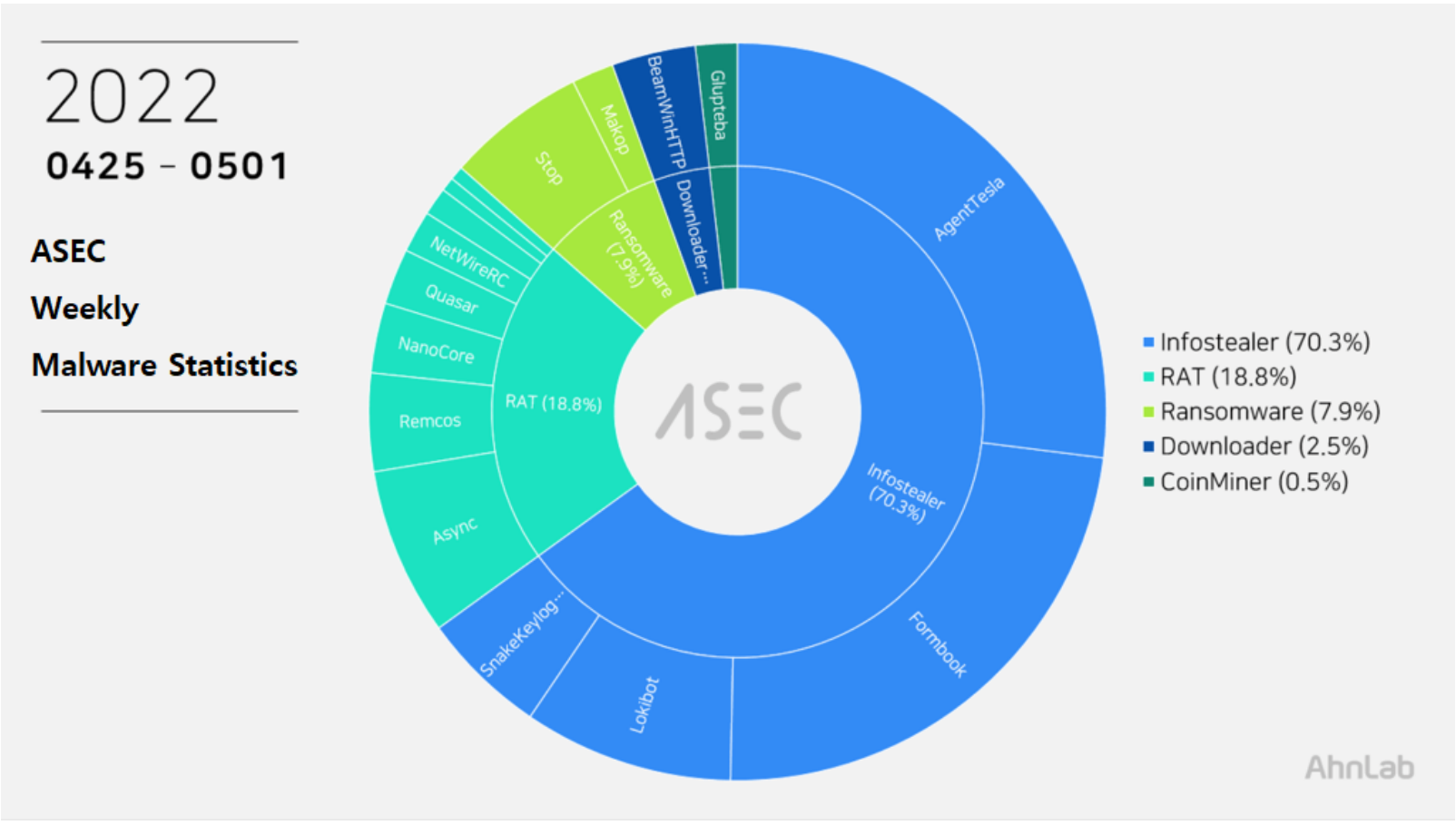
Posted on May 9, 2022

ASEC Weekly Malware Statistics (April 25th, 2022 – May 1st, 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 25th, 2022 (Monday) to May 1st, 2022 (Sunday).

For the main category, info-stealer ranked top with 70.3%, followed by RAT (Remote Administration Tool) malware with 18.8%, ransomware with 7.9%, downloader with 2.5%, and coinminer with 0.5%.



2022
0425 - 0501
ASEC
Weekly
Malware Statistics
AgentTesla
Glupteba
BeamWinHTTP
Downloader...
Makop
Stop
Ransomware (7.9%)
NetWireRC
Quasar
NanoCore
Remcos
RAT (18.8%)
Async
SnakeKeylog...
Lokibot
Formbook
Infostealer (70.3%)
ASEC
Infostealer (70.3%)
RAT (18.8%)
Ransomware (7.9%)
Downloader (2.5%)
CoinMiner (0.5%)
AhnLab

Top 1 – AgentTesla

AgentTesla is an infostealer that ranked first place with 38.6%. 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: ftp.bluecomunidad.com user: rb9ja@bluecomunidad.com pw: D+i*u=****cV

- server: mail.teknovateplas.com sender: marketing@teknovateplas.com receiver: zamanic62@gmail.com user: marketing@teknovateplas.com pw: tekm****020$
- server: mail.myremediez.com sender: help@myremediez.com receiver: willycoker01@yandex.com user: help@myremediez.com pw: 12****456
- server: smtp.advqnce.com sender: user1@advqnce.com receiver: user1@advqnce.com user: user1@advqnce.com pw: S!****g6
- server: mail.keeprojects.in sender: quality@keeprojects.in receiver: quality@keeprojects.in user: quality@keeprojects.in pw: quali****!

