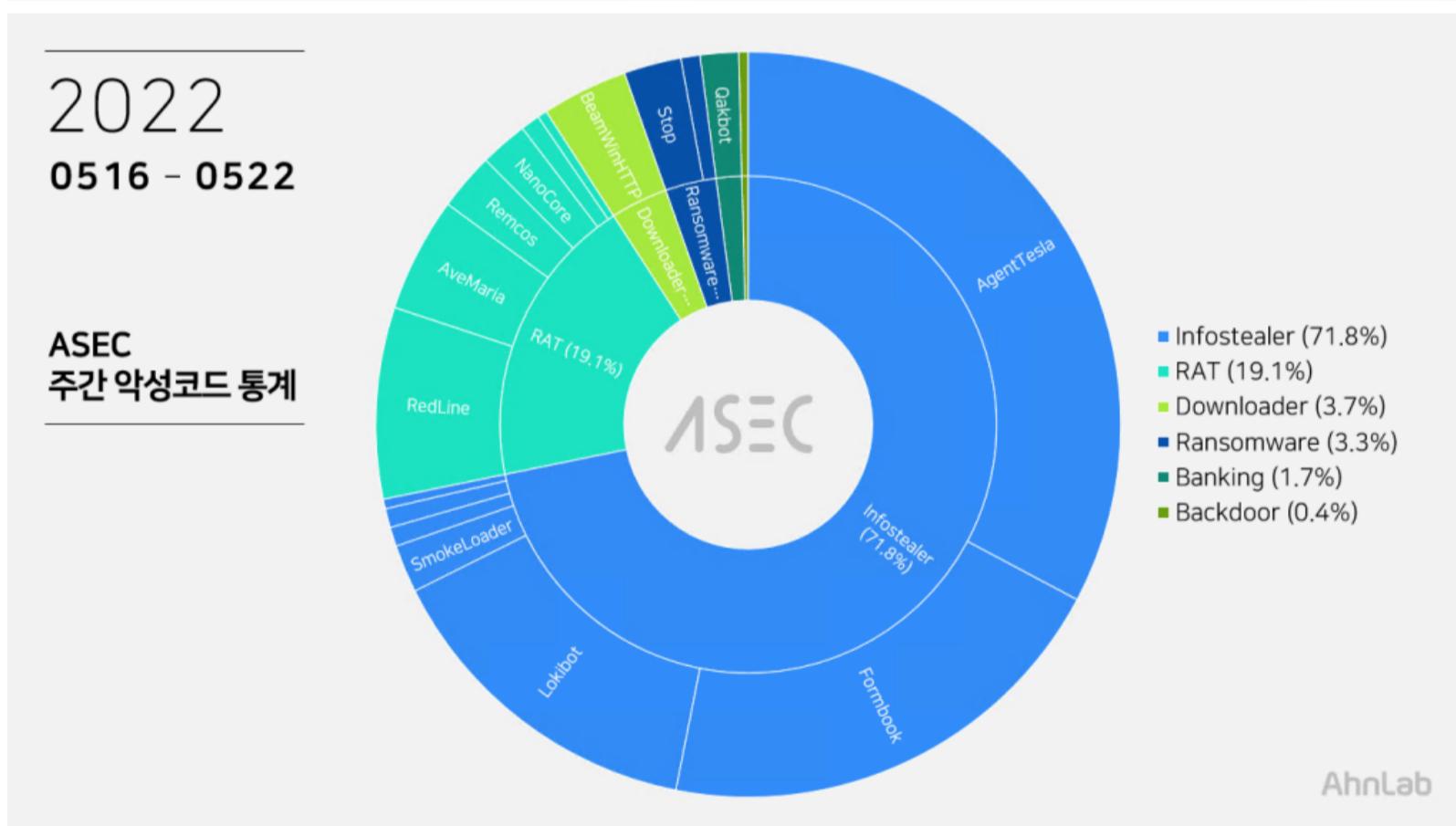
