



**UPWORK ÜZERİNDEN
FREELANCE
ÇALIŞANLARI HEDEF
ALAN SALDIRILAR**



@infinitemitlab1



@infinitemlabs1096



@infinitemitlabs



@infinitemlabs

Upwork Üzerinden Freelance Çalışanları Hedef Alan Saldırıları

İnternet üzerinden günde milyonlarca uygulama, makale vb. dosyanın indirilmesi ile Trojan yazılımlarında çok rahat bulaştığı bu dönemde hacker grupları hedefini freelance iş bulma sitelerine çevirmektedir. Blue team ekibimiz tarafından Upwork Global Inc. üzerinden freelance çalışanları hedef alan zararlı yazılım elde etmiştir. Bu yazılım bir klasör içerisinde gizlenmiş bir şekilde bulunmakta ve bu klasörün içerisinde bir adet word ikonu ile değiştirilmiş .exe uzantılı .NET dosyası, klasör içerisine gizlenmiş bir adet C++ ile yazılmış .exe uzantılı çalıştırılabilir bir dosya ve beş adet .jpg dosyası bulunmaktadır.

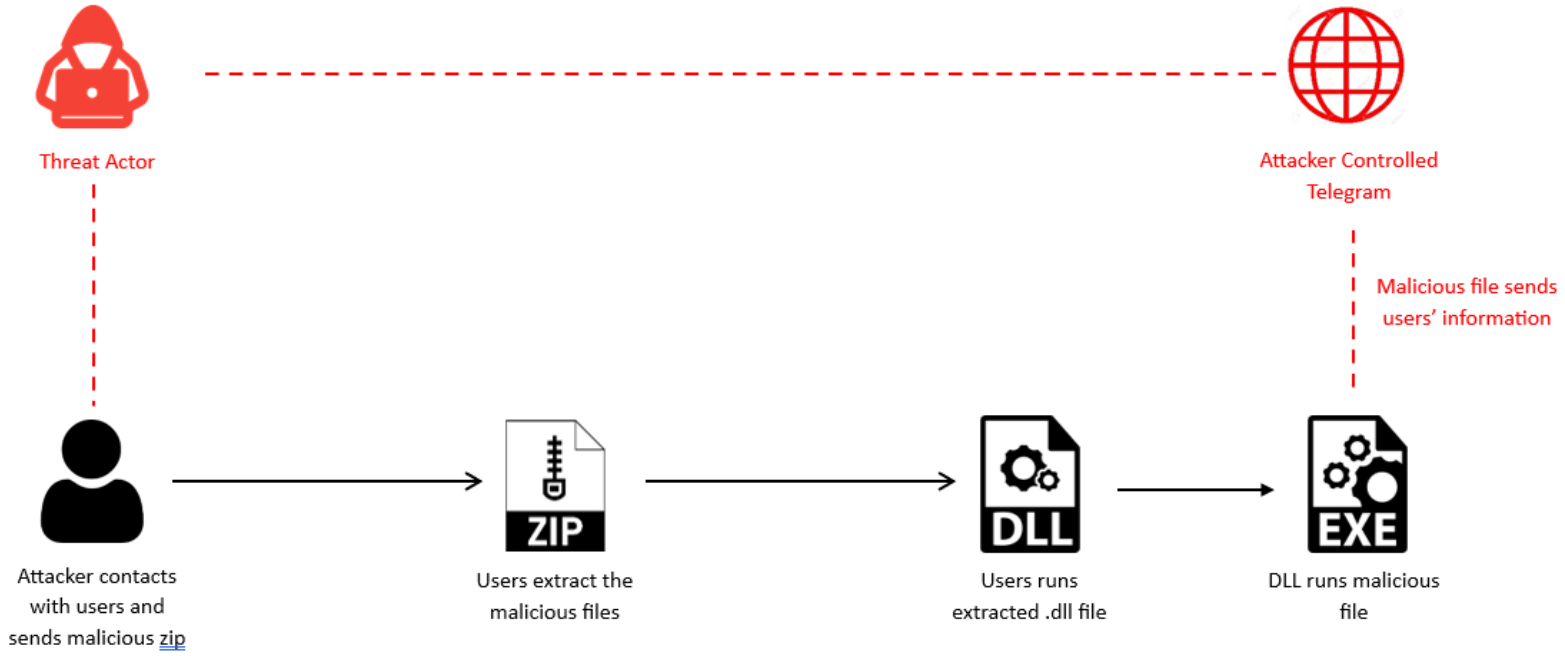
Akış şu şekildedir; ilk olarak word ikonu konularak gizlenen .Net dosyası kurban tarafından çalıştırılıyor. Bu dosyanın amacı bulunduğu dizindeki tüm .exe uzantılı dosyaları bulup onları tek tek çalıştırmaktır. Aynı klasörde bulunan diğer .exe uzantılı gizli dosya kullanıcı izni olmadan arka planda çalışmaktadır.

