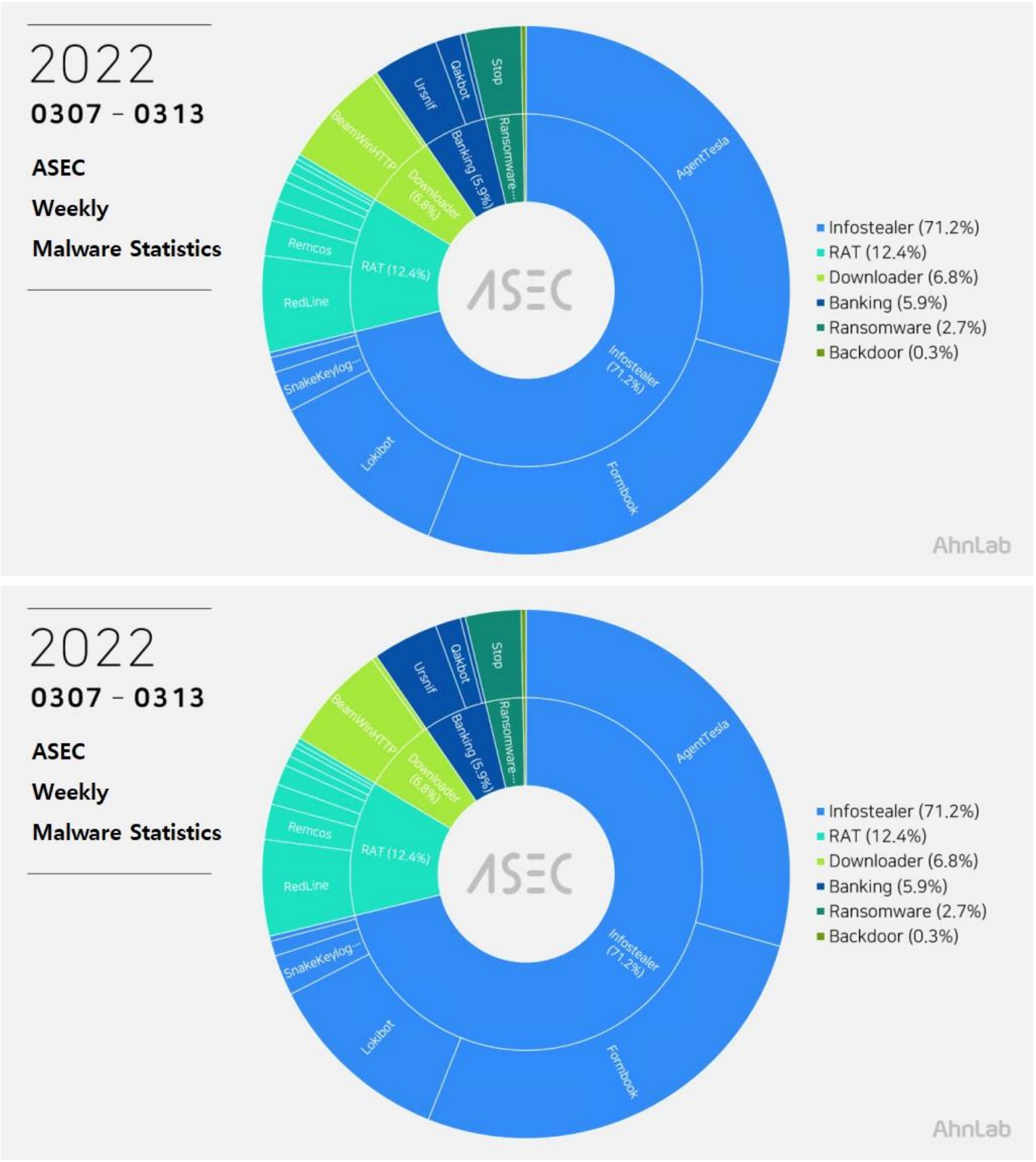
Posted on March 18, 2022

ASEC Weekly Malware Statistics (March 7th, 2022 – March 13th, 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 7th, 2022 (Monday) to March 13th, 2022 (Sunday).

For the main category, info-stealer ranked top with 71.2%, followed by RAT (Remote Administration Tool) with 12.4%, downloader with 6.8%, banking malware with 5.9%, ransomware with 2.7%, and backdoor with 0.3%.



