virus BULLETIN Covering the global threat landscape

BETA EXPLOIT PACK: ONE MORE PIECE OF CRIMEWARE FOR THE INFECTION ROAD!

Aditya K. Sood
Michigan State University, USA

Rohit Bansal
Independent Security Researcher, USA

Browser exploit packs (BEPs) or exploit kits are used extensively in drive-by download attacks to infect target systems on the Internet. BEPs are used to distribute advanced malware to end-user systems after exploiting vulnerabilities in browsers' components or embedded plug-ins. BEPs are hosted on compromised domains and victims are coerced into visiting those domains either through spear phishing or through URLs shared on social networks and so on. On visiting a compromised domain, the victim's browser is fingerprinted and if a vulnerable component is found, the respective exploit is served and malware is downloaded onto the system. In previous papers, we have presented details of the BlackHole [1], Sweet Orange [2] and Styx [3] BEPs to highlight their design and tactics. Several of the techniques used by Beta Browser Exploit Pack (Beta BEP) are very similar to those used by these exploit packs.

Beta BEP (which is unrelated to the Beta bot) is the latest exploit kit in development. At BlackHat USA 2014 [4], we discussed several fundamental weaknesses in the command and control (C&C) panels used by various pieces of crimeware. The idea of that research was to look for potential issues in web-based C&C panels and to reveal how to find security flaws in them in order to gather intelligence. It came as no surprise that we were able to find our way into a Beta BEP C&C panel and gather some intelligence about the structure and working of the Beta exploit pack. The author of the exploit pack did revoke and take down the panel shortly after we had found our way in, but not before we had extracted some meaty details from it.

We have been studying this exploit pack and gathering data for several weeks now – publishing delays are an unavoidable part of the process of releasing intelligence. Meanwhile, we discovered that another researcher had released an analysis of a very similar exploit kit under the name of 'Sundown EK' [5]. In his analysis, the researcher covered details of the network traffic and how the infection is triggered. He reported certain things that are very similar to what we found in our analysis of Beta BEP, as well as some that are slightly different:

1. The BEP under discussion in this article is sold in the underground market under the name of 'Beta'; the one analysed in [5] has been given the name 'Sundown' by the researcher who discovered it. The analysis of Sundown covers the BEP's initial testing URLs, which is why the exploits used and URL structure are similar in nature to those we see in Beta.

2. In [5], the version of Sundown analysed is '0.1a', whereas we analysed version 3.0 of Beta BEP. The author of the exploit kit actually claims Beta as copyleft (a method of making software free so that it can be modified and extended by other developers, thereby maintaining the 'free software' clause). We are not sure that copyleft makes any sense in the context of software that is sold in the underground market, and if source code is shared it will be modified accordingly.

3. The Sundown exploit kit is still under development and it appears that the author is testing it for effectiveness. We have not encountered any real-time cases of Beta BEP version '3.0' being used in the wild, but since it is also in a testing phase, we believe that it will be running live somewhere privately. We tried to access the configured URLs we found in the C&C but all of the domains had been taken down and no active infection URLs were detected.

4. The rental price of Beta BEP is between $2,000 per month and $100 per day.

As a research community, it's always good practice to collaborate and share intelligence so that we can tackle issues in a more granular way.

C&C PANEL

Primarily, the Beta BEP consists of the following components:

- A component for collecting statistics on successful infections.
- A component that will upload a malicious executable and check whether it can bypass anti-virus engines.
- A component that is used to configure domains for serving exploits and which checks the domains for potential detection or flagging by anti-virus engines.

