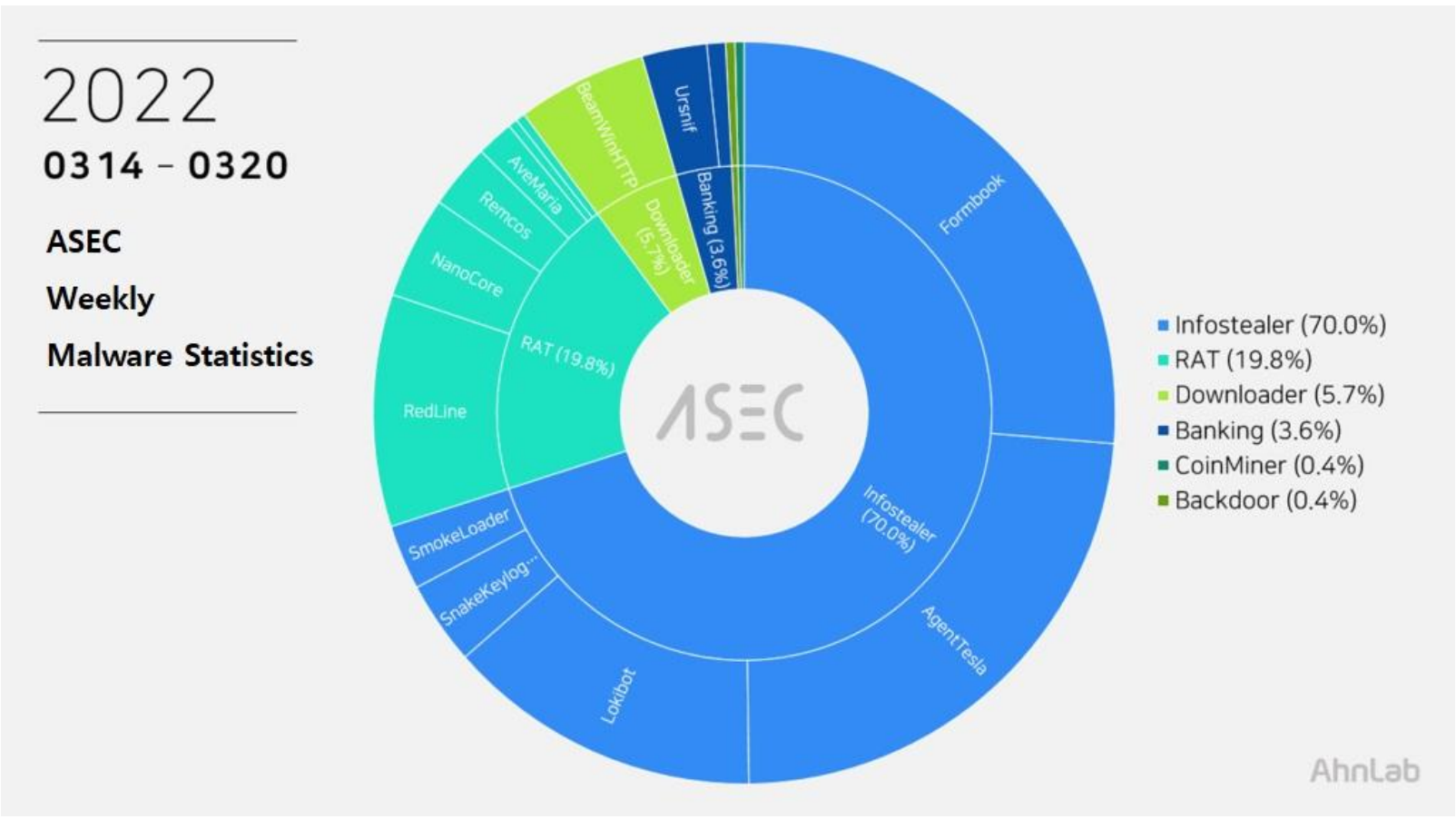
