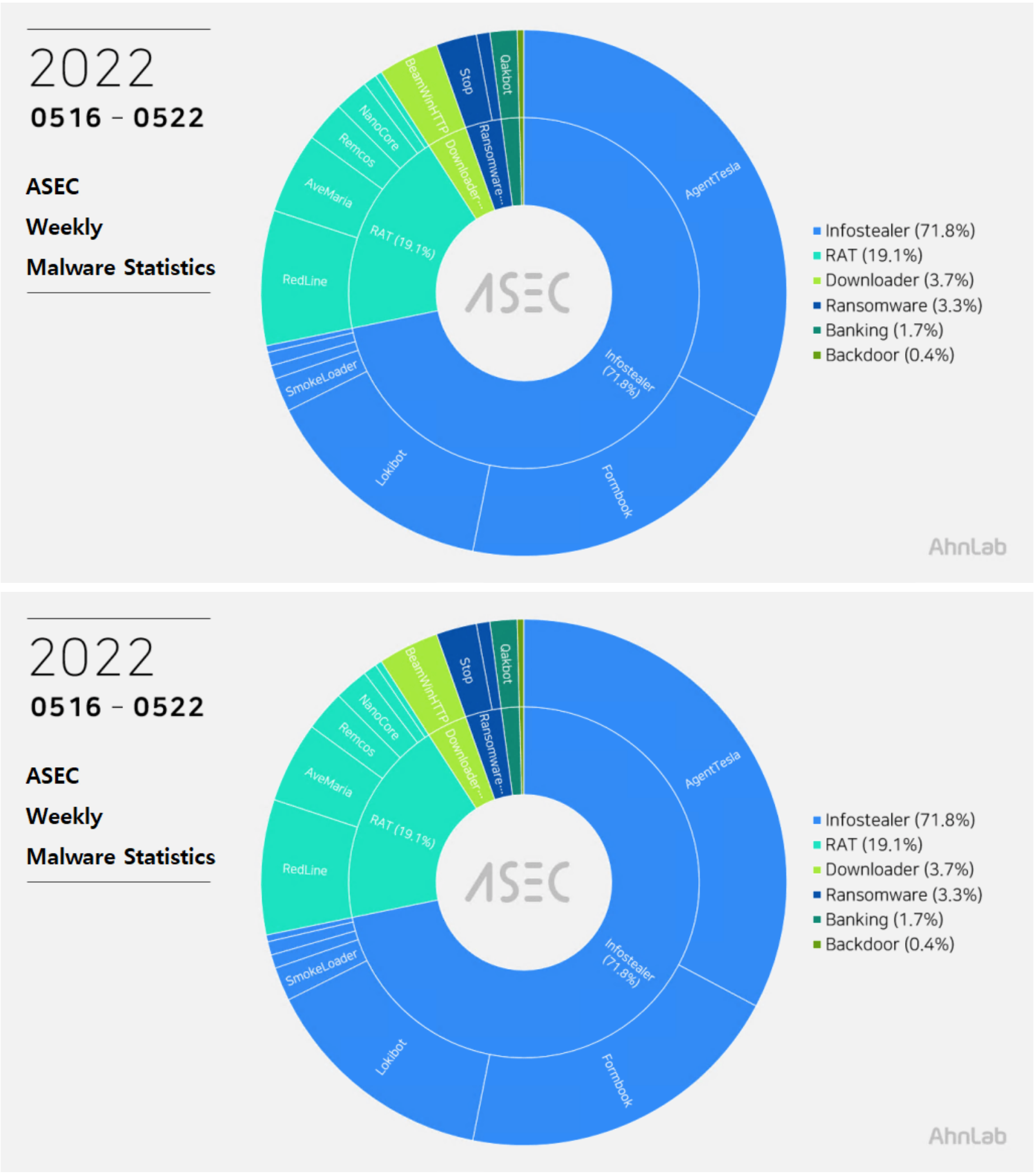
Posted on May 27, 2022

ASEC Weekly Malware Statistics (May 16th, 2022 – May 22nd, 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 16th, 2022 (Monday) to May 22nd, 2022 (Sunday).

For the main category, info-stealer ranked top with 71.8%, followed by RAT (Remote Administration Tool) malware with 19.1%, downloader with 3.7%, ransomware with 3.3%, banking malware with 1.7%, and backdoor with 0.4%.



Top 1 – AgentTesla

AgentTesla is an infostealer that has taken first place once again with 32.8%. It is an info-stealer that leaks user credentials saved in web browsers, emails, and FTP clients.

