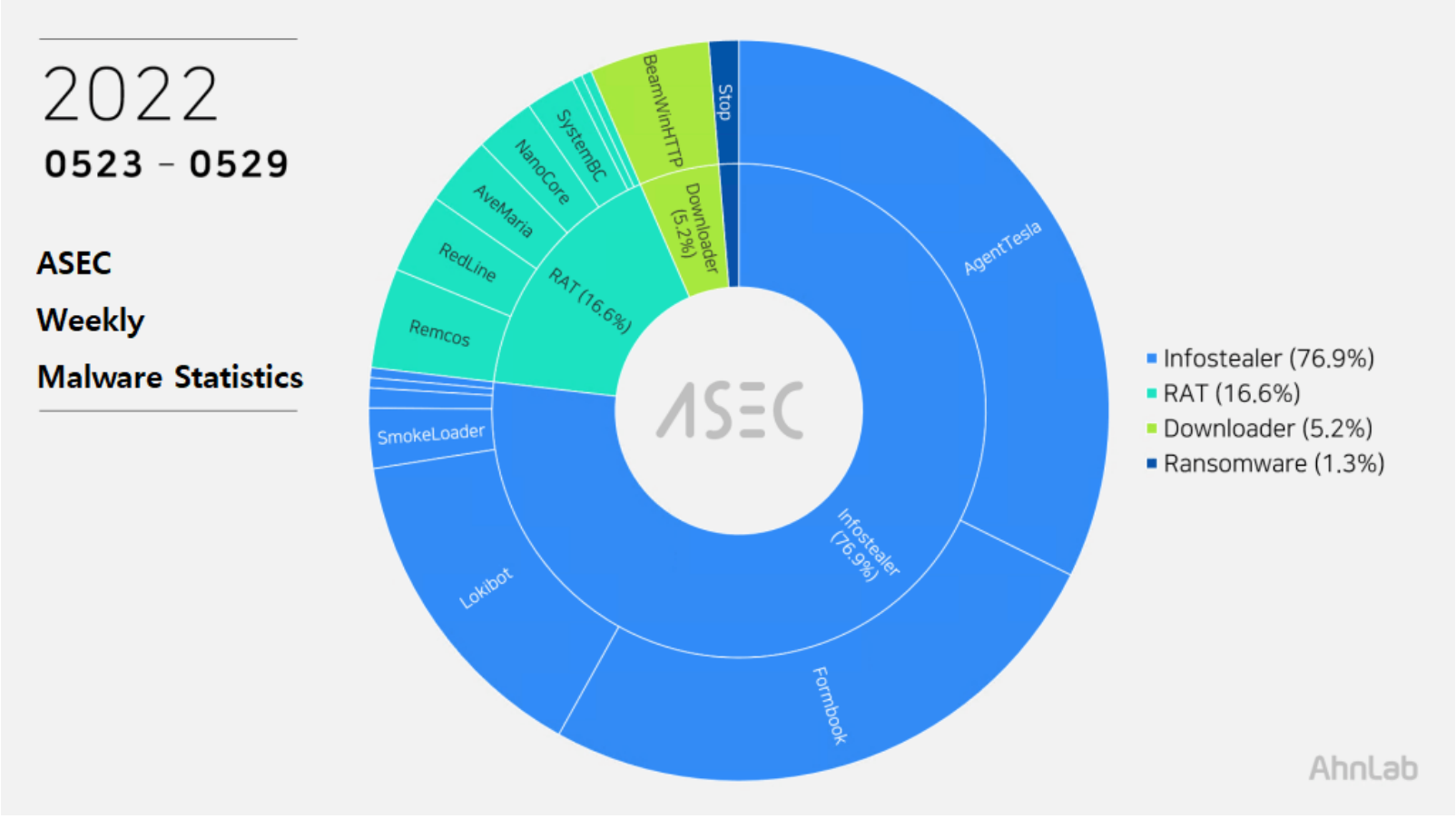
