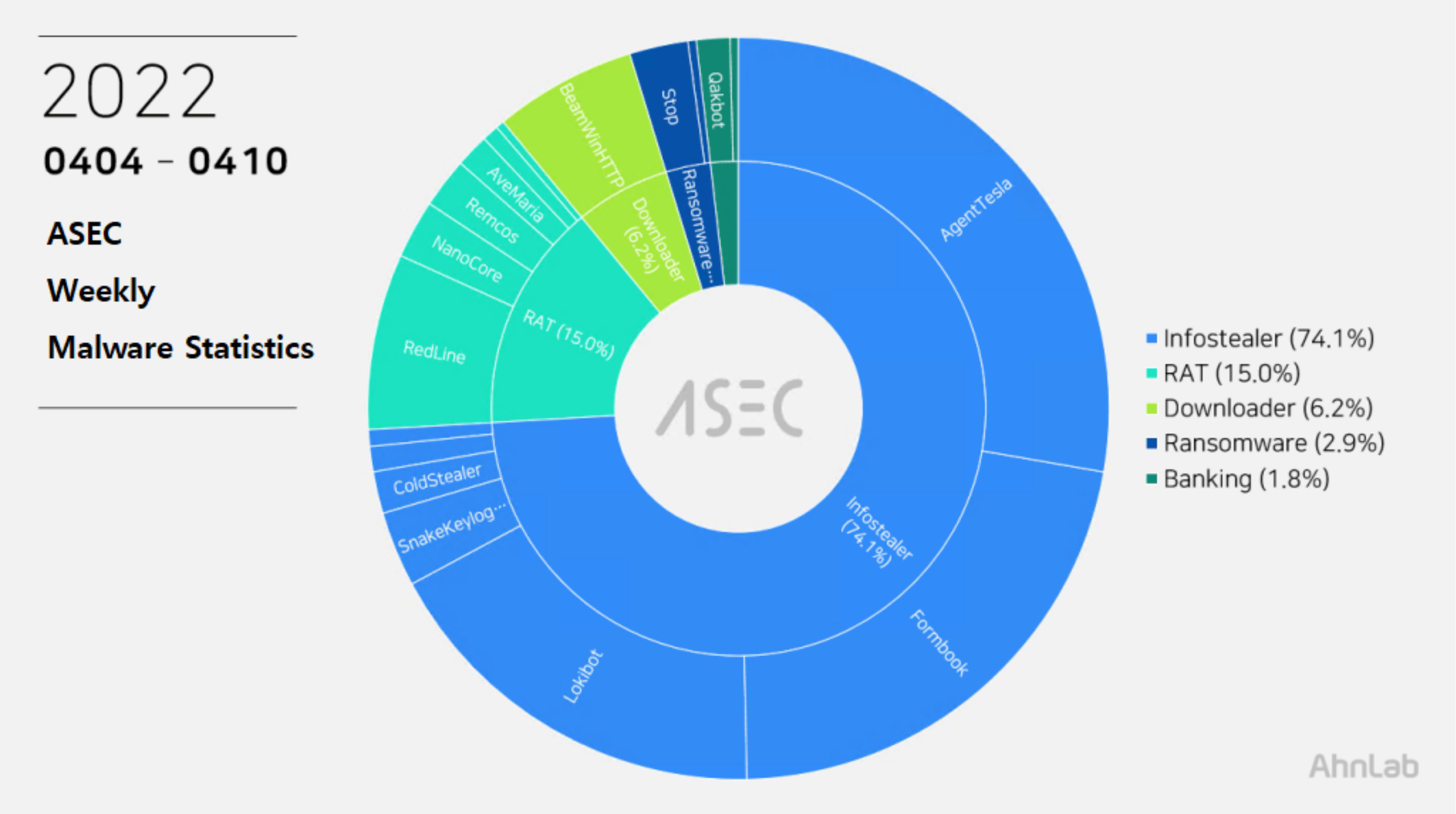
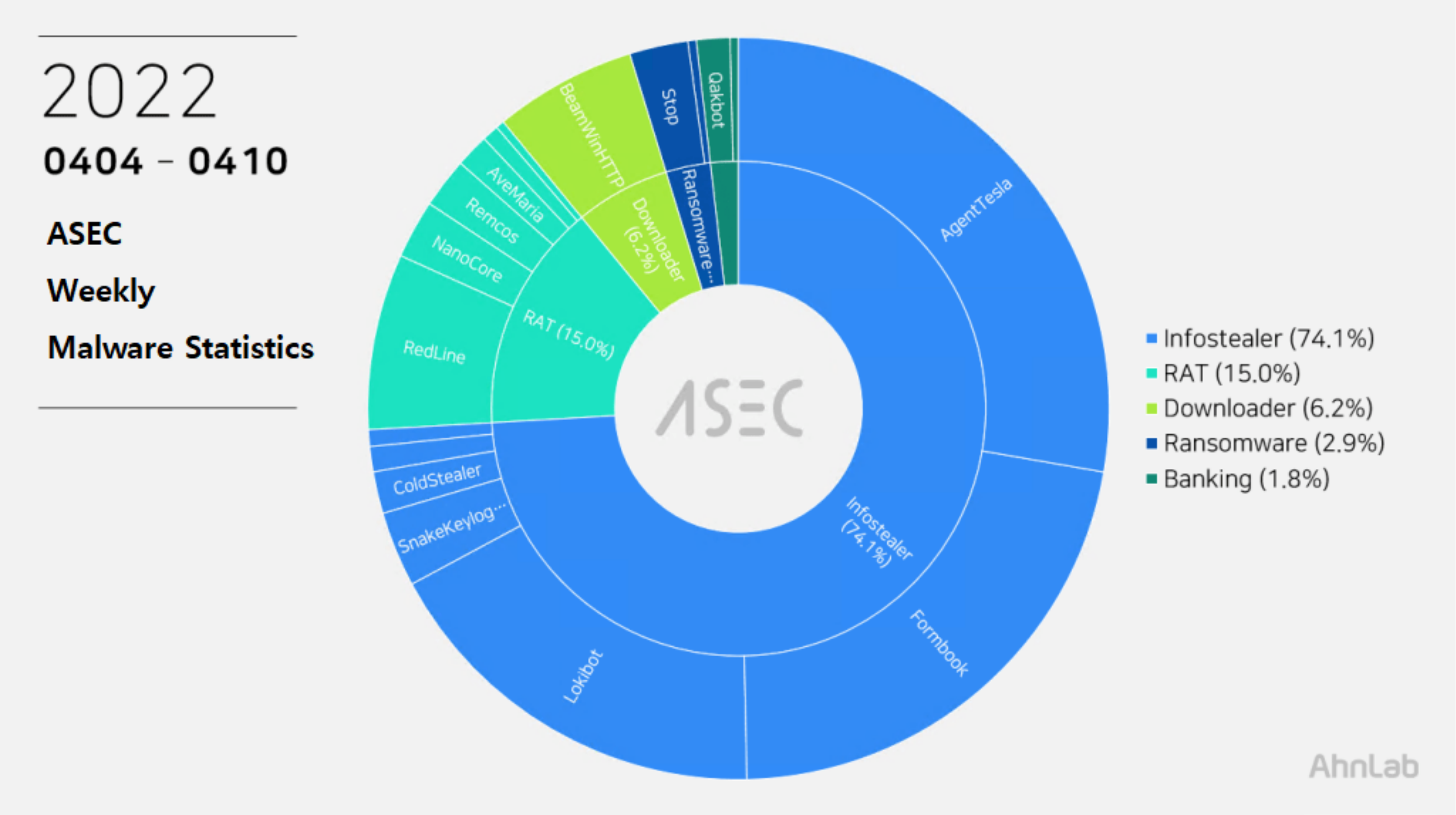
Posted on April 14, 2022