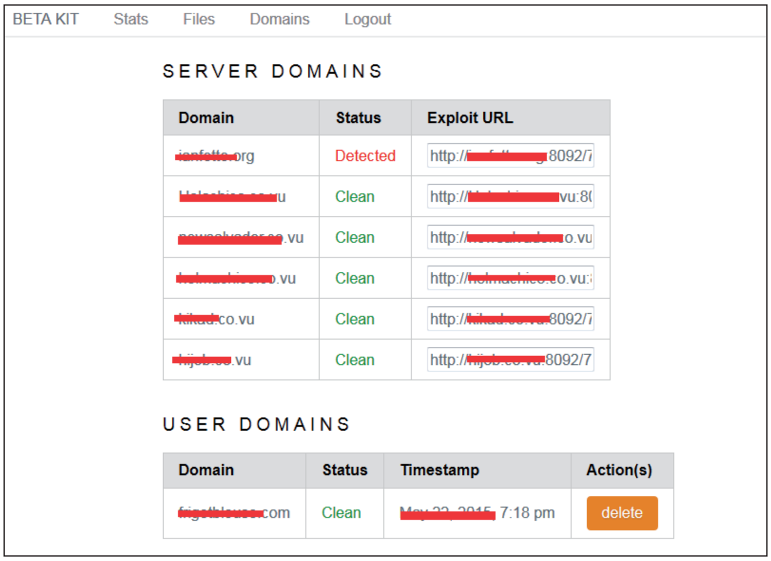
Listing 1 shows the basic structure of the Beta BEP that was configured on the C&C server.

```
http://<beta_cpanel.com>:8092/SDDS/private/panel.php?s
ection=stats
http://<beta_cpanel.com>:8092/SDDS/private/panel.php?
section=files
http://<beta_cpanel.com>:8092/SDDS/private/panel.php?
section=domains
http://<beta_cpanel.com>:8092/SDDS/private/panel.php
```

Listing 1: Beta BEP C&C structural components.

TARGET DOMAIN SCANNING

Beta BEP has a built-in functionality for determining the effectiveness of the domain that is used to deploy the exploit or executable which is served to the victim's machine during an attack. When a vulnerability is found and an exploit successfully executed, the infected domain is queried in order to download the malicious executable. Beta BEP uses Scan4You [6], which is a freely available service that will check the robustness of a target domain (hosting exploits or malicious executables) against various anti-virus engines to verify its rate of detection. The idea is to check up front whether or not the configured exploit URL can be detected as malicious. Avoiding exposure to detection solutions is important in order for the malware to be served in a stealthy manner. If the target domain is found to be included on blacklists or flagged as malicious, a new one can easily be configured by the Beta BEP controller in order to continue



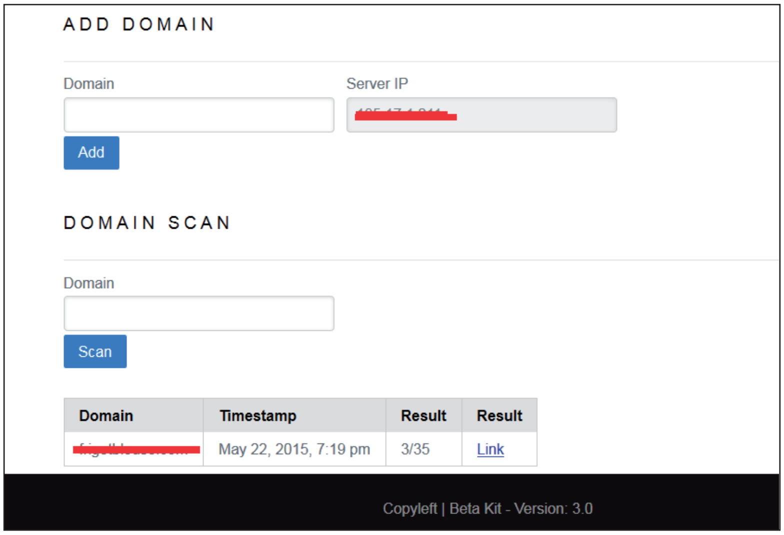
SERVER DOMAINS

Domain	Status	Exploit URL
[redacted]org	Detected	http://[redacted]8092/i
[redacted]u	Clean	http://[redacted]vu:8(
[redacted].vu	Clean	http://[redacted]o.vu
[redacted].vu	Clean	http://[redacted]o.vu:
[redacted]co.vu	Clean	http://[redacted]8092/i
[redacted].vu	Clean	http://[redacted]8092/7

USER DOMAINS

Domain	Status	Timestamp	Action(s)
[redacted]com	Clean	[redacted] 7:18 pm	delete

Figure 1: Target domains are tested against the Scan4You service.



ADD DOMAIN

Domain

Server IP [redacted]

DOMAIN SCAN

Domain

Domain	Timestamp	Result	Result
[redacted]	May 22, 2015, 7:19 pm	3/35	Link

Copyleft | Beta Kit - Version: 3.0

Figure 2: Beta BEP domain-scanning component.

the infection spreading mechanism. Figures 1 and 2 show how Beta BEP scans the target URLs and domains to verify their detection rate by various security vendors.

The structure of the exploit-serving URLs is presented in Listing 2.

