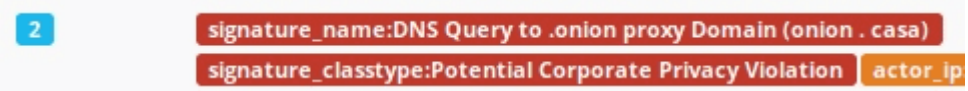
Nearly undetectable Qarallax RAT spreading via spam

Archived: 2026-04-05 21:46:50 UTC

Hi everyone, here's Matteo Lodi, member of the Incident Response Team.

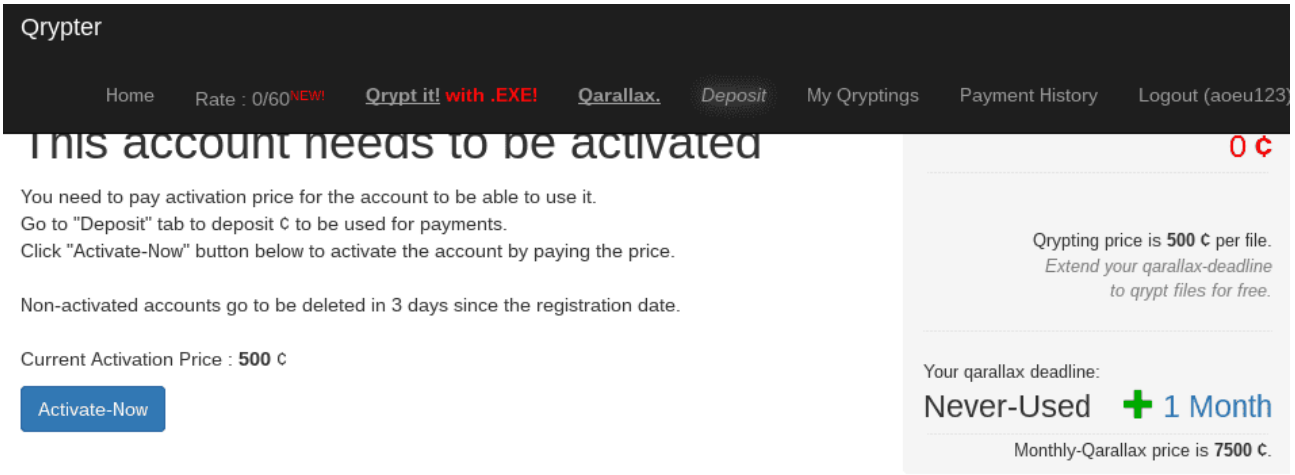
This time i want to talk about a new threat we detected randomly while analyzing the alerts generated by our platform.

Everything starts from the analysis of a little and alone level 2 ET signature called "***ET PRO POLICY DNS Query to .onion proxy Domain (onion . casa)***".



At the beginning, the only evidence we got from the traffic analysis are many DNS queries followed by 4 HTTPS contacts to the following weird domain: ***vvrhhhnaijyj6s2m[.]onion[.]casa***

We found that onion.casa is a proxy used to access to hidden services behind the renowned TOR network. In details, if we visit the site, we can find that the domain in question hosts a site which claim to sell a malware known as ***Qarallax***.



Qarallax is a RAT (remote access tool) and infostealer. This malware was born from an open-source software known ***LaZagne***. At this time, this artifact let an attacker to execute different kinds of operations inside the infected machine:

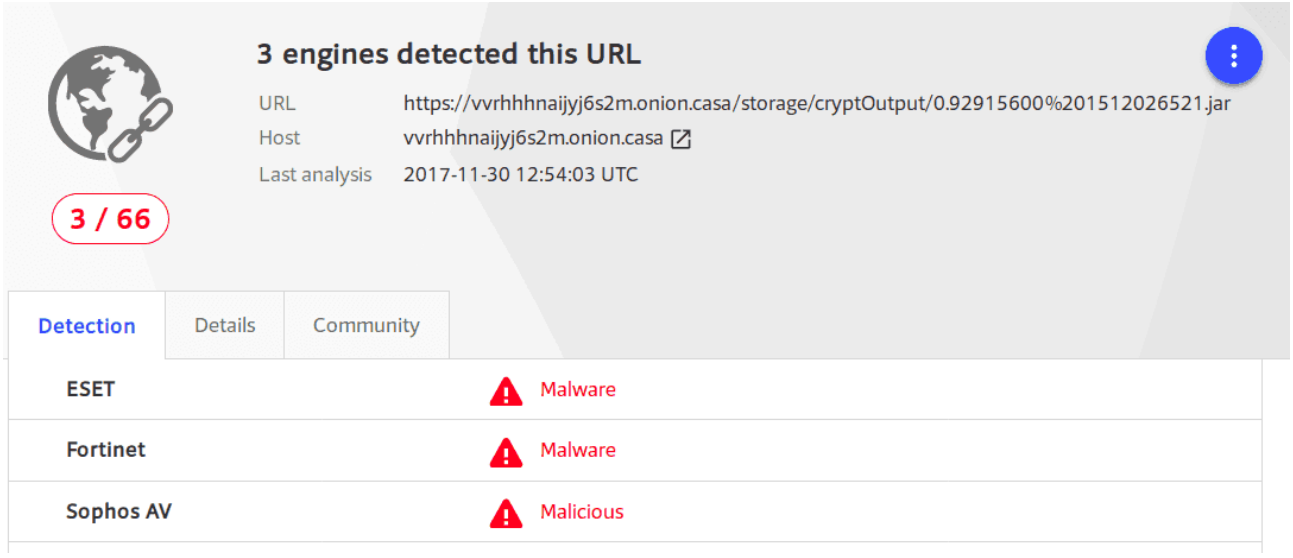
- Catch mouse movements and clicks
- Catch keyboard inputs
- Record the output of the webcam and of the screen
- Find and steal every kind of credential stored inside the machine

There's a group called ***Quaverse*** which claim to be the R&D behind this threat, constantly working to evolve and upgrade the malware. Their objective is to sell the agent as a RaaS (RAT as a Service).

The file is a JAVA application that runs on operating systems with JAVA Runtime Environment (JRE) installed. It runs silently in the background without any indication to the user.

At this time, we had no evidence that the host that contacted the suspicious domain is infected, but we are strongly suggested to investigate further to understand if this is a real threat.

We tried to look for some intelligence feeds from the internet, looking if someone else has found some useful infos about the domain in question. At the beginning, we checked from Google, Twitter and Reverse but we didn't found anything. Then, checking VirusTotal, we found that they list the following URL as a malicious one: hxxps://vvrhhhnaijyj6s2m[.]onion[.]casa/storage/cryptOutput/0.92915600%201512026521.jar



Wow, only 3 hits and no sample uploaded to VT. However, at that time, we got an idea about what the SSL connections did: downloading a ***.jar*** file containing, with high probability, the malware.

Meanwhile, we contacted the client and, luckily, the host infected was a virtual machine that got reverted to a clean state and the AV Agent detected and stopped the execution of the malware.

Afterwards, the real questions were:

- how did they get the malware?
- was the attack targeted or opportunistic?

The day after, inside our spamtrap, we retrieved a sample called "IMG6587JPG..jar", identified as malicious (8.2/10 score) by our sandbox. The first thing where we put our attention was the traffic this sample generated towards the suspicious domain.

Connects to Tor Hidden Services through a Tor gateway (1 event)	
domain	vvrhhhnaijyj6s2m.onion.casa

That's it! Probably we found the malware our client got and, luckily, it came from a normal email spam tricking the user to open a fake image containing the infostealer.

