Trik Spam Botnet Leaks 43 Million Email Addresses

bleepingcomputer.com/news/security/trik-spam-botnet-leaks-43-million-email-addresses/

Catalin Cimpanu

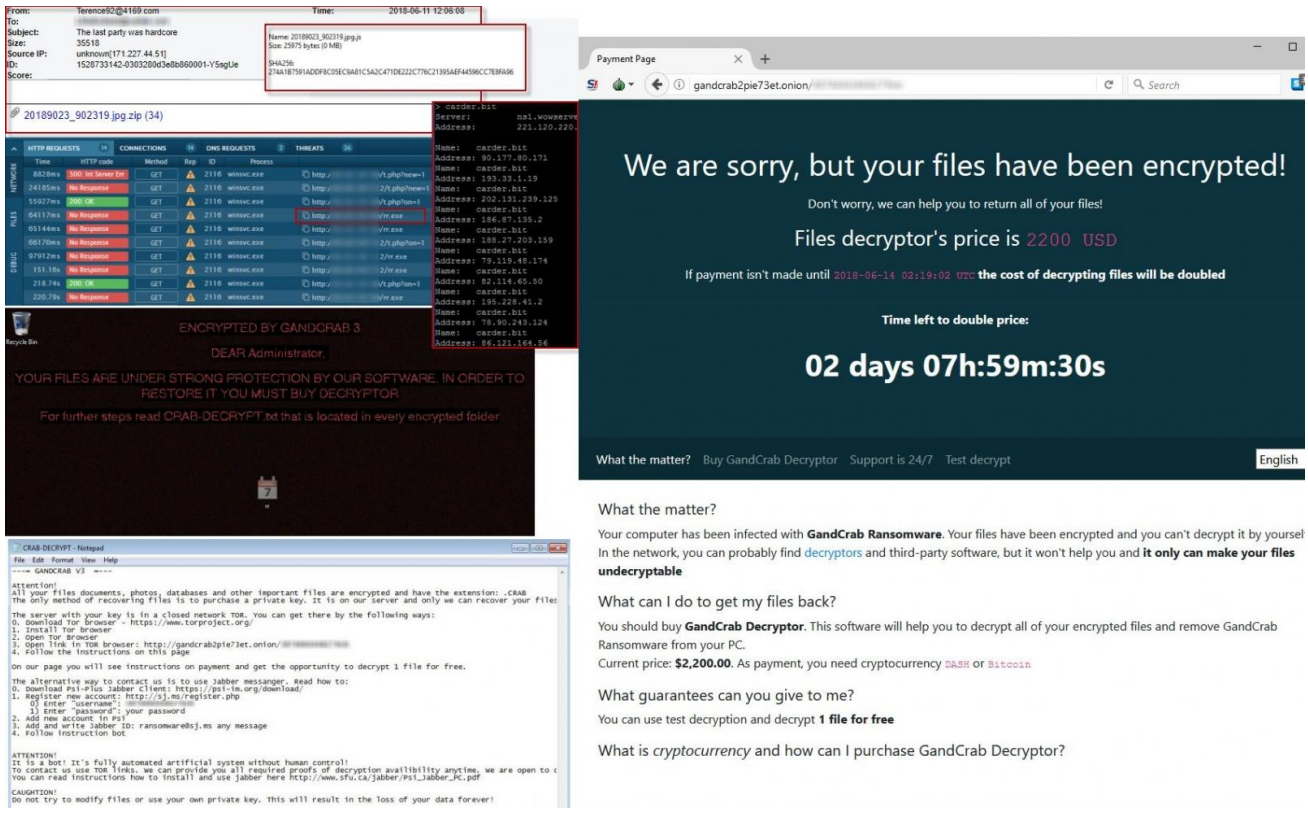
By
Catalin Cimpanu

- June 12, 2018
- 11:22 AM
- 3

Over 43 million email addresses have leaked from the command and control server of a spam botnet, a security researcher has told Bleeping Computer today.

The leaky server came to light while a threat intelligence analyst from Vertek Corporation, was looking into a recent malware campaign distributing a version of the Trik trojan, which was later infecting users with a second-stage payload —the GandCrab 3 ransomware.