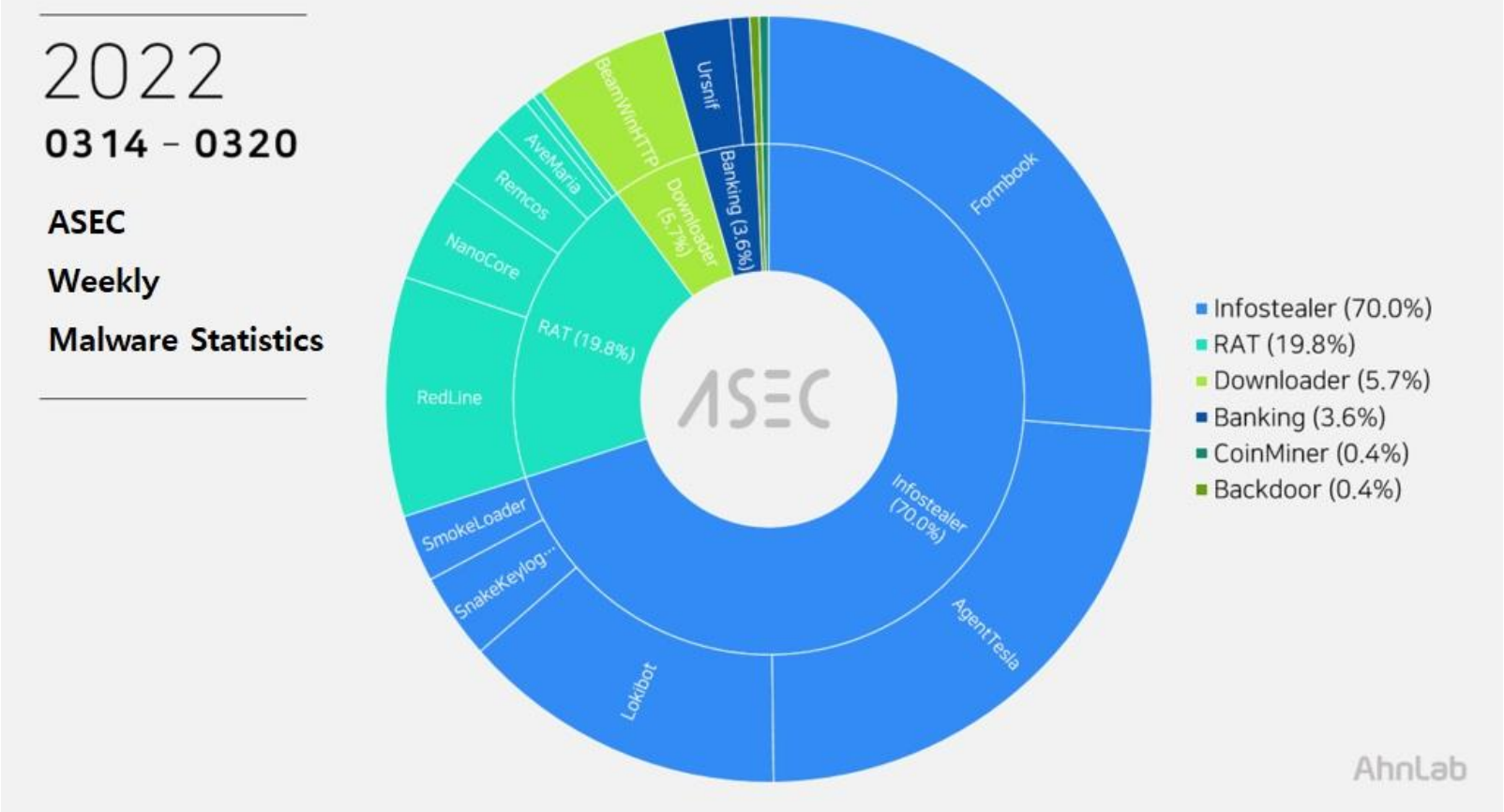
Posted on March 30, 2022