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.

- OFFER_AND_PICTURES.exe
- PT HCU2435.exe
- STR-DD225227.exe
- INVOICE.exe
- PURCHASE_ORDER.exe
- PO_#102-00549338.exe
- Updated_SOA.exe
- Remittance_Advise.exe
- Shipping_Documents.exe
- SHIPMENT_STATUS.exe
- printouts of outstanding as of 27-04-2022.exe
- Revised_Documents.exe
- ENQ 3720014088.exe
- new order#22.exe
- NEW_PO#.exe
- 2022_QUOTE-RFQ-22-03794.exe
- QNLNSAHMD2202897.exe
- MT1032776380.exe
- Re,_texiles_product.exe
- PO4522435545545553WQR.exe
- PO_8773645_90222364_989_00111283838448_2022.exe
- SCAN_04355_wire_swift_00000000001.exe

Top 2 — Formbook

Formbook ranked second place with 21.3%.

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

- PI-Order_IS01OCT5_xlxs.exe
- DHL_SHIPMENT_NOTIFICATION.exe
- New_Purchas_Order.exe
- Invoice_&_Packlist.exe
- invoice no. Q1-4001028L.exe
- Shipping_Documents.bat.exe
- Catalogue_Request_Sheet_and_Product_Inquiry.exe
- Shipping_Documts.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.banceout3[.]com/ceah/
- hxxp://www.beputis4[.]com/afj0/
- hxxp://www.berdisen[.]com/mt6e/

- hxxp://www.besasin09[.]com/c1rg/
- hxxp://www.binges66v[.]com/eggp/
- hxxp://www.breskizci[.]com/bs8f/
- hxxp://www.buggy4t[.]com/ocgr/
- hxxp://www.conjupy[.]online/a23w/
- hxxp://www.demtate[.]xyz/d23n/
- hxxp://www.fadsek[.]xyz/u27o/
- hxxp://www.getdetzag[.]xyz/kt03/
- hxxp://www.ipoyce[.]online/d1n3/
- hxxp://www.keropy[.]xyz/s4s9/
- hxxp://www.moukse[.]com/n35q/
- hxxp://www.mutoros[.]com/tu46/
- hxxp://www.nerosbin[.]info/n4w3/
- hxxp://www.nifaji[.]com/uj3c/
- hxxp://www.nu865ci[.]com/g5so/
- hxxp://www.penuay[.]online/p84g/
- hxxp://www.rasiorbee[.]com/amdf/
- hxxp://www.renaziv[.]online/mh76/
- hxxp://www.rezcoat[.]online/b1s5/
- hxxp://www.singmos[.]online/o18j/
- hxxp://www.yevosiz[.]online/b11y/

Top 3 — Lokibot

Lokibot ranked third place with 7.4%. 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_AWB2045829822.exe
- Swift_Copy.exe

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

- hxxp://103.147.185[.]85/1/fre.php
- hxxp://164.90.194[.]235/?id=21460643090716570
- hxxp://198.187.30[.]47/p.php?id=21645050038542306
- hxxp://198.187.30[.]47/p.php?id=23287771531910382
- hxxp://198.187.30[.]47/p.php?id=3129435466035640
- hxxp://198.187.30[.]47/p.php?id=36500205676958835
- hxxp://198.187.30[.]47/p.php?id=5566589175702602
- hxxp://37.0.8[.]87/freshlogs/fre.php
- hxxp://45.133.1[.]45/me/five/fre.php
- hxxp://62.197.136[.]176/userbob/five/fre.php
- hxxp://62.197.136[.]186/oluwa/five/fre.php
- hxxp://controlsvr1[.]ga/Concord/fre.php
- hxxp://panel-report-logs[.]ml/dandollars/fre.php
- hxxp://plxnva67001gs6gljacjpqudhatjqf[.]gq/Concord/fre.php
- hxxp://sempersim[.]su/ge25/fre.php
- hxxp://sempersim[.]su/gf4/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php

Top 4 — Stop Ransomware

Stop Ransomware ranked fourth place with 6.9%. 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://zerit[.]top/dl/build2.exe
- hxxp://fuyt[.]org/fhsgtsspen6/get.php
- hxxp://fuyt[.]org/files/1/build3.exe

Top 5 — NanoCore

NanoCore was ranked fifth place with 5.0%. It is a RAT malware developed with .NET. Like njRAT, it can perform various commands given by the attacker such as information leakage including keylogging.

Similar to AgentTesla, Formbook, AveMaria, and Remcos, the NanoCore is packed with .NET packing and distributed through attached files in spam emails. As such, the file names reported are not much different from those of other malware distributed through spam emails. Recently, multiple cases of distribution of compressed files disguised as the following files were discovered.

- lot902019302023.pdf\8asy2eja8ctafvm.exe
- img.111009102890.jpg\z8xwvm80rrz8x5z.exe
- IMG.4436663726277.JPG.z\tbdwk2odkwtidii.exe
- doc00200249489354.pdf.lzh\qpmivwhymdzmdno.exe
- kakaotalk_20220520_1342128.pdf.lzh\fmjxnvlgmlj49pf.exe
- 00909978299.lzh\xxuhj5pkutszx9a.exe

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

- strongest.ddns[.]net:54761
- naga0.ddns[.]net:54761
- lowspeed.ddns[.]net:50421
- greatman.hopto[.]org:9070
- 91.193.75[.]221:4040
- 62.197.136[.]29:6932

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