BEDEP

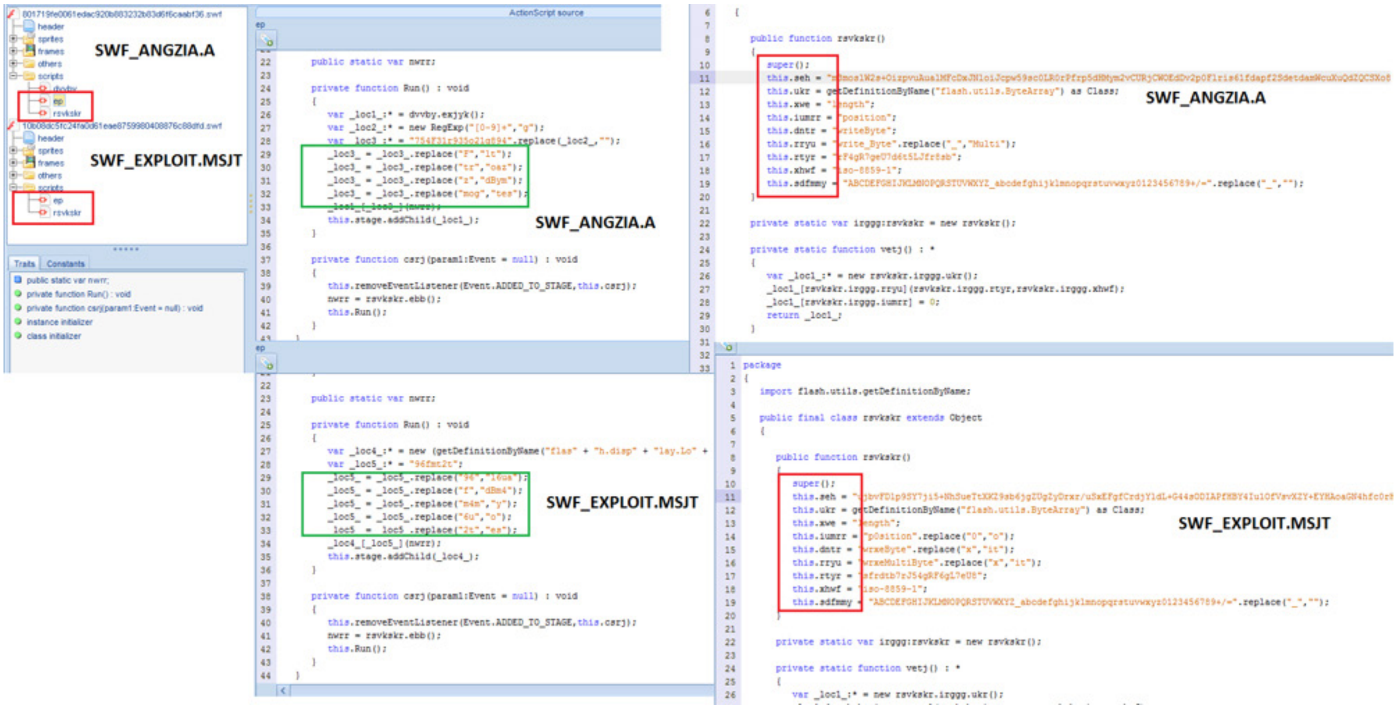
Introduction

Zero-day vulnerability exploit incidents topped the security headlines in late January to early February 2015. The vulnerabilities[1] involved some versions of Adobe® Flash® Player[2] and were discovered to be two different ones. The first incident was designated as CVE-2015-0311[3] and the second incident as CVE-2015-0313.[4]

The first zero-day incident was discovered by security researcher Kafeine[5] and involved malvertisements posted on legitimate sites being used to deliver the exploit to vulnerable systems. Our analysis showed that the Angler exploit kit was used here.

The second zero-day, discovered by Trend Micro, also displayed the same delivery of the threat and exploitation method, with the dailymotion.com, a legitimate site, identified as the hosting site. Certain similarities in the obfuscation method of the exploit delivery initially showed that the Angler. Further analysis, including a feedback from Kafeine, proved that the Hanjuan exploit kit was used in this instance.

