Hunting down crackstorage.com R2

01.12.2009 R2 (intermediate release, *not finished!*)
Peter Kleissner

http://crackstorage.com/ is the largest hoster for cracks and keygens. When searching for them from sites like http://keygens.nl/ they link to crackstorage.com for the download. http://crackstorage.net/ is an exact mirror of the site. They look like:

crackstorage.com - Terms and Conditions

crackstorage.com is a social project that hosts public freeware files. All files are uploaded by internet surfers and are shared for free.

If you are going to abuse on any content on crackstorage.com you ARE NOT ALLOWED to enter and use crackstorage.com.
If you are going to post a complaint on crackstorage.com you ARE NOT ALLOWED to enter and use crackstorage.com.
If you post any abuse on crackstorage.com that means that you violated crackstorage.com terms and condidtions.
If you produce any complaint against crackstorage.com that means that you violated crackstorage.com terms and condidtions because you are not allowed to enter and use crackstorage.com if you are going to produce any abuses.

Anyway, If you think that some file breaks certain regulations, please send us an email and we will immediately remove it. Email can be found here.
DMCA - Content Removal

Their site is unchanged since February 2008 and was introduced in January 2008.

The text contains a spelling mistake (see below), there stands "condidtions" instead of conditions.

---

crackstorage.net - Terms and Conditions

crackstorage.net is a social project that hosts public freeware files. All files are uploaded by internet surfers and are shared for free.

If you are going to abuse on any content on crackstorage.net you ARE NOT ALLOWED to enter and use crackstorage.net.
If you are going to post a complaint on crackstorage.net you ARE NOT ALLOWED to enter and use crackstorage.net.
If you post any abuse on crackstorage.net that means that you violated crackstorage.net terms and condidtions.
If you produce any complaint against crackstorage.net that means that you violated crackstorage.net terms and condidtions because you are not allowed to enter and use crackstorage.net if you are going to produce any abuses.

Anyway, If you think that some file breaks certain regulations, please send us an email and we will immediately remove it. Email can be found here.
DMCA - Content Removal

How they stay out of court

1) crackstorage.com hosts only cracks

   ⇨ They say if you abuse them, you violate their terms.
   ⇨ They put an inactive removal email address to comply with DMCA.
   ⇨ When downloading a crack, you have to check the "agree to the terms" box.

2) Other sites only index those cracks (they say "files")

   ⇨ They say they only index files automatically.
   ⇨ They put their servers outside the U.S. where DMCA does not apply.
   ⇨ Only for private purposes, no commercial running of the site.

Additionally it is important to say that crackstorage.com has protected their cracks, so that only partner sites can link to their cracks (they pass an identifier). So whatever their partners are doing, it is crackstorage.com call.

For the DMCA see http://crackstorage.net/dmca.php, where the inactive email address removal@crackstorage.com is offered.

Technical protection of cracks

When downloading cracks, for example "Snow for Windows" (http://keygens.nl/crack/71759/), it will pass a hash and a crack identifier to the crackstorage.com website:

```
<h2>Crack download from KEYGENS.NL<br>Snow for Windows.zip</h2><form
method="post" action="http://crackstorage.net/get_uploaded_file.php"><input
type="hidden" name="download" value="063eab4ec7dc128f1e2ef7ec5f464181"
/><input type="hidden" name="id" value="1078147"><input type="submit"
name="Submit" value="Download Crack and Keygen"></form><h2>
```

The crack identifier is in this case 1078147 and identifies the crack, the 32 byte value is an encoded value that identifies the crack search engine and the time. The crack id remains always the same; the hash is calculated new on every site refresh. For example:

```
download                              id
707d02508ed8901757fb8d1ad4fa5c7a      1078147
1e8bd657759314ae1bf8a6d8730e17a4      1078147
aa9d3bf8478eaa78cc97287cc3a6daaf      1078147
c2b0dcd7d98360b13a5db6426ae51e09      1078147
a09d0c52d922aa32f2b08f2263cbb0af      1078152
```

They expire.

