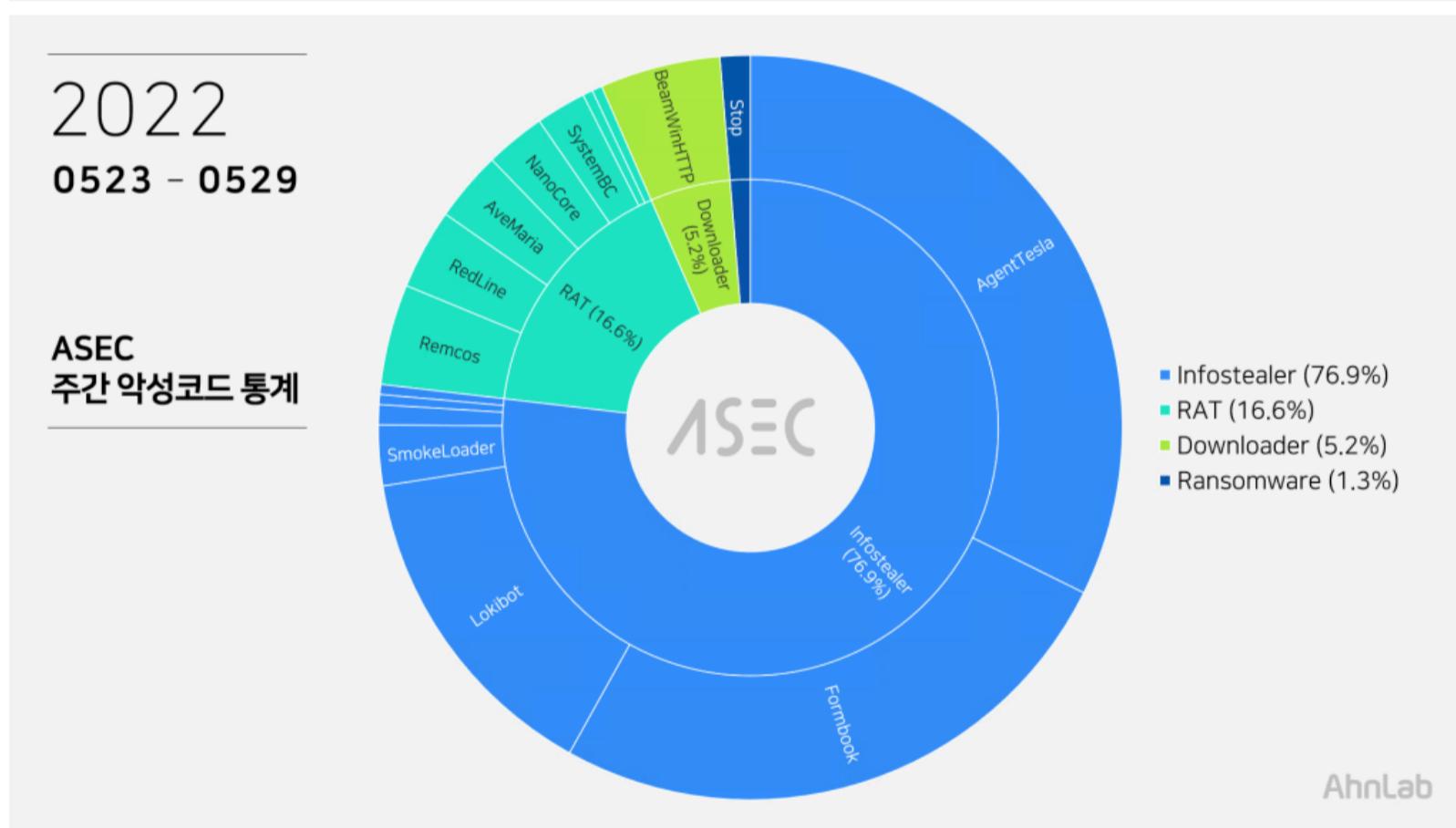
