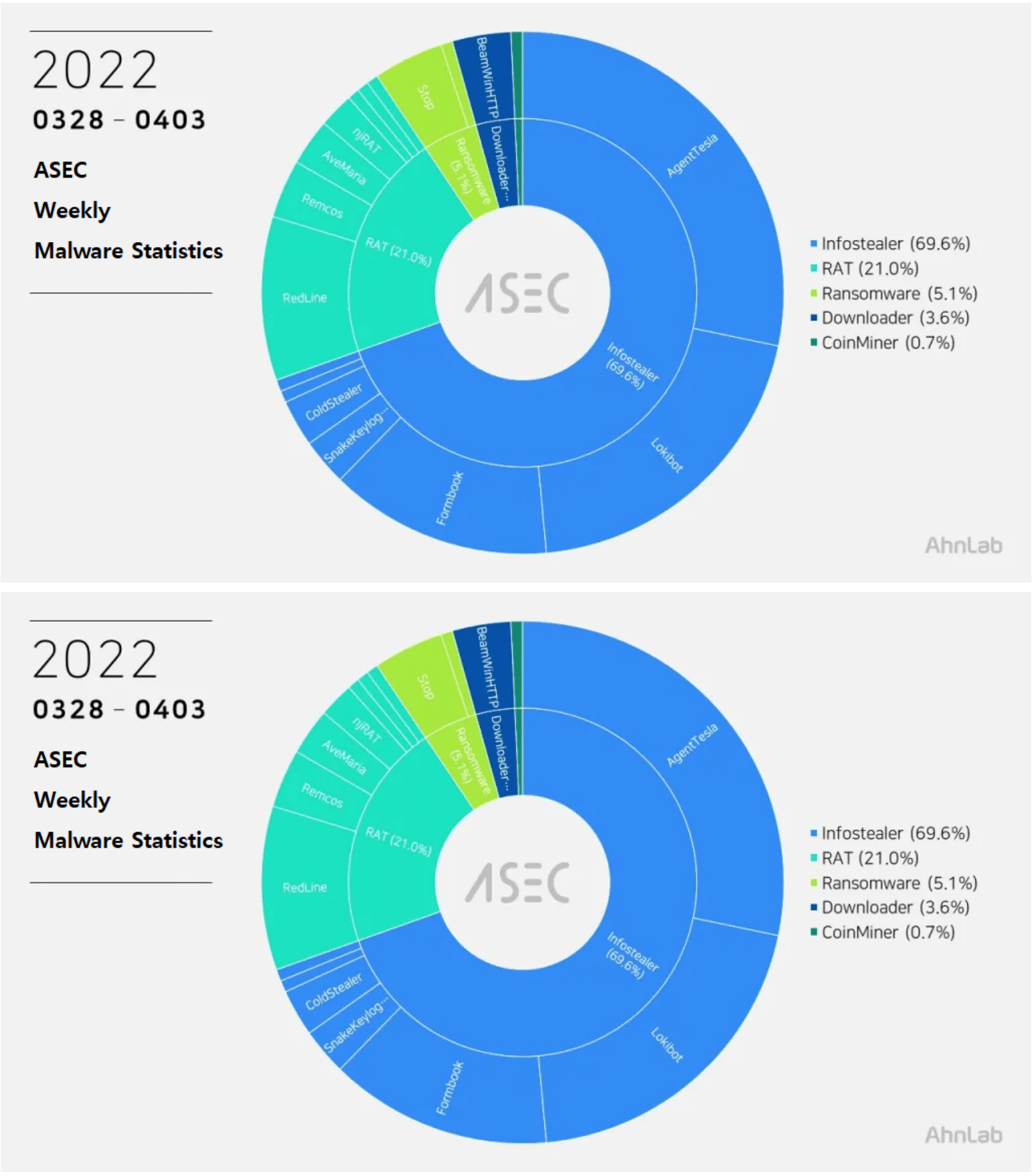
Posted on April 7, 2022

ASEC Weekly Malware Statistics (March 28th, 2022 – April 3rd, 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 March 28th, 2022 (Monday) to April 3rd, 2022 (Sunday).

For the main category, info-stealer ranked top with 69.6%, followed by RAT (Remote Administration Tool) malware with 21.0%, ransomware with 5.1%, downloader with 3.6%, and CoinMiner with 0.7%.



Top 1 – AgentTesla

AgentTesla ranked first place with 28.3%. 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.avadis-co[.]com (216.40.42[.]5) sender : yousefi@avadis-co[.]com receiver : bak.pavoll@gmail[.]com user : yousefi@avadis-co[.]com pw : 9*******1
- server : mail.conteudopuro[.]eu (94.46.176[.]210) sender : scott@conteudopuro[.]eu receiver : scott@conteudopuro[.]eu user : scott@conteudopuro[.]eu pw : 1&********-6

- server : smtp.uk-custom[.]com (208.91.198[.]143) sender : office@uk-custom[.]com receiver : office@uk-custom[.]com user : office@uk-custom[.]com pw : PF******v9
- server : webmail.cbiperu[.]com (158.69.52[.]114) sender : jcanola@cbiperu[.]com receiver : jcanola@cbiperu[.]com user : jcanola@cbiperu[.]com pw : J2*******1@
- server : mail.demetrology.com[.]my (103.8.25[.]76) sender : faiz.aimi@demetrology.com[.]my receiver : teahyunkoo@gmail[.]com user : faiz.aimi@demetrology.com[.]my pw : de*******20

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.

- DUBAI HCU 21EDD.exe
- REF 123694691.exe
- Arrival_Notice.exe
- stp.jpg
- documents.exe
- Transfer Confirmation 100241703_PDF.exe
- TRANSACTION ADVICE.exe

Top 2 — Lokibot

Lokibot ranked second place with 20.3%. 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.

- SI_DRAFT_SCAN_PO346314_pdf.exe
- UFJ_Bank_Outward_Remittance_Nichias_pdf.exe
- vbc.exe
- csrss.exe

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

- hxxp://sempersim[.]su/bb/fre.php
- hxxp://sempersim[.]su/ge14/fre.php
- hxxp://outlook-webpage-auth[.]ml/worldwide/logs/fre.php
- hxxp://s474079.smrtp[.]ru/Panel/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php
- hxxp://gaviscon[.]ml/Kent2/fre.php
- hxxp://62.197.136[.]176/userbob/five/fre.php
- hxxp://62.197.136[.]186/oluwa/five/fre.php
- hxxp://gaviscon[.]tk/Concord/fre.php
- hxxp://brokenskulltechnologies[.]gq/Marshall/fre.php

Top 3 — Formbook

Formbook is an infostealer that ranked third place with 13.8%.

Like other info-stealer, it is mainly distributed through spam emails. The distributed file names are close to each other.

- PAYMENT ADVICE (2).exe
- TT Copy.exe
- DHL. INV03296411.exe
- Request for Quotation_pdf.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.buresdx[.]com/be4o/
- hxxp://www.budistx[.]com/qbks/
- hxxp://www.buresdx[.]com/cbgo/
- hxxp://www.funtabse[.]com/pout/
- hxxp://www.besrbee[.]com/yrcy/
- hxxp://www.gingure[.]com/e0ep/
- hxxp://www.alpeshpate[.]com/mwfc/
- hxxp://www.fendoremi[.]com/cm5a/
- hxxp://www.neurosise[.]com/op53/
- hxxp://www.price-hype[.]com/mnqo/

Top 4 — RedLine

RedLine ranked fourth place with 10.1%. 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:

- 185.197.74[.]202:9516
- 62.204.41[.]166:27688
- 185.215.113[.]20:21921
- 193.150.103[.]37:21330
- 188.34.167[.]94:36709

Top 5 — Stop Ransomware

Stop Ransomware ranked fifth place with 4.3%. It is malware that is distributed mainly using exploit kit. This malware encrypts certain files in user PC, and has been distributed in various forms and is still continuously being distributed.

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