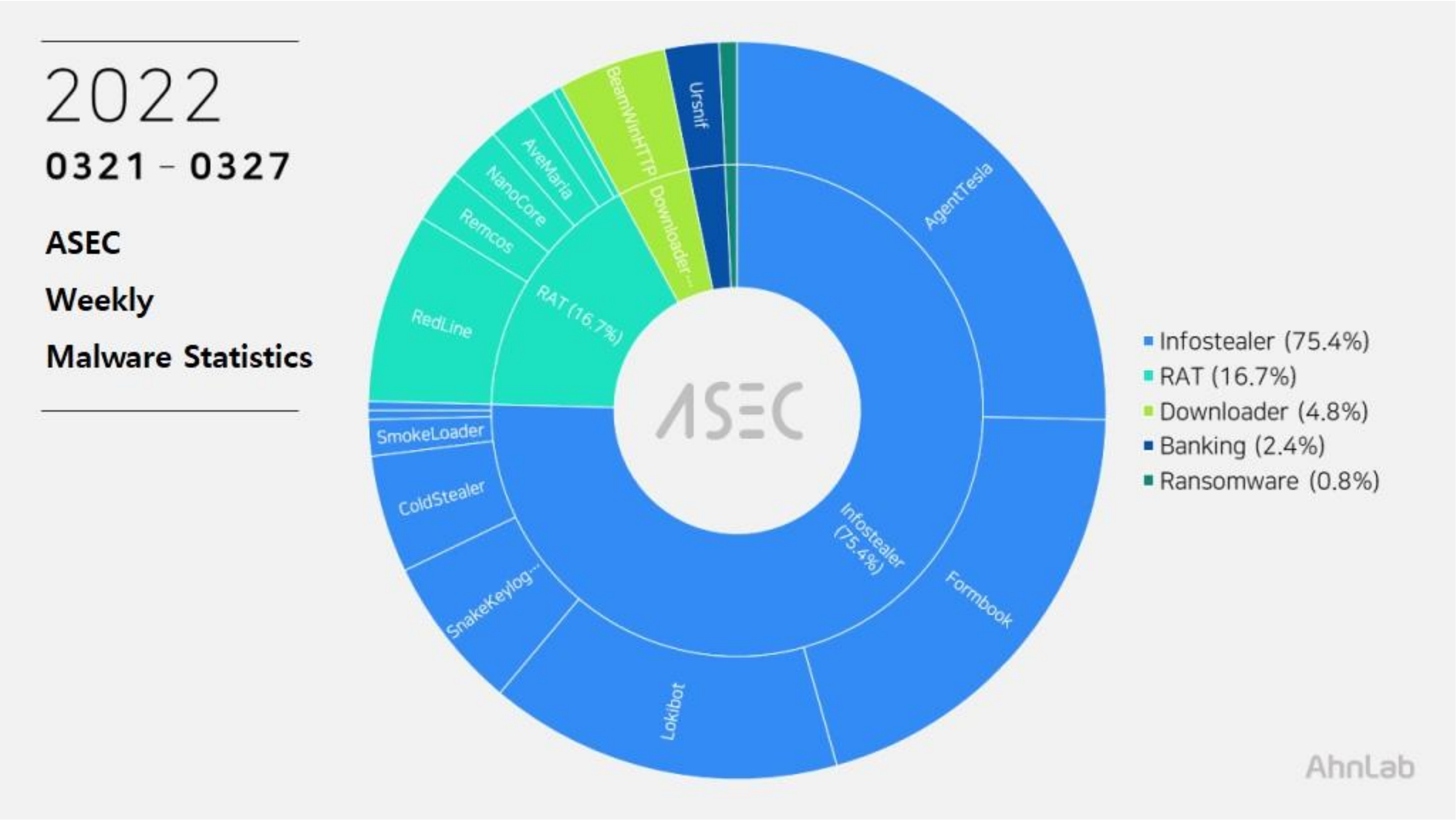
