE32	6.61551	82%	00000000	00045c00	Tekrar yükle
Entropy Bytes					
Bölge	İsim	Ofset	Boyut	Entropy	Durum
	PE Header	00000000	00000400	2.71888	paketlenmemiş
	Seçim(0)['.text']	00000400	0002f600	6.54967	paketlenmiş
	Seçim(1)['.rdata']	0002fa00	00010e00	5.62228	paketlenmemiş
	Seçim(2)['.data']	00040800	00003000	6.63888	paketlenmiş
	Seçim(3)['.rsrc']	00043800	00000200	4.71268	paketlenmemiş
	Seçim(4)['.reloc']	00043a00	00002200	6.45059	paketlenmemiş

Görsel 6 alaiw.exe'nin DIE Aracında İncelenmesi

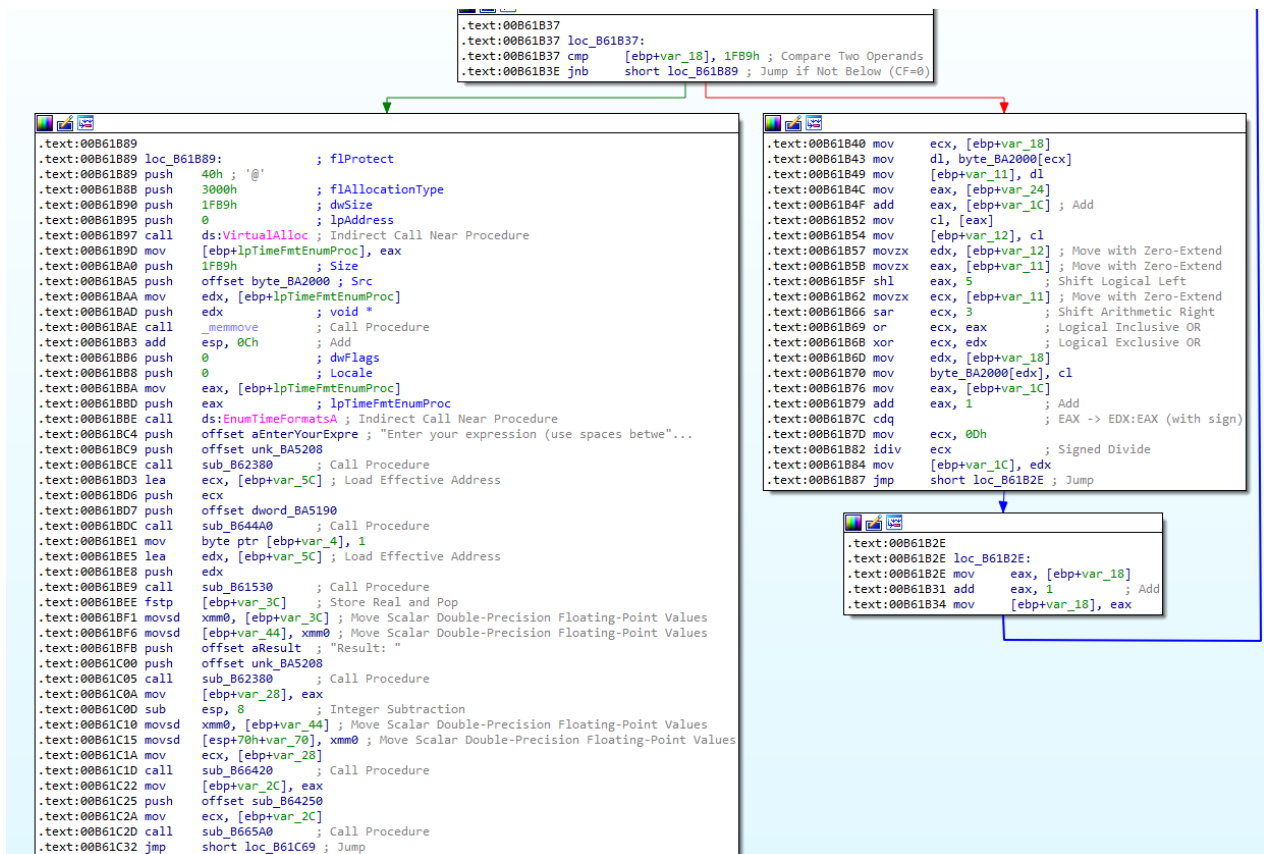
Kernel32.dll	Winpool.drv	Crypt32.dll
Loadperf.dll	Wininet.dll	Rtutils.dll
User32.dll		

Tablo 3 Kullanılan Bazı DLL'ler

Zararlı'nın kullandığı bazı DLL'ler tablo 3'te gösterilmektedir.

Dinamik Analiz

Zararlı daha önce oluşturmuş olduğu şifrelenmiş “**qqscag.po**” dosyasını “**vtwkwntewuzvb**” anahtar ifadesini kullanarak çözmektedir. Bu şekilde shellcode'u oluşturmaktadır. Bu kodu, **VirtualAlloc** API'si ile ayrılan belleğe memmove fonksiyonu ile kopyalamaktadır. Daha sonrasında **EnumTimeFormatsA** API'sini kullanarak shellcode'u çalıştırmaktadır.