Bu zararlı ilk olarak kurban sistemde çalışması için gerekli dll dosyalarını yükliyor. Ardından bulunduğu dizinde “dbghelp” adında bir dll dosyasını arıyor. Daha sonra OpenSSL üzerinde işlemler yapabilmek için yapılandırma dosyası olan “openssl.cnf” arıyor. Kurban sistemde bulunan tüm tarayıcıların “Google Chrome, Microsoft Edge, Opera vs.” çerezlerinin bulunduğu “Cookies” dosyalarını tarıyor. Devamında ise ekranın anlık görüntüsünü alabilmek için screenCapture adı verilen bir program yükleyip kurban cihazın ekranının anlık görüntüsünü almaktadır.

Zararlı bu işlemlerinin ardından tüm topladığı verileri .txt uzantılı dosyaların içerisine ayrı ayrı yazıp kurban sistemin internet sağlayıcısının “Türk Telekom, Turkcell vs.” IP adresi ile isimlendirilen “C:\\Users*\\AppData\\Local” dizinine bir klasör oluşturmakta ve tüm bu topladığı verileri oluşturduğu klasörün içerisine atmaktadır. Ardından bu klasörü sıkıştırarak TCP bağlantısı kurup Telegram üzerinden yollamakta ve daha sonra kurban cihazdan bu .zip uzantılı dosyayı silmektedir. Tüm bu işlemlerin ardından TCP bağlantısını koparıp işlemini sonlandırmaktadır.

Zararlı dosyanın analizi sırasında Windows 7,8,8.1 gibi sistemlerde zararlı işlemler gerçekleştirmediği, Windows 10 ve üzeri sistemlerde zararlı işlemlerini gerçekleştirdiği tespit edilmiştir.

Attack Chain



Hacker ile Kurulan İletişim

İlk olarak zararlı aktörler teklif yollayarak kurbanlarla iletişime geçmektedir. Ardından zararlı dosyayı kurbanlara yollayıp incelemek amacıyla açtırmaktadır. Zararlı aktörler ile kurulan iletişim şu şekildedir :

The screenshot shows the Upwork interface with a search bar and navigation menu. The job title is "run ads on facebook" and the user's question is "You: i don't understand?". The offer details are as follows:

- Rate: \$50.00/hr
- Limit: 20 hrs/week
- View details

The offer was accepted on Wednesday, May 10, at 10:01 AM. The user's question is: "Hi, when should we start running facebook ads? Can you give the details of the job?".

The screenshot shows the Upwork interface with a search bar and navigation menu. The job title is "run ads on facebook" and the user's question is "You: i don't understand?". The conversation is as follows:

- 9:01 AM GMT+1 run ads on facebook
- 11:10 AM: Hi, i want to run ads on facebook. Do you have experience running Facebook ads?
- 11:11 AM: yes, of course 😊 I have been in this business for 4 years. Is the company that we will publish ads from an e-commerce site or from the service sector? I have experience from both
- 11:35 AM: this is my facebook page and website. <https://www.facebook.com/ElectricBikeScooterCarUK/> <https://www.electricbikescooterco.uk/>

The screenshot shows the Upwork interface with a search bar and navigation menu. The job title is "run ads on facebook" and the user's question is "You: i don't understand?". The conversation is as follows:

- 9:01 AM GMT+1 run ads on facebook
- 11:41 AM: okey, great. Have you done advertising work before, will it be your first? Do you have an existing advertising account?
- yes
- My company's goal is to reach customers, office workers, middle and high income people. The goal of this project is to increase sales. i want to run ads on facebook and budget will be 8000-10000\$ a month. We already have an ad account. i can invite you to our business group on facebook and i will send you the project details, I have prepared a file that includes .project information, and articles .images . and the campaign stats from the beginning of the year to now. can i have your email address?

Search

run ads on facebook
You: i don't understand?

5/17/23

9:02 AM GMT+1 run ads on facebook

Schedule a meeting Record with Loom View Contract

11:43 AM
can you forward the mail to this address?

11:44 AM
sure
please check our email, invitation and project data.
You need to extract the file by winrar with password 312123 to see the details.
check the project details and come back here , all right . thank you

11:45 AM
Ok, I'll check and get back to you. thanks

11:45 AM
okay

Search

run ads on facebook
You: i don't understand?

5/17/23

9:03 AM GMT+1 run ads on facebook

Schedule a meeting Record with Loom View Contract

12:02 PM
The transmitted file is in exe format, could you please forward the word version?

12:08 PM
It is the application created to protect the archive and organize the planning projects
we programmed to avoid theft by rival company, just open the file the doc file will open

we have security settings for the project to avoid stealing from rival company , hope you understand
I can't take data out of security without permission sir

12:49 PM
Unfortunately, the file cannot be opened this way, I could not understand the problem.

Search

run ads on facebook
You: i don't understand?

5/17/23

9:04 AM GMT+1 run ads on facebook

Schedule a meeting Record with Loom View Contract

1:03 PM
The file appears to be empty. I think it takes my ip address and desktop screenshot and sends it to you. Why do you need this?

1:16 PM
Chrome password information, cookie information, system information, screenshots, ip address. You collect them, zip them and send them to yourself via the api telegram. I will report you.

ended the contract 1:20 PM
View details

Wed, May 17

WhatsApp chat interface showing a contact's profile and a context menu.