ASEC Weekly Malware Statistics (April 4th, 2022 – April 10th, 2022)

The ASEC analysis team is using the ASEC automatic analysis system RAPIT to categorize and respond to known malware. This post will list weekly statistics collected from April 4th, 2022 (Monday) to April 10th, 2022 (Sunday).

For the main category, info-stealer ranked top with 74.1%, followed by RAT (Remote Administration Tool) malware with 15%, downloader with 6.2%, ransomware with 2.9%, and banking malware with 1.8%.





Top 1 — AgentTesla

AgentTesla is an infostealer that ranked first place with 27.7%. It is an info-stealer that leaks user credentials saved in web browsers, emails, and FTP clients.

Recently collected samples use the following email servers and user accounts when leaking the collected information.

- server: mail.waterchem.com[.]tr(109.232.216[.]96) sender: admin@waterchem.com[.]tr receiver: ugo@waterchem.com[.]tr user: admin@waterchem.com[.]tr pw: 2022pa*****$
- server: mail.newoasisbld[.]com(103.125.80[.]50) sender: sales@newoasisbld[.]com receiver: info-ctg@qandqbd[.]com user: sales@newoasisbld[.]com pw: S*****2022

- server: smtp.sbtsrne[.]com(208.91.198[.]143) sender: janla@sbtsrne[.]com receiver: janla@sbtsrne[.]com user: janla@sbtsrne[.]com pw: Jn*****97

As most are distributed through spam emails disguised as invoices, shipment documents, and purchase orders, the file names contain such words shown above (Invoice, Shipment, P.O. — Purchase Order). Multiple collected samples were disguised as files with extensions of pdf and xlsx.