Adres	Hex		UNICODE	
0053F434	0D 30 4D 77	48 7A 2E 00	00 00 00 00 2A 00 00 2A*
0053F444	C4 00 2E 00	30 00 00 30	00 00 00 64 F4 53 00	A.=. . . .S
0053F454	00 00 00 00	80 00 00 00	58 00 00 10 02 00 12	. . .X. . .
0053F464	10 9A 30 00	01 00 00 00	00 00 00 0A 00 00 00	.0. . . .
0053F474	0E 00 00 00	F8 95 30 00	F8 95 30 00 F3 95 30 00	. . .0.0.0
0053F484	00 00 00 00	2C 00 00 00	00 00 2E 00 34 F5 53 01
0053F494	DC E3 53 00	10 9A 30 00	3C F7 53 00 CD 4D 51 77	.S.O.S..
0053F4A4	F1 20 78 04	FE FF FF FF	36 34 4D 77 61 34 4D 77	
0053F4B4	12 00 00 00	20 00 00 00	F2 95 30 00 F0 95 30 00	. . .0.0
0053F4C4	12 00 00 00	09 00 00 00	00 00 00 79 00 75 00yu
0053F4D4	65 00 61 00	61 00 6A 00	73 00 73 00 6F 00 78 00	eaajssox
0053F4E4	78 00 68 00	64 00 64 00	00 00 8D 76 60 00 69 00	xhdd..mi
0053F4F4	72 00 72 00	62 00 77 00	77 00 67 00 70 00 2E 00	rbbwgp.
0053F504	65 00 78 00	65 00 00 00	70 00 6C 00 75 00 70 00	exe.plup
0053F514	70 00 79 00	69 00 69 00	65 00 6E 00 00 00 8C 76	pytien..
0053F524	71 00 71 00	73 00 63 00	61 00 71 00 2E 00 70 00	qqscaq.p
0053F534	6F 00 00 00	00 00 00 00	00 00 00 00 00 88 01 00	O.
0053F544	58 00 00 00	50 34 2E 00	00 00 00 78 F5 53 00	X.S
0053F554	78 F5 53 00	27 91 8C 76	F8 95 30 00 58 00 00 00	.S...OX.
0053F564	50 4E 30 00	00 00 14 00	00 00 00 F8 95 30 00	.0.0
0053F574	00 00 00 00	78 F6 53 00	1F 82 8C 76 1F 04 00 00	. . .S. . .
0053F584	00 00 14 00	00 00 00 00	06 F5 53 00 00 00 00 00S. .
0053F594	01 00 00 00	00 00 00 00	00 00 00 00 00 00 00 00

Daha sonra zararlı **yueaajssoxxhdd**, **mirrbwwgp.exe**, **pluppyien** ve **qqscag.po** string'lerini **deobfuscation** ile belleğe yerleştirmektedir.

50	FF95 4CFFFFFF	push eax
85C0	0F85 42010000	call dword ptr ss:[ebp-B4]
FF75 08	0F85 42010000	test eax, eax
0F85 42010000	FF75 08	jne 1408E4
0F85 42010000	0F85 42010000	push dword ptr ss:[ebp+8]
0F85 42010000	0F85 42010000	lea eax, dword ptr ss:[ebp+8]

<SHGetFolderPathW>]=<shell32.SHGetFolderPathW>		
Döküm3 Döküm4 Döküm5 İzle 1 [x=] Yerel Değişkenler Yapı		
00 4C E0 53 00	00 00 00 00	UNICODE
00 3C 00 00 00	08 00 0A 00S..
00 6F 00 72 00	43 00 3A 00	...SorC:
00 72 00 73 00	5C 00 7A 00	\Users\
00 5C 00 41 00	70 00 70 00	\App
00 5C 00 52 00	6F 00 61 00	Data\Roaming...
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	00 00 00 00 00
00 00 00 00 00	00 00 00 00 00

Görsel 9 SHGetFolderPathW API'si ile Dosya Yoluna Ulaşılmış

SHGetFolderPathW API'si ile “C:\Users\%username%\AppData\Roaming” dosya yoluna ulaşmaktadır.

push edi	call 140073	ECX 8FF3CC1F
push 7F8C1007	lea ecx, dword ptr ss:[ebp-18]	EDX FF5953AF
push ecx	call eax	EBP 0053E56C
push eax	call 140073	ESP 0053E548
push FF5953AF	push edi	ESI 75A345BF
mov esi, eax	call 140073	EDI 750742C8
push dword ptr ss:[ebp+8]	mov edi, eax	EIP 00140406
call esi	call 140073	EFLAGS 00000202
cmp eax, 1	je 14041A	ZF 0 PF 0 AF 0
push 0		OF 0 SF 0 DF 0
		CF 0 TF 0 IF 1

[ebp+8]:L"C:\\Users\\	\\AppData\\Roaming\\yueajsssoxxhdd"
-----------------------	-------------------------------------

LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

Görsel 10 "PathFileExistW" ve "CreateDirectoryW" API'si

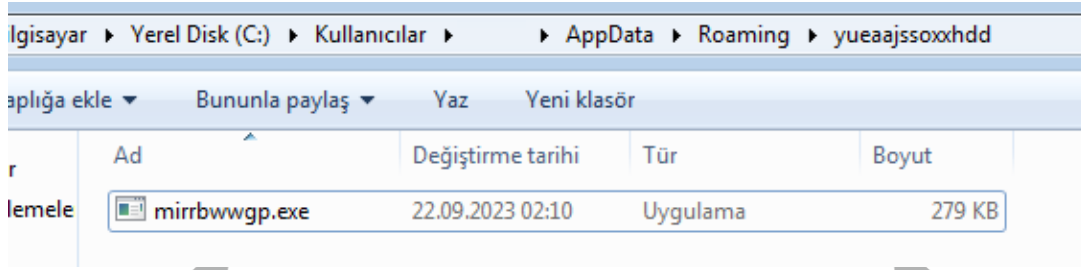
PathFileExistW API'si ile “C:\Users\%username%\AppData\Roaming\yueajsssoxxhdd” dosya dizininin varlığını kontrol etmekte ve yoksa **CreateDirectoryW** API'si ile bu dosya dizinini oluşturmaktadır.

The screenshot displays a debugger interface with several windows:

- Assembly Window:** Shows a list of instructions starting from address 0014026C. The instructions include `push 7FD6A366`, `push edi`, `call 140073`, `lea ecx, dword ptr ss:[ebp-34]`, `push ecx`, `push eax`, `call 140073`, `push 7FE63623`, `push edi`, `mov esi, eax`, `call 140073`, `push 7F8D727F`, `push edi`, `mov dword ptr ss:[ebp-4], eax`, `call 140073`, `push 7F847ADD`, `push edi`, `mov dword ptr ss:[ebp-10], eax`, `call 140073`, `push 7FE7F840`, `push edi`, `mov dword ptr ss:[ebp-14], eax`, `call 140073`, `push 7FE1F1FB`, `push edi`, `mov dword ptr ss:[ebp-18], eax`, `call 140073`, `push 7FD6F495`, `push edi`, `mov dword ptr ss:[ebp-C], eax`, `call 140073`, `push 7F750C`, `push dword ptr ss:[ebp+C], eax`, `call 140073`, `mov dword ptr ss:[ebp-1C], eax`, `call 140073`, `cmp eax, 1`, `je 140373`, and `push ebx`.
- CPU Window:** Shows the state of the CPU registers. `EAX` is 75071282, `ECX` is FFFCFC75, `EDX` is 7FD6E495, `EBP` is 0053E568, `ESP` is 0053E524, `ESI` is 75A345BF, and `EDI` is 75060000. The `EIP` is 001402E1.
- Stack Window:** Shows the stack memory. The top of the stack is at address 0053E524, and it contains the path `&L"C:\\Users\\...\\AppData\\Local\\Temp\\api.dll`.
- Memory Window:** Shows a list of memory addresses and their corresponding hex values. The addresses range from 0053E4FC to 0053F60C.

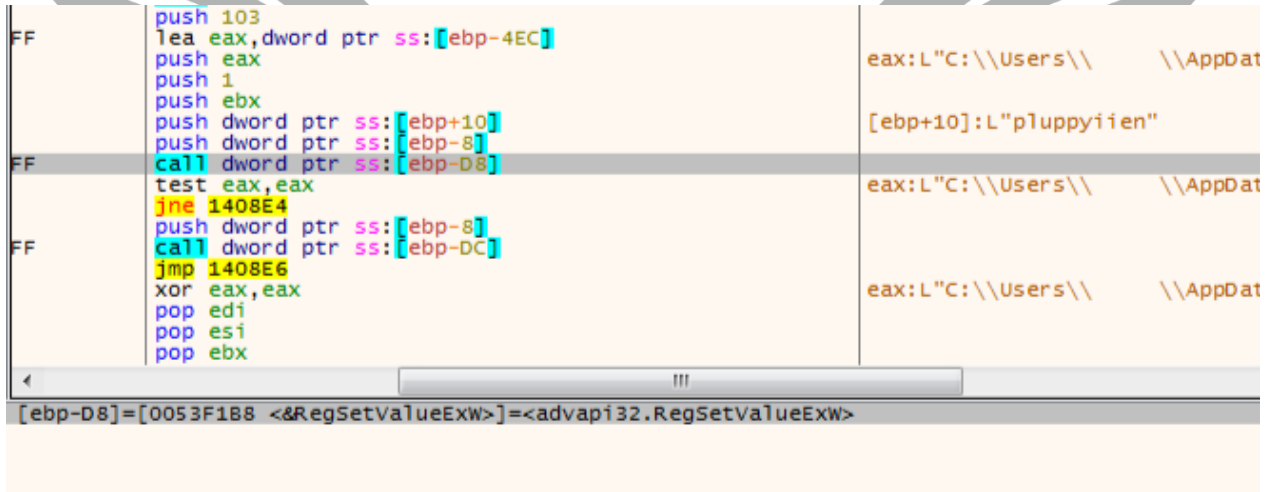
Görsel 11 Dinamik API Çözümleme

Görsel 11’de gösterilen call çağrılarını ile sırasıyla **LoadLibrary**, **PathFileExistsW**, **CreateFileW**, **GetFileSize**, **VirtualAlloc**, **ReadFile**, **CloseHandle**, **WriteFile** API’lerini çözümlemekte ve adreslerini belleğe kaydetmektedir.

