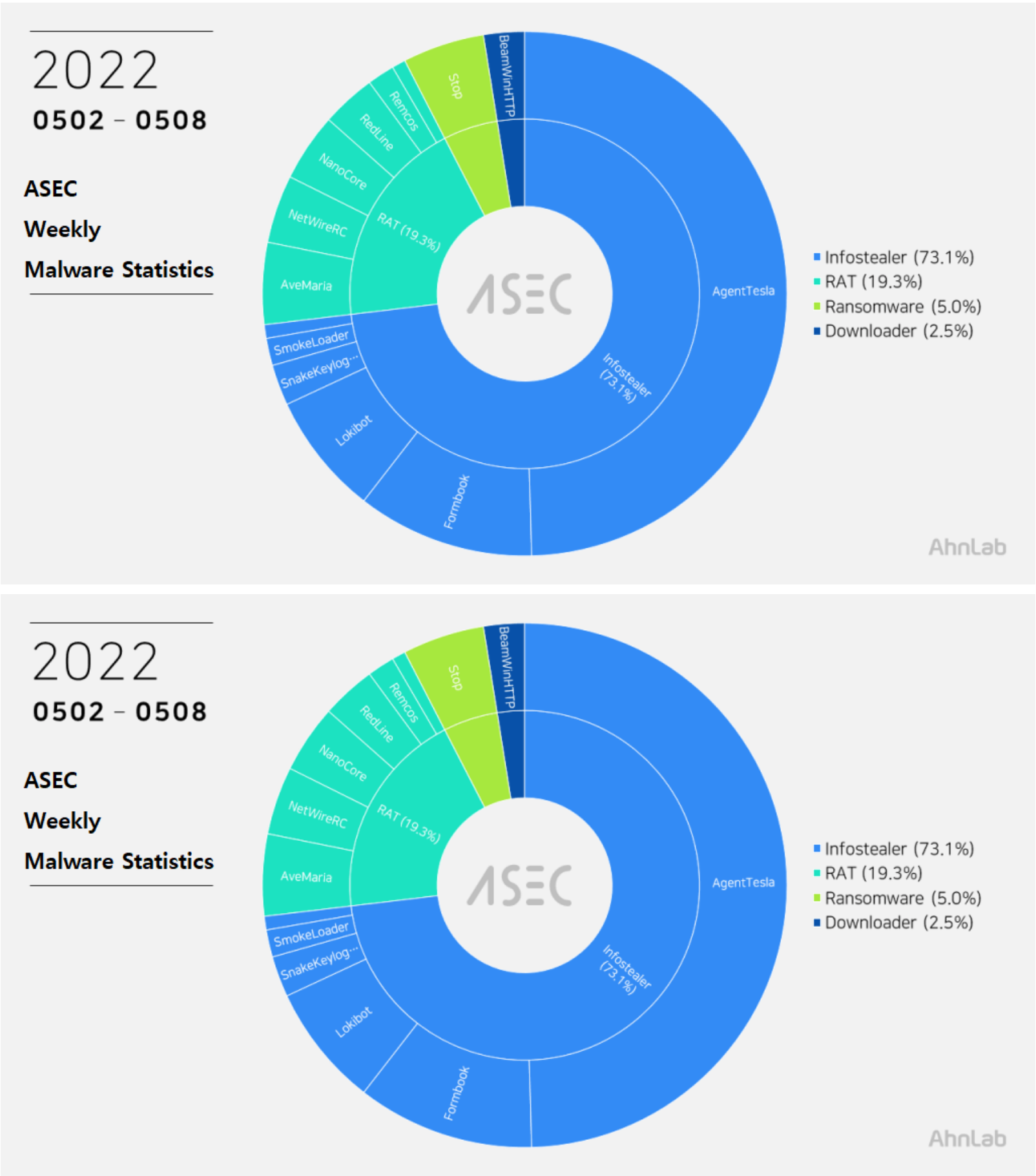
Posted on May 12, 2022

ASEC Weekly Malware Statistics (May 2nd, 2022 – May 8th, 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 May 2nd, 2022 (Monday) to May 8th, 2022 (Sunday).

For the main category, info-stealer ranked top with 73.1%, followed by RAT (Remote Administration Tool) malware with 19.3%, ransomware with 5.0%, and downloader with 2.5%.