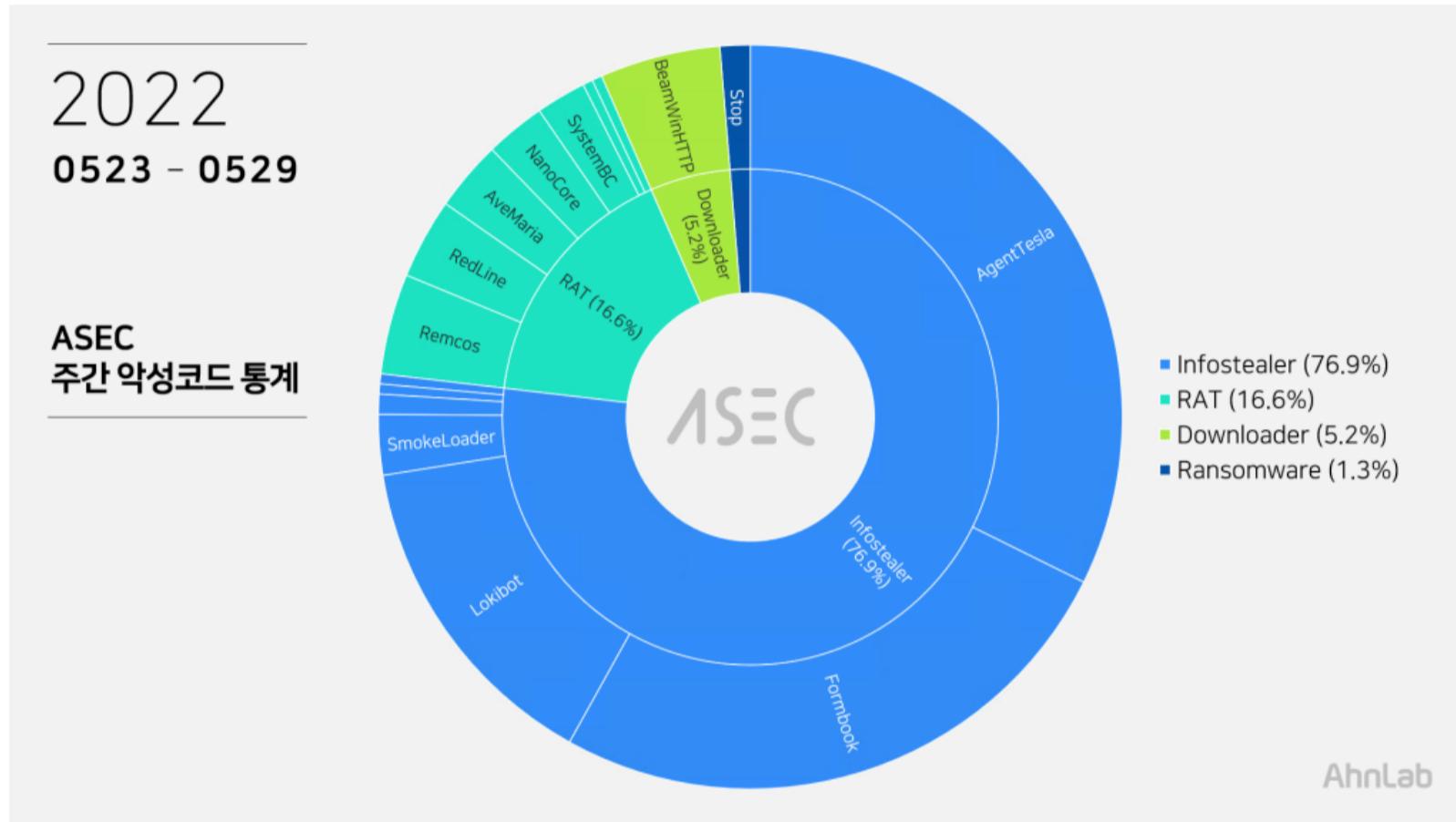