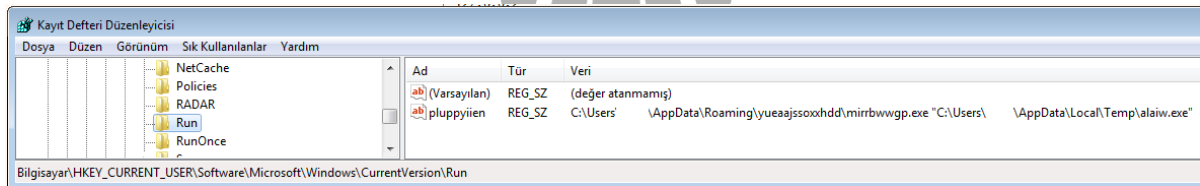


Görsel 12 Kendisini mirrbwwgp.exe Dosyası Olarak Kopyalayan alaiw.exe

Bu API'leri kullanarak **mirrbwwgp.exe** ismiyle kendisini "**C:\Users\%username%\AppData\Roaming\yueaajssoxxhdd**" dosya dizinine kopyalamaktadır.



Görsel 13 RegSetValueExW ile Kalıcılığın Sağlanması



Görsel 14 "pluppyien" Anahtarının Oluşturulması

Kalıcılığını sağlamak için kayıt defterine ulaşarak **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** konumuna "**pluppyien**" anahtarını oluşturmaktadır. Bu şekilde sistem her açıldığında zararlı kendini çalıştırmaktadır.

68 04000008	push 8000004	explorer.exe	2568	0,23	72,41 MB
6A 00	push 0	wintoolservice.exe	2672		1,53 MB
6A 00	push 0	wintools64.exe	2680	0,15	1,74 kB/s
6A 00	push 0	VMToolsHookProc.exe	4868		780 kB
8D85 44F8FFFF	lea eax,dword ptr ss:[ebp-78C]	ProcessHacker.exe	3960	0,40	23,89 MB
50	push eax	x32dbg.exe	2332	0,50	156 B/s
FF55 84	call dword ptr ss:[ebp-7C]	alaiw.exe	4856		384,71 MB
85C0	test eax,eax	alaiw.exe	488		388 kB
75 05	jne 140AD5	ida.exe	3436	0,32	183,48 MB
E9 F8020000	jmp 140DCD	alaiw.exe	1600		383,13 MB
C785 54FCFFFF 0700010	mov dword ptr ss:[ebp-3AC],10007	notepad++.exe	3504		11,86 MB
8D85 54FCFFFF	lea eax,dword ptr ss:[ebp-3AC]	chrome.exe	1592	0,10	135,61 MB
50	push eax	gozmon.exe	3588		3,76 MB
FF75 D0	push dword ptr ss:[ebp-30]	gozmon64.exe	3828	0,05	30,52 kB/s
FF55 80	call dword ptr ss:[ebp-80]	HxD.exe	4628	1,08	12,64 MB
85C0	test eax,eax	die.exe	516		22,97 MB
75 05	jne 140AF5				
E9 D8020000	jmp 140DCD				
6A 00	push 0				
6A 04	push 4				
8D45 B4	lea eax,dword ptr ss:[ebp-4C]				
50	push eax				

Görsel 18 Askıya Alma Modunda Çalışan Dosya

GetModuleFileNameW API'si kullanarak bulunduğu dosyanın yolunu elde etmektedir. Daha sonra bu dosya yolunu, **CreateProcessW** API'sine parametre olarak vererek alaiw.exe'yi kendi altında **askıya alma** modunda (**suspend modda**) başlatmaktadır.

Görsel 15'teki algoritmayla çözdüğü veriyi, **GetThreadContext**, **ReadProcessMemory** ve **SetThreadContext** API'lerini kullanarak **askıya alma** modunda çalıştırdığı alaiw.exe'nin içine yazmaktadır. alaiw.exe bir **alt süreç** olarak çalışırken bu işlem sonrasında ana süreç olarak çalışmaya devam etmektedir.

alaiw.exe'ye eklenen kodların olduğu bellek bölgesi (görsel 16) **dump** edilerek incelenmeye devam edilmiştir.

