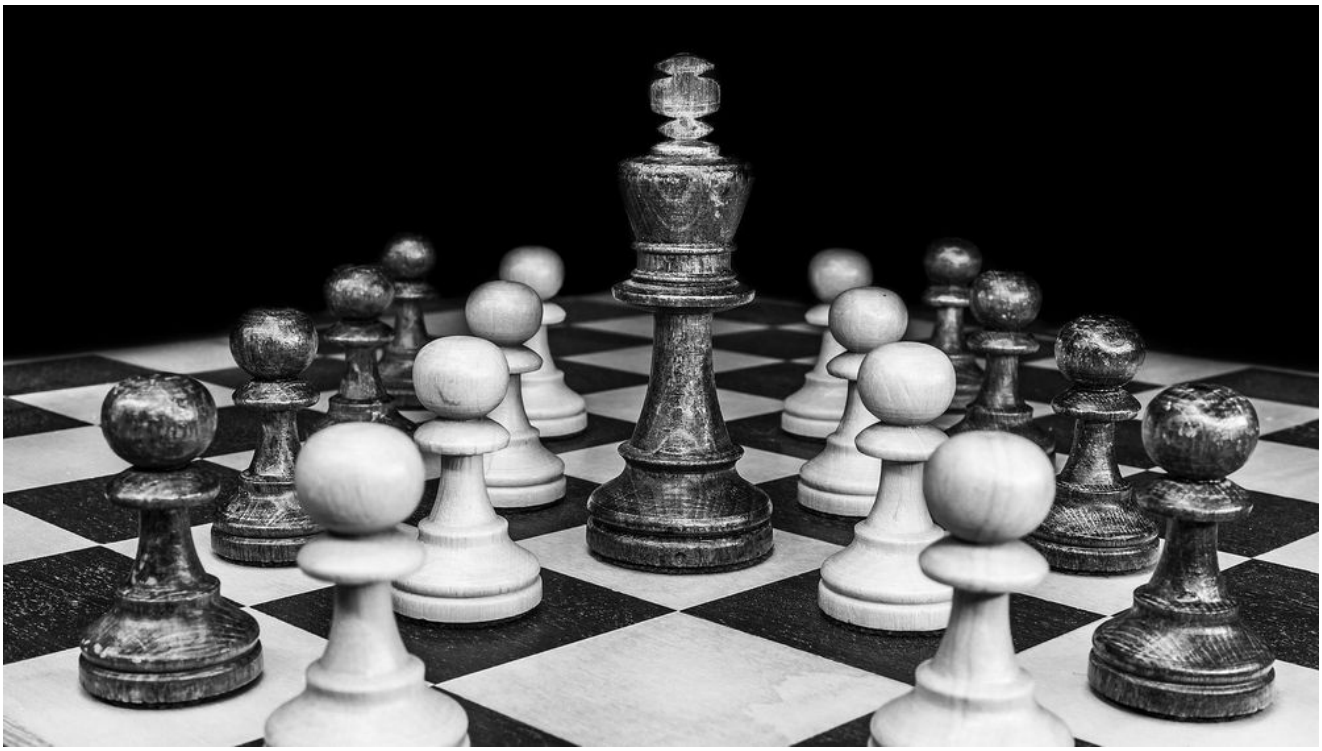
TrickBot is Dead. Long Live TrickBot!

labs.bitdefender.com/2020/11/trickbot-is-dead-long-live-trickbot/

Anti-Malware Research
4 min read



TrickBot still crawls despite law enforcement kneecapping operation. It's operators are scrambling to restore the botnet back to its former glory, Bitdefender researchers have found. An analysis of samples reveals updated communication mechanisms, new C2 infrastructure that uses Mikrotik routers, and packed modules

TrickBot has arguably been one of the most popular Trojans for the past couple of years, used by threat actors mostly because of its modular design and highly resilient infrastructure. Bitdefender researchers even analyzed one of its modules earlier this year, particularly because it targeted telecom, education, and financial services in the US and Hong Kong.

However, when Microsoft decided to take down TrickBot before the US elections, fearing the massive botnet could be used to thwart the voting process in some way, the endeavor proved to be more like a "kneecapping" operation rather than cutting the hydra's heads. This was likely a short-term tactic, potentially just to make sure that TrickBot wouldn't cause any issues during the elections.

Key Findings:

- Mikrotik routers used as C&C servers
- Version update responses are digitally signed with bcrypt for some
- Plugin sever list no longer contains hidden services

The group behind TrickBot seems to have actively pushed new versions of the Trojan and maintained the full list of modules used in previous versions. However, in the recently analyzed samples, it seems that the shareDll – or mshareDll in its packed version – was no longer present. In fact, now there's only the shareDll, which is packed, with mshareDll completely removed. This probably indicates that TrickBot operators are moving away from unpacked modules, cleaning up their list of lateral movement modules to only use packed ones.

Versioning

Before Trickbot's takedown, the latest known version was `1000513`, from **August 19, 2020**. However, on **November 3rd**, we found the new "`2000016`" version that seems to feature all the improvements mentioned above. TrickBot operators seem to have then settled on going back to the original format, but resetting the versioning. Consequently, the latest version we've found is now "`100003`", available from November 18.