The obfuscation method in this case involves the function used to load and execute the exploit loadbyte(). The function itself is obfuscated through string operations. In both attacks, this method is used in near-identical fashion to load the malicious Flash file with the exploit code detected as SWF_ANGZIA.A[6] for the first attack, and SWF_EXPLOIT.MSJT[7] for the second.



```
      public static var nwrr;

      private function Run() : void
      {
         var _loc1_:* = dvvby.exjyk();
         var _loc2_:* = new RegExp("[0-9]+","g");
         var _loc3_:* = "754F31r935o21g894".replace(_loc2_,"");
         _loc3_ = _loc3_.replace("F","lt");
         _loc3_ = _loc3_.replace("tr","oaz");
         _loc3_ = _loc3_.replace("z","dBym");
         _loc3_ = _loc3_.replace("mog","tes");
         _loc1_[_loc3_](nwrr);
         this.stage.addChild(_loc1_);
      }

      private function csrj(param1:Event = null) : void
      {
         this.removeEventListener(Event.ADDED_TO_STAGE,this.csrj);
         nwrr = rsvkskr.ebb();
         this.Run();
      }
   }
```

```
      public static var nwrr;

      private function Run() : void
      {
         var _loc4_:* = new (getDefinitionByName("flas" + "h.disp" + "lay.Lo" +
         var _loc5_:* = "96fmt2t";
         _loc5_ = _loc5_.replace("96","16ua");
         _loc5_ = _loc5_.replace("f","dBm4");
         _loc5_ = _loc5_.replace("m4m","y");
         _loc5_ = _loc5_.replace("6u","o");
         _loc5_ = _loc5_.replace("2t","es");
         _loc4_[_loc5_](nwrr);
         this.stage.addChild(_loc4_);
      }

      private function csrj(param1:Event = null) : void
      {
         this.removeEventListener(Event.ADDED_TO_STAGE,this.csrj);
         nwrr = rsvkskr.ebb();
         this.Run();
      }
   }
```

```
   {

      public function rsvkskr()
      {
         super();
         this.seh = "nJmoslW2s+OizpvuAualMFcDxJNloiJcpw59sc0LR0rPfrp5dHMym2vCURjCWOEdDv2p0Flris61fdapf2SdetdamWcuXuQdZQCSXo8
         this.ukr = getDefinitionByName("flash.utils.ByteArray") as Class;
         this.xwe = "length";
         this.iumrr = "position";
         this.dntr = "writeByte";
         this.rryu = "write_Byte".replace("_","Multi");
         this.rtyr = "rF4gR7geU7d6t5LJfr8sb";
         this.xhwf = "iso-8859-1";
         this.sdfmmy = "ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz0123456789+/=".replace("_","");
      }

      private static var irggg:rsvkskr = new rsvkskr();

      private static function vetj() : *
      {
         var _loc1_:* = new rsvkskr.irggg.ukr();
         _loc1_[rsvkskr.irggg.rryu](rsvkskr.irggg.rtyr,rsvkskr.irggg.xhwf);
         _loc1_[rsvkskr.irggg.iumrr] = 0;
         return _loc1_;
      }
```

```
package
{
   import flash.utils.getDefinitionByName;

   public final class rsvkskr extends Object
   {

      public function rsvkskr()
      {
         super();
         this.seh = "ujbvFDlp9SY7ji5+NhSueTtXKZ9sb6jgZUgZyOrxr/uSxEfgfCrdjYldL+G44sODIAPfHBY4Iu1OfVsvXZY+EYHAoaGN4hfc0rH
         this.ukr = getDefinitionByName("flash.utils.ByteArray") as Class;
         this.xwe = "length";
         this.iumrr = "p0sition".replace("0","o");
         this.dntr = "wrxeByte".replace("x","it");
         this.rryu = "wrxeMultiByte".replace("x","it");
         this.rtyr = "sfrdtb7rJ54gRF6gL7eU8";
         this.xhwf = "iso-8859-1";
         this.sdfmmy = "ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz0123456789+/=".replace("_","");
      }

      private static var irggg:rsvkskr = new rsvkskr();

      private static function vetj() : *
      {
         var _loc1_:* = new rsvkskr.irggg.ukr();
```

Figure 1. Similar obfuscation methods between two recent zero-days

Another similarity is the malware used as a payload. The payload in both attacks have been identified as BEDEP,[8] a malware family whose main purpose is advertising fraud, turning any system it infects into a member of its botnet.