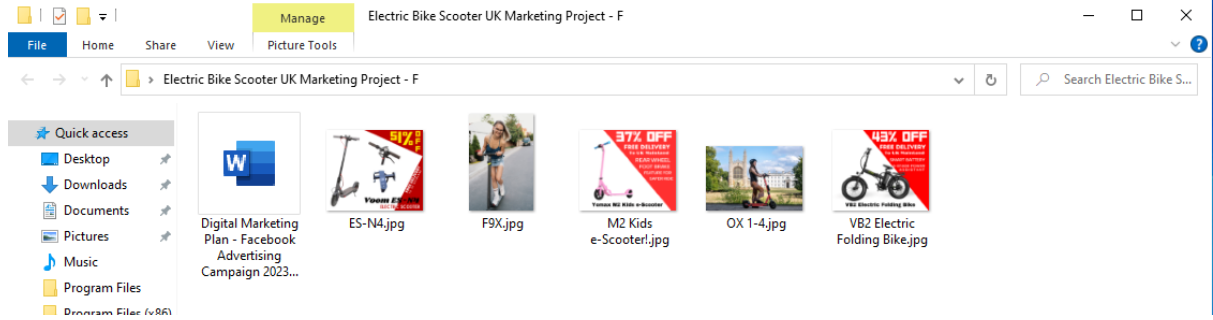
Top bar: Call icon, Info icon, Profile picture, Name, Status, and Close icon (X).

Contact details: 9:08 AM GMT+1 (2 h behind), run ads on facebook.

Context menu options:

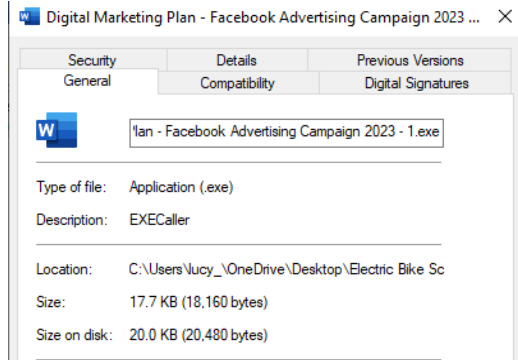
- Profile picture, Name, Status, and Arrow icon (>)
- United Kingdom (2 h behind) and Arrow icon (>)
- Go to 1:1 Room and Arrow icon (>)
- Block [Name] and Arrow icon (>)

Zararlı Dosyaya Genel Bakış



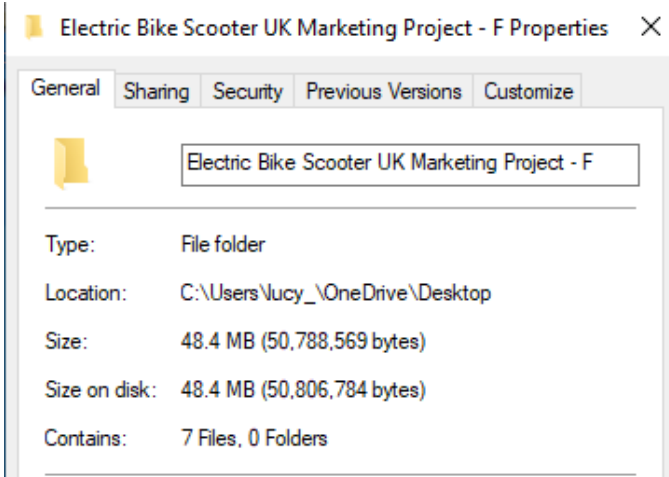
Şekil 1- Zararlı dosyanın bulunduğu klasör

Elde edilen dosyaya ilk bakışta bir adet word ve beş adet .jpg uzantılı dosya olduğu görülmektedir.



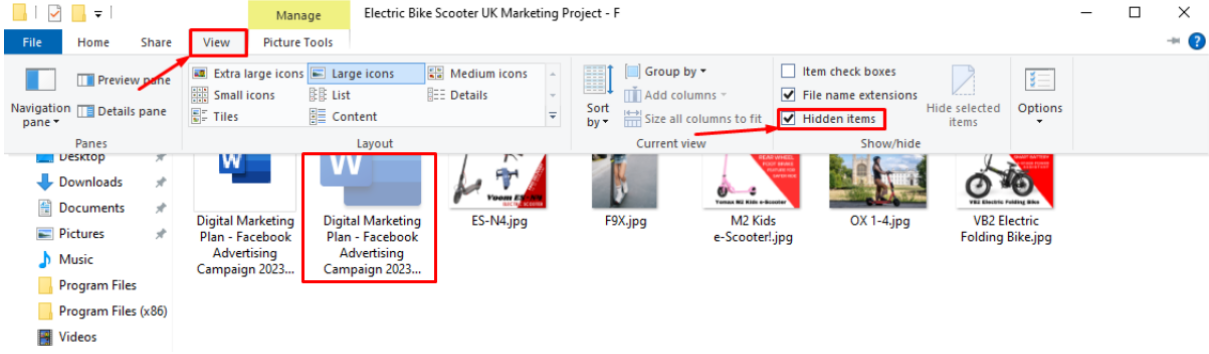
Ancak biraz incelendiğinde word dosyası gibi görünen dosyanın aslında .exe uzantılı bir çalıştırılabilir dosya olduğu ve iconu'nun word belgelerinin iconu ile değiştirildiği görülmektedir.