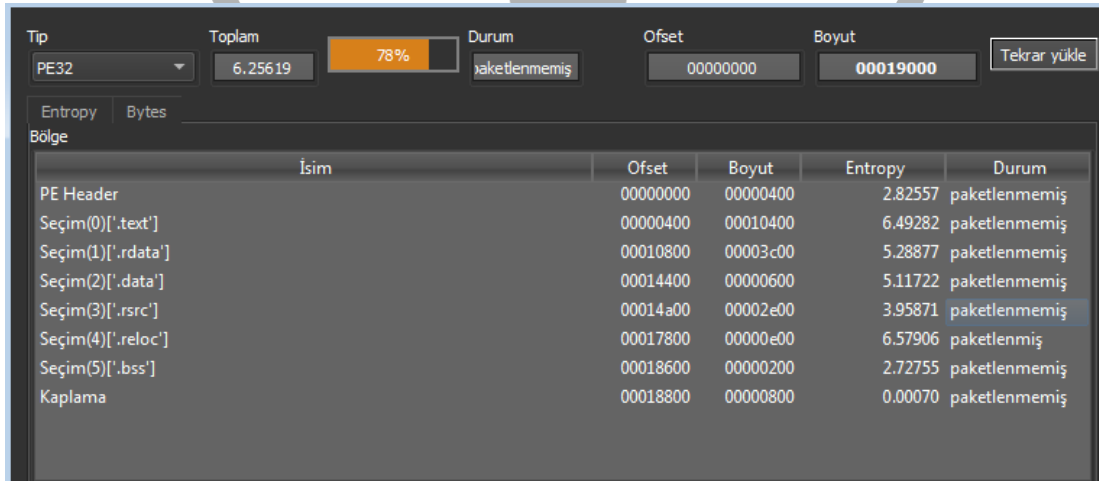
warzone160.exe Analizi

Adı	warzone160.exe
MD5	bfa56fb7698757d5316e3cd458008541
SHA256	a4470593f2ebc45b1be6f2d432c90f1a5120dab98427bb6aed8319235b52d4cb
Dosya Türü	Portable Executable 32 (x86)

Dump edilen dosya “**warzone160**” olarak isimlendirilmiştir. Dosyanın MD5, SHA256 gibi bilgileri yukarıdaki tabloda yer almaktadır.

Statik Analiz

warzon160.exe DIE aracında incelendiğinde **paketlenmiş** olduğu görülmektedir.



Tip	Toplam	Durum	Ofset	Boyut	Tekrar yükle
PE32	6.25619	78%	00000000	00019000	
Entropy	Bytes				
Bölge					
İsim	Ofset	Boyut	Entropy	Durum	
PE Header	00000000	00000400	2.82557	paketlenmemiş	
Seçim(0)['.text']	00000400	00010400	6.49282	paketlenmemiş	
Seçim(1)['.rdata']	00010800	00003c00	5.28877	paketlenmemiş	
Seçim(2)['.data']	00014400	00000600	5.11722	paketlenmemiş	
Seçim(3)['.rsrc']	00014a00	00002e00	3.95871	paketlenmemiş	
Seçim(4)['.reloc']	00017800	00000e00	6.57906	paketlenmiş	
Seçim(5)['.bss']	00018600	00000200	2.72755	paketlenmemiş	
Kaplama	00018800	00000800	0.00070	paketlenmemiş	

Görsel 19 warzone160.exe'nin DIE Aracında İncelenmesi

Dinamik Analiz

4587	14113.566432	192.168.96.132	194.180.48.209	TCP	66	49559 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4588	14115.942755	194.180.48.209	192.168.96.132	TCP	60	9409 → 49559 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4589	14116.449734	192.168.96.132	194.180.48.209	TCP	66	[TCP Retransmission] 49559 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4590	14118.840999	194.180.48.209	192.168.96.132	TCP	60	9409 → 49559 [RST, ACK] Seq=34622698 Ack=1 Win=64240 Len=0
4591	14119.350810	192.168.96.132	194.180.48.209	TCP	62	[TCP Retransmission] 49559 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
4592	14121.253851	Vmware_cc:b3:5d	Vmware_fb:4d:28	ARP	42	Who has 192.168.96.2? Tell 192.168.96.132
4593	14121.254087	Vmware_fb:4d:28	Vmware_cc:b3:5d	ARP	60	192.168.96.2 is at 00:50:56:fb:4d:28
4594	14121.661752	194.180.48.209	192.168.96.132	TCP	60	9409 → 49559 [RST, ACK] Seq=4197400481 Ack=1 Win=64240 Len=0
4595	14122.876918	192.168.96.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
4596	14123.878035	192.168.96.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
4597	14124.878321	192.168.96.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
4598	14125.879197	192.168.96.1	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
4599	14126.028754	192.168.96.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4600	14126.676157	192.168.96.132	192.168.96.2	DNS	81	Standard query 0x3de3 192.168.96.2
4601	14126.678106	192.168.96.2	192.168.96.132	DNS	97	Standard query response 0x3de3 A 192.168.96.2
4602	14126.678334	192.168.96.132	194.180.48.209	TCP	66	49560 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4603	14127.030799	192.168.96.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4604	14128.032056	192.168.96.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4605	14129.033636	192.168.96.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4606	14129.053151	194.180.48.209	192.168.96.132	TCP	60	9409 → 49560 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4607	14129.559685	192.168.96.132	194.180.48.209	TCP	66	[TCP Retransmission] 49560 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4608	14131.933621	194.180.48.209	192.168.96.132	TCP	60	9409 → 49560 [RST, ACK] Seq=1647120699 Ack=1 Win=64240 Len=0
4609	14132.445641	192.168.96.132	194.180.48.209	TCP	62	[TCP Retransmission] 49560 → 9409 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM
4610	14134.763000	194.180.48.209	192.168.96.132	TCP	60	9409 → 49560 [RST, ACK] Seq=4199943123 Ack=1 Win=64240 Len=0
4611	14136.329689	192.168.96.1	192.168.96.255	UDP	86	57621 → 57621 Len=44

Görsel 20 Wireshark'ta Elde Edilen Veriler

Zararlı devamlı olarak **194[.]180[.]48[.]209[:]9409** soketine bağlanmayı deneyerek komuta kontrol sunucusuyla iletişim kurmaya çalışmaktadır. **Bağlantı sağlanamadığı** için bu işlem sürekli tekrar etmektedir.

