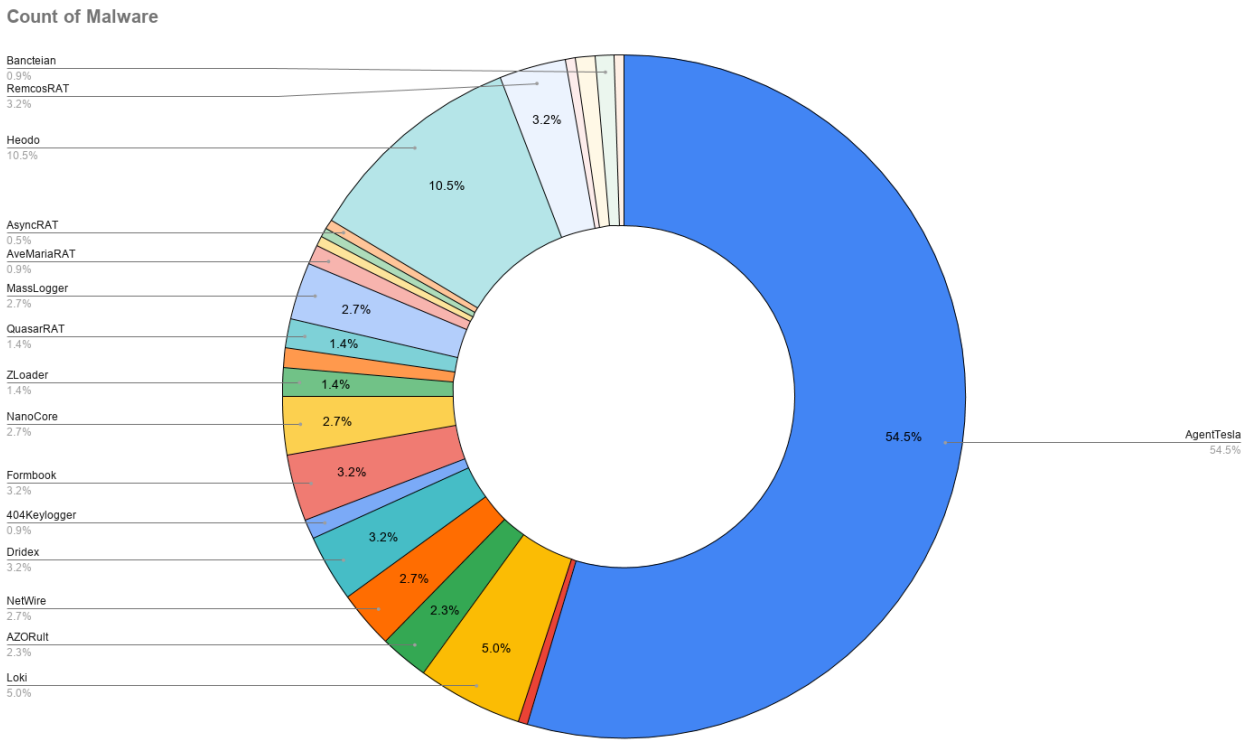
Observed Malware Campaigns – October 2020

vulnerability.ch/2020/11/observed-malware-campaigns-october-2020/

Corsin Camichel November 1, 2020



An output of my most recent script (see my post "Malicious Attachment Analysis Script"), is the ability to create statistics and the data-set to understand what kind of malware campaigns are being delivered by email attachments.