ASEC Weekly Malware Statistics (March 14th, 2022 – March 20th, 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 14th, 2022 (Monday) to March 20th, 2022 (Sunday).

For the main category, info-stealer ranked top with 70.0%, followed by RAT (Remote Administration Tool) with 19.8%, downloader with 5.7%, banking malware with 3.6%, CoinMiner with 0.4%, and backdoor with 0.4%.





Top 1 – Formbook

Formbook ranked first place with 26.3%.

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.

- remittance_details.exe
- LIST_OF_.EXE
- purchase_Order.exe
- Shipping_Documents.exe
- Copia_de_pago_bancario.exe
- March 15th 2022 Monthly Inspection Notification\zuf8gpog5obhvls.exe
- BookOrder_(3)◯◯\zuf8gpog5obhvls.exe
- NEW_ORDER_003DB52.exe
- SCAN_DOCUMENTS.exe
- Contract(XX_Construction)\ceqnotjaj1hudct.exe
- XX_Construction(March14th_Blueprint)\rivhal1bfjf2hen.exe
- International_Document-194-Purchase_LOI-XX-dong\rivhal1bfjf2hen.exe
- ItemDetails\rivhal1bfjf2hen.exe
- BG V.085(07)-REVISED DRAFT BL.exe
- Estimate — bsgs p3 project Paint Work\wsn3k09khinyfim.exe
- XXX\wsn3k09khinyfim.exe
- March 15th 2022 Monthly Inspection Notification\wsn3k09khinyfim.exe
- PAYMENT_COPY.exe
- OFFER.exe
- qoutation.exe
- INVOICE.exe
- KGA20-AC-B6 RFQ Mancuso Nro.6315-22 6313.exe
- banking details.pdf.exe
- PROFORMA_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.ocvcoins[.]com/sued/
- hxxp://www.nropes[.]com/dgrg/
- hxxp://www.plick-click[.]com/w6ot/
- hxxp://fendoremi[.]com/p4sm/
- hxxp://www.pordges[.]com/pot0/
- hxxp://www.cesiesis[.]com/rhen/
- hxxp://www.cures8t[.]com/p9iu/
- hxxp://www.gingure[.]com/mc3w/
- hxxp://www.topvadexo[.]xyz/nr09/
- hxxp://www.hughers3[.]com/cbgo/
- hxxp://www.catdanos[.]com/c6bi/
- hxxp://www.nifaji[.]com/vfm2/
- hxxp://www.alenoce[.]online/id02/
- hxxp://www.mydactil[.]online/e0l9/
- hxxp://www.ducer[.]info/ge32/
- hxxp://www.heinousas[.]com/sj8q/
- hxxp://www.price-hype[.]com/apg5/
- hxxp://vrezvrez[.]com/private/
- hxxp://www.arches2[.]com/c20t/
- hxxp://www.floricg[.]online/b0h3/

- hxxp://www.budistx[.]com/eoww/
- hxxp://www.hutclus[.]online/m0e8/

Top 2 — AgentTesla

AgentTesla is an infostealer that ranked second place with 23.5%. 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.cbiperu[.]com sender: jcanola@cbiperu[.]com receiver: jcanola@cbiperu[.]com user: jcanola@cbiperu[.]com pw: J2111****1@
- server: mail.swarnford[.]in sender: audit@swarnford[.]in receiver: hhamadi@tangafresh[.]com user: audit@swarnford.in pw: F!g***56
- server: mail.orchidexports[.]biz sender: belinda.ruston@orchidexports[.]biz receiver: boxs2599@gmail[.]com user: belinda.ruston@orchidexports[.]biz pw: q6M5****OWDO

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 3 — Lokibot

Lokibot ranked third place with 13.8%. 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://164.90.194[.]235/?id=54083300496945222
- hxxp://75bccc18b4d1631c2ecda542c872db27[.]gq/BN1/fre.php
- hxxp://212.192.241[.]50/3i030/pin.php
- hxxp://chrisupdated[.]xyz/ttboi/panel/five/fre.php
- hxxp://hstfurnaces[.]net/gd21/fre.php
- hxxp://frostandkeeling[.]cf/Ausin4/fre.php
- hxxp://62.197.136[.]186/oluwa/five/fre.php
- hxxp://outlook-webpage-auth[.]ml/worldwide/logs/fre.php
- hxxp://qtd8gcdoplav737wretjqmaiy[.]gq/Kent2/fre.php

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:

- 92.255.57[.]154:11841
- xabigyarall[.]xyz:80
- rtrkolada[.]xyz:80
- 65.21.1[.]119:24371
- 49.12.69[.]202:40517
- 194.87.109[.]41:4608
- 193.150.103[.]37:21330
- 185.215.113[.]122:15386

Top 5 — BeamWinHTTP

BeamWinHTTP is a downloader malware that ranked fifth place with 5.7%. 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
- hxxp://ads-memory[.]biz
- hxxp://luipartners[.]com
- hxxp://stenlihard[.]com

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