Şekil 2- Word dosyası gibi görünen çalıştırılabilir dosya



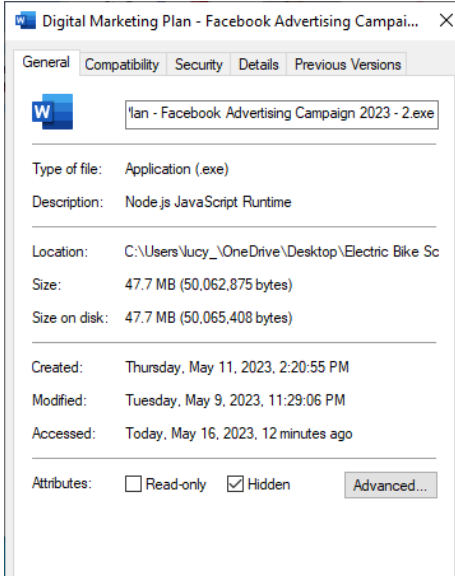
Klasör biraz daha incelendiğinde 48.4MB olduğu görülmektedir. Ancak içerisindeki dosyaların boyutları ile karşılaştırılınca bu boyutu karşılamadığı görülmektedir.

Şekil 3- Zararlı klasörün içeriği



Şekil 4- Klasör içerisinde gizlenen zararlı dosya

Ardından gizli dosya olabileceği düşünülerek gizli dosyaların görünürlüğü açıldığında ise work iconuna sahip bir gizli dosyanın olduğu görülmektedir.



Tekrardan bu dosyada incelendiğinde ise bu dosyanın ilk bulunan dosya gibi word iconuna sahip ancak 47.7MB boyutunda .exe uzantılı çalıştırılabilir bir dosya olduğu görülmektedir.

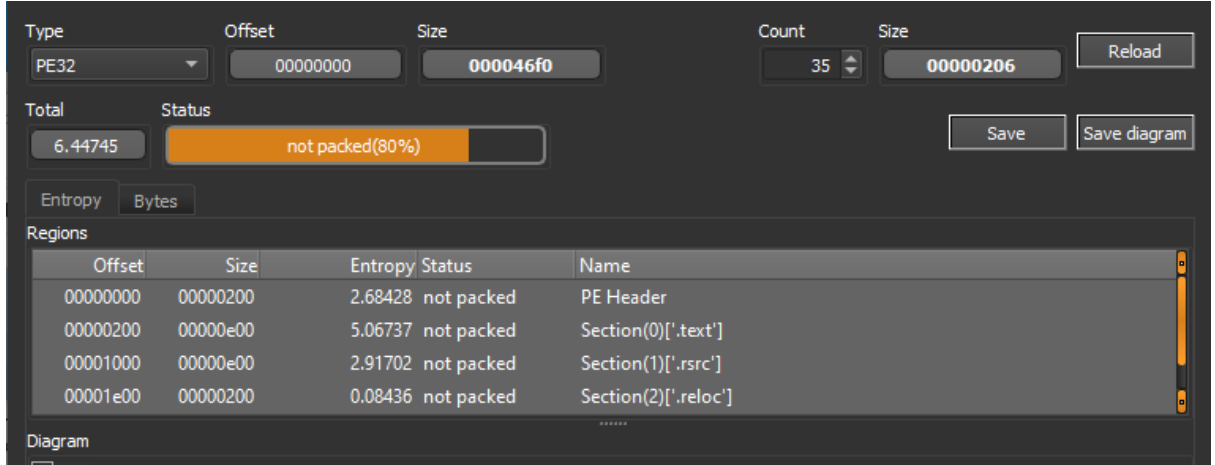
Şekil 5- Word dosyası gibi görünen diğer zararlı dosya

EXECaller.exe Analizi

Statik Analiz

İlk olarak klasör içerisinde bulunan gizli olmayan dosyanın analiz işlemine başlanmıştır.

Adı	Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe
MD5	e50c75046cba3d78eea37cafe11610bb
SHA256	d6549c64b044ec6391dd9cf96307df6234f56c2357f18db5a5246138179cae25
Dosya Türü	PE32 / Exe



Şekil 6- EXECaller'ın paketleme işleminin ve entropy değerinin analizi

Dosyanın statik analizi yapılırken paketleme işleminin yapıp yapılmadı kontrol edilmiştir ve paketleme işleminin yapılmadığı tespit edilmiştir.

The image shows a screenshot of a file analysis tool window titled "Digital Marketing Plan - Face". The window displays two tables of file properties. The first table lists basic file information, and the second table lists more detailed file metadata.

Property	Value
File Name	C:\Users\lucy_\OneDrive\Desktop\Electric Bike Scooter UK Marketing...
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	17.73 KB (18160 bytes)
PE Size	8.00 KB (8192 bytes)

FileDescription	EXECaller
FileVersion	1.0.0.0
InternalName	EXECaller.exe
LegalCopyright	Copyright © 2023
LegalTrademarks	
OriginalFilename	EXECaller.exe
ProductName	EXECaller
ProductVersion	1.0.0.0

Şekil 7- EXECaller üzerinde yapılan statik analiz

Dosyanın statik analizi yapılırken .NET ile yazılmış olduğu görülmektedir. Ardından biraz daha incelendiğinde ise orjinal isminin aslında "EXECaller" olduğu dikkat çekmiştir.

Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\System32\ntdll.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\ntdll.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFile	C:\Windows\Prefetch\DIGITAL MARKETING PLAN - FACE-51AD6557.pf
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	QueryStandardInformationFile	C:\Windows\Prefetch\DIGITAL MARKETING PLAN - FACE-51AD6557.pf
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	ReadFile	C:\Windows\Prefetch\DIGITAL MARKETING PLAN - FACE-51AD6557.pf
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CloseFile	C:\Windows\Prefetch\DIGITAL MARKETING PLAN - FACE-51AD6557.pf

Şekil 8- Zararlının .pf uzantılı dosya oluşturması

EXECaller “C:\\Windows\\Prefetch” dizinine “DIGITAL MARKETING PLAN-FACE-51AD6557” adında .pf uzantılı bir dosya oluşturup bu dosyanın içeriğini okuduğu görülmektedir.

Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\user32.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\win32u.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\gdi32.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\gdi32full.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\msvc_p_win.dll
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Load Image	C:\Windows\SysWOW64\ucrtbase.dll

Şekil 9- Dll yüklemesi

Zararlı dosya, işlemlerini gerçekleştirebilmek için birçok dll dosyasını yüklediği görülmektedir.

Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\loversions.1.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFileMapping	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\loversions.1.db	FILE LOCKED WITH ONLY READERS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	QueryStandardInformationFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\loversions.1.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFileMapping	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\loversions.1.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CloseFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\loversions.1.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	QueryStandardInformationFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFileMapping	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	FILE LOCKED WITH ONLY READERS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	QueryStandardInformationFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CreateFileMapping	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	SUCCESS
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	CloseFile	C:\Users\lucy\AppData\Local\Microsoft\Windows\Caches\{AFBF5F1A-8E69-4C77-AF34-C647E37CA0D9}.1\ver0000000000000004.db	SUCCESS

Şekil 10- Zararlının .db uzantılı birçok database dosyası oluşturması

“C:\\Users*\\AppData\\Local\\Windows\\Caches” dizininde birden fazla .db uzantılı dosya oluşturduğu görülmektedir. Bu dosyaları sadece okuyucu izni ile kilitletiği görülmektedir.

Digital Marketing Plan - Facebook Advertising Campaign 2023 - 1.exe	6924	Process Create	C:\Users\lucy\OneDrive\Desktop\Electric Bike Scooter UK Marketing Project - F\Digital Marketing Plan - Facebook Advertising Campaign 2023 - 2.exe
Digital Marketing Plan - Facebook Advertising Campaign 2023 - 2.exe	4312	Thread Create	

Şekil 11- Zararlı işlemler için yeni bir process oluşturma

Zararlı daha sonra aynı dizinde bulunan diğer .exe uzantılı dosyaları çalıştırmak için yeni bir process oluşturur.

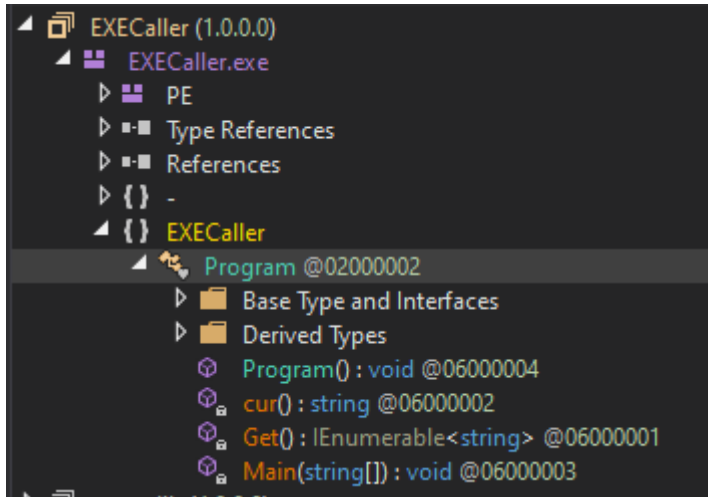
Dinamik Analiz

```
using System.IO;
using System.Linq;

namespace EXECaller
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x0002050 File Offset: 0x0000250
        private static IEnumerable<string> Get()
        {
            List<string> source = Directory.GetFiles(Directory.GetCurrentDirectory()).ToList<string>();
            source = (from x in source
                where true
                select x).ToList<string>();
            return source.ToList<string>();
        }
    }
}
```

Şekil 12- Kod karmaşıklığı analizi

EXECaller dosyasının kaynak kodu incelendiğinde ise kod karmaşıklığı (obfuscate) işleminin uygulanmadığı, fonksiyon ve parametre adlarının direk okunabildiği görülmektedir.



EXECaller dosyasının genel yapısı incelendiğinde tek bir modülün bulunduğu basit bir program olduğu görülmektedir.