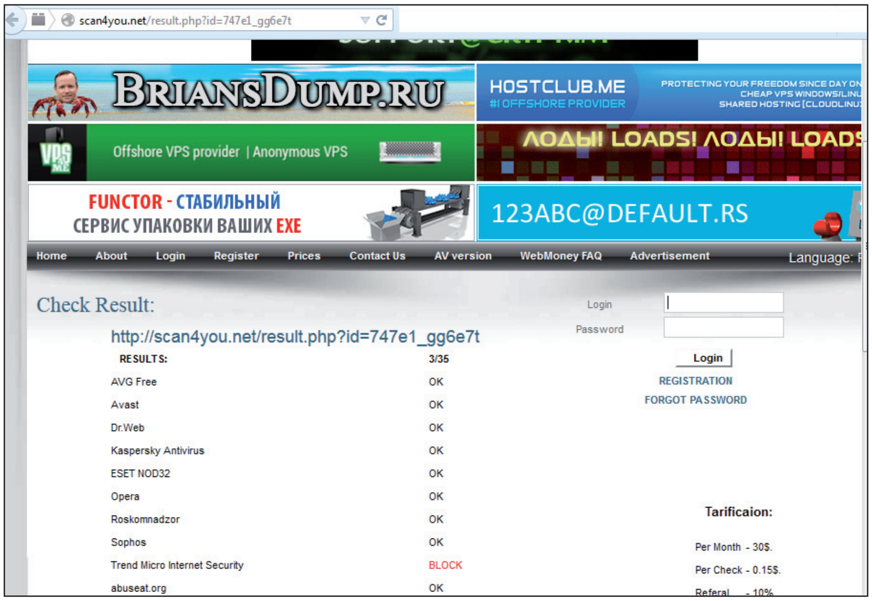
```
http://www.example.com:8092/776576YTU76876867HYTUYTUY
TUYHYTUYHTFY/drgdrfydtuytygtryfgtrfgtrfg.php

http://www.example.org:8092/776576YTU76876867HYTUYTUY
TUYHYTUYHTFY/drgdrfydtuytygtryfgtrfgtrfg.php

http://example.co.vu:8092/776576YTU76876867HYTUYTUYTU
YHYTUYHTFY/drgdrfydtuytygtryfgtrfgtrfg.php
```

Listing 2: Structure of exploit-service URLs.

Part of the URL uses an encoding scheme, but we are not sure what type of encoding is used. Incorporating obfuscated strings into URLs is a technique commonly used by BEPs in order to bypass certain detection solutions. Figure 3 shows one of the configured domains being tested for maliciousness using the Scan4You service.

MALICIOUS EXECUTABLE SCANNING

Beta BEP allows only one file at a time to be uploaded to the C&C, which then gets compressed and embedded in the required exploit. At this point, it seems that multiple malware files are not supported: if the malicious executable needs to be replaced, the previous executable (or binary)



Check Result:

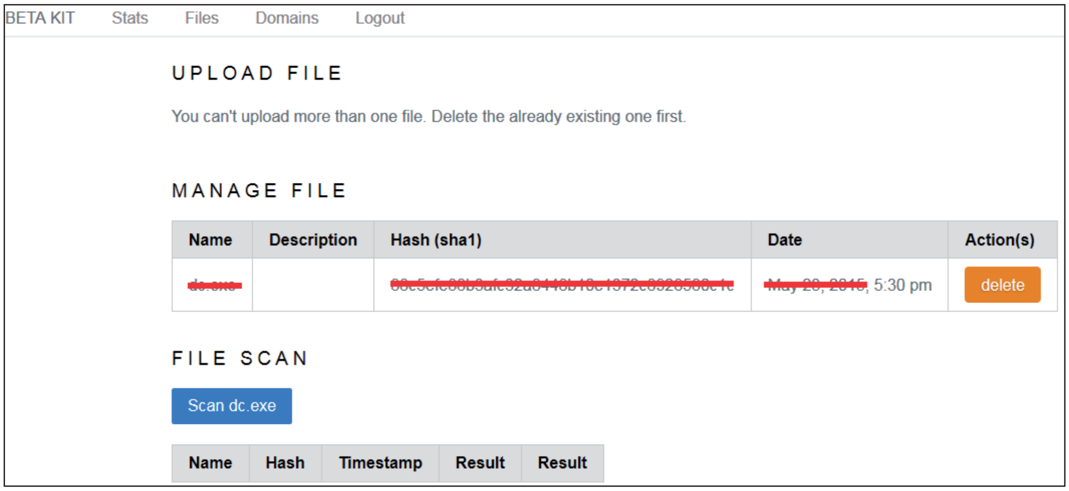
http://scan4you.net/result.php?id=747e1_gg6e7t