- New Purchase Order — April_06_2022.exe
- dangxianfood import request.exe
- ATTACHMENT.exe
- MT101 Swift_ Remittance Invoice.exe
- TQ-202577_ Al Laith.doc..exe
- NEW PO 14071103501_pdf.exe
- Pago Factura.exe

Top 2 — Formbook

Formbook ranked second place with 21.9%.

Like other info-stealer, it is mainly distributed through spam emails. The distributed file names are close to each other. As for the files shown in the list below, the embolden filenames changed the name of the parent folder and distributed them using email to their targets. In other words, it is assumed that the filename of the attachment (compressed file or folder in the file) is distributed after changing its name. Thus, users should be cautious when opening the attachments sent from unknown users.

- New Order #TX110804#.exe
- Image000004.exe
- Dhl _SHIPPING DOC — #0036284639289.exe
- product list of trial order _00123133.exe
- PO2204-012SP (TOP URGENT).exe
- Pro Forma_pdf.exe QUOTATION.exe
- invoice.exe

As Formbook is injected in a normal process that is in the directory of explorer.exe and system32, the malicious behaviors are performed by the normal process. Besides user credentials in the web browser, the malware can steal various information through keylogging, clipboard grabbing, and web browser form grabbing.

Below is the list of confirmed C&C server URLs of Formbook.

- hxxp://www.webtrajpylive[.]online/bs11/
- hxxp://www.stageyor[.]online/gn27/
- hxxp://www.pordges[.]com/ok4e/
- hxxp://www.neurosise[.]com/op53/
- hxxp://www.mydactil[.]online/e0l9/
- hxxp://www.keepitng[.]com/inga/
- hxxp://www.kartye[.]xyz/pd21/
- hxxp://www.globalfabtol[.]online/b11y/
- hxxp://www.gingure[.]com/e0ep/
- hxxp://www.gimbases[.]com/cnt4/
- hxxp://www.demtate[.]xyz/d23n/
- hxxp://www.dactil[.]xyz/s09m/
- hxxp://www.cures8t[.]com/p9iu/

Top 3 — Lokibot

Lokibot ranked third place with 17.5%. It is an info-stealer that leaks information about programs such as web browsers, email clients, and FTP clients.

Being a malware that is distributed through spam emails, it shares similar file names with other malware spam emails.

- MLOADER.exe
- vloader.exe

- qloader.exe
- hloader.exe
- updated_order.exe
- Cuserspublicvbc.exe
- vbc.exe
- Arrival Notice_XSS26005.exe

As shown below, most Lokibot C&C server URLs tend to end in fre.php.

- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php
- hxxp://sempersim[.]su/bb/fre.php
- hxxp://sdgcd[.]xyz/Mine/PWS/fre.php
- hxxp://outlook-webpage-auth[.]ml/worldwide/logs/fre.php
- hxxp://iowipalbv6atsy[.]cf/Exodus1/fre.php
- hxxp://hyatqfuh9olahvxf[.]gq/BN3/fre.php
- hxxp://85.202.169[.]172/remote/five/fre.php
- hxxp://62.197.136[.]186/oluwa/five/fre.php
- hxxp://62.197.136[.]176/userbob/five/fre.php

Top 4 — RedLine

RedLine ranked fourth place with 7.7%. The malware steals various information such as web browsers, FTP clients, cryptocurrency wallets, and PC settings. It can also download additional malware by receiving commands from the C&C server. Like BeamWinHTTP, there have been numerous cases of RedLine being distributed under the disguise of a software crack file.

The following are the confirmed C&C server domains for RedLine:

- 116.202.106[.]111:9582
- 185.200.191[.]18:80
- 185.215.113[.]122:15386
- 193.150.103[.]37:21330
- 193.150.103[.]38:80
- 141.95.227[.]187:6238
- 91.243.59[.]131:7171

Top 5 — BeamWinHTTP

BeamWinHTTP is a downloader malware that ranked fifth place with 6.2%. BeamWinHTTP is distributed via malware disguised as PUP installer. When it is executed, it installs PUP malware Garbage Cleaner, and can download and install additional malware at the same time.

Recently, there have been numerous cases of distribution by the dropper disguised as a software crack file. The ASEC analysis team is responding to this malware using the alias ‘MulDrop.’ See the following blog post for more information on the malware.

The confirmed C&C server URL is as follows.

- hxxp://appwebstat[.]biz/info.php
- hxxp://ads-memory[.]biz/patner/hooker.php
- hxxp://hogwartsfog[.]com/checkversion.php
- hxxp://212.192.246[.]217/access.php

Subscribe to AhnLab’s next-generation threat intelligence platform ‘AhnLab TIP’ to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:weekly statistics