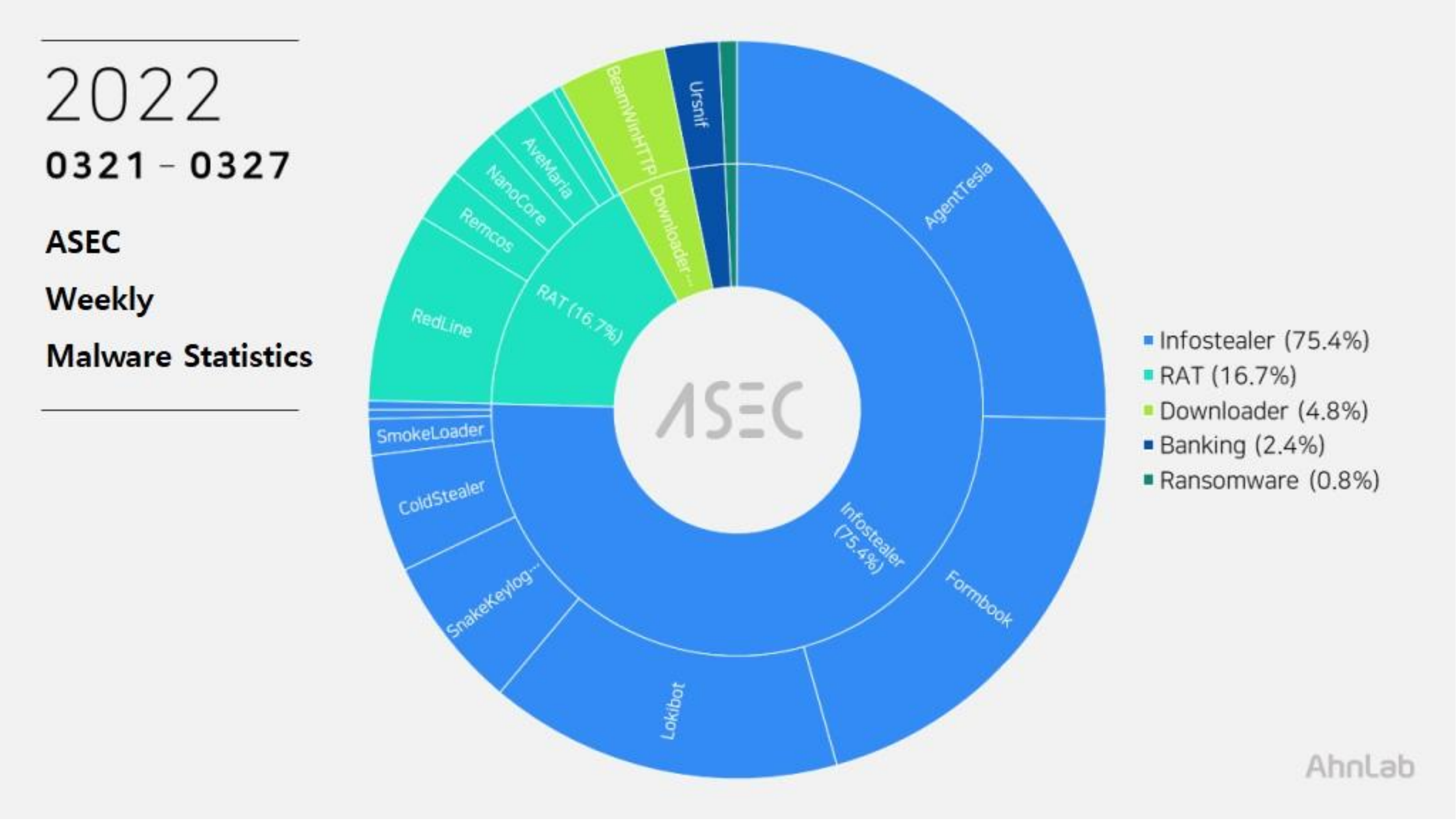
Posted on March 30, 2022