Top 1 – AgentTesla

AgentTesla is an infostealer that ranked first place with 29.4%. 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.alimentostolten[.]cl (177.221.140[.]71) sender moo3@alimentostolten.cl receiver moo3@alimentostolten.cl user moo3@alimentostolten.cl pw icui*****@
- server mail.atharvashipping[.]co (107.180.38[.]104) sender stanley@atharvashipping.co receiver sharif@kadenasportwear.com user stanley@atharvashipping.co pw S*******5
- server mail.escueladeseguridadmaritima[.]com (160.153.132[.]203) sender julieta@escueladeseguridadmaritima.com receiver officestore2022@gmail.com user julieta@escueladeseguridadmaritima.com pw JUs******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.

- IATF 16949 LOC&ISO 9001 & ISO 14001 signed contrct.pdf_2.exe
- PO 102230.PDF (Savana Delhi MedicChem. Private Ltd) Signed Copy.exe
- ORDER FOR FU.exe
- PO-HBK3092022.exe
- AWB NO.5646219901-Invoice & Shipping Documents.exe
- AWB N0 — 30296411_Invoice Documets 2022.exe
- INVOICE — JPg.exe
- AmBank Malaysia Swift Copy.exe
- STATEMENT_OF_ACCOUNT.exe
- Quote_order#098799.exe
- dhl shippping documents.pdf.exe
- PAYMENT_SLIP.exe
- URGENT__P_O.exe

Top 2 — Formbook

Formbook ranked second place with 26.6%.

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, ‘bmpdsani22-0049rs_1.exe’ and ‘enhptcdzxlpgiuy.exe’, they changed the name of the parent folder, and distributed them using email to their targets. In other words, the malware was made differently by changing the compressed filename of the file attached to the phishing email. Thus, users should take extra caution when opening the file sent from unknown users.

- EUR_18630-7014608032022-pdf.pif.exe
- PO_00107_03_22.exe
- Enquiry.exe
- PROFORMA_INVOICE.exe
- Commercial-Invoice.exe
- Swift_copy.exe
- XX Construction Inc. 2022 Commence for Defect Repair, Contract for Completion\bmpdsani22-0049rs_1.exe
- Estimate Inc. XXX Infrastructure 20220307_104249\bmpdsani22-0049rs_1.exe
- XXXX Estimate\bmpdsani22-0049rs_1.exe
- XXXXX BioTech Purchase Order ph meter\enhptcdzxlpgiuy.exe
- XXX Country Product Unit Price(220311)_XXXX Mart\enhptcdzxlpgiuy.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.mimihin[.]com/s32s/
- hxxp://www.cesiesis[.]com/rmpc/
- hxxp://www.hapocun[.]link/o09u/
- hxxp://www.redandseven[.]com/nhc5/
- hxxp://www.arches2[.]com/qbkr/
- hxxp://www.budistx[.]com/s9m1/
- hxxp://www.onegaitom[.]online/g2e7/

Top 3 — Lokibot

Lokibot ranked third place with 11.5%. 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.

- orden de compra_pdf_____.exe
- PO 220803-04A.exe
- update status of order 07G050.exe
- 193026588 Swift Copy.exe
- CRIBER-(P.O_H6790074)_scan0394.exe
- PO 3360.exe

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

- hxxp://hstfurnaces[.]net/gd10/fre.php
- hxxp://nesofirenit[.]gq/stats/fre.php
- hxxp://chrisupdated[.]xyz/ttboi/five/fre.php
- hxxp://dfrcy[.]xyz/MV1/w2/fre.php
- hxxp://qtd8gcdoplav737wretjqmaiy[.]cf/Kent1/fre.php
- hxxp://75bccc18b4d1631c2ecda542c872db27[.]gq/BN1/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php

Top 4 — BeamWinHTTP

BeamWinHTTP is a downloader malware that ranked fourth place with 6.5%. 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

Top 5 — RedLine

RedLine ranked fifth place with 5.9%. 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:

- f0642513.xsph[.]ru
- 45.142.212[.]178
- deyneyab[.]xyz
- rtrkolada[.]xyz
- 5.206.227[.]11

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