C&C infrastructure

In terms of communication between victims and C&Cs, TrickBot update responses seem to have been digitally signed using `bcrypt`, potentially in an effort to impede future takedowns. This particular improvement ensures that each new update for TrickBot is legitimate. This particular behavior was observed for the `2000016` version, but not for the `100003` version.

The C&C servers for the "`100003`" version seem to involve only the use of Mikrotik routers:

IP	COUNTRY
103.131.157.161	BD
103.52.47.20	ID
102.164.206.129	ZA
103.131.156.21	BD
103.150.68.124	Not found
103.30.85.157	ID
103.131.157.102	BD

103.146.232.5	Not found
103.156.126.232	Not found

Another interesting change is that, among the updated C&C sever list, there's also an EmerDNS domain used as a backup in case no known C&C server responds. What's interesting about this particular domain is that the EmerCoin key (`EeZbyqoTUrr4TpnBk67iApX2Wj3uFbACbr`) used to administer the server, also administers some C&C servers that belong to the Bazar backdoor. The analyzed sample (`82e2de0b3b9910fd7f8f88c5c39ef352`) uses the `morganfreeman.bazar` domain, which has the 81.91.234.196 IP address and running `Mikrotik v6.40.4` .

Plugin server configuration

There are also some major differences between the lists of plugin server configurations, as seen below:

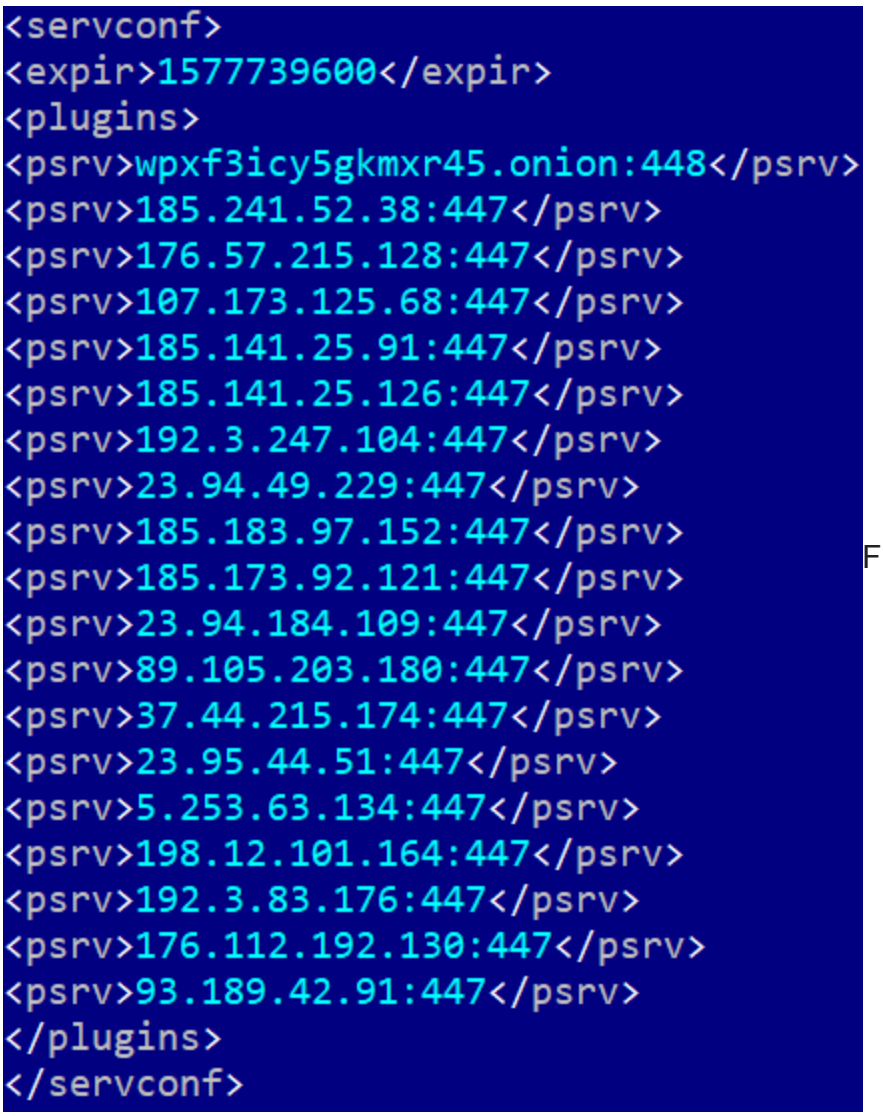


Fig. 1 – Previous versions of TrickBot plugin server configurations

```
<servconf>
<expir>1609459199</expir>
<plugins>
<psrv>185.163.47.182:447</psrv>
<psrv>94.140.115.91:447</psrv>
<psrv>95.153.31.186:447</psrv>
<psrva>151.23.11.124:7459</psrva>
<psrva>74.152.136.52:4477</psrva>
<psrva>57.145.60.143:44218</psrva>
<psrva>61.36.42.237:4008</psrva>
</plugins>
</servconf>
```

Fig. 2 – New versions of TrickBot plugin server configurations

IP	COUNTRY
156.96.62.82	US
62.108.34.45	DE
185.234.72.248	DE
195.123.241.206	US
194.5.249.216	RO
195.123.240.238	US
46.21.153.247	US
195.123.241.207	US
156.96.119.28	US

TrickBot operators have apparently eliminated the Tor plugin services and have added the new `<psrva>` tags, which seem to be obfuscated IPs, a technique also used by the Bazar backdoor. Although these look like legitimate IP address, they're not.