Top 1 – AgentTesla

AgentTesla is an infostealer that has taken first place once again with 49.6%. It is an info-stealer that leaks user credentials saved in web browsers, emails, and FTP clients.

> How AgentTesla Malware is Being Distributed in Korea

It uses e-mail to leak collected information, and there are samples that used FTP or Discord API. C&C information of recently collected samples is as follows.

- server: mail.stylestyrofoamind[.]com user: socialmedia@stylestyrofoamind[.]com pw: Qwe****786

- server: mail.ocenmasters[.]com sender: suganthi@ocenmasters[.]com receiver: suwika.on@cj-l[.]net user: suganthi@ocenmasters[.]com pw: donb****12345
- server: us2.smtp.mailhostbox[.]com user: az@gcmce[.]com pw: DANI****16

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.

- 104_PICIF_RIYADH_SOSHEET_1033.exe
- AVVISO_DI_SPEDIZIONE_DHL_xls.exe
- bank_details.exe
- Confirmation.exe
- MV.JUNE_XIN_SHIP_PARTICULARS.xlsx.exe
- new order#22.exe
- PO_#_FJCHM300012.exe
- purchase_order.exe
- PURCHASE_ORDER.exe
- SCAN- AWB 5032675620_MAY 2022.exe
- STATEMENT_OF_ACCOUNT_(SOA).exe

Top 2 — Formbook

Formbook ranked second place with 10.9%.

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

- 657573-ordin.exe
- DHL_EXPRESS.exe
- Invoice_Payment_Advice.exe
- Order_IS010CT5.exe
- REQ FOR QUOTATION.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.b8ceex[.]com/gias/
- hxxp://www.brasbux[.]com/t59n/
- hxxp://www.cablinqee[.]com/fk84/
- hxxp://www.mentication[.]com/s2q8/
- hxxp://www.mentication[.]com/s4ig/
- hxxp://www.nerosbin[.]info/n4w3/
- hxxp://www.rasiorbee[.]com/amdf/

Top 3 — Lokibot

Lokibot malware ranked third place with 7.6%. It is an info-stealer that leaks information about programs such as web browsers, email clients, and FTP clients.

> Lokibot Malware Disguised as Phishing E-mail Requesting for Estimate

Being a malware that is distributed through spam emails, it shares similar file names with other malware spam emails.

- DHL Receipt_AWB811470484778.exe
- DHL_256_007.exe
- fedex receipt_awb5305323204643.exe

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

- hxxp://198.187.30[.]47/p.php
- hxxp://85.202.169[.]172/remote/five/fre.php
- hxxp://lasgidivibescontrol[.]com/lest/five/fre.php
- hxxp://sempersim[.]su/gf10/fre.php
- hxxp://sempersim[.]su/gf13/fre.php
- hxxp://sempersim[.]su/gf7/fre.php

Top 4 — AveMaria

AveMaria ranked fourth place with 5.0%. AveMaria is RAT (Remote Administration Tool) malware with remote control feature that receives commands from the C&C server and performs a variety of malicious behaviors.

AveMaria malware has been distributed via spam emails similar to AgentTesla, Lokibot, and Formbook malware. Additionally, it is packeted and distributed in a form of .NET to bypass detection. As such, the file names reported are not much different from those of other malware distributed through spam emails.

- AKMG MAY ORDER LIST SOA.exe
- PO#30063763006377.pdf.exe
- Quotation#56220.PDF.exe
- STATEMENT OF ACCOUNT (SOA).exe

The following are the confirmed C&C servers of AveMaria.

- 185.140.53[.]174:2404
- 185.183.98[.]169:5678
- 5.2.68[.]67:443

Top 5 — Stop Ransomware

Stop Ransomware ranked fifth place with 5.0%. It is malware that is distributed mainly using exploit kit. This malware encrypts certain files on user PC, and has been distributed in various forms and is still continuously being distributed. The recently distributed samples perform ransomware behavior by installing Vidar, which is an infostealer.

The following is the C&C server URL of Stop ransomware.

- hxxp://ugll[.]org/fhsgtsspen6/get.php
- hxxp://ugll[.]org/test1/get.php
- hxxp://ugll[.]org/test3/get.php
- hxxp://zerit[.]top/dl/build2.exe
- hxxp://ugll[.]org/files/1/build3.exe

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