RESULTS:	3/35
AVG Free	OK
Avast	OK
Dr.Web	OK
Kaspersky Antivirus	OK
ESET NOD32	OK
Opera	OK
Roskomnadzor	OK
Sophos	OK
Trend Micro Internet Security	BLOCK
abuseat.org	OK

Tarificaion:

Per Month - 30$.
Per Check - 0.15$.
Referal - 10%

Figure 3: Scan4You service in action.



UPLOAD FILE

You can't upload more than one file. Delete the already existing one first.

MANAGE FILE

Name	Description	Hash (sha1)	Date	Action(s)
[redacted]		[redacted]	[redacted], 5:30 pm	delete

FILE SCAN

Name	Hash	Timestamp	Result	Result

Figure 4: File uploading and scanning capability in Beta BEP.

file must be deleted and cleaned in order to provide a clean environment for the new executable to be incorporated into the exploits. Like the exploit-serving URLs, the uploaded malware executable is scanned to check its rate of detection by anti-virus engines. Figure 4 shows the file uploading and scanning functionality of Beta BEP.

EXPLOITS FOR SPECIFIC VULNERABILITIES

Table 1 shows the exploits that are supported by Beta BEP as part of its design. There is the possibility for more exploits to be added and/or existing exploits removed later on. As can be seen from the CVEs, Flash exploits are preferred. This is because of the recent rise in the number of remote code execution vulnerabilities in Flash.

INFECTION STATISTICS

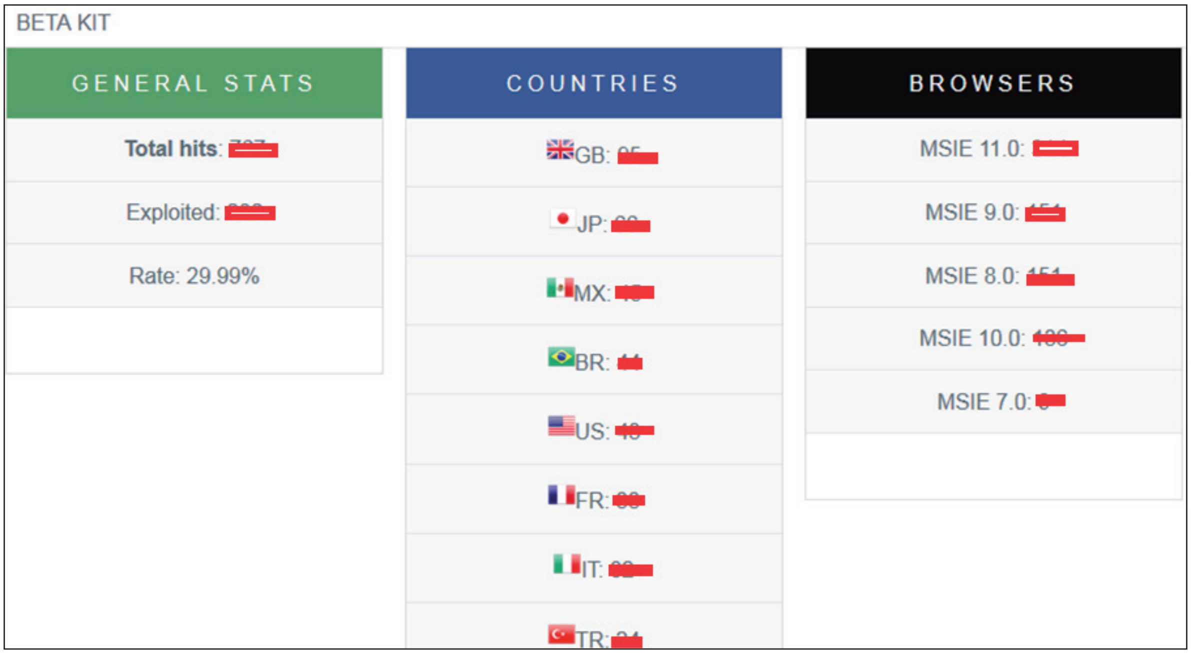
We know that most crimeware service providers rent out BEPs to collect money based on successful pay-per infections (PPI). However, BEPs can also be sold directly for a lump sum. We found that Beta BEP collects the following statistics:

- Information about compromised browsers
- Details of the countries in which successful infections have triggered, which means that geo-location tagging is enabled in Beta BEP
- Numbers of successful infections (or exploited end-user machines), hit rate and so on.