The `<srva>` tag appears to only be used for C&C servers, a number that seems to have been reduced considerably compared to previous TrickBot versions.

Victims of the new version

Based our own telemetry, the most reports from systems that have encountered this new version of TrickBot seem to involve connections from Malaysia, followed by the United States, Romania, Russia and Malta.

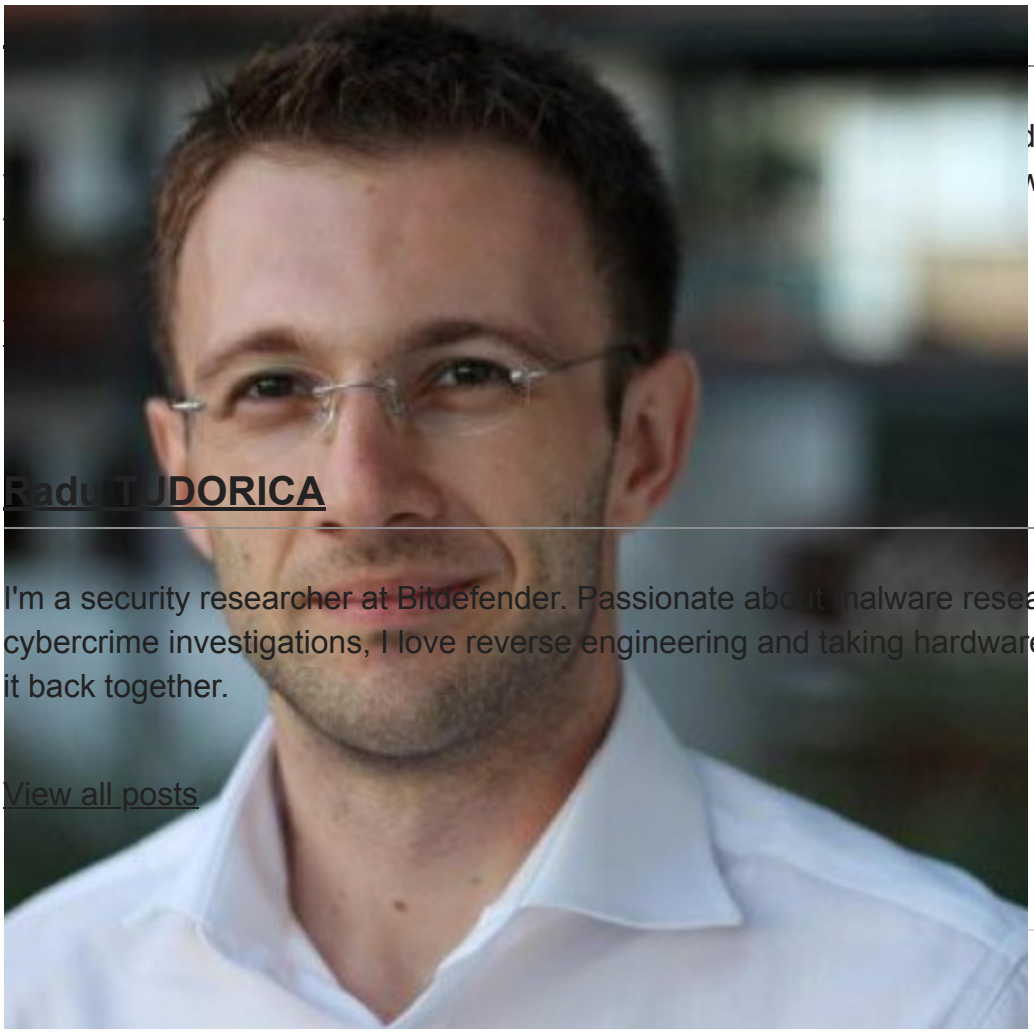
Conclusions

Completely dismantling TrickBot has proven more than difficult, and similar operations in the past against popular Trojans has proven that the cybercriminal community will always push to bring back into operation something that's profitable, versatile and popular. TrickBot might have suffered a serious blow, but its operators seem to be scrambling to bring it back, potentially more resilient and difficult to extirpate than ever before.

TAGS

anti-malware research

AUTHOR



ding energy. That's
ws editor for the past

Radu TUDORICA

I'm a security researcher at Bitdefender. Passionate about malware research, APTs, and cybercrime investigations, I love reverse engineering and taking hardware apart and putting it back together.

View all posts