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.permagraf.com[.]mx (174.136.37[.]109) sender : danny@permagraf.com[.]mx receiver : danny@permagraf.com[.]mx user : danny@permagraf.com[.]mx pw : icui****@@

- server : mail.subnet-group[.]com (206.189.39[.]129) sender : edna@subnet-group[.]com receiver : eh746746@gmail[.]com user : edna@subnet-group[.]com pw : cr****h1t
- server : mail.focuzauto[.]com (166.62.10.[]145) sender : whford@focuzauto[.]com receiver : obtxxxtf@gmail[.]com user : whford@focuzauto[.]com pw : Gd****rd@2016

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.

- inv TS00005597.exe
- PO.exe
- payment.exe
- COMPROBANTE DE RETIRO SPEI No.79433161_20220520_0230_pagos_transferencia.pdf_pag
- Aviso de pago.pdf.exe
- DN_SACX20176287763680.exe
- Payment Advice.exe
- PROFORMA INVOICE.exe

Top 2 — Formbook

Formbook ranked second place with 20.3%.

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

- RECEIPT_.EXE
- PDF-SCAN-ORDER.exe
- payment_slip_098473.exe
- PURCHASE ORDER FOR GPI ,KAGAL MIDC.exe
- PO0826728826726.exe
- FATURA.exe
- DHL SHIPMENT NOTIFICATION 1146789443.exe
- Fattura_855.pdf.exe
- Scan -166774678237277478382394878384744 pdf.exe
- payment_slip_098473.exe
- Proof_Of_Payment.exe
- NEW_ORDE.EXE
- Swift.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.bestrewlinq[.]xyz/mg11/
- hxxp://www.caobatins[.]com/tdht/
- hxxp://www.demtate[.]xyz/d23n/
- hxxp://www.englishkap[.]xyz/sn12/
- hxxp://www.fusersing[.]com/guba/
- hxxp://www.gulebic[.]com/u2po/
- hxxp://www.hecsearc[.]com/pb0u/
- hxxp://www.japbom[.]online/d6co/
- hxxp://www.lesotip[.]online/m74s/
- hxxp://www.myqmetrbs[.]com/smwr/
- hxxp://www.pleqwag[.]online/b94h/
- hxxp://www.rabies36[.]com/n8m8/
- hxxp://www.scramet[.]online/xw72/

- hxxp://www.tumpiums[.]com/he8c/
- hxxp://www.veminis[.]com/zu08/

Top 3 — Lokibot

Lokibot malware ranked third place with 14.5%. 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.

- Shipping Documents.exe
- Quote.exe garuba1.exe
- Order#051822.exe
- Purchase order.exe
- FedEx Receipt_AWB#5305323204643.exe
- copia rápida_pdf_____.exe

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

- hxxp://198.187.30[.]47/p.php?id=77061076177087l1
- hxxp://sempersim[.]su/fo/fre.php
- hxxp://debsfletchofu[.]cf/debsfletch/logs/fre.php
- hxxp://45.133.1[.]20/rex/five/fre.php
- hxxp://85.202.169[.]172/goodlife/five/fre.php
- hxxp://hyatqfuh9olahvxf[.]gq/BN3/fre.php
- hxxp://vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php
- hxxp://unitedcourierparcel[.]com/cjg/loki/fre.php
- hxxp://lokaxz[.]xyz/fc/bk/ss.php
- hxxp://hyatqfuh9olahvxf[.]ga/Legend/fre.php

Top 4 — RedLine

RedLine ranked fourth place with 8.3%. 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:

- iclarinyerac[.]xyz:81
- 212.192.246[.]122:4251
- 194.36.177[.]115:41097
- 193.233.48[.]58:38989
- 193.150.103[.]38:40169
- 193.106.191[.]253:4752
- 185.242.85[.]232:80
- 185.230.143[.]91:44624
- 185.215.113[.]75:80
- 185.215.113[.]201:21921
- 152.89.219[.]248:19932
- 141.95.211[.]151:34846
- 109.107.191[.]37:1657
- 104.168.44[.]52:80

Top 5 — AveMaria

AveMaria ranked fifth 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.

- Yeni sipariş _WJO-001, pdf.exe
- 19042022- PL.exe
- ikmoerezx94218.exe
- CustomAttributeFormatExcept.exe
- FieldBuil.exe

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

- 37.0.14[.]206:5208
- 104.128.191[.]44:8080
- 79.134.225[.]69:3431
- 2.56.56[.]88:2405
- 154.118.103[.]139:5207
- 80.66.64[.]147:5207
- 194.147.140[.]211:9897

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