Zararlı çalıştığında **“septembre[.]duckdns[.]org”** domainine bağlanmaya çalıştığı gözlenmiştir. Ancak sunucu aktif olmadığı için bağlantı sağlayamamıştır. Bu sebeple analiz **statik** olarak incelenmeye devam edilmiştir.

push 1C pop edx lea ecx,dword ptr ss:[ebp-10] call warzone160.D1051C push warzone160.D22938 lea ecx,dword ptr ss:[ebp-10] call warzone160.D13230 push dword ptr ss:[ebp-10] call dword ptr ds:[&PathFileExistsW]	edx:EntryPoint D22938:L"\\Google\\Chrome\\User Data\\Default\\Login D
--	--

Görsel 21 Google Chrome Tarayıcısı

push eax push 20019 push 0 push warzone160.D2351C push 80000001 call dword ptr ds:[&RegOpenKeyExA] test eax,eax jne warzone160.D18912 lea ecx,dword ptr ss:[ebp-4]	D2351C:"software\\Aerofox\\FoxmailPreview"
--	--

Görsel 22 Foxmail E-posta Servisi

push eax call warzone160.D11052 add esp,14 lea edx,dword ptr ss:[ebp-28C] mov ecx,warzone160.D22F0C call warzone160.D1A8E2 pop ecx lea eax,dword ptr ss:[ebp-28C] push eax lea ecx,dword ptr ss:[ebp-28] call warzone160.D133A8 lea eax,dword ptr ss:[ebp-98] push eax lea eax,dword ptr ss:[ebp-28C] push eax call dword ptr ds:[&GetBinaryTypeW] push ecx lea eax,dword ptr ss:[ebp-28] mov ecx,esp push eax call warzone160.D133F3 mov ecx,edi call warzone160.D1A190 test eax,eax jne warzone160.D192A1 push ecx lea eax,dword ptr ss:[ebp-28] mov ecx,esp push eax call warzone160.D133F3 mov ecx,edi call warzone160.D1A190 test eax,eax jne warzone160.D192A1 mov esi,dword ptr ss:[ebp-14] jmp warzone160.D19702 push warzone160.D22F2C lea ecx,dword ptr ss:[ebp+8] call warzone160.D13230 lea eax,dword ptr ss:[ebp+8] push eax lea ecx,dword ptr ss:[ebp-20] call warzone160.D133F3 push warzone160.D22EA0 lea ecx,dword ptr ss:[ebp-20] call warzone160.D13230 push warzone160.D22E38 lea ecx,dword ptr ss:[ebp-24] call warzone160.D133A8 push eax lea ecx,dword ptr ss:[ebp-14] call warzone160.D131FD mov ecx,dword ptr ss:[ebp-24] call warzone160.D158F8 push ebx lea ecx,dword ptr ss:[ebp-14] call warzone160.D13038 push dword ptr ss:[ebp-20] push esi jmp warzone160.D196D1 mov esi,dword ptr ss:[ebp-34] lea ecx,dword ptr ss:[ebp-38] inc esi push warzone160.D22E38 mov dword ptr ss:[ebp-34],esi call warzone160.D133A8	edx:EntryPoint D22F0C:L"thunderbird.exe" D22F2C:L"\\Thunderbird\\" D22EA0:L"profiles.ini" D22E38:L"profile" D22E38:L"profile"
--	--

Görsel 23 Thunderbird E-posta Servisi

Statik analiz ve string taraması yapıldığında görsel 21, 22, 23'te de görüldüğü üzere zararlının bazı tarayıcılardan ve **e-posta** servislerinden parola ve **istemci ayarları** gibi verileri çalmayı hedeflediği anlaşılmıştır.

```
00012CA0 6E 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 n.t.v.e.r.s.i.o.
00012CB0 6E 00 5C 00 52 00 75 00 6E 00 5C 00 00 00 00 00 n.\.R.u.n.\.....
00012CC0 63 6D 64 2E 65 78 65 20 2F 43 20 70 69 6E 67 20 cmd.exe /C ping
00012CD0 31 2E 32 2E 33 2E 34 20 2D 6E 20 32 20 2D 77 20 1.2.3.4 -n 2 -w
00012CE0 31 30 30 30 20 3E 20 4E 75 6C 20 26 20 44 65 6C 1000 > Nul & Del
00012CF0 20 2F 66 20 2F 71 20 00 22 00 00 00 53 00 4F 00 /f /q ."...S.O.
00012D00 46 00 54 00 57 00 41 00 52 00 45 00 5C 00 5F 00 F.T.W.A.R.E.\._.
00012D10 72 00 70 00 74 00 6C 00 73 00 00 00 49 00 6E 00 r.p.t.l.s...I.n.
00012D20 73 00 74 00 61 00 6C 00 6C 00 00 00 5C 00 53 00 s.t.a.l.l...\.S.
00012D30 79 00 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 y.s.t.e.m.3.2.\.
00012D40 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 00 00 c.m.d...e.x.e...
```

Görsel 24 CMD Komutu

Görsel 24'te görülen **Cmd** komutu ile **geçerli olmayan** bir IP adresine gönderilen ping talepleri aracılığıyla saldırının saptanmasını karmaşıktırmayı hedeflemektedir. Bunun yanı sıra, **Del /f /q** komutu, kötü amaçlı yazılımın tespit edilmesi durumunda, kendisini izin almadan silme amacını taşımaktadır.

