AMADEY

Teknik Analiz Raporu

İçindekiler

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.

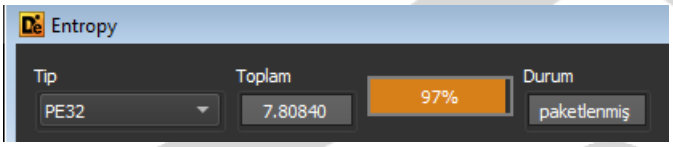
Temel olarak Amadey başka bir virüsün enfekte olmasını sağlamak amacıyla e-posta, çevrimiçi reklamlar, sosyal mühendislik gibi yollar kullanılarak gönderilir.

Ön İnceleme

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

Zararlının 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 DIE 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;

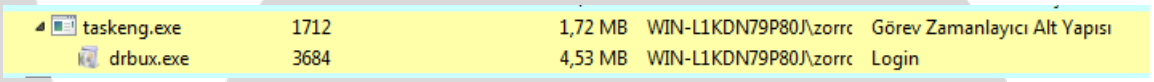
Clbcatq.exe	Cryptbase.dll	Gdiplus.dll	Kernel32.dll	İmm32.dll
Ntl.dll	Ole32.dll	Propsys.dll	Shell32.dll	Shlwapi.dll
User32.dll	Userenv.dll	Usp10.dll	Uxtheme.dll	Version.dll
Comctl32.dll	Wininet.dll	Oleaut32.dll	Lpk.dll	Msctf.dll

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.