ASEC Weekly Malware Statistics (20220523 ~ 20220529)

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 23, 2022 to Sunday, May 29, 2022.

Infostealer took the first place with 76.9% of categories, followed by RAT (Remote Administration Tool) malware with 16.6%, downloaders with 5.2%, and ransomware with 1.3%.



Top 1 — AgentTesla

AgentTesla, an infostealer malware, ranked first with 32.3%, 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 : 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.xls[.]af (144.76.114.106) sender : info@xls[.]af receiver : ranjqnupreti3@gmail[.]com user : info@xls[.]af pw : Kab****42@

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.

- 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 악성코드는 25.8%로 2위를 기록하였다.



메일을 통해 유포 중인 사

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.

- 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.xlsx
- Order_673N78333_xlsx.xlsx

- Quotation-2328333.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.

- [http://www.simplybans\[.\]com/ng9o/](http://www.simplybans[.]com/ng9o/)
- [http://www.momentum6\[.\]com/tn61/](http://www.momentum6[.]com/tn61/)
- [http://www.breskizci\[.\]com/bg5r/](http://www.breskizci[.]com/bg5r/)
- [http://www.temp-bait\[.\]com/amdf/](http://www.temp-bait[.]com/amdf/)
- [http://www.click-tokens\[.\]com/ta3t/](http://www.click-tokens[.]com/ta3t/)
- [http://www.exilings\[.\]com/ygkp/](http://www.exilings[.]com/ygkp/)
- [http://www.hecsearc\[.\]com/pb0u/](http://www.hecsearc[.]com/pb0u/)
- [http://www.caramelshubs\[.\]com/crqp/](http://www.caramelshubs[.]com/crqp/)
- [http://www.motarasag\[.\]com/sr4i/](http://www.motarasag[.]com/sr4i/)
- [http://www.bravesxx\[.\]com/mwfc/](http://www.bravesxx[.]com/mwfc/)

- [http://www.travelsagas\[.\]com/a5qd/](http://www.travelsagas[.]com/a5qd/)

Top 3 – Lokibot

Lokibot 악성코드는 14.4%로 3위를 기록하였다. Lokibot은 인포스틸러 악성코드로서 웹 브라우저, 메일 클라이언트, FTP 클라이언트 등의 프로그램들에 대한 정보를 유출한다.



구매 주문서 메일로 위장하

여 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.

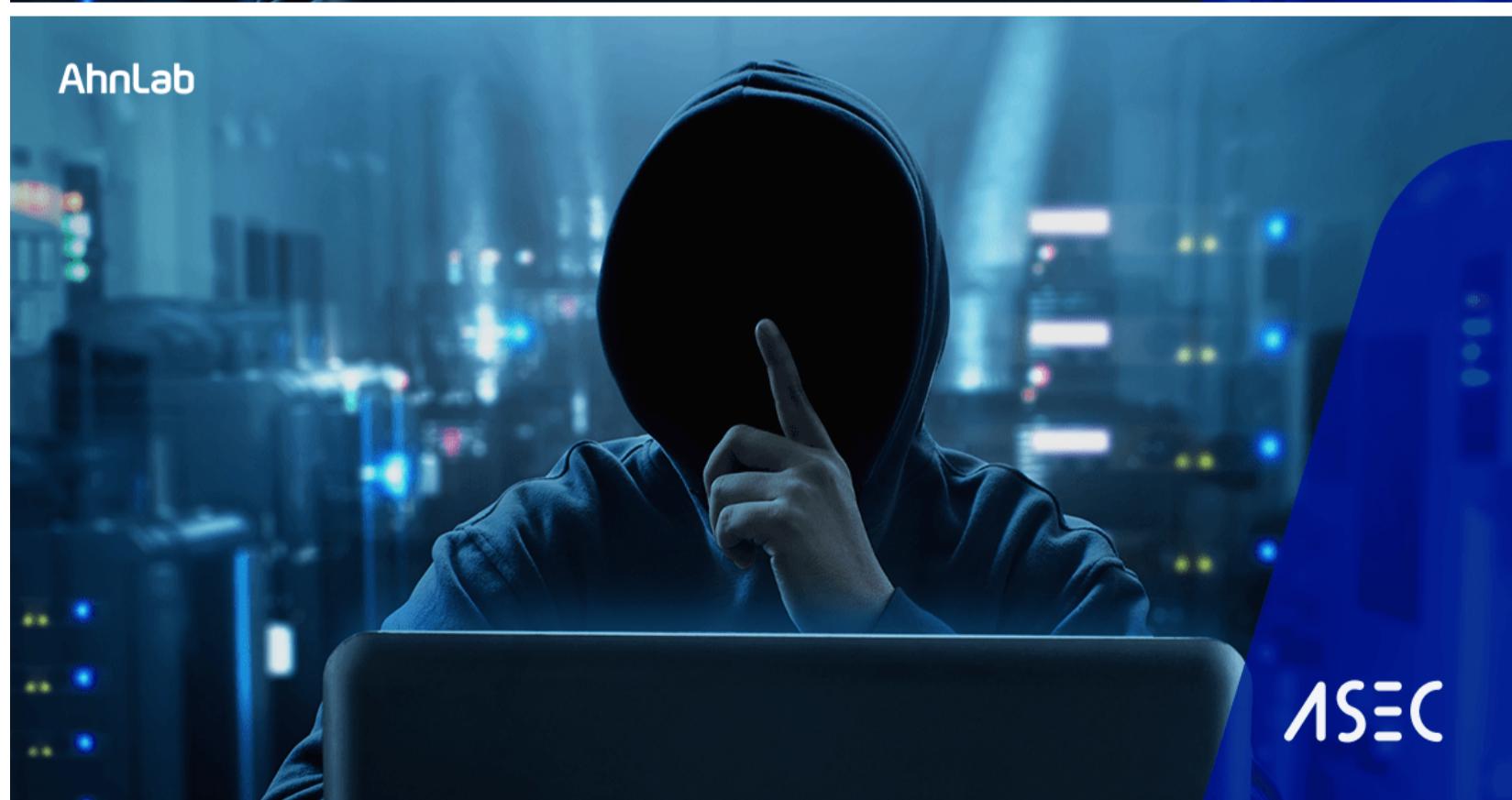
- SH22-OD03-22.exe
- COTIZACIÓN.pdf.exe
- HB1231_SEQ.22_PO_inquiry.exe
- PO063680.exe UF_86064_HG.exe
- PO_OPBM2.exe
- DATOS BANCARIOS DE REEMBOLSO DE PAGO.exe
- SEOC**** INDUSTRY.exe
- HB1231_SEQ.22_PO_inquiry.exe