<pre>mov ecx, eax call dword ptr ds:[<&GetAsyncKeyState>] test ax, ax mov dl, bl setne cl call warzone160.D17949 test al, al lea ecx, dword ptr ds:[esi+20]</pre>	
<pre>push ecx call dword ptr ds:[<&wsprintfw>] add esp, c lea ecx, dword ptr ss:[ebp-14] call warzone160.D17966 mov ebx, dword ptr ss:[ebp-4] jmp warzone160.D17908 cmp esi, 66 ja warzone160.D1771D je warzone160.D17713 cmp esi, 20 ja warzone160.D17691 je warzone160.D17687 cmp esi, 11 ja warzone160.D17658 je warzone160.D17781 sub esi, 8 je warzone160.D17651 sub esi, 1 je warzone160.D17647 sub esi, 4 je warzone160.D1763D sub esi, 3 je warzone160.D17908 jmp warzone160.D178A2 mov ecx, warzone160.D22814 jmp warzone160.D17906 mov ecx, warzone160.D22838 jmp warzone160.D17906 mov ecx, warzone160.D22828 jmp warzone160.D17906 sub esi, 12 je warzone160.D177D8 dec esi sub esi, 1 je warzone160.D1767D sub esi, 7 jne warzone160.D178A2 mov ecx, warzone160.D22870 jmp warzone160.D17906 mov ecx, warzone160.D22860 jmp warzone160.D17906 mov ecx, warzone160.D22810 jmp warzone160.D17906 cmp esi, 62 ja warzone160.D176E2 je warzone160.D176D8 sub esi, 2D je warzone160.D176CE sub esi, 1 je warzone160.D176C4 sub esi, 32 je warzone160.D1768A sub esi, 1 jne warzone160.D178A2 mov ecx, warzone160.D228A0 jmp warzone160.D17906 mov ecx, warzone160.D2289C jmp warzone160.D17906 mov ecx, warzone160.D22890 jmp warzone160.D17906 mov ecx, warzone160.D2287C jmp warzone160.D17906 mov ecx, warzone160.D228A4 jmp warzone160.D17906 sub esi, 63</pre>	<p>66: 'f'</p> <p>20: ' '</p> <p>D22814:L "[ENTER] \r\n"</p> <p>D22838:L "[TAB]"</p> <p>D22828:L "[BKSP]"</p> <p>D22870:L "[ESC]"</p> <p>D22860:L "[CAPS]"</p> <p>62: 'b'</p> <p>D22890:L "[DEL]"</p> <p>D2287C:L "[INSERT]"</p>

Görsel 25 Keylogger

Görsel 25'te **GetAsyncKeyState** API'si ile ENTER, TAB, BKSP, ESC, CAPS, DEL, INSERT gibi özel **tuş vuruşlarını kaydettiği** anlaşılmaktadır.

<pre> ush ebp mov ebp,esp ub esp,18 ush esi ush edi or edi,edi ea ecx,dword ptr ss:[ebp-c] ush warzone160.D23688 mov dword ptr ss:[ebp-4],edi a11 warzone160.D133AB ea eax,dword ptr ss:[ebp-4] mov dword ptr ss:[ebp-14],edi ush eax ush 20119 ush edi ush dword ptr ss:[ebp-c] mov dword ptr ss:[ebp-10],edi ush 80000002 a11 dword ptr ds:[<<RegOpenKeyExW>] est eax,eax ne warzone160.D18FD0 ea eax,dword ptr ss:[ebp-14] ush eax ush warzone160.D236FC ea ecx,dword ptr ss:[ebp-8] a11 warzone160.D133AB </pre>	<p>D23688:L"SYSTEM\\CurrentControlSet\\Services\\TermService\\Parameters"</p> <hr/> <p>D236FC:L"ServiceDll"</p>
---	---

Görsel 26 Uzaktan Erişim Sağlanması

Zararlı "SYSTEM\\CurrentControlSet\\Services\\TermService\\Parameters" yolundaki **ServiceDll** kaydına ulaşmaktadır. Bu şekilde **Uzak Masaüstü Protokolü (RDP)** ile cihaza uzaktan erişim sağlamaktadır ve cihazı kontrol etmeyi mümkün kılmaktadır.

YARA Kuralı

```
import "hash"

rule avemariarat {

    meta:

        author = "Team-5"

    strings:

        $hex_1 = { 55 58 54 48 45 4D 45 00 55 53 45 52 45 4E 56 00 53 45 54
55 50 41 50 49 00 41 50 50 48 45 4C 50 00 50 52 4F 50 53 59 53 00 44 57 4D 41 50
49 00 43 52 59 50 54 42 41 53 45 00 4F 4C 45 41 43 43 00 43 4C 42 43 41 54 51 00
4E 54 4D 41 52 54 41 }

        $hex_2 = { 50 33 C0 68 50 67 42 00 50 50 68 00 00 00 04 50 50 50 FF
75 08 50 FF 15 ?? ?? ?? ?? }

        $str1 = "http://nsis.sf.net/NSIS_Error" wide

        $str2 = "\\Microsoft\\Internet Explorer\\Quick Launch" wide

        $api1 = "DialogBoxParamW" ascii

        $api2 = "RegSetValueExW" ascii

        $api3 = "CreateProcessW" ascii

        $api4 = "ExitProcess" ascii

        $api5 = "WriteFile" ascii

        $api6 = "FindNextFileW" ascii

    condition:

        hash.md5 (0, filesize) == "d802bc50f7321efb13358d27280910ca" or (all of ($str*)
and (5 of ($api*))) or (all of ($hex_*)) }
```

```

import "hash"

rule alaiw_d {

    meta:

        author = "Team-5"

        description = "AveMariaRAT"

        weight = "10"

    strings:

        $algorithm1 = { C1 E0 05 0F B6 4D EF C1 F9 03 0B C8 33 CA 8B
55 E8 88 8A ?? ?? ?? ?? } //Shellcode decryption algorithm

        $str1 = "vtwkwntewuzvb"

        $str2 = "find.exe"

        $str3 = "-w %ws -d C -f %s"

        $str4 = "\\System32\\cmd.exe"

        $str5 = "SELECT * FROM logins"

        $str6 = "Accounts\\Account.rec0"

        $str7 = "cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q"

        $str8 = "SOFTWARE\\Microsoft\\Windows
NT\\CurrentVersion\\Winlogon\\SpecialAccounts\\UserList"

