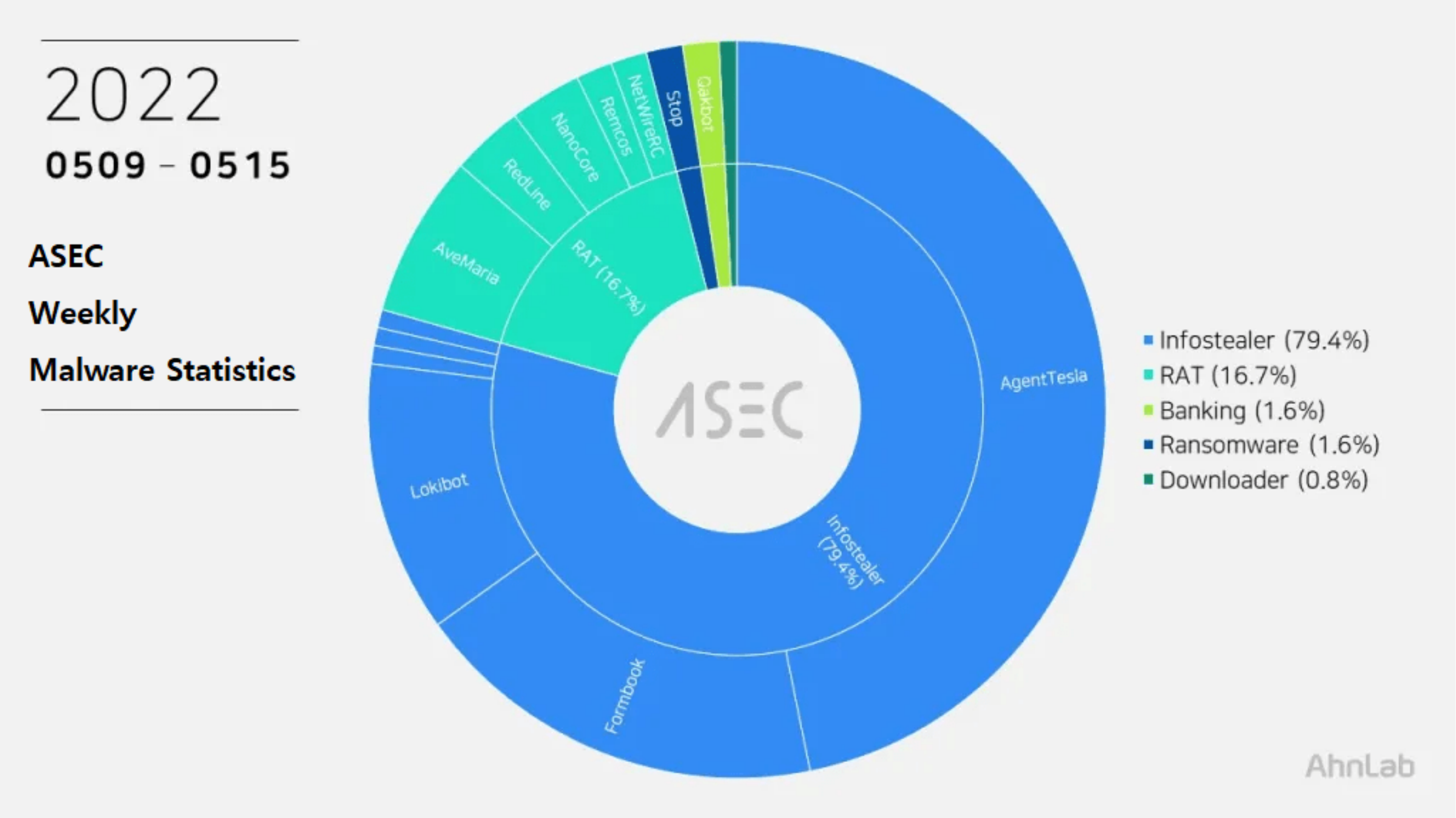