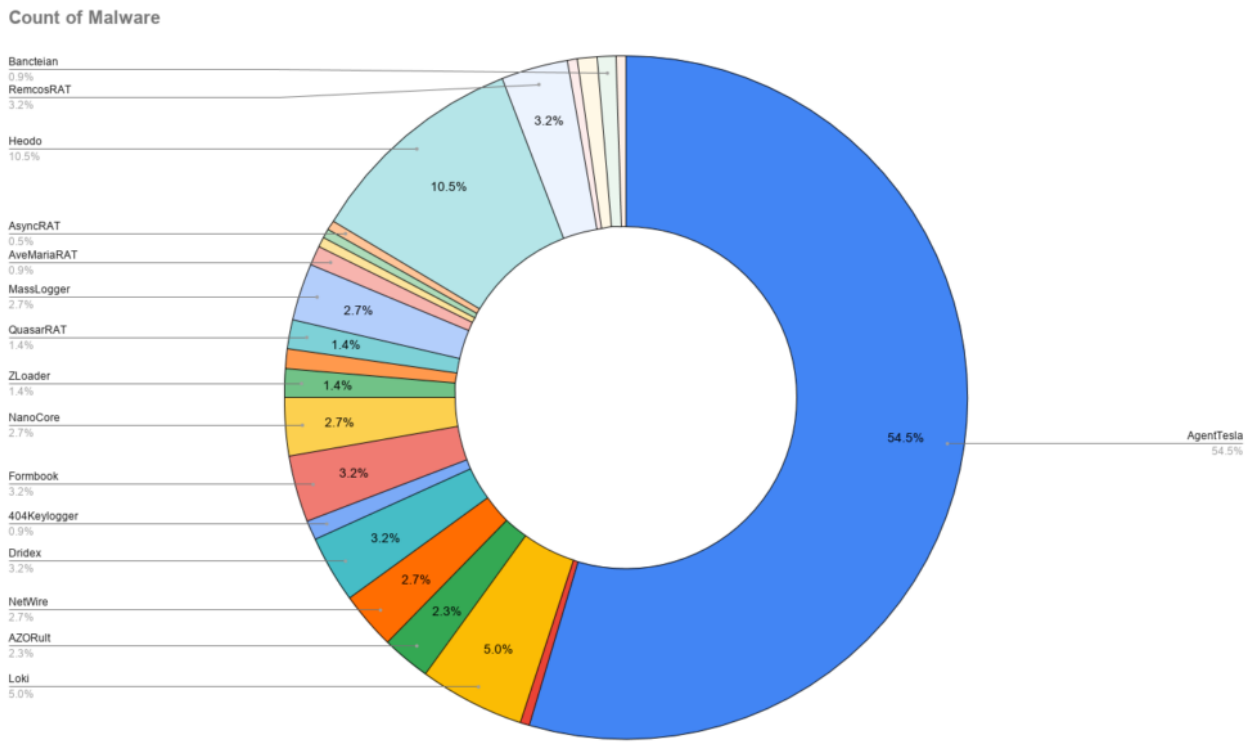
In October 2020 I received a total of **76,888 emails (2,480 per day)** to my spam traps. Obviously not all of the emails contained a malicious attachment, as the emails also fall into the categories phishing emails, general spam (e.g. drugs, prizes won), others.
From all emails received, a total of **221 unique malicious attachments** have been identified. There have been far more malicious files, but they are either not identified or a duplicate by file hash and thus not reported here. Also, if a malware campaign consisted of links to downloads, they are also not included in this list.

The vast majority (over 50%) is being identified as malware family "AgentTesla" by MalwareBazaar signatures.

Malware	Count
AgentTesla	120

Malware	Count
Heodo	23
Loki	11
Dridex	7
Formbook	7
RemcosRAT	7
MassLogger	6
NanoCore	6
NetWire	6
AZORult	5

Top 10 malware families observed in October 2020



The largest sector receiving those emails is **legal services**. That is something I have observed for a while and now I got the data set that clearly confirms my assumption.

The top 10 sectors in my spam trap targeted by malware this month are:

Sector	Count

Sector	Count
legal	137
electronics / import	21
non-profit	13
free service	12
banking	7
electronics	7
newspaper	5
recruitment	3
sport marketing	3
advertising agencies	2

Top 10 sectors receiving malicious email attachments
Also interesting observation, legal services are mostly targeted by "**AgentTesla**" malware, followed by "**Loki**" and "**Formbook**" and "**NetWire**". All tools used to steal sensitive information and documents or remotely control an infected computer.

If you have any questions, please post a comment or send me a message on Twitter @cocaman.