ASEC Weekly Malware Statistics (March 21st, 2022 – March 27th, 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 21st, 2022 (Monday) to March 27th, 2022 (Sunday).

For the main category, info-stealer ranked top with 75.4%, followed by RAT (Remote Administration Tool) with 16.7%, downloader with 4.8%, banking malware with 2.4%, ransomware with 0.8%.





Top 1 – AgentTesla

AgentTesla ranked first place with 25.4%. 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.contrivekota[.]in sender : info1@contrivekota[.]in receiver : hokota@contrivekota[.]in user : info1@contrivekota[.]in pw : Contr****23$

- server : mail.atifnazar[.]com sender : yasir@atifnazar[.]com receiver : nelsonson202@gmail[.]com user : yasir@atifnazar[.]com pw : anazar@*****@
- server : mail.alimentostolten[.]cl sender : moo7@alimentostolten[.]cl receiver : moo7@alimentostolten[.]cl user : moo7@alimentostolten[.]cl pw : icui4****@

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.

- BL7237207220.exe
- Bukti-Transfer..exe
- Facturas Pagadas al Vencimiento Senders Name Confirming.bbvapdf.exe
- FEDEX Online Customer Advisory AWB BL Draft Commercial. Invoice 202005173534231972.pdf.exe
- GSC CONTRACT ORDER.exe
- Inquiries_55MT.exe
- INV.0011040.2022.Img.exe
- RE TM 1200 203417 521.exe
- solu.jpg.exe

Top 2 — Formbook

Formbook is an infostealer that ranked second place with 20.2%.

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

- DHL Express Shipment Receipt.exe inquiry.exe
- INVOICE.exe
- New Order 3346585857.exe
- PAYMENT COPY.exe
- Proforma Invoice BE_603928.exe
- PURCHASE_ORDER.exe
- Quotation 6000063442 — REQUIRE SLURRY.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.abros88[.]com/46uq/
- hxxp://www.amenosu[.]com/b8eu/
- hxxp://www.arches2[.]com/qbkr/
- hxxp://www.budistx[.]com/s9m1/
- hxxp://www.cures8t[.]com/p9iu/
- hxxp://www.gunnipes[.]com/t90i/
- hxxp://www.plick-click[.]com/w6ot/
- hxxp://www.pordges[.]com/ok4e/

Top 3 — Lokibot

Lokibot ranked third place with 15.5%. 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.

- _ORD2697685.exe
- Copy_Of_Remittance.exe
- FEB INVOICES.exe
- persetujuan reeksport eks import sementara.pdf.exe
- PO #220321-2A.exe

- PO #220322-01A.exe
- PO 220324-0221A.exe

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

- hxxp://furnaceshst[.]net/ge1/fre.php
- hxxp://furnaceshst[.]net/ge10/fre.php
- hxxp://furnaceshst[.]net/gd12/fre.php
- hxxp://mailsvr1[.]tk/BN1/fre.php
- hxxp://outlook-webpage-auth[.]ml/debsfletch/logs/fre.php
- hxxp://dlokis[.]xyz/cy/keke.php
- hxxp://sempersim[.]su/ge9/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php

Top 4 — RedLine

RedLine ranked fourth place with 8.3%. 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:

- 188.68.205[.]115:17645
- 193.106.191[.]253:4752
- 193.150.103[.]38:80
- 194.87.109[.]41:4608
- birja1[.]com:80

Top 5 — SnakeKeylogger

Taking fifth place with 6.7%, 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 and user accounts when leaking collected information. The following is the accounts used by recently collected samples.

- mail.ayg.com[.]tr sender: e.basarici@ayg[.]com.tr receiver: e.basarici@ayg[.]com.tr user: e.basarici@ayg[.]com.tr pw: g)*g^****;vn
- mail.iskarosgb[.]com.tr sender: iskar@iskarosgb.com[.]tr receiver: saleseuropower2@yandex[.]com user: iskar@iskarosgb[.]com.tr pw: pi1****1C
- smtp.perrnatherm[.]net sender: sw@perrnatherm[.]net receiver: allshapewebmail@gmail[.]com user: sw@perrnatherm[.]net pw: jn****T1

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