```

```
$w1 = "http://5.206.225.104/dll/msvc140.dll" wide

$w2 = "http://5.206.225.104/dll/softokn3.dll" wide

$w3 = "http://5.206.225.104/dll/mozglue.dll" wide

$w4 = "http://5.206.225.104/dll/vcruntime140.dll" wide

$w5 = "http://5.206.225.104/dll/freebl3.dll" wide

$w6 = "http://5.206.225.104/dll/nss3.dll" wide

$w7 =
"C:\\Users\\louis\\Documents\\workspace\\MortyCrypter\\MsgBox.exe"
wide

$w8 = "\\Google\\Chrome\\User Data\\Default\\Login Data" wide

$w9 = "profiles.ini" wide

condition:

    hash.md5(0,filesize) == "fa0be3eb24b13d060a0ae4e25c22ef1c" or
    (((5 of $str*) or (7 of $w*)) or ($algorithm1 and (2 of $w*)))

}
```



```
rule warzone {  
  
    meta:  
  
        author = "Team-5"  
  
    strings:  
  
        $str1 = "find.exe"  
  
        $str2 = "-w %ws -d C -f %s"  
  
        $str3 = "\\System32\\cmd.exe"  
  
        $str4 = "SELECT * FROM logins"  
  
        $str5 = "Accounts\\Account.rec0"  
  
        $str6 = "cmd.exe /C ping 1.2.3.4 -n 2 -w 1000 > Nul & Del /f /q"  
  
        $str7          =          "SOFTWARE\\Microsoft\\Windows  
NT\\CurrentVersion\\Winlogon\\SpecialAccounts\\UserList"  
  
  
        $w1 = "http://5.206.225.104/dll/msvcpl140.dll" wide  
  
        $w2 = "http://5.206.225.104/dll/softokn3.dll" wide  
  
        $w3 = "http://5.206.225.104/dll/mozglue.dll" wide  
  
        $w4 = "http://5.206.225.104/dll/vcruntime140.dll" wide  
  
        $w5 = "http://5.206.225.104/dll/freebl3.dll" wide
```

```

    $w6 = "http://5.206.225.104/dll/nss3.dll" wide

    $w7                                     =
"C:\\Users\\louis\\Documents\\workspace\\MortyCrypter\\MsgBox.exe"
wide

    $w8 = "\\Google\\Chrome\\User Data\\Default\\Login Data" wide

    $w9 = "profiles.ini" wide

    $e1 = "hostname"

    $e2 = "encryptedUsername"

    $e3 = "encryptedPassword"

    $v1 = "vaultcli.dll"

    $v2 = "VaultOpenVault"

    $v3 = "VaultCloseVault"

    $v4 = "VaultEnumerateItems"

    $v5 = "VaultGetItem"

    $v6 = "VaultFree"

condition:

    ((5 of ($str*)) or (4 of ($w*))) or ((all of ($e*)) and (all of ($v*)))

}

```

MITRE ATTACK TABLE

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	C&C	Exfiltration
Gather Victim Network Information (T1590)	Command and Scripting Interpreter (T1059)	Create Account (T1136)	Process Injection (T1055)	Deobfuscate/Decode Files or Information (T1140)	OS Credential Dumping (T1003.008)	Application Layer Protocol (T1071.004)	Exfiltration Over C2 Channel (T1041)
Gather Victim Host Information (T1592)	Shared Modules (T1129)	Boot or Logon Autostart Execution (T1547)	Create or Modify System Process (T1543.003)	Masquerading (T1036)			
	Native API (T1106)						

Çözüm Önerileri

1. Güncel antivirüs koruması kullanılmalıdır
2. Bilinmeyen kaynaklardan dosya indirilmemelidir
3. Bilinmeyen linklere tıklanmamalıdır
4. Bilinmeyen harici cihazlar kullanılırken dikkat edilmelidir
5. Teknoloji okuryazarı olunmalıdır
6. İşletim sistemi güncel tutulmalıdır
7. Güvenilmeyen e-postalar açılmamalıdır

HAZIRLAYANLAR

Barış TURAL

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

Betül ŞAHİN

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

Zeynep ÖZDEMİR

<https://www.linkedin.com/in/zeynep-ozdemir/>