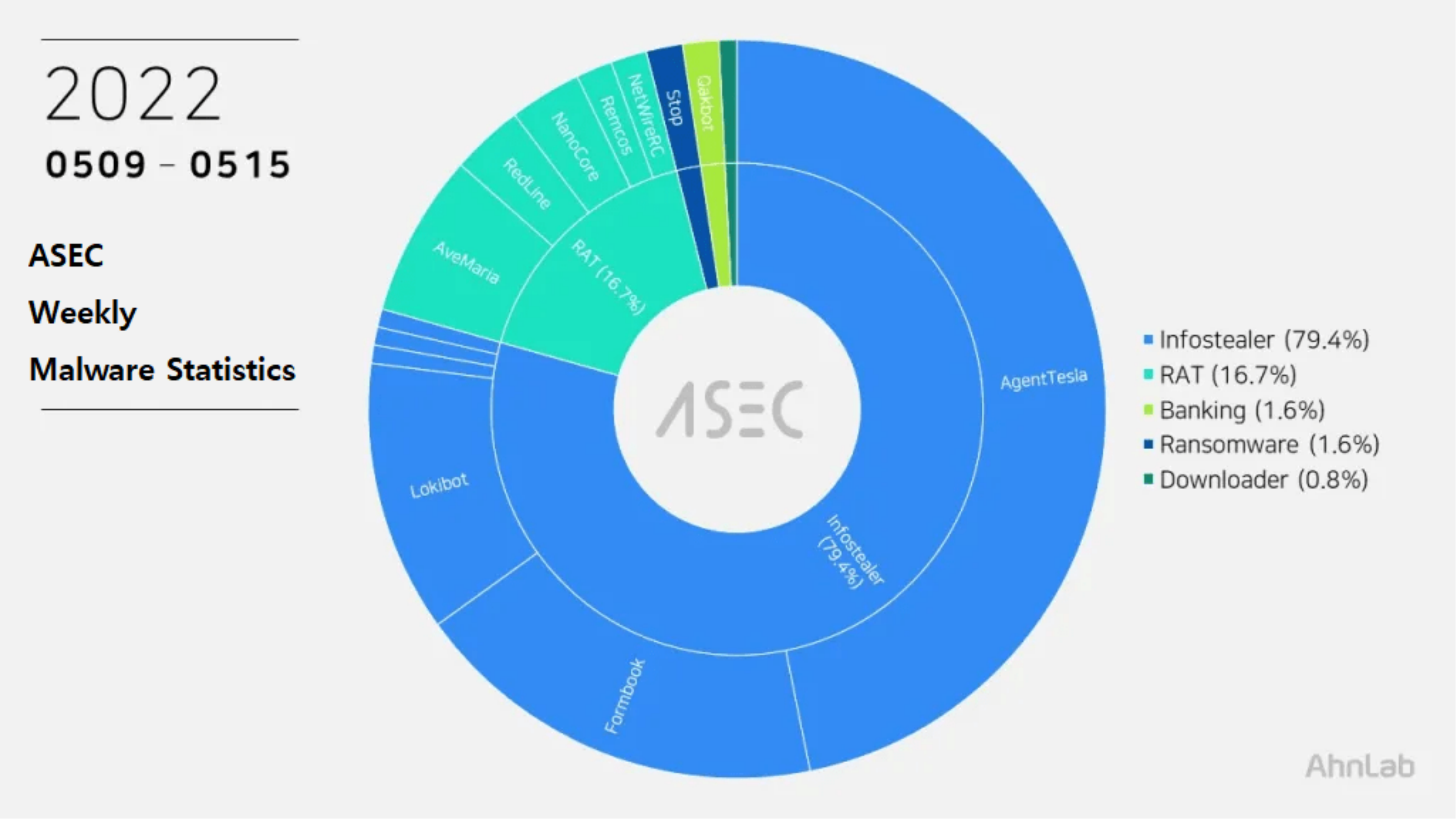
Posted on May 23, 2022