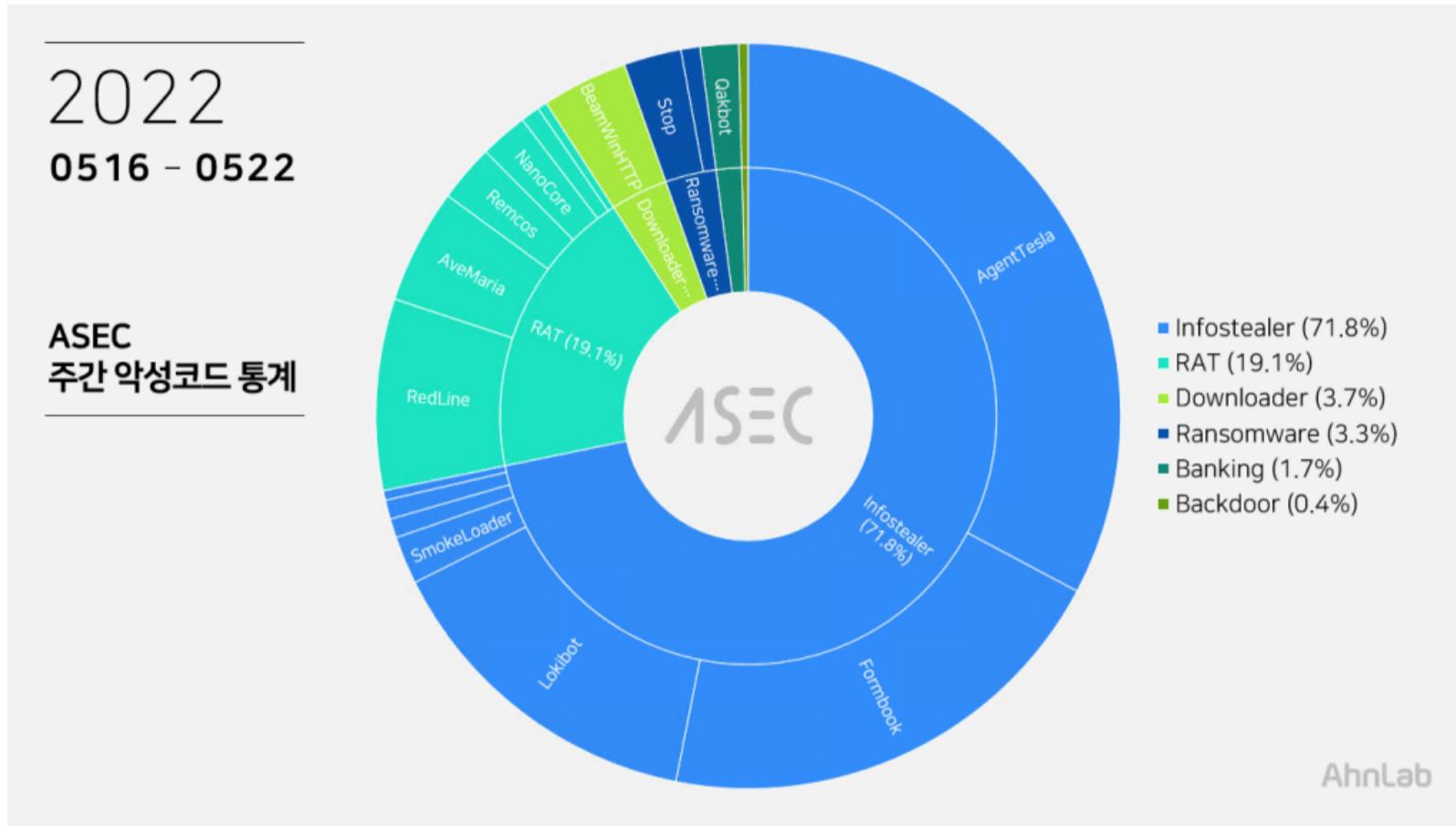


