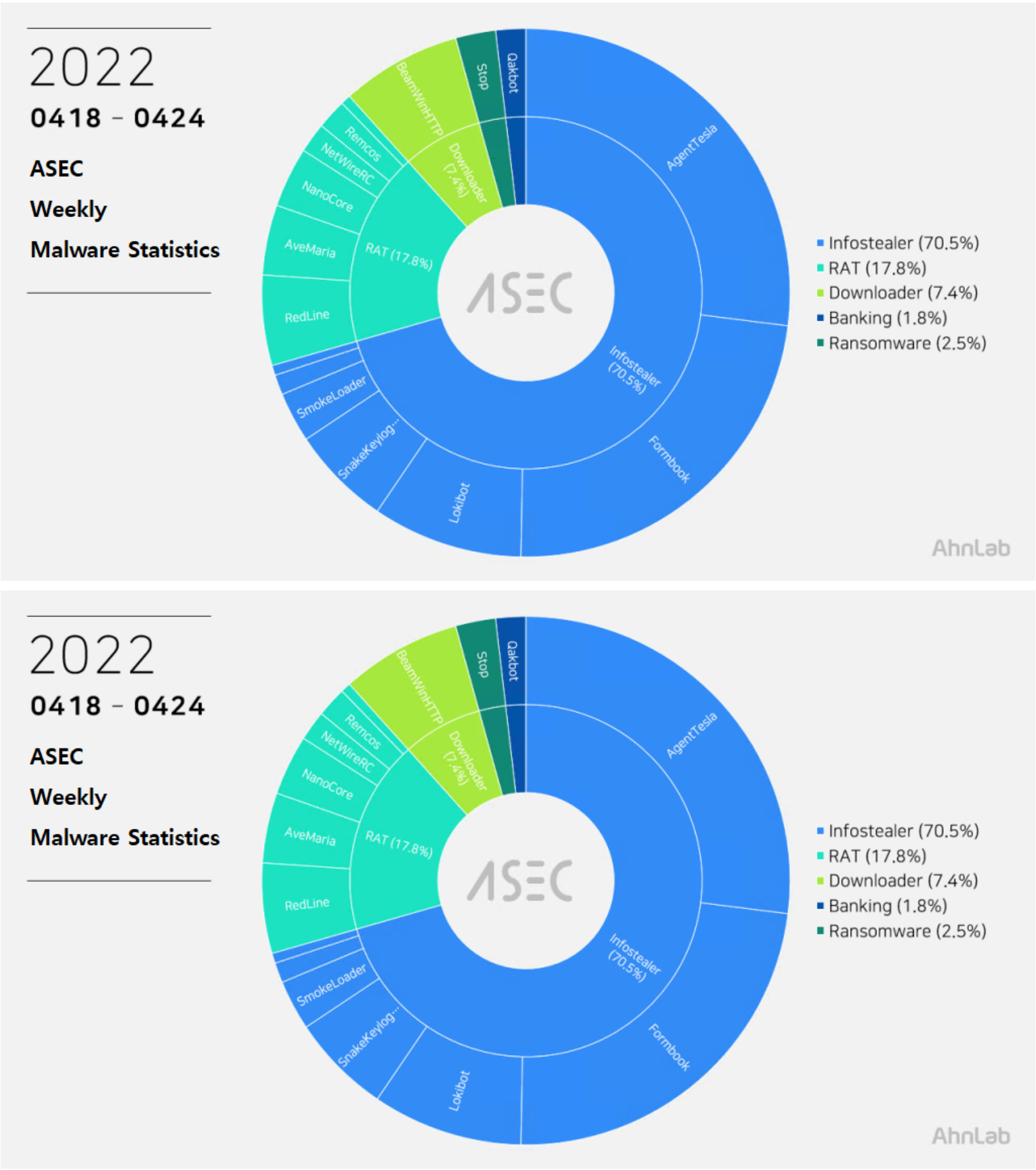
Posted on April 26, 2022

ASEC Weekly Malware Statistics (April 18th, 2022 – April 24th, 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 April 18th, 2022 (Monday) to April 24th, 2022 (Sunday).

For the main category, info-stealer ranked top with 70.5%, followed by RAT (Remote Administration Tool) with 17.8%, downloader with 7.4%, banking malware with 1.8%, ransomware with 2.5%.