ASEC Weekly Malware Statistics (May 9th, 2022 – May 15th, 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 9th, 2022 (Monday) to May 15th, 2022 (Sunday).

For the main category, info-stealer ranked top with 79.4%, followed by RAT (Remote Administration Tool) malware with 16.7%, banking malware with 1.6%, ransomware with 1.6%, and downloader with 0.8%.





Top 1 – AgentTesla

AgentTesla is an infostealer that has taken first place once again with 46.8%. 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-mails 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.ocenmasters[.]com (198.54.126[.]161) sender: suganthi@ocenmasters[.]com receiver: suwika.on@cj-l[.]net user: suganthi@ocenmasters[.]com pw: do*******345

- server: mail.focuzauto[.]com (166.62.10[.]145) sender: whford@focuzauto[.]com receiver: obtxxxtf@gmail[.]com user: whford@focuzauto[.]com pw: Gd*********16
- server: mail.rnfreight[.]com (108.170.27[.]202) sender: docs1@rnfreight[.]com receiver: zakirrome@ostdubai[.]com user: docs1@rnfreight[.]com pw: O9*****3

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.

- Bank slip.pdf.ex
- SEOUL KOREA.exe
- CASTEC VINA TRADING CO. — NEW PO2022CTV06.exe
- Transfer application form.exe
- compra de orden.xlsx.exe
- SWIFT MESSAGE.exe
- compra de orden.pdf.exe
- DHL_Express Shipping DOCs.exe
- Consignment Documents.exe
- pending orders.exe
- AWB & Shipping Doc.exe
- DHL SHIPMENT NOTIFICATION 1146789443.bat

Top 2 — Formbook

Formbook ranked second place with 18.3%.

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

- berthing.exe
- nuevo pedido.pdf.exe
- 0000356.pdf.exe
- DANG XIAN LIST FOR MAY 2022.exe
- ĐƠN HÀNG MỚI ĐỂ MUA,pdf.exe
- IRQ2207799_Xlxs.exe
- New Orders.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.temp-bait[.]com/n4w3/
- hxxp://www.breskizci[.]com/bs8f/
- hxxp://www.renaziv[.]online/mh76/
- hxxp://www.brasbux[.]com/dx3n/
- hxxp://www.melasco[.]xyz/f43e/
- hxxp://www.clemov[.]xyz/b62r/
- hxxp://www.copikta[.]online/gb10/
- hxxp://www.yevosiz[.]online/b11y/
- hxxp://www.fraxom[.]xyz/sn03/
- hxxp://www.keropy[.]xyz/s4s9/

Top 3 — Lokibot

Lokibot malware ranked third place with 11.9%. 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.

- vbc.exe
- DHL2_324.exe
- orden de compra_pdf____.exe
- winlog.exe
- DHL Receipt_#AWB811470484778.exe

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

- hxxp://sempersim[.]su/gf10/fre.php
- hxxp://sempersim[.]su/fo/fre.php
- hxxp://sempersim[.]su/gf7/fre.php
- hxxp://sempersim[.]su/gf2/fre.php
- hxxp://85.202.169[.]172/remote/five/fre.php
- hxxp://198.187.30[.]47/p.php?id=19957150644816880
- hxxp://198.187.30[.]47/p.php?id=21645050038542306
- hxxp://198.187.30[.]47/p.php?id=36500205676958835

Top 4 — AveMaria

AveMaria ranked fourth place with 7.1%. 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 being distributed as spam mail

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.

- PO09876544567.PDF.exe
- QUOTATION56220.PDF.exe
- DHL SHIPMENT NOTIFICATION 1146789443.bat
- PROJEXT FE-KA-00020 Order 00013433.jpeg.exe
- ORDER598752579098.PDF.exe

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

- 76.8.53[.]133:1198
- 185.183.98[.]169:5678
- 52.12.175[.]156:5252
- 194.5.98[.]225:4545

Top 5 — RedLine

RedLine ranked fifth place with 3.2%. 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:

- 91.241.19[.]112:37425
- iclarinyerac[.]xyz:81

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

AhnLab TIP
빠르게 변화하는 보안 위협
최적의 의사결정
안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요
atip.ahnlab.com

Categories:Malware Information

Tagged as:weekly statistics