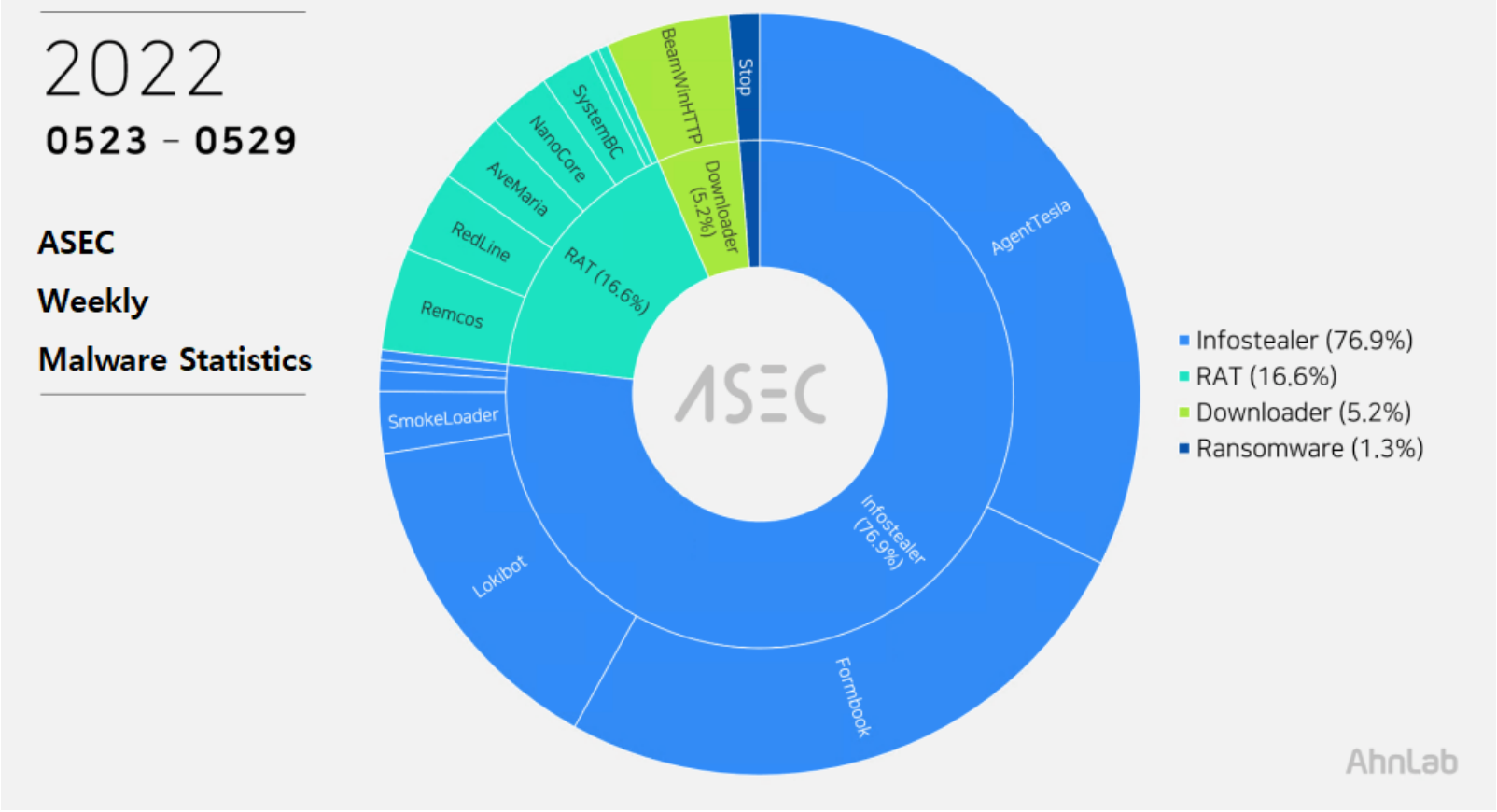
Posted on June 2, 2022

