

RBN - New and Improved Storm Botnet for 2008

Obviously the Russian Business Network (RBN) is working overtime during the Christmas and New Year holiday, no doubt planning for many in the ISP security and anti-spam arena to be on skeleton staff.

Many will now have already seen reports of the Storm Botnet outbreak which started on December 24th “MerryChristmasDude” with good write up at ComputerWorld and for technical details at ISC Sans or HolisticInfoSec (links on footer). This picture is changing rapidly and by December 26th there were new web sites “Uhavepostcard” , “HappyCards2008” and no doubt more to come over the next few days.

Three of the key web sites have the following registrant information, all registered via “ANO REGIONAL NETWORK INFORMATION CENTER DBA RU (Russia)” in chronological order:

Domain Name: MERRYCHRISTMASDUDE.COM - Creation Date: Nov 27 2007

Domain Name: UHAVEPOSTCARD.COM - Creation Date: Dec 23 2007

Domain Name: HAPPYCARDS2008.COM - Creation Date: Dec 26 2007

The key objective for the RBN is to rebuild the Storm Botnet which is shown in various reports over the last few months, from a few million enslaved PCs to more recently a few 100,000’s. One can only further guess as to what the RBN’s main goal is to use a rebuilt Storm Botnet for, e.g. earlier DDOS (Denial of Service attack) on Estonia.

There are some interesting elements concerning which make this attack innovative:

Although much of that detected is conventional spam, however there is also a large amount of spam which is getting through many anti-spam defenses due to the use of “fake” BlogSpot (Blogger) links for example on a small sample;

```
hxxp://dantipXXXX.blogspot.com/?soapwierzpordeecaspewtkk153trajspeak  
hxxp://isakovkapitonXXXX.blogspot.com/?harkwierzpordeecaspewtkk153trajfloor
```

The common part of the suffix is “pewtkk153traj” which redirects to Geocities web sites and then a further redirect to the Storm exploit domains.

Although most have identified as the Zhelatin Storm email worm or variant, it is also as the more recent fake codec downloads, dependent upon where the unfortunate user has come from. This now shows a “polymorphic” format, i.e. the virus or exploit has the ability to alter its signature in an attempt to combat anti-virus tools.

The fast-flux technique used to avoid detection in this case is actually "double-flux"; characterized by multiple nodes within the network registering and de-registering their addresses (see sample maps below taken within one hour periods and show the fast-flux DNS changes). It is also safe to say this newer Storm Network has now also has improved defense mechanisms, if examined too closely.

Computerworld - Storm Worm Christmas

Computerworld - Storm New Year

ISC Sans - Anticipated Storm

HolisticInfoSec