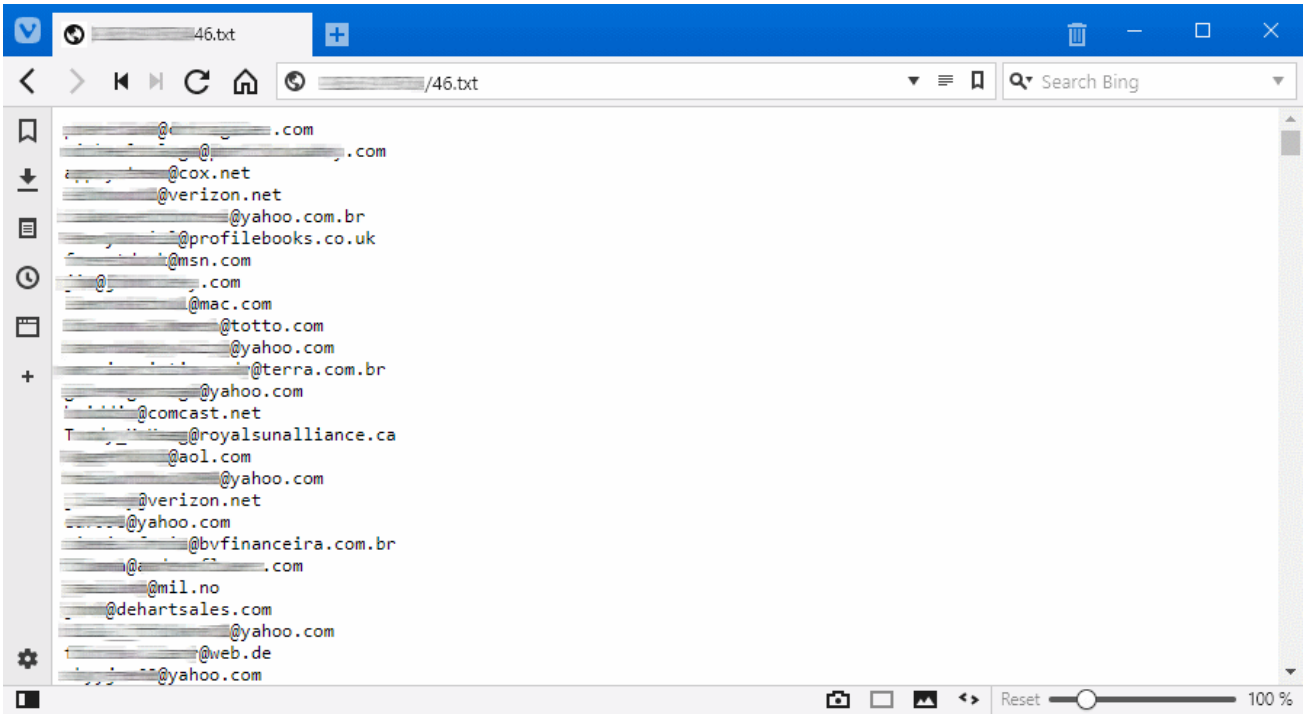
The Vertek researcher discovered that Trik and GandCrab would download the malicious files that infected users' systems from an online server located on a Russian IP address.



The researcher told Bleeping Computer that the group behind this operation misconfigured its server and left its content accessible to anyone accessing the IP directly.

On this server, he discovered 2201 text files, labeled sequentially from 1.txt to 2201.txt containing chunks of roughly 20,000 email addresses, each.

The Vertek researcher believes the operators of this server have been using these recipient lists to service other crooks who contracted their services to distribute various malware strains via malspam campaigns.



Server leaks 43,555,741 unique email addresses

"We pulled all of them to validate that they are unique and legitimate," the researcher told Bleeping Computer earlier today. "Out of 44,020,000 potential addresses, 43,555,741 are unique."

The researcher is now working with Australian security expert Troy Hunt, the owner of the Have I Been Pwned service, to determine how many of these emails are new and how many have been previously leaked in other data dumps.

"The email addresses are from everywhere," the researcher told us. " There were 4.6 million unique email domains. Everything from .gov to .com, and domain of several private businesses."

The Vertek researcher has analyzed the files and broke down the email addresses per domain. In a list the researcher shared with us earlier today (embedded at the bottom of this article), he points out that the vast majority of email addresses are old, from antiquated email services such as Yahoo (10.6 million) and AOL (8.3 million).

Surprisingly, while there are many custom email domains included in the leak, there are very few Gmail addresses included, suggesting the email addresses database is either incomplete, or this malware campaign intentionally targeted users using older email services.

The Trik trojan

The Trik trojan is a classic malware downloader. It infects computers and assembles them into a giant botnet. The botnet's operators use these computers to send out new spam campaigns, or they sell "install space" to other crooks, allowing them to deliver more pontent threats to Trik victims, similarly to how they rented install space to the GandCrab crew for the campaign Vertek stumbled on.