Şekil 13- Zararlı dosyanın genel yapısı

```
namespace EXECaller
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x0002050 File Offset: 0x0000250
        private static IEnumerable<string> Get()
        {
            List<string> source = Directory.GetFiles(Directory.GetCurrentDirectory()).ToList<string>();
            source = (from x in source
                where true
                select x).ToList<string>();
            return source.ToList<string>();
        }
    }
}
```

Şekil 14- Dizin içerisinde bulunan dosyaların listelenmesi

Kaynak kodun dinamik analiz işlemi sırasında “Get()” metodu bulunur ve bu metod, mevcut dizindeki tüm dosyaları bulur ve bu dosyaların listesini döndürür.

```
// Token: 0x06000002 RID: 2 RVA: 0x000020A4 File Offset: 0x000002A4
private static string cur()
{
    return AppDomain.CurrentDomain.FriendlyName.Replace('x', 'x');
}
```

Şekil 15- Kaynak kodun analizi

Ardından “cur()” metodu bulunmaktadır. Bu metot mevcut uygulamanın adını alır ve “x” karakterlerini tekrardan “x” karakteri ile değiştirir.

```
// Token: 0x06000003 RID: 3 RVA: 0x000020CC File Offset: 0x000002CC
private static void Main(string[] args)
{
    try
    {
        string value = Program.cur();
        IEnumerable<string> enumerable = Program.Get();
        foreach (string text in enumerable)
        {
            bool flag = text.EndsWith(".exe") && !text.EndsWith(value);
            if (flag)
            {
                Process.Start(new ProcessStartInfo
                {
                    CreateNoWindow = true,
                    FileName = text,
                    WindowStyle = ProcessWindowStyle.Hidden
                });
                Console.WriteLine("Execute " + text);
                break;
            }
        }
    }
    catch (Exception ex)
    {
    }
}
```

Şekil 16- Ana fonksiyonun analizi

Devamında Main fonksiyonu yer almaktadır. Bu fonksiyon incelendiğinde ise try catch yapısı kullanıldığı görülmektedir. Main fonksiyonunda ilk olarak “Get()” metodunu çağırarak mevcut dizindeki tüm .exe uzantılı dosyaları bulur. Ardından mevcut dizinde bulunan tüm .exe uzantılı dosyaları kullanıcı izni olmadan tek tek çalıştırır.

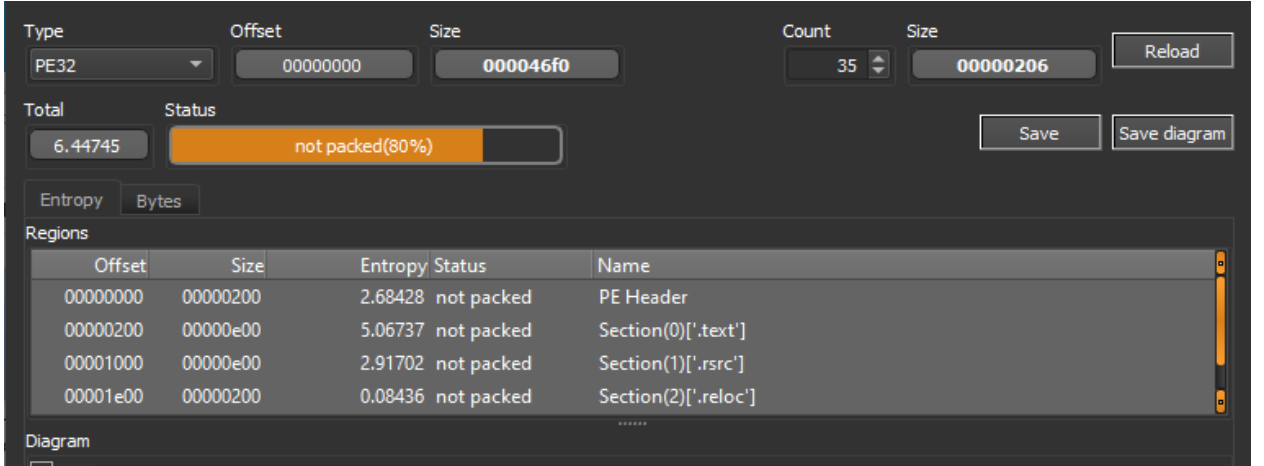
Node.exe Analizi

Ardından aynı dizinde bulunan node.exe olarak adlandırılan gizli dosyanın analizine başlanmıştır.

Adı	Digital Marketing Plan - Facebook Advertising Campaign 2023 - 2.exe
MD5	57339648bb57b052146d70ba601afe71
SHA256	572366fbe92b4cd5d6a753ab0247fdd883b3b118ee0bf2f1d6e1c9e2a debd119
Dosya Türü	PE64 / Exe

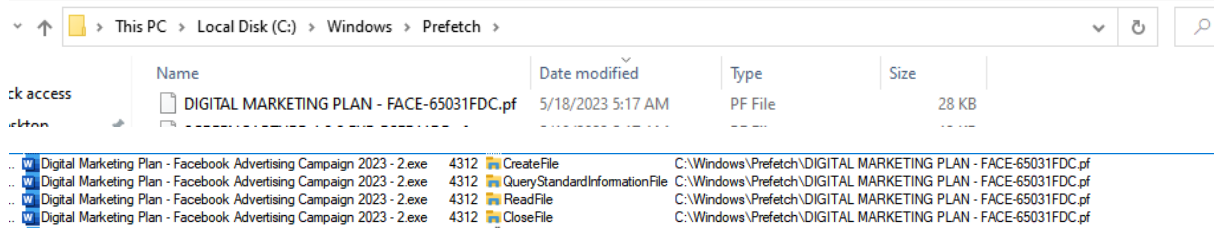
W	Digital Marketing Plan - Fa...	11812	6.35	1.69 MB/s	62.59 MB	LUCY\lucy_	Node.js JavaScript Runtime
ca	conhost.exe	7764	0.06	1.4 kB/s	6.56 MB	LUCY\lucy_	Console Window Host
ca	cmd.exe	3616			4.39 MB	LUCY\lucy_	Windows Command Processor