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

- 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
- vmopahtqdf84hfvsqepalcbch63gdyvah[.]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

5.2% 로 4위를 차지한 BeamWinHTTP는 다운로더 악성코드이다. PUP 설치 프로그램으로 위장한 악성코드를 통해 유포되는데, BeamWinHTTP 가 실행되면 PUP 악성코드인 Garbage Cleaner를 설치하고, 동시에 추가 악성코드를 다운로드하여 설치할 수 있다.



나 몰래 악성코드가 설치된

다고?! BeamWinHTTP 악성코드! – ASEc BLOG ASEc 분석팀에서 매주 게시하고 있는 주간 악성코드 통계에서도 확인되듯, 최근들어 다운로더형 악성코드인 BeamWinHTTP가 몇 주 사이에 눈에 띄게 많이 발생하고 있다. 지난 ASEc 주간 악성코드 통계에 따르면 BeamWinHTTP 악성코드는 Top 3으로 분류될 정도로 많은 유포가 이루어지고 있으며, 실행할 때마다 각기 다른 악성코드를 다운로드하고 있기 때문에 각별한 주의

가 필요하다. BeamWinHTTP 악성코드는 PUP 설치 프로그램에 의해 실행되어지는데, 사용자들은 웹 상에서 자신이 원하는 프로그램을 설치하려다 아래와...

최근 들어서는 S/W 크랙 다운로드를 위장하여 유포되는 드로퍼형 악성코드에 의해 유포되는 수량이 상당하다. ASEC 분석팀에서는 이러한 악성코드를 “MulDrop” 진단명으로 대응 중이며, 해당 악성코드에 대한 정보는 아래 블로그를 참고하길 바란다.



S/W 다운로드 위장, 다양한

종류의 악성코드 유포 – ASEC BLOG ASEC 분석팀에서는 기존 다수의 블로그 포스팅을 통해 상용 소프트웨어의 Crack, Serial 등의 키워드로 검색되는 악성 사이트로부터 유포되는 CryptBot 악성코드에 대하여 언급하며 사용자의 주의를 당부하였다. 이러한 악성 사이트로부터 유포되는 악성코드는 CryptBot 악성코드가 대다수이지만, 간혹 타 악성코드가 유포되곤 한다. 본 블로그에서는 동일 유형의 악성코드 유포 중 CryptBot을 제외한 타 악성코드에 대하여 언급하고자 한다. 기존의 블로그에서도 언급했듯이 해당 악성코드는 검색엔진에 특정 상용 소프트웨어의 Cr...

다음은 확인된 C&C 서버 주소이다.

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

Top 5 – Remcos

이번 주는 Remcos가 4.4%로 5위를 차지했다. Remcos는 RAT 악성코드로서 키로깅을 포함한 정보 유출 및 다양한 공격자의 명령을 수행할 수 있다.



스팸 메일로 유포 중인

Remcos RAT 악성코드 – ASEC BLOG Remcos is a RAT (Remote Administration Tool) malware that has been continuously distributed through spam emails for several years. Remcos is sold by the manufacturer as a RAT tool for remote management through the following website, and it is updated regularly to the latest. If you look at the functions described on the Remcos website, it is written that they can be used for remote support or for the purpose of deleting or tracking sensitive data in case of theft. Of course, it is true that these functions are supported. But keylogging, screenshot capture...

Remcos is packed with .net-shaped packers like malicious codes such as AgentTesla, Formbook, and NanoCore, and is distributed through attachments in spam emails. Recently, a number of cases disguised as a specific tool are also found.

The following is the confirmed Remcos C&C server address.

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

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

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

AhnLab TIP

빠르게 변화하는 보안 위협 최적의 의사결정

안랩의 차별화된 위협 인텔리전스와 함께 시작해 보세요

atip.ahnlab.com

Categories: [Malware information](#)

Tagged as: [Weekly Statistics](#)