This report provides an in-depth technical description of the malware BEDEP.

Threat Details

BEDEP was first spotted in September 14, 2014. Identified as backdoor malware, BEDEP's malicious routines include advertising fraud and downloading of other malicious files onto an affected system. From our analysis, we believe that its main purpose is to induct the system it infects into a botnet, most likely to perform other malicious activities (besides advertising fraud).Attackers can even command vulnerable Dynamic Host Configuration Protocol (DHCP) server to execute arbitrary code on client systems.

Arrival Routine and Concealment Method

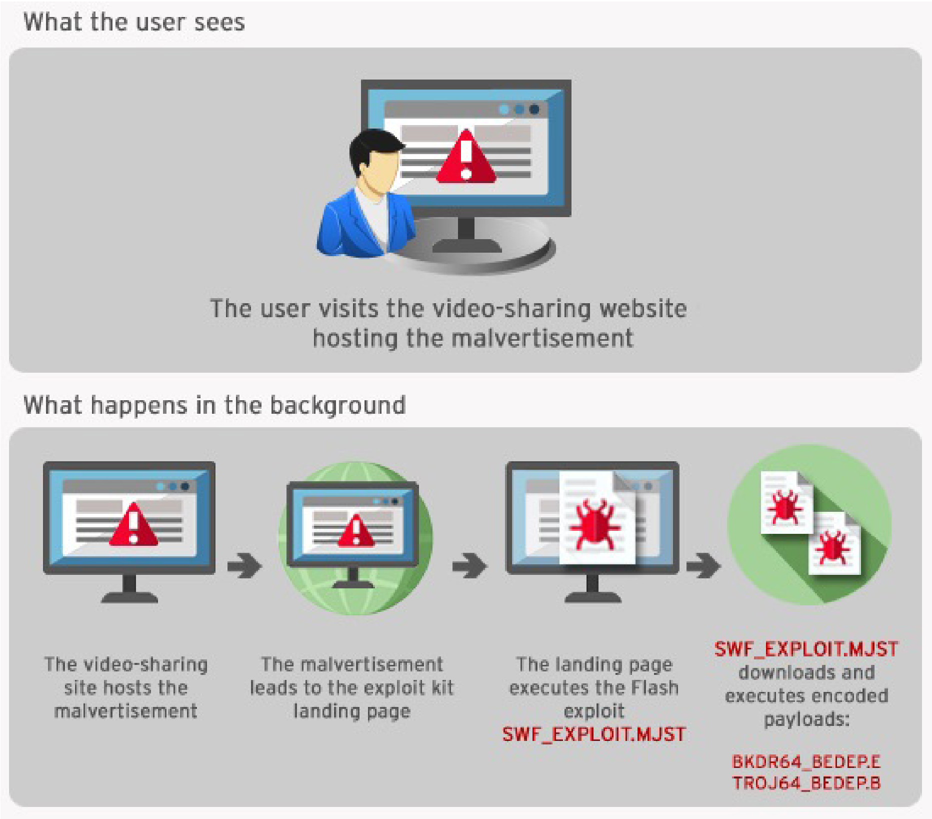

What the user sees
The user visits the video-sharing website hosting the malvertisement
What happens in the background
The video-sharing site hosts the malvertisement
The malvertisement leads to the exploit kit landing page
The landing page executes the Flash exploit SWF_EXPLOIT.MJST
SWF_EXPLOIT.MJST downloads and executes encoded payloads:
BKDR64_BEDEP.E
TROJ64_BEDEP.B

Figure 2. How BEDEP arrives

BEDEP usually arrives into systems either as the final payload of a malvertisement attack (as described in the January 2014 zero-day Flash vulnerability incidents) or by being downloaded by a potentially unwanted application (PUA)[9] installer. PUAs are software that may not harbor malicious code but could expose a user to threats like information theft or other downloaded malware.

In the first method, a system is infected when its user unwittingly visits a site that hosts malvertisements. The malvertisement then leads the user to a landing page hosting the exploit, which in turn, downloads BEDEP strains onto vulnerable systems, specifically, BKDR64_BEDEP.E[10] and TROJ64_BEDEP.E. These downloaded BEDEP strains are then executed without user authorization. The exploit file is detected in the Angler attack as SWF_ANGZIA.A and SWF_EXPLOIT.MJST.