Şekil 17- Zararlı dosyanın kurban sistemde oluşturduğu process tree



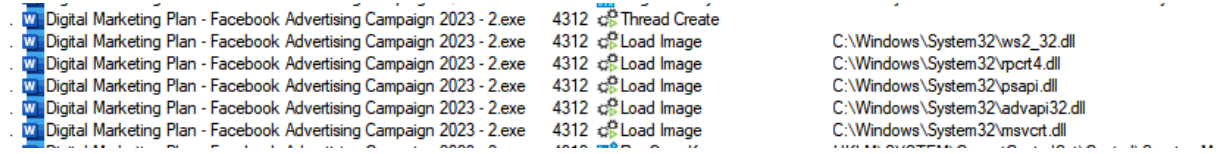
Şekil 18- Ana zararlının paketleme işleminin ve entropi değerinin analizi

Dosyanın statik analizi yapılırken paketleme işleminin yapılıp yapılmadı kontrol edilmiştir ve paketleme işleminin yapılmadığı tespit edilmiştir.



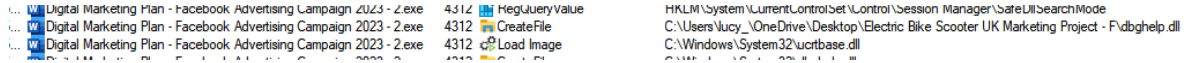
Şekil 19- Zararlının .pf uzantılı dosya oluşturması

Zararlı “C:\\Windows\\Prefetch” dizinine “DIGITAL MARKETING PLAN-FACE-65031FDC” adında .pf uzantılı bir dosya oluşturup bu dosyanın içeriğini okuduğu görülmektedir.



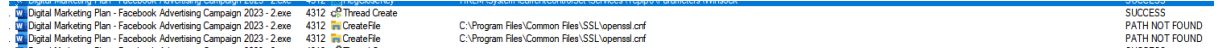
Şekil 20- Zararlının dll yüklemesi

Zararlı dosya, işlemlerini gerçekleştirebilmek için birçok dll dosyasını yüklediği görülmektedir.



Şekil 21- Dll taraması

Zararlı bulunduğu dizinde “dbghelp” gibi birçok farklı dll dosyası aramaktadır ancak aynı dizinde bulunmadığı için NAME NOT FOUND döndürmektedir.



Şekil 22- Openssl üzerinde işlemler

Zararlı dosya, kurban cihazda openssl yapılandırma dosyası olan “openssl.cnf” dosyasını aramaktadır.

Name	Date modified	Type	Size
app.manifest	5/17/2023 4:24 AM	MANIFEST File	1 KB
screenCapture_1.3.2.bat	5/17/2023 4:24 AM	Windows Batch File	14 KB
screenCapture_1.3.2.exe	5/17/2023 4:24 AM	Application	13 KB

Şekil 27- Anlık ekran görüntüsü almak için program yüklemesi yapma

screenCapture_1.3.2.exe	2352	Thread Create	C:\Users\Lucy\AppData\Local\Temp\screenCapture\screenCapture_1.3.2.exe
screenCapture_1.3.2.exe	2380	Load Image	C:\Users\Lucy\AppData\Local\Temp\screenCapture\screenCapture_1.3.2.exe
screenCapture_1.3.2.exe	2380	Load Image	C:\Windows\System32\ntdll.dll
screenCapture_1.3.2.exe	2380	Create File	C:\Windows\Prefetch\SCREENCAPTURE_1.3.2.EXE-B5FB11DE.pf
screenCapture_1.3.2.exe	2380	QueryStandardInformationFile	C:\Windows\Prefetch\SCREENCAPTURE_1.3.2.EXE-B5FB11DE.pf
screenCapture_1.3.2.exe	2380	Read File	C:\Windows\Prefetch\SCREENCAPTURE_1.3.2.EXE-B5FB11DE.pf
screenCapture_1.3.2.exe	2380	Close File	C:\Windows\Prefetch\SCREENCAPTURE_1.3.2.EXE-B5FB11DE.pf

Şekil 28- Anlık ekran görüntüsü alma

Kurban sistemlerde screenCapture adında bir program kurulumu gerçekleştirdiği daha sonra bu programı çalıştırmak için yeni bir process oluşturduğu görülmektedir.

screenCapture_1.3.2.exe	2352	Write File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg
screenCapture_1.3.2.exe	2352	Write File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg
screenCapture_1.3.2.exe	2352	Write File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg
screenCapture_1.3.2.exe	2352	Write File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg
screenCapture_1.3.2.exe	2352	Write File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg
screenCapture_1.3.2.exe	2352	Close File	C:\Users\Lucy\AppData\Local\Temp\2023417-4312-bu91wo.wo1fv.jpg

Şekil 29- Anlık ekran görüntüsü alma

Ardından bu program aracılığı ile kurban sistemin anlık ekran fotoğrafını aldığı tespit edilmiştir.

Network Analizi

192.168.130.152	192.168.130.2	DNS	69 Standard query 0x7dc7 A ipinfo.io
192.168.130.2	192.168.130.152	DNS	85 Standard query response 0x7dc7 A ipinfo.io A 34.117.59.81
192.168.130.152	192.168.130.2	DNS	76 Standard query 0x5299 A api.telegram.org
192.168.130.2	192.168.130.152	DNS	92 Standard query response 0x5299 A api.telegram.org A 149.154.167.220



The screenshot shows the ApatDNS application interface. It has a title bar with the name 'ApatDNS' and standard window controls. Below the title bar, there are two tabs: 'Capture Window' and 'DNS Hex View'. The main content area displays a table with the following data:

Time	Domain Requested	DNS Returned
05:14:28	ipinfo.io	FOUND
05:14:30	ipinfo.io	FOUND
05:14:32	ipinfo.io	FOUND
05:14:34	api.telegram.org	FOUND

Şekil 33- Zararlının kurban sistemde yaptığı DNS sorguları

Zararlı dosya kurban sistemde “ipinfo.io ve “api.telegram.org” domain adreslerine DNS sorgusu yaptığı tespit edilmiştir.

YARA Kuralı

```
import "hash"

rule execaller

{

    meta :

        description = "EXECaller YARA Kuralı"

        author = "InfinitumIT Blue Team"

        file_name = "EXECaller.exe"

        date = "18/05/2023"

        md5 = "e50c75046cba3d78eea37cafe11610bb"

    strings :

        $s1 = "Sectigo Public Code Signing CA R36"

        $s2 = "230505145359Z0?"

        $s3 = "New Jersey1"

        $s4 = "Jersey City1"

        $a_pdb = "EXECaller.pdb"

        $a_url1 = "http://ocsp.comodoca.com0"

        $a_url2 = " https://sectigo.com/CPS0"

        $a_url3 = "8http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y"

    condition: uint16(0) == 0x5A4D and filesize <= 1MB and (any of ($s*) and all
of ($a*))

}
```

```
import "hash"

rule node
{
    meta :

        description = "Node YARA Kuralı"

        author = "InfinitumIT Blue Team"

        file_name = "node.exe"

        date = "18/05/2023"

        md5 = "57339648bb57b052146d70ba601afe71"

    strings :

        $s1 = "@param {number} id"

        $s2 = "@param {number | object} [offsetOrOptions]"

        $s3 = "if (offset == null) {"

        $s4 = "offset = 0;"

        $s5 = "} else {"

        $s6 = "WAVAWH"

        $s7 = "VIA Padlock x86_64 module, CRYPTOGAMS by
<appro@openssl.org>"

    condition: uint16(0) == 0x5A4D and filesize <= 1MB and (any of ($s*))
}
```

MITRE ATTACK TABLOSU

Reconnaissance	Execution	Persistence	Privilege Escalation	Discovery	Credential Access	C&C	Collection
T1595 Active Scanning				T1217 Browser Information Discovery	T1555 Credentials from Password Stores	T1001 Data Obfuscation	T1560 Archive Collected Data
T1592 Gather Victim Host Information				T1083 File and Directory Discovery			T1113 Screen Capture
T1589 Gather Victim Identity Information							T1119 Automated Collection

Çözüm Önerileri

- Güncel ve Lisanslı Bir Antivirüs Yazılımı Kullanın:** Güvenilir bir antivirüs programı kullanmak, trojanları tespit etmek ve temizlemek için önemlidir. Antivirüs yazılımınızı düzenli olarak güncelleyin ve taramaları düzenli olarak yapın.
- İndirmeleri ve E-posta Eklerini Dikkatlice İnceleyin:** Bilinmeyen kaynaklardan veya şüpheli sitelerden dosya indirmekten kaçının. E-posta eklerini dikkatli bir şekilde inceleyin ve tanımadığınız veya güvenmediğiniz kişilerden gelen dosyaları açmayın.
- Yazılımları ve İşletim Sistemini Güncel Tutun:** Güncellemeler, güvenlik açıklarını kapatmak için önemlidir. İşletim sistemi, tarayıcılar, eklentiler ve diğer yazılımlarınızı güncel tutun.
- Güçlü ve Karmaşık Şifreler Kullanın:** Hesaplarınız için güçlü, benzersiz ve karmaşık şifreler kullanın. Şifrelerinizi düzenli olarak değiştirin ve mümkünse iki faktörlü kimlik doğrulama (2FA) kullanın.
- İnternet Bağlantısı ve Wi-Fi Ağınıza Güvence Altına Alın:** Güvenilir bir güvenlik duvarı kullanarak internet bağlantınızı koruyun. Kablosuz ağınıza için güçlü bir şifre kullanın ve varsayılan ayarları değiştirin.
- Güvenilir Kaynaklardan Yazılım İndirin:** Yazılım indirirken resmi ve güvenilir kaynakları tercih edin. Çeşitli yazılım ve oyunları korsan veya şüpheli kaynaklardan indirmek trojan riskini artırır.