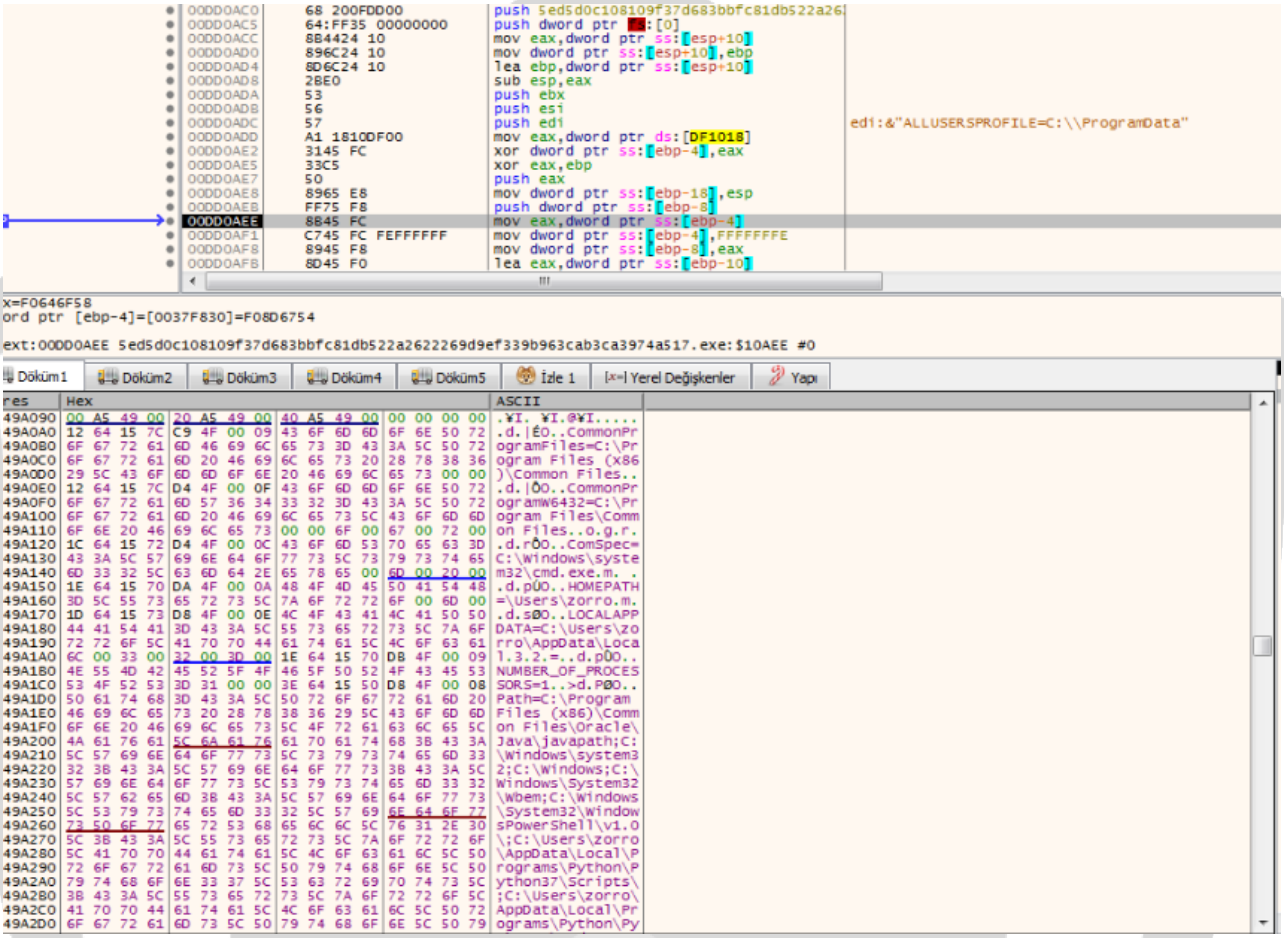


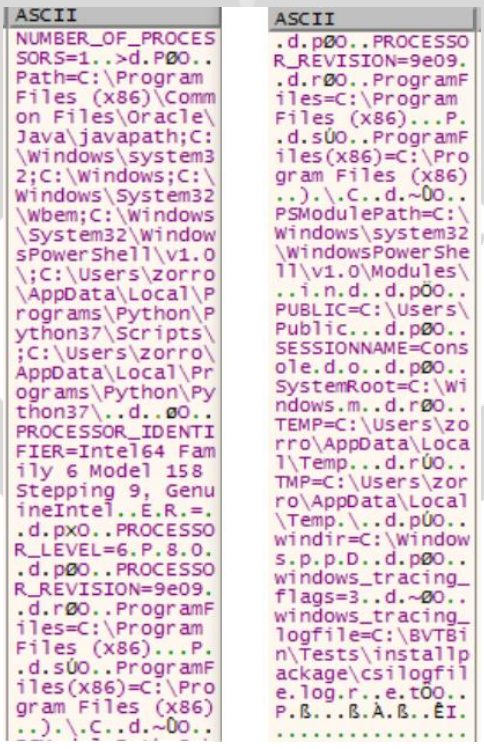
C:\Users\zorro\AppData\Local\Temp yolunu alıp Temp klasörünün içine CreateFile API'si ile 15212987719733412987 adlı binary dosyası oluşturmaktadır.

```
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.

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

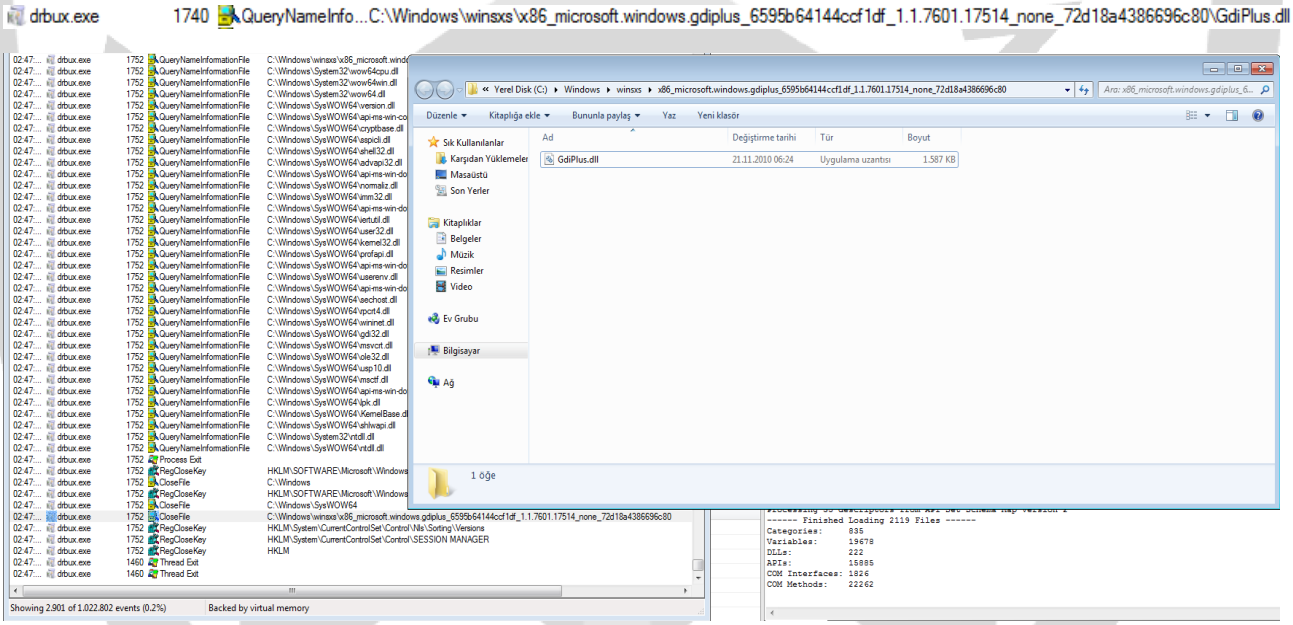




Zararlı"C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll" yolunu almaktadır.

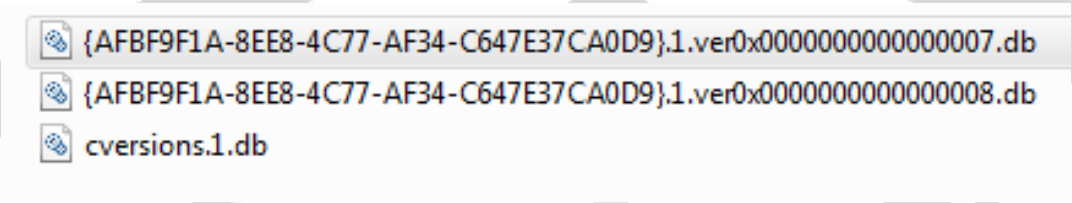
```
edi:L"C:\\Windows\\winsxs\\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\\GdiPlus.dll"
```

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.



Zararlının 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”



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

Zararlının içindeki önemli API’ler;

ShellExecuteA	CreateThread	CreateFileA	LoadLibraryA
CreateProcessA	SuspendThread	CreateMutexW	WriteFile
ReadFile	ReadConsoleW	DeleteFileW	IsDebuggerPresent
VirtualAlloc	TerminateProcess	LoadLibraryExW	SetUnhandledExceptionFilter
Sleep	ResumeThread	CreateFileW	UnhandledExceptionFilter
HttpOpen RequestA	InternetOpenUrlW	InternetWriteFile	InternetReadFile
InternetOpenA	InternetConnectA	GdipGetImage Encoders	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 zararlının debug edilmesini zorlaştırmaktadır.

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

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

Network Analizi

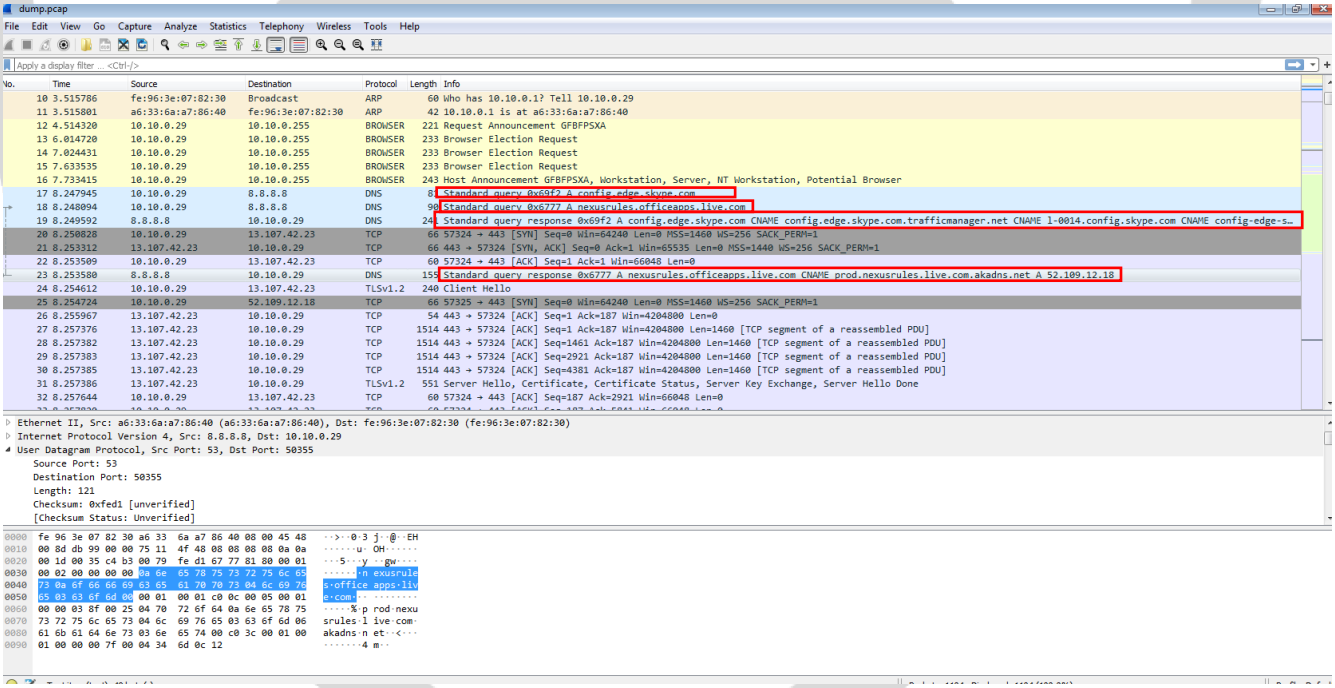
Process Monitor'e 194.58.103.2.cloudvps.regruhosting[.]ru adresine bağlantı isteği atıldığı görülmektedir.

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.