ASEC Weekly Malware Statistics (May 23rd, 2022 – May 29th, 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 23rd, 2022 (Monday) to May 29th, 2022 (Sunday).

For the main category, info-stealer ranked top with 76.9%, followed by RAT (Remote Administration Tool) malware with 16.6%, downloader with 5.2%, and ransomware with 1.3%.





Top 1 – AgentTesla

AgentTesla is an infostealer that has taken first place once again with 32.3%. 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 : dannyreports@permagraf.com[.]mx user : danny@permagraf.com[.]mx pw : icui****@@

- server : mail.tejarathotel[.]af (144.76.114.106) sender : info@tejarathotel[.]af receiver : ranjqnupreti3@gmail[.]com user : info@tejarathotel[.]af pw : Kab****22#
- server : mail.kls[.]af (144.76.114.106) sender : info@kls[.]af receiver : ranjqnupreti3@gmail[.]com user : info@kls[.]af pw : Kab****42@

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.

- AWB & Shipping Documents.exe
- SCAN 023.exe
- REQUISITION FOR MV BRAVERY ACE.docx.exe
- documents of 20-2185-2.exe
- 000993827-4429MX.pdf.exe
- account statement .exe
- Orden de compra.pdf.exe
- CMA-CGM DOC #AKI0418107.exe
- PDA Query — 180397-05-16-22 Port Agency Appointment_pdf.exe
- MV PACIFIC ENDEAVOR V2202 — USD55,000.pdf.exe

Top 2 — Formbook

Formbook ranked second place with 25.8%.

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

- two_months_salary_receipts.exe
- ItemsRequest.PDF.exe
- PURCHASING INQUIRY.PDF.exe
- Transferencia 001.exe
- (PO#1164031.exe
- SWIFT.exe
- PO#71099583.exe INQ R138-CR-MO.exe
- Price Quote Request.exe CTM Copy_xlsx.exe
- Order_673N78333_xlsx.exe
- Quotation-2328333.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.

- http://www.simplybans[.]com/ng9o/
- http://www.momentums6[.]com/tn61/
- http://www.breskizci[.]com/bg5r/
- http://www.temp-bait[.]com/amdf/
- http://www.click-tokens[.]com/ta3t/
- http://www.exilings[.]com/ygkp/
- http://www.hecsearc[.]com/pb0u/
- http://www.caramelshubs[.]com/crqp/
- http://www.motarasag[.]com/sr4i/
- http://www.bravesxx[.]com/mwfc/
- http://www.travelsagas[.]com/a5qd/

Top 3 — Lokibot

Lokibot malware ranked third place with 14.4%. 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.

- SH22-OD03-22.exe
- COTIZACIÓN.pdf.exe
- HB1231_SEQ.22_PO_inquiry.exe
- PO063680.exe UF_86064_HG.exe
- PO_OPBM2.exe
- DATOS BANCARIOS DE REEMBOLSO DE PAGO.exe
- SEOC**** INDUSTRY.exe
- HB1231_SEQ.22_PO_inquiry.exe

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

- 198.187.30[.]47/p.php?id=24066800920482691
- 85.202.169[.]172/kelly/five/fre.php
- sempersim[.]su/gg8/fre.php
- lokaxz[.]xyz/fc/bk/ss.php
- pgixx[.]xyz/Smd/PWS/fre.php
- vmopahtqdf84hfvsqepalcbcch63gdyvah[.]ml/BN2/fre.php
- 62.197.136[.]176/liyan/five/fre.php
- 45.133.1[.]45/perez1/five/fre.php
- hyatqfuh9olahvxf[.]ml/Subject/fre.php
- 45.133.1[.]20/uche/five/fre.php
- umenako.co[.]vu/otm/five/fre.php

Top 4 — BeamWinHTTP

BeamWinHTTP is a downloader malware that ranked fourth place with 5.2%. 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.

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.

The confirmed C&C server URLs are as follows.

- glicefud[.]com/checkversion.php
- 37.0.8[.]39/access.php
- 212.192.246[.]217/access.php

Top 5 — Remcos

This week, Remcos ranked fifth place 4.4%. Remcos is a RAT malware that carries out various commands given by the attacker such as keylogging and information leaking.

Remcos is packed with a .NET packer and is distributed as attachments of spam mails, just like AgentTesla, Formbook, and NanoCore. Recently, there are some cases where it got distributed after disguising itself as a certain tool.

The confirmed C&C server URLs of Remcos are as follows.

- salesumishcn.ddns[.]net:9764
- 91.243.44[.]130

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