Figure 5 shows a snapshot taken from the Beta BEP deployment.

S. No.	CVEs	Description
1	CVE-2015-0311	Unspecified vulnerability in *Adobe Flash Player* through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on *Windows* and *OS X* and through 11.2.202.438 on *Linux* allows remote attackers to execute arbitrary code via unknown vectors.
2	CVE-2015-0359	Double free vulnerability in *Adobe Flash Player* before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on *Windows* and *OS X* and before 11.2.202.457 on *Linux* allows attackers to execute arbitrary code via unspecified vectors.
3	CVE-2015-0313	Use-after-free vulnerability in *Adobe Flash Player* before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on *Windows* and *OS X* and before 11.2.202.442 on *Linux* allows remote attackers to execute arbitrary code via unspecified vectors.
4	CVE-2014-0556	Heap-based buffer overflow in *Adobe Flash Player* before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on *Windows* and *OS X* and before 11.2.202.406 on *Linux*, *Adobe AIR* before 15.0.0.249 on *Windows* and *OS X* and before 15.0.0.252 on *Android*, *Adobe AIR* SDK before 15.0.0.249, and *Adobe AIR* SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors.
5	CVE-2014-6332	OleAut32.dll in OLE in *Microsoft Windows Server 2003 SP2*, *Windows Vista SP2*, *Windows Server 2008 SP2* and *R2 SP1*, *Windows 7* SP1, *Windows 8*, *Windows 8.1*, *Windows Server 2012 Gold* and *R2*, and *Windows RT Gold* and *8.1* allows remote attackers to execute arbitrary code via a crafted website, as demonstrated by an array-redimensioning attempt that triggers improper handling of a size value in the SafeArrayDimen function, a.k.a. 'Windows OLE Automation Array Remote Code Execution Vulnerability'.
6	CVE-2012-1876	*Microsoft Internet Explorer* 6 through 9, and 10 Consumer Preview, does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by attempting to access a nonexistent object, leading to a heap-based buffer overflow, a.k.a. 'Col Element Remote Code Execution Vulnerability'.

Table 1: Exploits provided in Beta BEP 3.0.



BETA KIT

GENERAL STATS	COUNTRIES	BROWSERS
Total hits: [redacted]	GB: [redacted]	MSIE 11.0: [redacted]
Exploited: [redacted]	JP: [redacted]	MSIE 9.0: [redacted]
Rate: 29.99%	MX: [redacted]	MSIE 8.0: [redacted]
	BR: [redacted]	MSIE 10.0: [redacted]
	US: [redacted]	MSIE 7.0: [redacted]
	FR: [redacted]	
	IT: [redacted]	
	TR: [redacted]	

Figure 5: Beta BEP stats panel.

CONCLUSION

As we have discussed, Beta BEP is not as active in the real market as, for example, Fiesta or Angler, but we believe that we will start to see it being used in the coming months. We were not able to collect enough data to dissect the network-level details of the BEP and understand how exactly the exploits are served, but we believe that revealing as much information as we know about Beta BEP will benefit the security research community, making researchers aware of the upcoming threat so that appropriate defences can be designed and put in place to combat it.

REFERENCES

[1] Browser Exploit Packs – Death with Bundled Exploits. http://www.virusbtn.com/pdf/conference/vb2011/VB2011-Sood-Enbody.pdf.

[2] What are browser exploit kits up to? A look into Sweet Orange and ProPack. https://www.virusbtn.com/virusbulletin/archive/2013/03/vb201303-SweetOrange-ProPack.

[3] Styx Exploit Pack: Insidious Design Analysis. https://www.virusbtn.com/virusbulletin/archive/2013/09/vb201309-Styx.

[4] Exploiting fundamental Weaknesses in Botnet C&C Panels. https://www.blackhat.com/docs/us-14/materials/us-14-Sood-What-Goes-Around-Comes-Back-Around-Exploiting-Fundamental-Weaknesses-In-Botnet-C&C-Panels-WP.pdf.

[5] Fast look at Sundown EK. http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html.

[6] Scan4You. http://scan4you[.]net.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

© 2015 Virus Bulletin Ltd, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP, England.
Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/