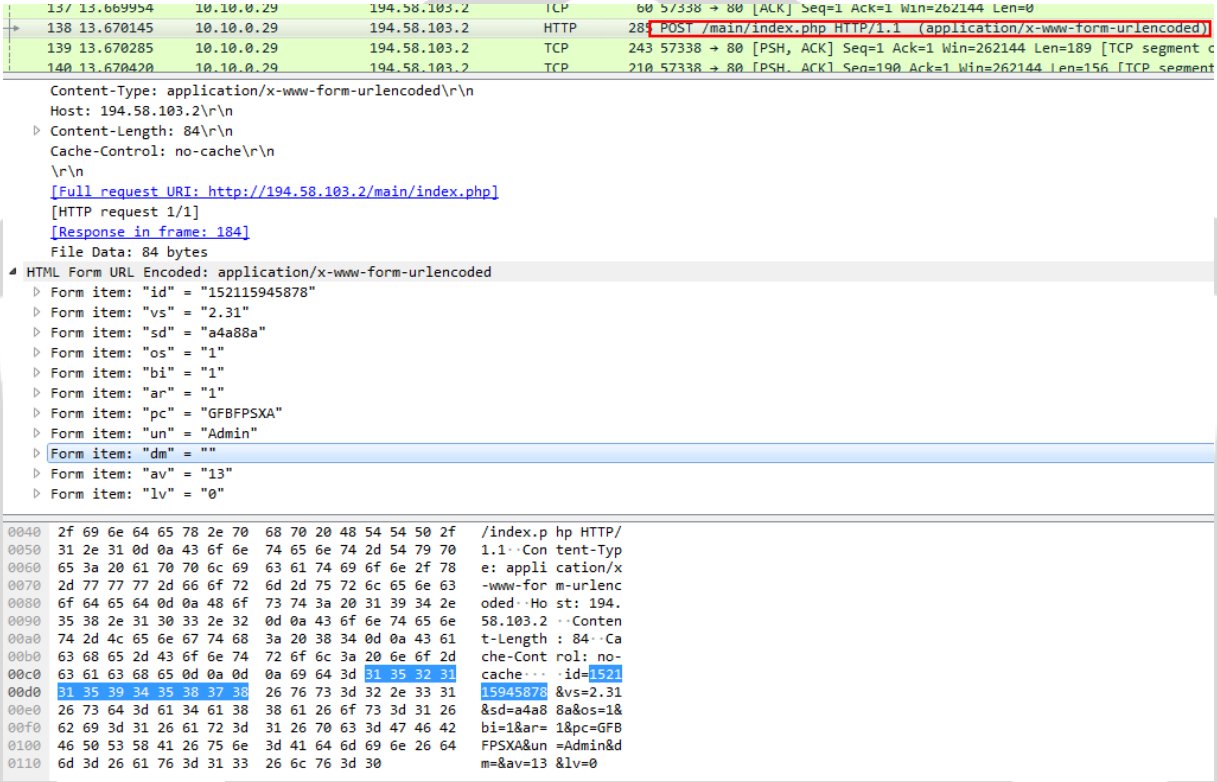
drbux.exe	1460	TCP Disconnect	WIN-L1KDN79P80J.localdomain:49217 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Disconnect	WIN-L1KDN79P80J.localdomain:49218 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP Connect	WIN-L1KDN79P80J.localdomain:49220 -> bethdahleen.com:http	SUCCESS
drbux.exe	1460	TCP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



<h2>Our services aren't available right now</h2> We're working to restore all services as soon as possible. Please check back soon.
04pQCYQAAAADRQdetuqNUQ4g6UBzx6oFRSVNUMzBFREdFMDEwOABFZGdl

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



Çözüm Önerileri

Amadey zararlısından korunmanın yolları şu şekildedir;

-Spam maillerin açılmamalıdır.

-İnternetten 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/