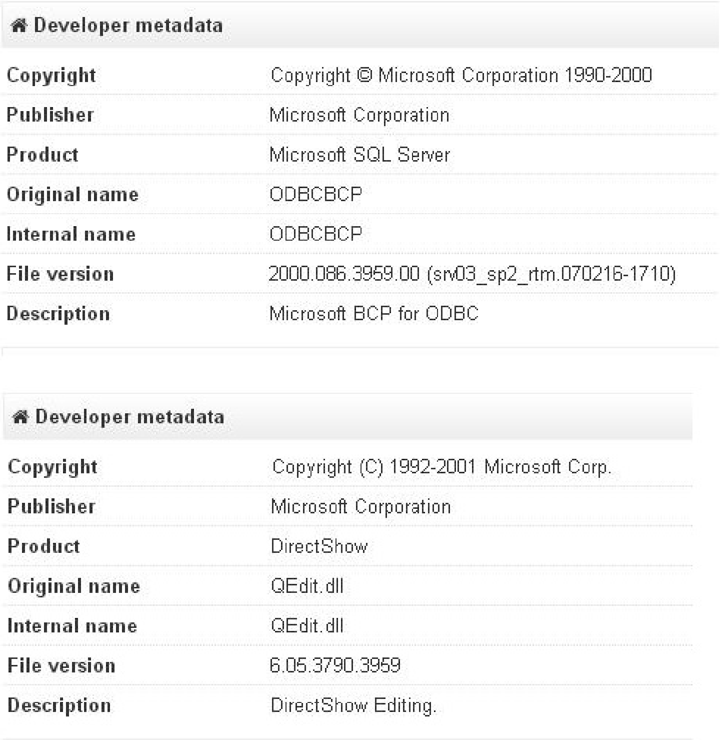
As for the second method, it is downloaded along with other component files by PUA/grayware that is voluntarily downloaded and installed by the user. The downloaded component file is discovered to be of the .DLL variety and bore the file name rifa.dll.

BEDEP and its strains are known to skirt detection because of its heavy encryption. It also comes manipulated Microsoft file properties to make it appear legitimate upon inspection.

Arrival Routine and Concealment Method

BEDEP strains feature the following malicious routines:

- Malicious code injection into processes (explorer.exe and iexplore.exe).
- Download and execute arbitrary code
- Connect to malicious URLs/remote malicious users
- Post stolen system information (build ID, bot ID, processor and OS version) to its C&C servers
- Update itself



Developer metadata

Copyright	Copyright © Microsoft Corporation 1990-2000
Publisher	Microsoft Corporation
Product	Microsoft SQL Server
Original name	ODBCBCP
Internal name	ODBCBCP
File version	2000.086.3959.00 (srv03_sp2_rtm.070216-1710)
Description	Microsoft BCP for ODBC

Developer metadata

Copyright	Copyright (C) 1992-2001 Microsoft Corp.
Publisher	Microsoft Corporation
Product	DirectShow
Original name	QEdit.dll
Internal name	QEdit.dll
File version	6.05.3790.3959
Description	DirectShow Editing.

Figure 3. BEDEP's fake Microsoft file properties

BEDEP also has the ability to distinguish the processor of the system it is infecting, installing either 32-bit or 64-bit variant, whichever is suitable. This bypasses the security measures of 64-bit versions and ensure that the execution of the malicious routines takes place.

Impact

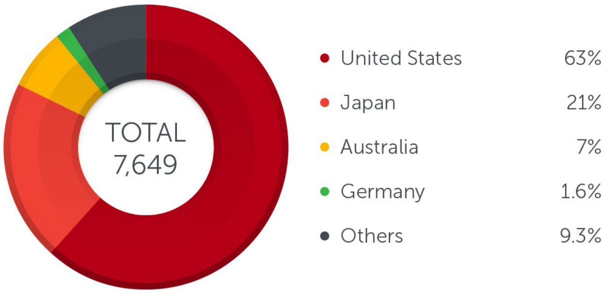


Figure 4. Total BEDEP infection count from November 2014 to February 2015

From November 2014 to February 2015, we kept track of BEDEP's infection count worldwide, taking into account all BEDEP strains currently in the wild, including their 32-bit and 64-bit variants. What we discovered:

- The U.S. is region with the highest number of infections during the four-month tracking period.