Top 1 – AgentTesla

AgentTesla is an infostealer that ranked first place with 27%. 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

Recently collected samples use the following email servers and user accounts when leaking the collected information.

- server mail.shekharlogistics[.]com (208.91.199[.]87) sender asm@shekharlogistics[.]com receiver pcompany157@gmail[.]com user asm@shekharlogistics[.]com pw a*****34

- server mail.rnfreight[.]com (108.170.27[.]202) sender docs1@rnfreight[.]com receiver zakirrome@ostdubai[.]com user docs1@rnfreight[.]com pw O***n3
- server mail.teknovateplas[.]com (103.195.185[.]115) sender marketing@teknovateplas[.]com receiver zamanic62@gmail[.]com user marketing@teknovateplas[.]com pw te*****0$

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.

- Payment Transfer.exe
- Payment_Notice_93653_23001.exe
- DHL Shipping Documents.exe
- Transfer Confirmation 1409675.exe
- RFQ-5560067999011000.exe
- Document.exe
- Quotation.exe
- Swift Copy.exe
- Invoices — Past Due.exe
- statement of account.exe
- new enquiry.exe
- Swift.docx.exe
- PO and payment.exe
- ZPSA-98T522—3326PAYMENT.exe
- Quotation-pdf_____.exe
- PO-PROFORMA INVOICE.exe
- 2022 Johnson& Johnson -PO- 216238068.exe
- Overdue Payment.jar.exe

Top 2 — Formbook

Formbook ranked second place with 23.3%.

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

- DHL Shipping Document.exe
- PO 01 MAGNETROL-ALS-31032022.exe
- PO Inv.pdf.exe
- PO42536383092872.exe
- PO-006134.exe
- Product Specification 01.exe
- doc88.exe
- outstanding overdue statements_xls.exe
- Inquiry_22602057.exe
- SOA March 310322.exe
- SO 101062171.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.alpeshpate[.]com/mwfc/
- hxxp://www.berdisen[.]com/ugfu/
- hxxp://www.cablinqee[.]com/dgi3/
- hxxp://www.gulebic[.]com/u2po/
- hxxp://www.hughers3[.]com/cbgo/

- hxxp://www.mutoros[.]com/tu46/
- hxxp://www.dufcot[.]xyz/i1a6/

Top 3 — Lokibot

Lokibot ranked third place with 9.2%. 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.

- Swift Copy-MT103_pdf.exe
- Factura comercial.pdf.exe
- DHL_Shipping_Documents.exe
- [Request Quotation]korea-6898078_cr-0659_contract order_dd.exe

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

- hxxp://62.197.136[.]176/li/five/fre.php
- hxxp://controlsvr1[.]cf/Concord/fre.php
- hxxp://lokaxz[.]xyz/fc/bk/tt.php
- hxxp://sempersim[.]su/gd17/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php
- hxxp://198.187.30[.]47/p.php?id=21460643090716570

Top 4 — BeamWinHTTP

BeamWinHTTP is a downloader malware that ranked fourth place with 7.4%. 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.

> Malware Being Sneakily Installed in My PC-BeamWinHTTP Malware

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.

> Various Types of Threats Disguised as Software Download Being Distributed

The confirmed C&C server URL is as follows.

- hxxp://212.192.246[.]217/access.php
- hxxp://goldenchests[.]com/checkversion.php
- hxxp://fixholidey[.]com/checkversion.php

Top 5 — SnakeKeylogger

Taking the fifth place with 6.1%, SnakeKeylogger is an info-stealer type malware that leaks information such as user key inputs, system clipboards, and browser account information.

> Snake Keylogger Being Distributed via Spam E-mails

Like AgentTesla, this malware uses e-mail servers and user accounts when leaking collected information. The following are the accounts used by recently collected samples.

- host : mail.alfalahchemicals[.]com (65.60.35[.]98) sender: rafay.yousuf@alfalahchemicals[.]com receiver: princenewman1111@gmail[.]com user: rafay.yousuf@alfalahchemicals[.]com pw: pa*****56
- host : mail.stilltech[.]ro (192.185.100[.]146) sender: office@stilltech[.]ro receiver: christophermartins016@gmail[.]com user: office@stilltech[.]ro pw: eu*****5ro

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