Crackstorage.com does not check the referrer; if, then they could deny completely downloading cracks linked from non-authorized sites. The above code is from keygens.nl and looks in html as:

```
It`s free and safe to use all cracks and keygens downloaded from KEYGENS.NL
So download Snow for Windows.zip keygen or crack then unzip it to any folder and run to
crack Snow for Windows.zip There are no viruses or any exploits on this site, you are on
keygen server optimized for surfer.

Crack download from KEYGENS.NL
Snow for Windows.zip

  Download Crack and Keygen

Direct download Snow for Windows


The time of Snow for Windows.zip crack or keygen download page generation is more than
zero seconds. Use downloaded crack with keygen and have a fun, but if you like cracked
software - buy it ;)
```

This protection is actually a nice thing and effective against crack-site copiers, so they are able to secure their own business.

When being at http://crackstorage.net/get_uploaded_file.php, the website asks for entering a captcha code and for agreeing to their terms and condition:

The "Use this link" address is resolved from the hash (!) passed with the HTML POST, NOT from the HTML referrer. This requires the crackstorage.com website to have a solid database behind, which indexes all cracks and legitimate crack sites.

The source of the above HTML form is:

```
Snow for Windows.zip<form method="post"
action="/get_uploaded_file.php"><input type="hidden" name="gdid"
value="1078147"><input type="hidden" name="download"
value="fa24042e2bff097bf8d571961c6b5110" /><br><input type="hidden"
name="ssname" value="" /><br><table border=0 width=25% cellspacing=0
cellpadding=0><tr><td bgcolor="#000000"><table border=0 width=100%
cellspacing=1 cellpadding=3><tr><td bgcolor="#CCCCCC" align=middle>Input
verification number:<br><b>ATTENTION! You have only one attempt!</b><br><img
src= "/cap/key.php?key=1078147"><br><input size="15" type="text"
name="check"><br></td></tr></table></td></tr></table><input type="checkbox"
name="agreed" >Check this box if you agree with crackstorage.net <a href="/"
target="_blank"><strong>Terms and Conditions</strong></a><br><input
type="submit" name="Submit" value="Download File"></form><br><table border=0
width=100% cellspacing=0 cellpadding=0><tr><td bgcolor="#000000"><table
border=0 width=100% cellspacing=1 cellpadding=3><tr><td bgcolor="#CCCCCC"
align=middle>Use this link <a
href="http://keygens.nl/crack/71759/">http://keygens.nl/crack/71759/</a> to
link to this
download.</td></tr></table></td></tr></table><br><br>Partners:<br>
```

When manually visiting the captcha generation site (http://crackstorage.com/cap/key.php?key=1078147), it will always show the same captcha number for a crack:

                      etc.

This would make it easy to resolve the number by a program. The hash you see in the source above is exactly the same calculated as when linking to the download site.

If you go normally to http://crackstorage.net/get_uploaded_file.php, without the referrer it will show you:

Link expired. You came here through improper link.You must search at first the file you need on any site linked below.

Partners:
www.astalavista.ms
www.crack.ms
serialcrackz.com

Link expired = hash is no longer valid (expired). Those partners are only few of many authorized ones.

When you want to make your own crack site (like keygens.nl), you will have to break the 32-byte hash creator that validates the referrer. Once the hash generation algorithm is known, the whole crackstorage.com database can be dumped automatically (by requesting all cracks and URLs with crack identifier and according hash).

In some first tests I could use the calculated hash by crackstorage.com and go to the download site linked from my site and download directly the crack linked from my site. This means it would be possible to dump all cracks using "stolen" hashes from a crackstorage.com partner (and just exchanging the crack identifiers).

The crackstorage.com website is quite small, there could only be following visible files figured out:

> http://crackstorage.com/index.php
> http://crackstorage.com/dmca.php
> http://crackstorage.com/mysite.css
> http://crackstorage.com/get_uploaded_file.php
> http://crackstorage.com/cap/key.php
> removal@crackstorage.com

crackstorage.net is an exact (backup) copy of crackstorage.com.