The Trik trojan has been an active threat for at least a decade but has recently seen a resurgence, according to this Proofpoint report.

In its earlier days, the malware operated primarily as a worm that self-spread via removable USB storage devices, Skype, or Windows Live Messenger chats. These worm-based variants had previously been tracked under the name of Phorpiex.

The malware evolved into a fully-fledged trojan years later, when it forked the codebase of the SDBot trojan and started using email spam as its main delivery & infection mechanism, while also switching to an IRC-controlled botnet architecture.

Trik is not the first spam botnet to leak its email addresses database. In August 2017, a spam operation known as Onliner leaked 711 million email addresses that it was using to spam users.

At the time of writing, the Trik C&C server that's leaking email addresses keeps going offline at intermittent intervals.

Top 100 email domains included in the leaked data:

```
8907436 yahoo.com
8397080 aol.com
 788641 comcast.net
 433419 yahoo.co.in
 432129 sbcglobal.net
 414912 msn.com
 316128 rediffmail.com
 294427 yahoo.co.uk
 286835 yahoo.fr
 282279 verizon.net
 244341 bellsouth.net
 234718 cox.net
 227209 earthlink.net
 221737 yahoo.com.br
 191098 ymail.com
 174848 att.net
 156851 btinternet.com
 139885 libero.it
 120120 yahoo.es
 117175 charter.net
 112566 mac.com
 111248 mail.ru
 107810 juno.com
  92141 optonline.net
  86967 yahoo.ca
  78964 me.com
  73341 yahoo.com.ar
  71545 yahoo.in
  71200 rocketmail.com
  69757 wanadoo.fr
  68645 rogers.com
  65629 yahoo.it
  65017 shaw.ca
  64091 ig.com.br
  63045 163.com
  62375 uol.com.br
  57764 free.fr
  57617 yahoo.com.mx
  57066 web.de
  56507 orange.fr
  56309 sympatico.ca
  54767 aim.com
  51352 cs.com
  50256 bigpond.com
  48455 terra.com.br
  43135 yahoo.co.id
  41533 netscape.net
  40932 alice.it
  39737 sky.com
  39116 yahoo.com.au
  38573 bol.com.br
  38558 YAHOO.COM
  37882 excite.com
  37788 mail.com
  37572 tiscali.co.uk
```

```
37361 mindspring.com
37350 tiscali.it
36636 HOTMAIL.COM
36429 ntlworld.com
34771 netzero.net
33414 prodigy.net
33208 126.com
32821 yandex.ru
32526 planet.nl
32496 yahoo.com.cn
31167 qq.com
30831 embarqmail.com
30751 adelphia.net
30536 telus.net
30005 hp.com
29160 yahoo.de
28290 roadrunner.com
27558 skynet.be
26732 telenet.be
26299 wp.pl
26135 talktalk.net
26072 pacbell.net
26051 t-online.de
25929 netzero.com
25917 optusnet.com.au
25897 virgilio.it
25525 home.nl
25227 videotron.ca
24881 blueyonder.co.uk
24462 peoplepc.com
24435 windstream.net
24079 xtra.co.nz
23465 bluewin.ch
23375 us.army.mil
22433 hetnet.nl
22247 trainingelite.com
22021 yahoo.com.sg
21689 laposte.net
21336 ge.com
21130 frontiernet.net
21055 q.com
21034 mchsi.com
20882 webtv.net
20830 abv.bg
19425 insightbb.com
```

Related Articles:

Emotet botnet switches to 64-bit modules, increases activity

Microsoft detects massive surge in Linux XorDDoS malware activity

Phishing websites now use chatbots to steal your credentials

Fake crypto sites lure wannabe thieves by spamming login credentials

HTML attachments remain popular among phishing actors in 2022

- Botnet
- Data Leak
- Email
- GandCrab
- MalSpam
- Trik

Catalin Cimpanu

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

- Previous Article
- Next Article

Comments

NoseyNick - 3 years ago

I had an email address in this leak. It was a unique email address previously used ONLY at linkedin, before the linkedin breach (https://www.troyhunt.com/observations-and-thoughts-on-the-linkedin-data-breach). I suspect the linkedin leak was merged into the Trik Spam Botnet list.

- 

  KitchenTable - 3 years ago

  -
  -

  Can someone please file a GDPR complaint so the EU can start taking 4% of TrickBot's revenues?

- 

  Denis_11 - 3 years ago

  -
  -

  https://twitter.com/denis_miftakhov/status/1021400784632655874

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: