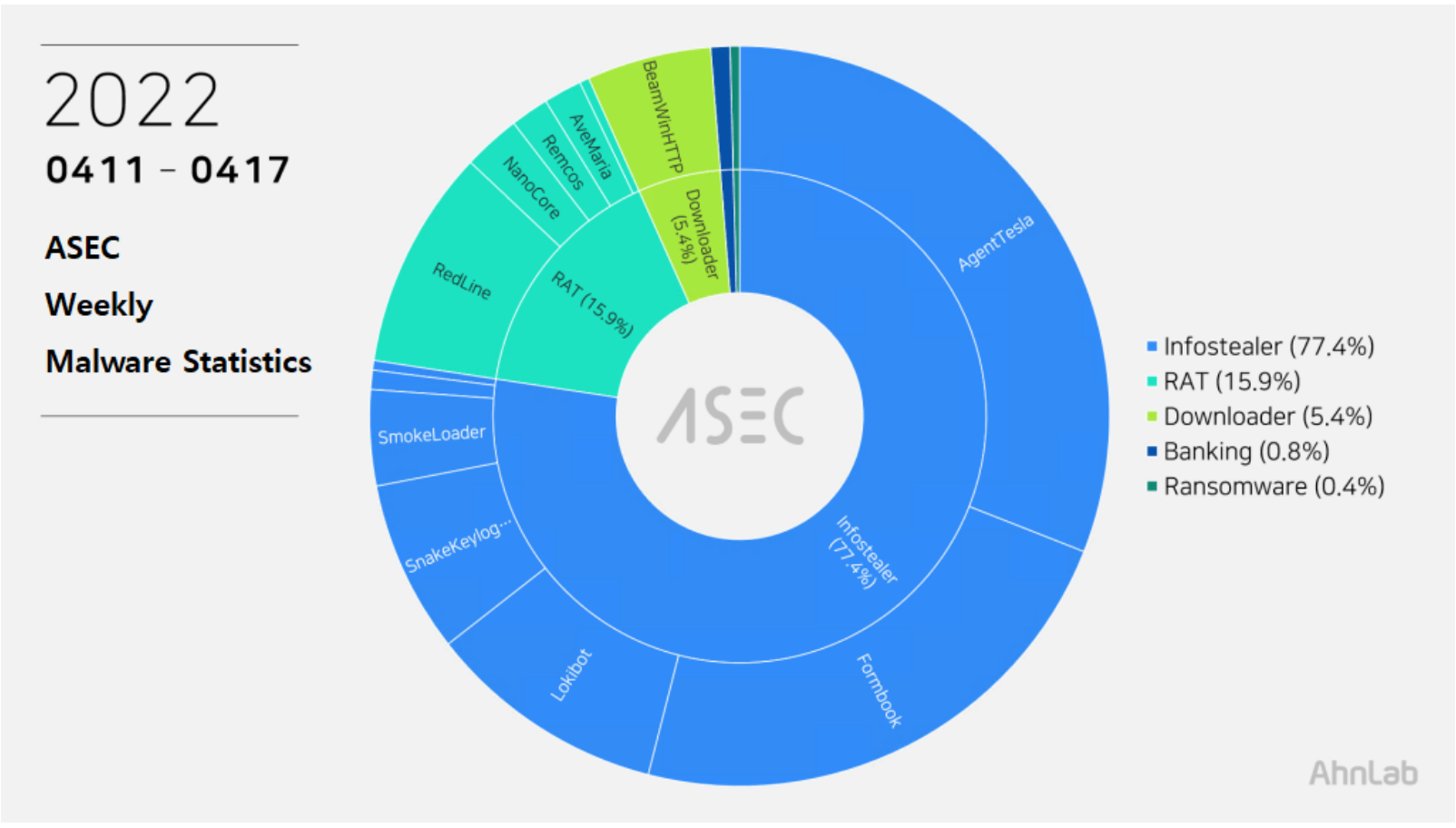
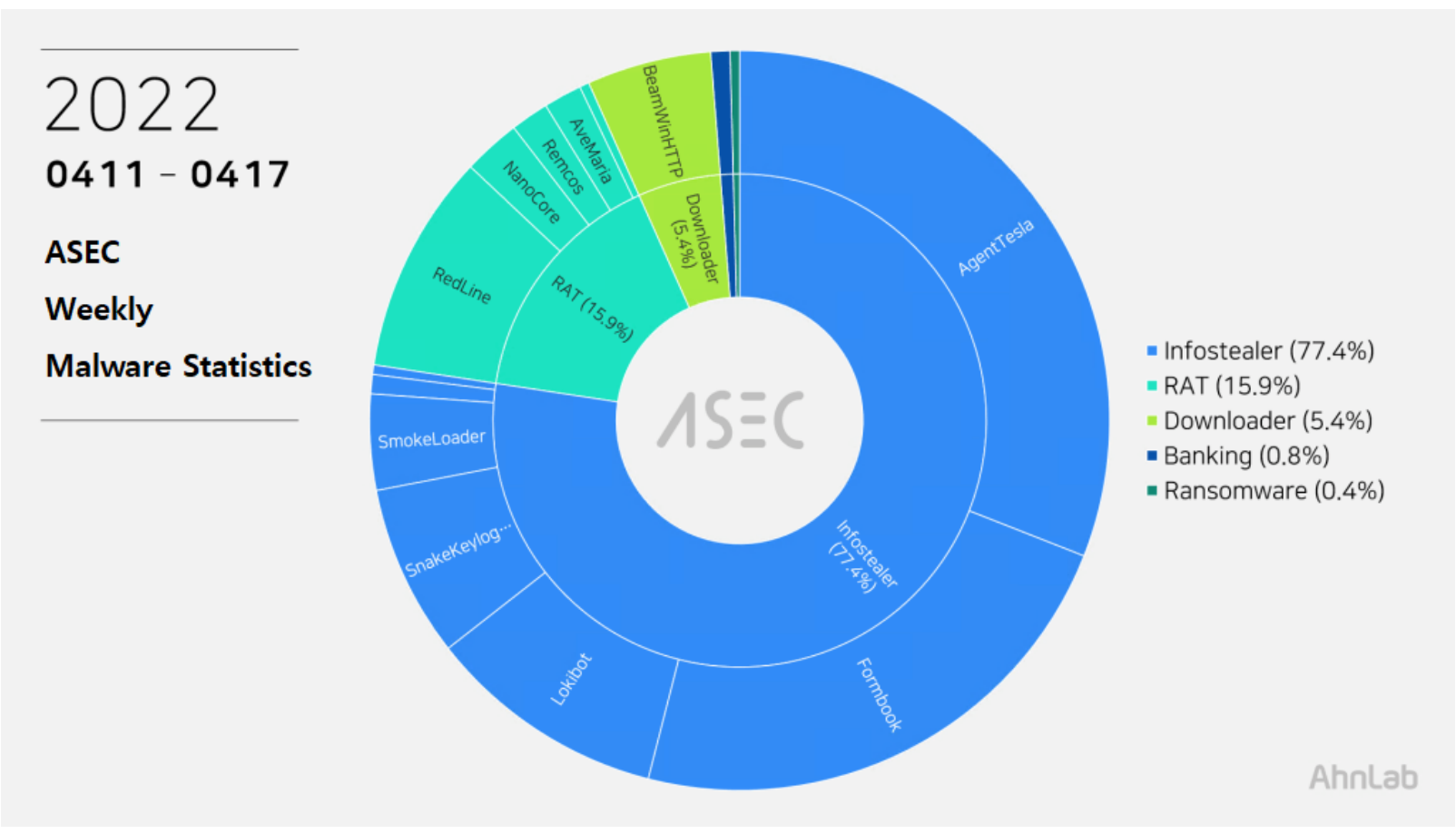
Posted on April 25, 2022

ASEC Weekly Malware Statistics (April 11th, 2022 – April 17th, 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 11th, 2022 (Monday) to April 17th, 2022 (Sunday).

For the main category, info-stealer ranked top with 77.4%, followed by RAT (Remote Administration Tool) with 15.9%, downloader with 5.4%, banking malware with 0.8%, and ransomware with 0.4%.





Top 1 – AgentTesla

AgentTesla is an infostealer that ranked first place with 31%. 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: smtp.taizingshipping[.]com (208.91.198[.]143) sender: breaktru@taizingshipping[.]com receiver: breaktru@taizingshipping[.]com user: breaktru@taizingshipping[.]com pw: Gw********2
- server: mail.contrivekota[.]in (184.168.102[.]151) sender: info1@contrivekota[.]in receiver: hokota@contrivekota[.]in user: info1@contrivekota[.]in pw: Co********3$

- server: mail.vvis.com[.]ph (46.21.149[.]90) sender: fatima@vvis.com[.]ph receiver: ranjqnupreti3@gmail[.]com user: fatima@vvis.com[.]ph pw: Ma*******7

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.

- Payment Swift_santander
- MT101.exe
- Quotation Sheet.exe
- STATEMENT OF ACOUNT.exe
- HDFC Bank 50% TT swift copy.exe
- PO 960074688.pdf.exe
- PRICE QUOTATION.exe
- PO363.exe

Top 2 — Formbook

Formbook ranked second place with 23%.

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.

- attachment_pdf.exe
- PI&BL.exe
- New Order.exe
- doh.exe
- orden_de_compra_de_abril.pdf.exe
- Payment_-_Sunrise_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.budistx[.]com/iqof/
- hxxp://www.hughers3[.]com/cbgo/
- hxxp://www.keepitng[.]com/inga/
- hxxp://www.nu865ci[.]com/g5so/
- hxxp://www.price-hype[.]com/apg5/
- hxxp://www.hips5r[.]com/p83q/
- hxxp://www.rugisdh[.]com/ud5f/
- hxxp://fendoremi[.]com/wesd/
- hxxp://www.demtate[.]xyz/d23n/

Top 3 — Lokibot

Lokibot ranked third place with 10.5%. 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.

- babaman.exe
- vbc.exe
- 20220414.exe
- loadme.exe

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

- hxxp://164.90.194[.]235/?id=58098847226041972
- hxxp://sempersim[.]su/ge17/fre.php
- hxxp://62.197.136[.]176/auzsin/five/fre.php
- hxxp://controlsvr1[.]tk/Concord/fre.php
- hxxp://45.133.1[.]45/me/five/fre.php
- hxxp://hyatqfuh9olahvxf[.]gq/BN3/fre.php

Top 4 — RedLine

RedLine ranked fourth place with 9.6%. 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:

- wailanyrrere[.]xyz:81
- 107.189.6[.]214:8
- 185.215.113[.]122:15386
- 116.202.106[.]111:9582

Top 5 — SnakeKeylogger

Taking fifth place with 7.5%, SnakeKeylogger is an info-stealer type malware that leaks information such as user key inputs, system clipboards, and browser account information.

Like AgentTesla, this malware uses e-mail servers, telegram, and FTP when leaking collected information. The following are the currently found account and C&C URLs.

- host : mail.stilltech[.]ro sender: office@stilltech[.]ro receiver: princenewman1111@gmail[.]com user: office@stilltech[.]ro pw: eu********55ro
- hxxps://api.telegram[.]org/bot5273807869:AAHdhflfgTbp8lRJ0nhI2erbz0crK0sBFlM/sendDocument?chat_id=1212297121
- hxxps://api.telegram[.]org/bot5243953302:AAGFyxwcILx3S0Gq834R9NN-9m6enfFssYk/sendDocument?chat_id=5255359287

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