Contacts

Their current registrant, administrative, technical and billing contact is:

```
Registration Service Provided By: RESELLERCLUB
Contact: +1.4152361970

Domain Name: CRACKSTORAGE.COM

Registrant:
    VPN Solutions Inc.
    Bill Chase        (fusionmadrgd@yahoo.com)
    Chillingston str. 29
    Beijing
    null,657023
    CN
    Tel. +1.4730222

Creation Date: 19-Jan-2008
Expiration Date: 19-Jan-2010

Domain servers in listed order:
    ns1.p8.ru
    ns2.p8.ru
```

Of course that is a fake address, company, name and mail address. I sent a mail to the yahoo mail address and got only a failure notice back:

```
<fusionmadrgd@yahoo.com>:
98.137.54.237 failed after I sent the message.
Remote host said: 554 delivery error: dd Sorry your message to
fusionmadrgd@yahoo.com cannot be delivered. This account has been disabled or
discontinued [#102]. - mta195.mail.sp2.yahoo.com
```

Also the removal@crackstorage.com did not work (the server did not accept the SMTP connection).

What domaintools.com knows about crackstorage.com:

- "VPN Solutions Inc." owns about 31 other domains
- fusionmadrgd@yahoo.com is a contact on the whois record of 31 domains
- 3 registrars have maintained records for this domain since 2008-01-19
- This domain has changed name servers 2 times over 1 year.
- Hosted on 5 IP addresses over 1 years.
- View 47 ownership records archived since 2008-01-20 .
- 17 other web sites are hosted on this server.

The very first who-is record was privacy protected, and registered with EstDomains (which was called to be in connection with the Russian Business Network and hosting illegal contents). On June 28 2008 the who-is information was changed from privacy protection to the above fake info.

Some information robtex.com knows about crackstorage.com:

DNS Records

base	record	name	ip	reverse	route	as
crackstorage.com	a		212.63.206.51	(none)	212.63.192.0/19	AS30880
	ns-soa	ns1.p8.ru	80.93.56.4		80.93.56.0/21	AS35569
	ns	ns1.p8.ru	80.93.56.4			
		ns2.p8.ru	80.93.48.54		80.93.48.0/21	AS35295

ip numbers of host
212.63.206.51

hostnames sharing ip with a-records
crack.ms
cracksfm.com
dutchserials.nl
www.crack.ms
www.cracksfm.com
www.crackstorage.com

nameservers used by this domain
ns1.p8.ru
ns2.p8.ru

domains sharing nameservers
1016.ru
1pointmsc.com
adamast.ru
astalavista.ms
atlasreal.ru
atlight.com
avda.ru
baget.ru
bishelp.ru

ip numbers of nameservers
80.93.48.54
80.93.56.4

reverse names of the nameservers
ns1.p8.ru
ns2.p8.ru

other names of the nameservers
nserv2.cracklook.com

domains sharing nameservers under another name
clean-cracks.com

subdomains
www.crackstorage.com

The mail address fusionmadrgd@yahoo.com was used for 46 other domains, including serialkey.net, flirtoccasions.com, clickandclick.org.

If you review the countries where crackstorage (.com and .net) were hosted, you will find out that only Netherlands and Sweden were and are used (presumably because of the law there).

Conclusion

Their site is technically cool and designed very well, including their full-backup design with crackstorage.net. It is low cost and very effective. They do not provide any valid contact possibility for crackstorage.com directly, so you can get only over their partner sites in contact with them.

For me it is personally interesting that no one yet tried to takedown crackstorage.com, normally huge software companies make complaints at the FBI, and then they investigate and try to take down at least the domains.

- not finished –

Some open questions: Who is behind this? In which country does crackstorage.com origins? It is hosted in Netherlands, however has the DMCA notice. (In Europe no one cares about DMCA)

The site probably origins from a country in middle Europe and the people behind have good connections to people in the U.S., so they included the DMCA notice (and did not want stress with FBI).

How to contact them?
There is no way over the crackstorage.com website. Probably only over the partners.

Which sites use crackstorage.com?
Currently open

Where does the money flow?
Currently open

Todo: changing title to "Hacking crackstorage.com" ;)