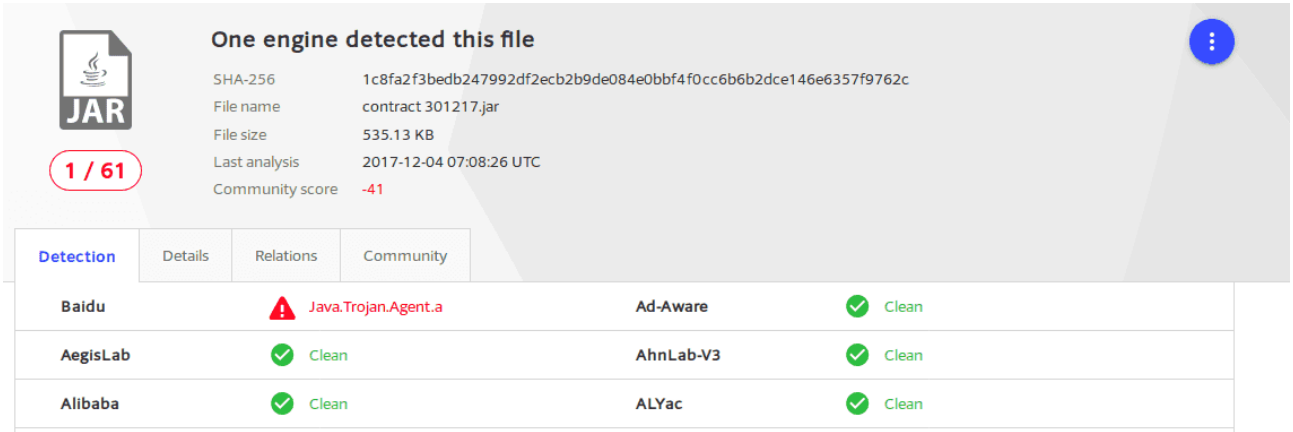
```
Sender: maite@inauxacomercial.com
Subject: New order_IMG_6587 JPG-2017
Dear Good day, Am interested in your product i saw online with our new purc
hase, feed us with more of your samples.
kindly exermine the new order and tell us your paymwent terms Thanks in Ant
icipation.
note:VERY URGENT
Regards
IBRAHIM M.D Commercial Department SUMINISTROS INDUSTRIALES CHEMICAL SL Pol.
ibrahim, 228000 Getafe Madrid Email : maite@inauxacomercial.com
```

Fun fact was that only 4 AV engines detected it. After 4 hours, finally, some other antivirus products started to identify that threat as malicious (15).

We said that to our client who could find the email that was the infection vector and send it to us. The Qarallax variant was almost identical to the one we caught just some minutes before. The only thing that changed was the email body (different language, from english to italian) and the name of the sample: PAGAMENTO.jar. Even in this case, the first time we send the sample to VT, only few antivirus were able to identify it.

Update

We detected some new similar samples. The malware capabilities are the same as before. The biggest difference is the proxy used to contact the C&C server: from onion[.]casa to onion[.]top. We want to underline that the threat is evolving day by day: every new sample we get to analyze is almost undetected by every kind of AV engine.



Conclusion

We found a new spam campaing delivering a RAT malware, nearly undetectable by IDS Signatures or AV engines.

IOC

Domains:

```
 vvrhhhnaijyj6s2m[.]onion[.]top
vvrhhhnaijyj6s2m[.]onion[.]top
```

RAT samples (MD5):

```
 f441dc0388afd3c4bca8a2110e1fa610
682f0260cd0bb8716d32485eebfe1d31
cb9da672613decdc800849a45f21c0b8
d77cfa2b68c744f3ba62f2e49a598ffa
d9adbb40a0ae557c5bf1d2dd2f85409d
42ecb562506ec1734cc291c0092753c5
702f6c5856591accb8cdd4bcfc46e114
```

Source: http://www.certego.net/en/news/nearly-undetectable-qarallax-rat-spreading-via-spam/