- Japan is the next hardest hit, with over 21% of the total infection count.

- The spike in infection count takes place in January and extends to February, accounting for more than half of total infections.

The peak in BEDEP's infection count in January can be attributed to the Adobe Flash zero-day vulnerability events, as well as the usage of the Angler exploit kit that takes advantage of the vulnerability itself. We can also look at this as proof of the effectiveness of the infection method used: malvertisements hosted on popular video-hosting websites. Delivering exploits through malvertisements is not a new tactic, but being able to lead users to a malicious URL without any interaction from the users' part makes this technique a serious threat.

Solutions and Recommendations

Properly configured endpoint solutions can ensure the prevention of BEDEP coming into the machine or network it's connected to.

Components of OfficeScan™ Endpoint Protection,[11] such as such as SmartScan, Web Reputation Service, Behavior Monitoring, and Smart Feedback offer the best protection against BEDEP by detecting malicious files.

Worry-Free™ Business Security/Services (WFBS/WFBS-SVC)[12] is also equipped with technologies that detect and remove BEDEP in infected machines and networks.

Some best practices that can be adopted to prevent BEDEP infection:

- **Think before you click**. Reckless browsing behavior often leads to a compromised online experience.

- **Update and patch**. Updating software is usually a baseline best practice for enterprise and home users. However, if the situation allows, disabling the vulnerable software (such as Flash in this instance) may be more advisable until the patch that addresses the vulnerability comes out.

- **Stay tuned**. Be in-the-know of the latest forms of infection used by cybercriminals. Read up on the latest in online security. This would give you a firm grasp on what to do to stay away from becoming a victim.

Trend Micro customers are protected from BEDEP and the elements that lead to its infection.

References

1. Weimin Wu. (January 22, 2015). *TrendLabs Security Intelligence Blog.* “Flash Greets 2015 With New Zero-Day.” Last accessed March 09, 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/flash-greets-2015-with-new-zero-day/.

2. Peter Pi. (February 02, 2015). *TrendLabs Security Intelligence Blog.* “Trend Micro Discovers New Adobe Flash Zero-Day Exploit Used in Malvertisements.” Last accessed March 09, 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements/.

3. The MITRE Corporation. (2015). *CVE.* “CVE-2015-0311.” Last accessed March 09, 2015, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0311.

4. The MITRE Corporation. (2015). *CVE.* “CVE-2015-0313.” Last accessed March 09, 2015, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0313.

5. Kafeine. (January 2015). *Malware Don’t Need Coffee.* “Unpatched Vulnerability (0day) in Flash Player Is Being Exploited by Angler EK.” Last accessed March 09, 2015, http://malware.dontneedcoffee.com/2015/01/unpatched-vulnerability-0day-in-flash.html.

6. Trend Micro Incorporated. (2015). *Threat Encyclopedia.* “SWF_ANGZIA.A.” Last accessed March 09, 2015, http://about-threats.trendmicro.com/malware.aspx?language=au&name=SWF_ANGZIA.A.

7. Trend Micro Incorporated. (2015). *Threat Encyclopedia.* “SWF_EXPLOIT.MJST.” Last accessed March 09, 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/SWF_EXPLOIT.MJST.

8. Trend Micro Incorporated. (2015). *Threat Encyclopedia.* “Putting Issues of BEDEP to Bed.” Last accessed March 09, 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/148/putting-issues-of-bedep-to-bed.

9. Trend Micro Incorporated. (2015). *Glossary.* “Potentially Unwanted App.” Last accessed March 09, 2015, http://www.trendmicro.com/vinfo/us/security/definition/potentially-unwanted-app.

10. Trend Micro Incorporated. (2015). *Threat Encyclopedia.* “BKDR64_BEDEP.E.” Last accessed March 09, 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR64_BEDEP.E.

11. Trend Micro Incorporated. (2015). *OfficeScan - Endpoint Protection.* Last accessed March 09, 2015, http://www.trendmicro.com/us/enterprise/product-security/officescan/.

12. Trend Micro Incorporated. (2015). *Worry-Free Business Security Services.* Last accessed March 09, 2015, http://www.trendmicro.com/us/small-business/product-security/worry-free-services/.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

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.

TREND MICRO™

Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll-free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003