## ASEC Weekly Malware Statistics ( 20220516 ~ 20220522 )

The ASEC analysis team uses the ASEC automatic analysis system RAPIT to classify and respond to known malicious codes. This post summarizes the statistics of malicious code collected for one week from Monday, May 16, 2022 to Sunday, May 22, 2022.

Infostealer took the first place with 71.8%, followed by RAT (Remote Administration Tool) malware with 19.1%, downloader with 3.7%, ransomware with 3.3%, banking with 1.7%, and backdoor with 0.4%.



### Top 1 — AgentTesla

AgentTesla, an infostealer malware, ranked first with 32.8%, following last week. AgentTesla is an infostealer-type malware that leaks user information stored in web browsers, mail and FTP clients.



How is AgentTesla malware

being distributed in Korea? — ASEC BLOG 올해 초부터 피싱 메일에 악성 파워포인트(\*.PPT) 파일이 첨부되어 유포중인 사례가 확인되고 있다. ASEC 분석팀에서는 최근 이러한 공격 방식을 통해 AgentTesla가 최종 실행된 것을 포착하여 이에 대해 알리려한다. 해외에서는 아래 블로그처럼 해외에서도 올 1월 정보유출형 악성코드 azorult가 메일에 첨부된 PPT를 통해 유포되었다. (해외 블로그 : <https://appriver.com/resources/blog/january-2020/powerpoint-malware-references-drake-lyrics-drop-lokibot-azorult...>)

수집한 정보 유출 시 메일을 활용하며 FTP나 Discord API 등을 사용하는 샘플도 존재한다. 최근 샘플들의 C&C 정보는 아래와 같다.

- 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

대부분 송장(Invoice), 선적 서류(Shipment Document), 구매 주문서(P.O. – Purchase Order) 등으로 위장한 스팸 메일을 통해 유포되기 때문에 파일명도 이와 관련된 단어 또는 문장이 사용된다. 확장자의 경우 pdf, xlsx와 같은 문서 파일로 위장한 샘플도 다수 존재한다.

- 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 악성코드는 20.3%로 2위를 기록하였다.



메일을 통해 유포 중인 새

로운 버전의 Formbook 악성코드 – ASEC BLOG Formbook은 Infostealer 유형의 악성코드로, 주로 메일의 첨부파일을 통해 유포되며 유포량이 매우 많다. ASEC 블로그에도 관련 게시글을 여러 차례 게시하였다. Formbook 악성코드의 C2 통신 방식 견적서/발주서 제목의 정보유출 악성코드 (Formbook) 주의! ASEC 분석팀은 최근 Formbook 악성코드가 이메일을 통해 새로운 버전으로 유포 중인 것을 확인했다. 기존 Formbook 악성코드는 내부에 버전을 의미하는 숫자가 “4.1”이었지만 최근 유포 중인 Formbook 악성코드는 “2.3”을 사용한다....

다른 인포스틸러 악성코드들과 동일하게 대부분 스팸 메일을 통해 유포되며 유포 파일명도 유사하다.

- 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

Formbook 악성코드는 현재 실행 중인 정상 프로세스인 explorer.exe 및 system32 경로에 있는 또 다른 정상 프로세스에 인젝션함에 따라 악성 행위는 두 정상 프로세스에 의해 수행된다. 웹 브라우저의 사용자 계정 정보 외에도 키로깅, Clipboard Grabbing, 웹 브라우저의 Form Grabbing 등 다양한 정보를 탈취할 수 있다.



Formbook 악성코드의 C2

통신 방식 – ASEC BLOG 대다수의 악성코드는 공격자의 명령 수신과 추가 악성 행위를 위해 C2(Command & Control server)를 활용한다. 공격자의 입장에서는 AV 제품의 감시망을 뚫고 사용자 PC에 악성코드를 감염시켜도 C2 접속이 차단되면 무용지물이다. 따라서 C2 정보 파악을 어렵게 하기 위해 가짜 C2와 통신을하거나, 단 한 개라도 작동을 보장하기 위해 많은 수의 C2를 사용하는 등의 다양한 기법을 사용한다. Formbook 악성코드는 이렇게 C2 파악이 어려운 대표적인 악성코드이다. 본 게시글에서는 Formbook 악성코드의 C2...

다음은 확인된 Formbook의 C&C 서버 주소이다.

- 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 악성코드는 14.5%로 3위를 기록하였다. Lokibot은 인포스틸러 악성코드로서 웹 브라우저, 메일 클라이언트, FTP 클라이언트 등의 프로그램들에 대한 정보를 유출한다.



구매 주문서 메일로 위장하여 유포 중인 Lokibot 악성코드 – ASEC BLOG Lokibot 은 인포스틸러 악성코드로서, 웹 브라우저, 메일 클라이언트, FTP 클라이언트 등 감염 PC에 설치된 다양한 프로그램들에서 계정 정보를 탈취하는 기능을 가지고 있다. 수 년 전부터 꾸준히 유포되고 있는 악성코드이지만, 아래의 주간 통계에서 확인되듯이 최근까지도 Top 5에 매주 포함되고 있는 것을 확인할 수 있다. asec.ahnlab.com/1371 Lokibot은 최근 AgentTesla, Formbook, AveMaria 등의 악성코드와 유사하게 대부분 스팸 메일을 통해 유포되고 있다. 또한 진단을 우회하기 위해... 스팸 메일을 통해 유포되는 다른 악성코드들과 유사한 파일명으로 유포된다."/>

- Shipping Documents.exe
- Quote.exe garuba1.exe
- Order#051822.exe
- Purchase order.exe

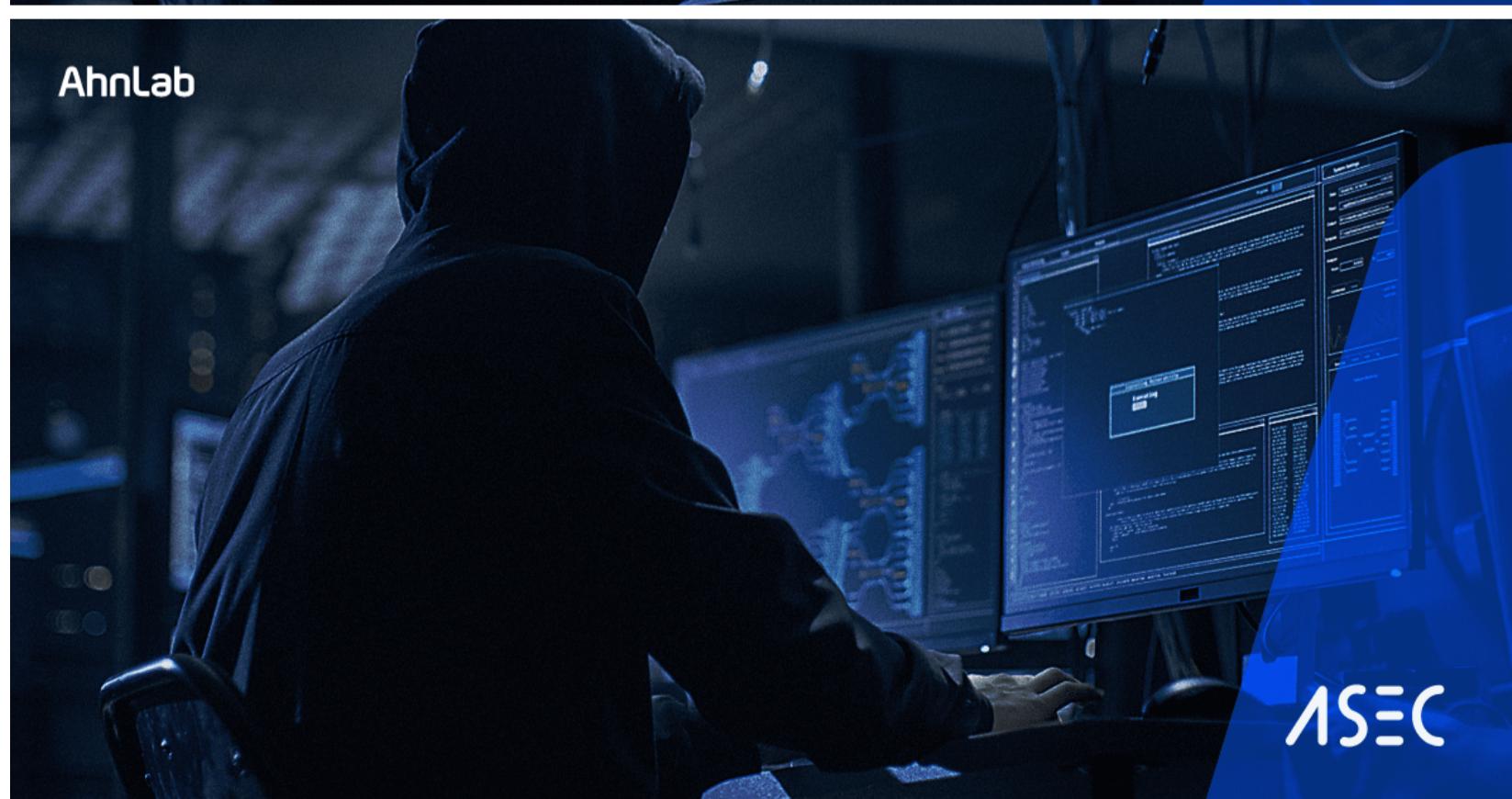
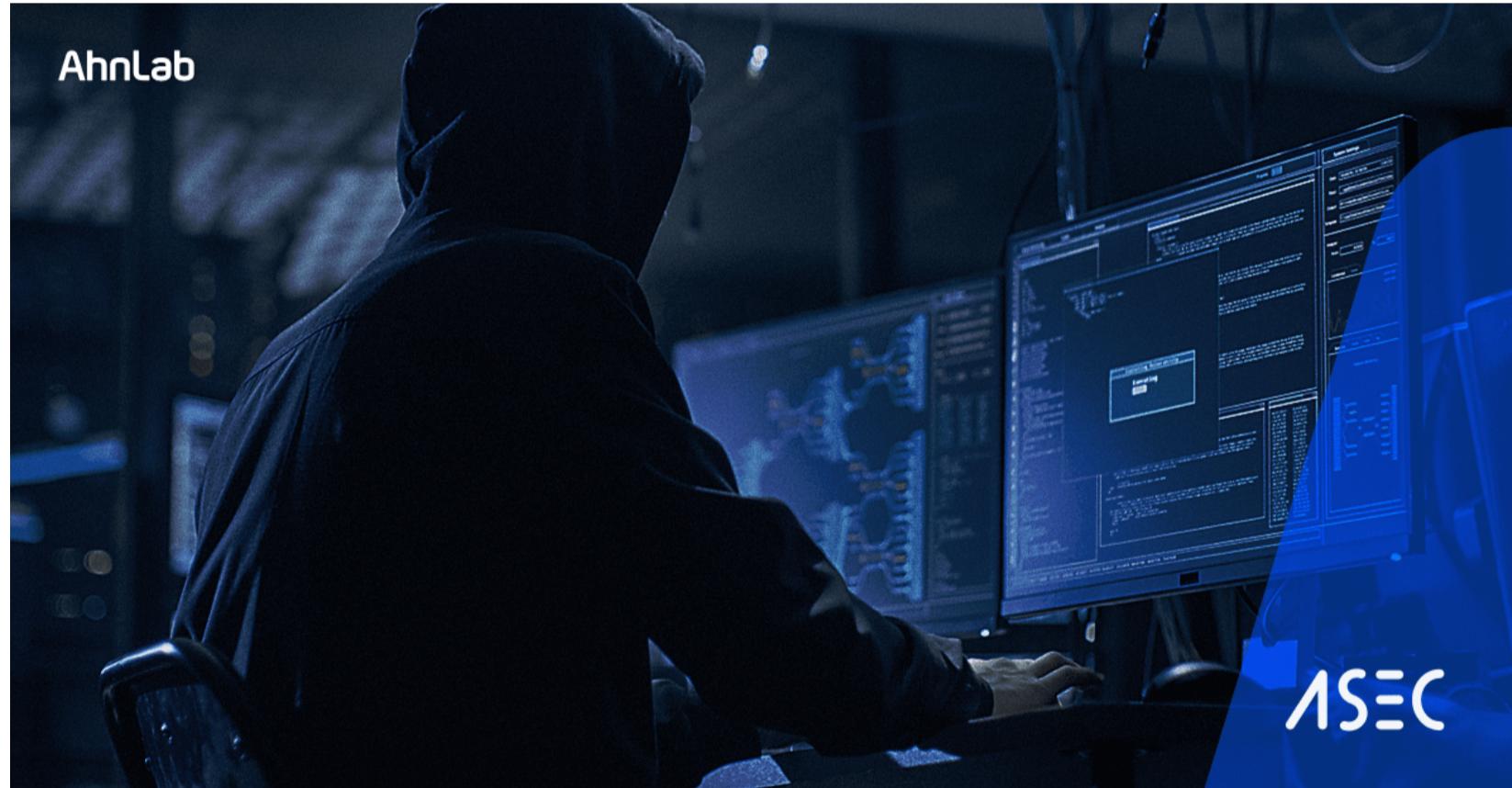
- FedEx Receipt\_AWB#5305323204643.exe
- copia rápida\_pdf\_\_\_\_\_\_.exe

대부분의 Lokibot 악성코드 C&C 서버 주소는 다음과 같이 fre.php로 끝나는 특징을 가지고 있다.

- hxxp://198.187.30[.]47/p.php?id=7706107617708711
- 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 악성코드는 8.3%로 4위를 기록하였다. RedLine 악성코드는 웹 브라우저, FTP 클라이언트, 암호화폐 지갑, PC 설정 등 다양한 정보를 탈취하며 C&C 서버로 부터 명령을 받아 추가 악성코드를 다운로드 할 수 있다. BeamWinHTTP와 마찬가지로 S/W 크랙 다운로드로 위장하여 유포되는 경우가 많다.



유튜브를 통해 유포 중인

RedLine 인포스틸러 – ASEC BLOG ASEC 분석팀은 최근 RedLine 인포스틸러 악성코드가 크랙 프로그램 다운로드 링크로 위장한 유튜브 사이트를 통해 유포 중인 것을 확인하였다. RedLine은 정보 유출 악성코드로서 웹 브라우저 및 FTP 클라이언트 프로그램에 저장되어 있는 사용자

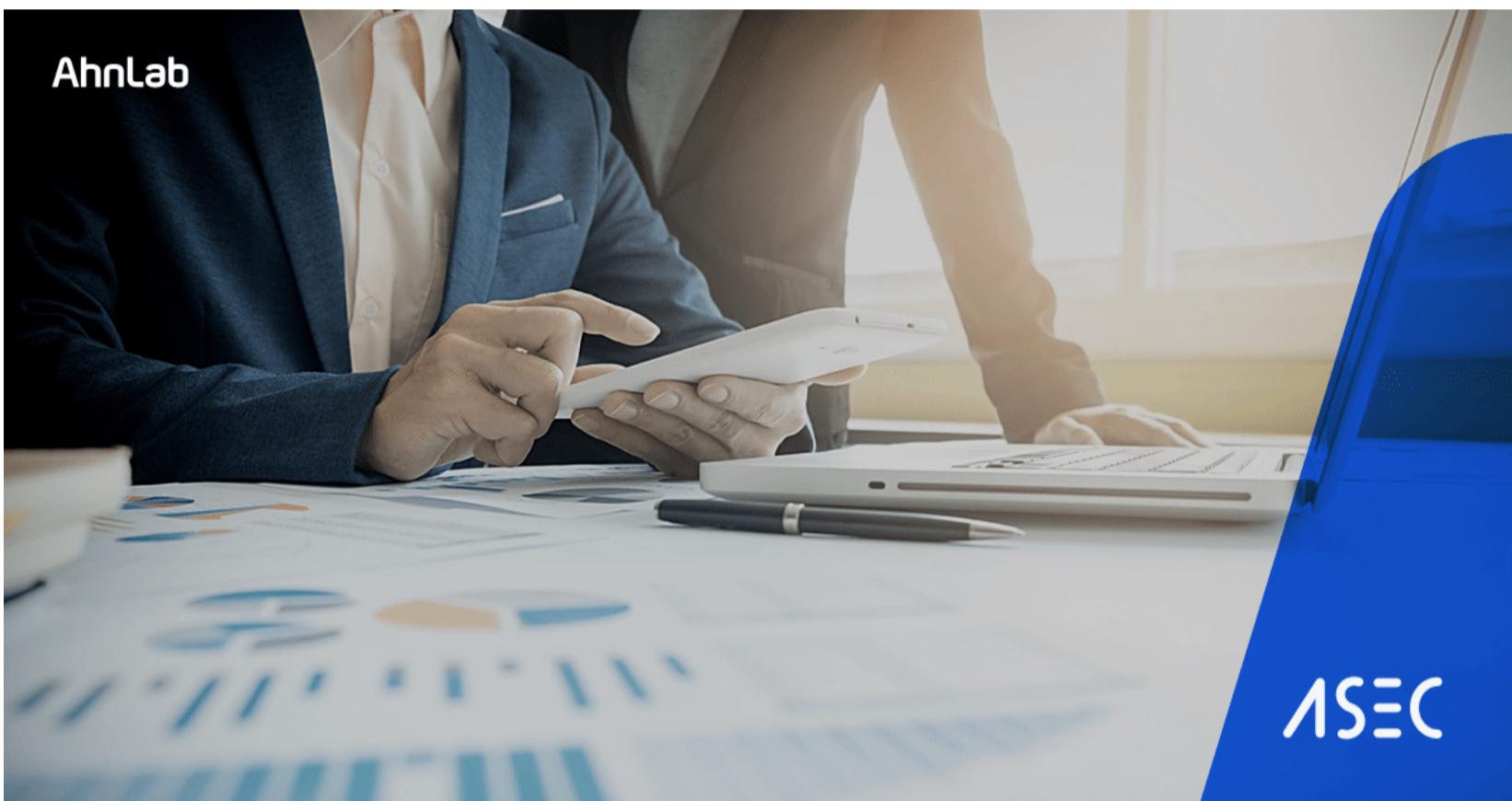
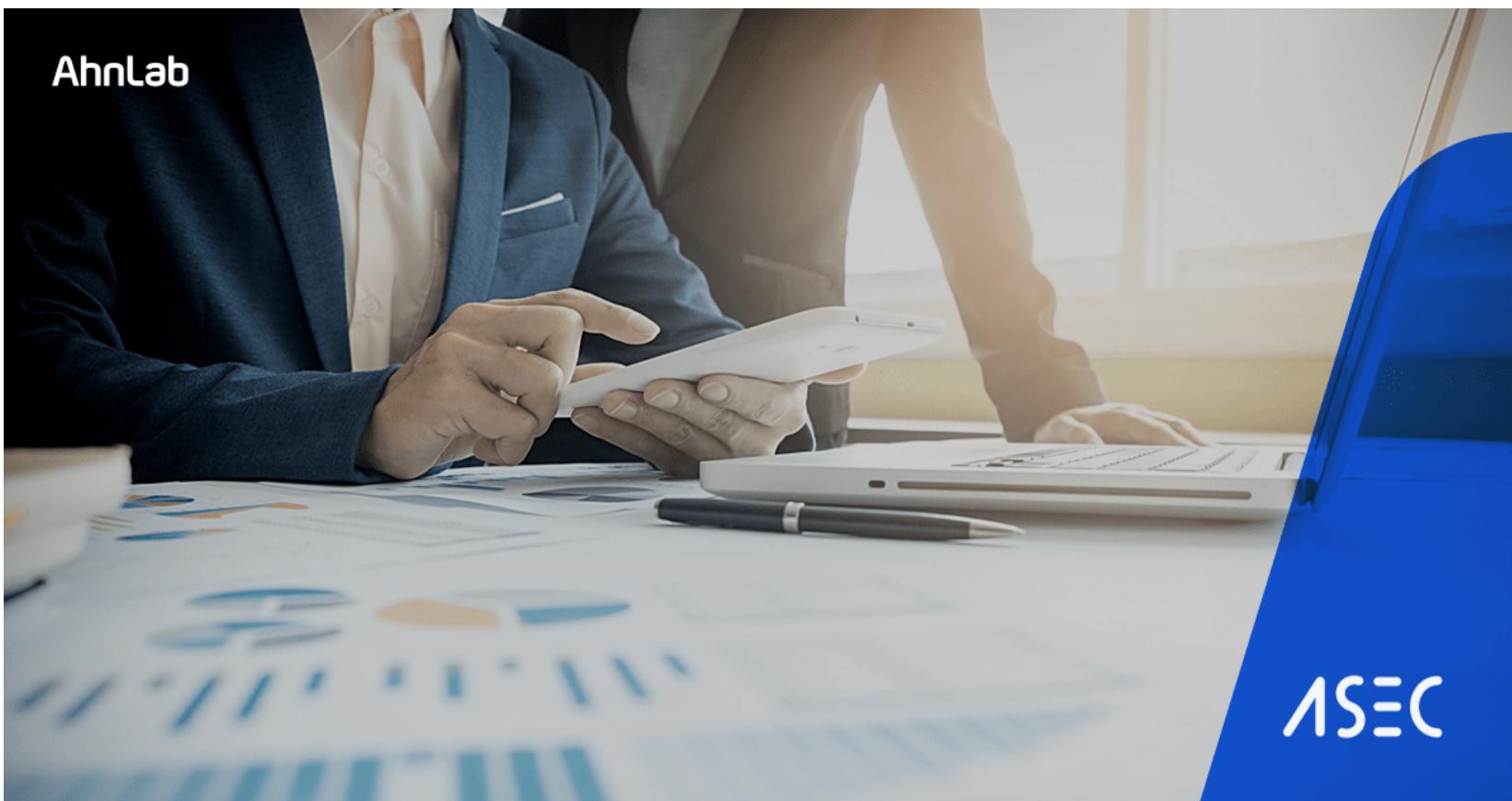
계정 정보나 스크린샷, 코인 지갑 주소 등 사용자 정보를 C&C 서버에 유출하는 기능을 갖는다. RedLine 악성코드가 최초로 확인된 것은 2020년 3월경으로 코로나 바이러스 이슈를 이용한 스팸 메일을 통해 유포된 것이 첫번째 사례이다. 이후부터 꾸준히 다양한 경로를 통해 유포되고...

다음은 확인된 RedLine의 C&C 서버 도메인이다.

- 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

이번주는 AveMaria가 5.0%를 기록하며 5위에 이름을 올렸다. AveMaria는 원격제어 기능의 RAT (Remote Administration Tool) 악성코드로서 C&C 서버에서 공격자의 명령을 받아 다양한 악성 행위를 수행할 수 있다.



스팸 메일로 유포 중인

AveMaria 악성코드 – ASEC BLOG AveMaria 는 원격제어 기능의 RAT (Remote Administration Tool) 악성코드로서 C&C 서버에서 공격자의 명령을 받아 다양한 악성 행위를 수행할 수 있다. 아래의 주간 통계에서도 확인 되듯이 Top 5 안에는 포함되지 않지만, 꾸준히 일정 비율을 차지하고 있다. AveMaria 악성코드는 최근 AgentTesla, Lokibot, Formbook 악성코드와 유사하게 대부분 스팸 메일을 통해 유포되고 있다. 또한 진단을 우회하기 위해 위의 악성코드들과 유사한 닷넷(.NET) 외형의 패커로 패킹되어 유포 중이...

AveMaria 악성코드는 최근 AgentTesla, Lokibot, Formbook 악성코드와 유사하게 대부분 스팸 메일을 통해 유포되고 있다. 또한 진단을 우회하기 위해 위의 악성코드들과 유사한 닷넷(.NET) 외형의 패커로 패킹되어 유포 중이다. 따라서 접수되는 파일명도 같이 스팸 메일을 통해 유포되는 악성코드들과 유사하다.

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

The following is the confirmed C&C server of AveMaria.

- 37.0.14[.]206:5208
- 104.128.91[.]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

Related IOCs and related detailed analysis information can be checked through AhnLab's next-generation threat intelligence platform 'AhnLab TIP' subscription service.



Categories: [Malware information](#)

Tagged as: [Weekly Statistics](#)