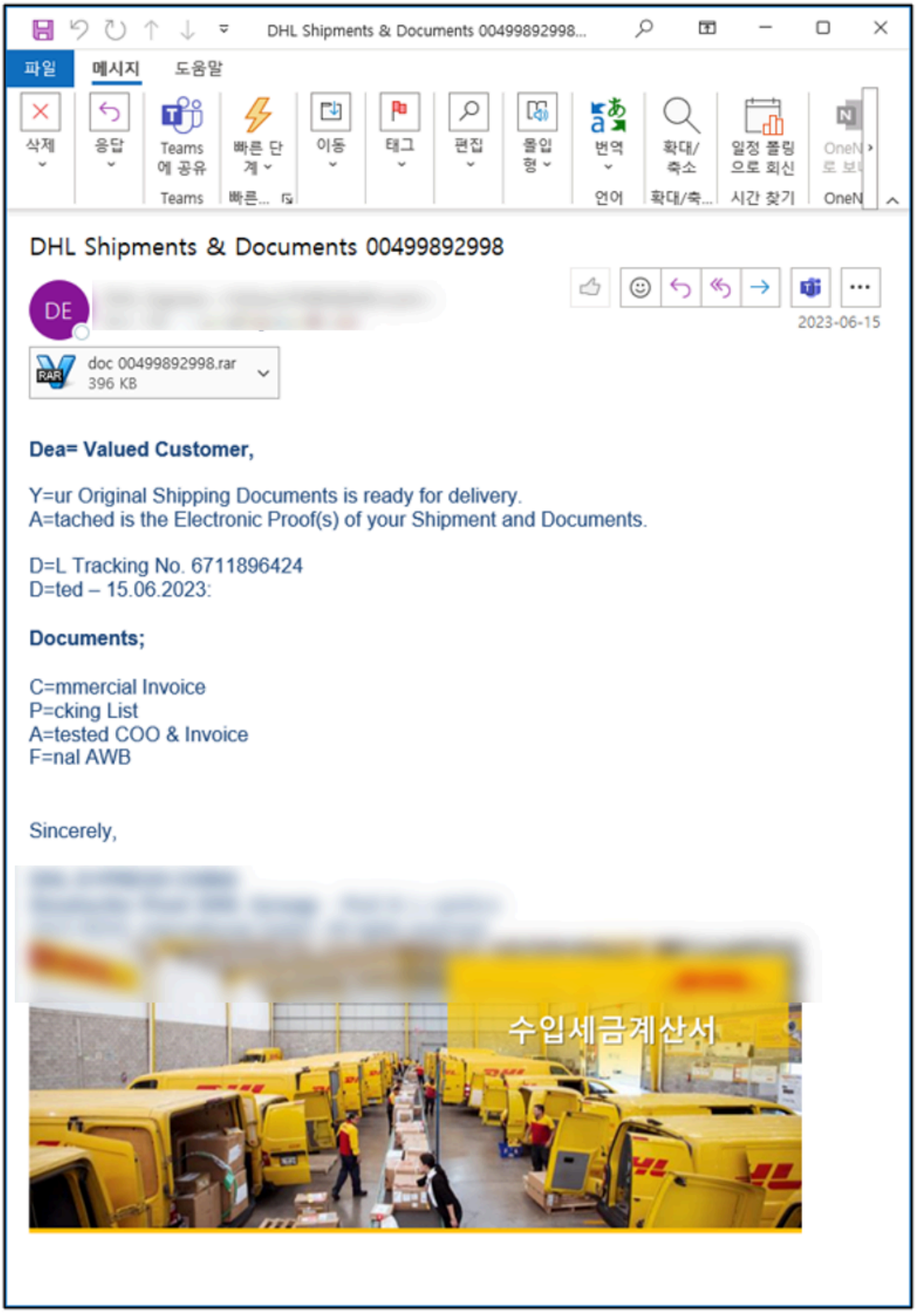
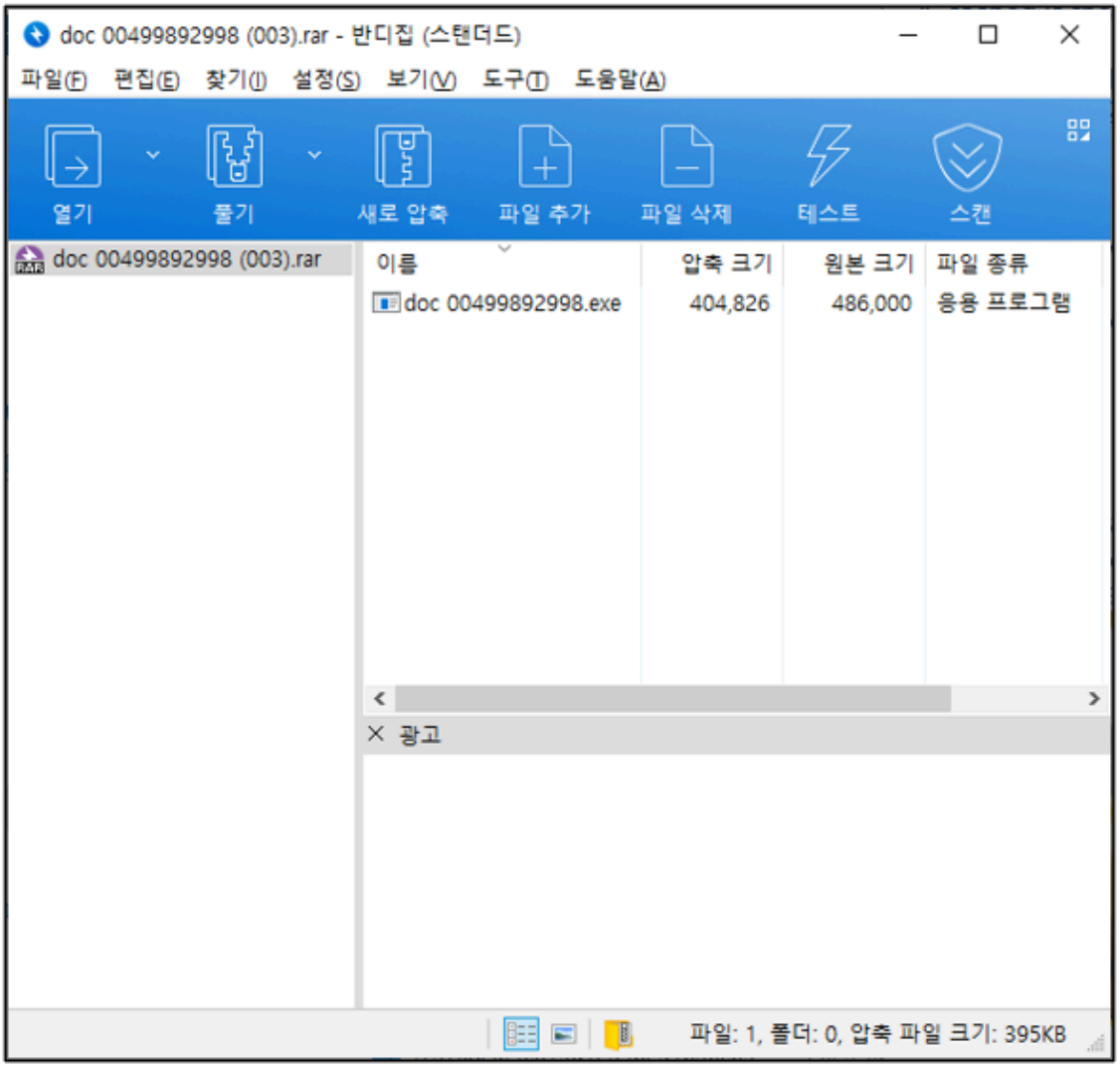
GuLoader Malware Disguised as Tax Invoices and Shipping Statements (Detected by MDS Products) - ASEC

By ATCP

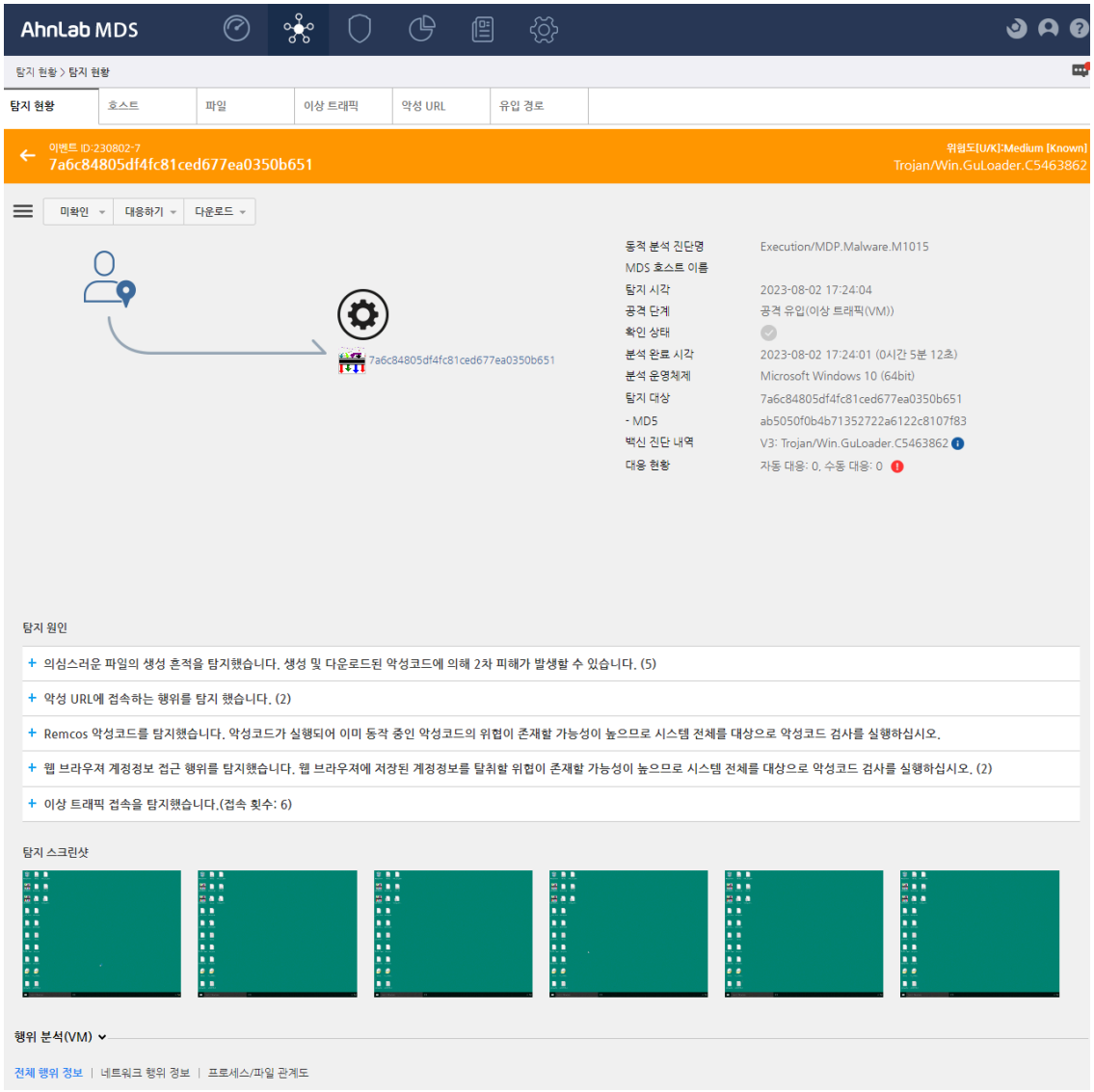
Published: 2023-08-03 · Archived: 2026-04-05 17:33:45 UTC

AhnLab Security Emergency response Center (ASEC) has identified circumstances of GuLoader being distributed as attachments in emails disguised with tax invoices and shipping statements. The recently identified GuLoader variant was included in a RAR (Roshal Archive Compressed) compressed file. When a user executes GuLoader, it ultimately downloads known malware strains such as Remcos, AgentTesla, and Vidar.


DHL Shipments & Documents 00499892998...
파일
메시지
도움말
삭제
응답
Teams 에 공유
빠른 단계
이동
태그
편집
몰입형
번역
확대/축소
일정 폴링으로 회신
언어
확대/축...
시간 찾기
DHL Shipments & Documents 00499892998
DE
2023-06-15
doc 00499892998.rar
396 KB
Dea= Valued Customer,
Y=ur Original Shipping Documents is ready for delivery.
A=tached is the Electronic Proof(s) of your Shipment and Documents.
D=L Tracking No. 6711896424
D=ted – 15.06.2023:
Documents;
C=mmercial Invoice
P=cking List
A=tested COO & Invoice
F=nal AWB
Sincerely,
수입세금계산서



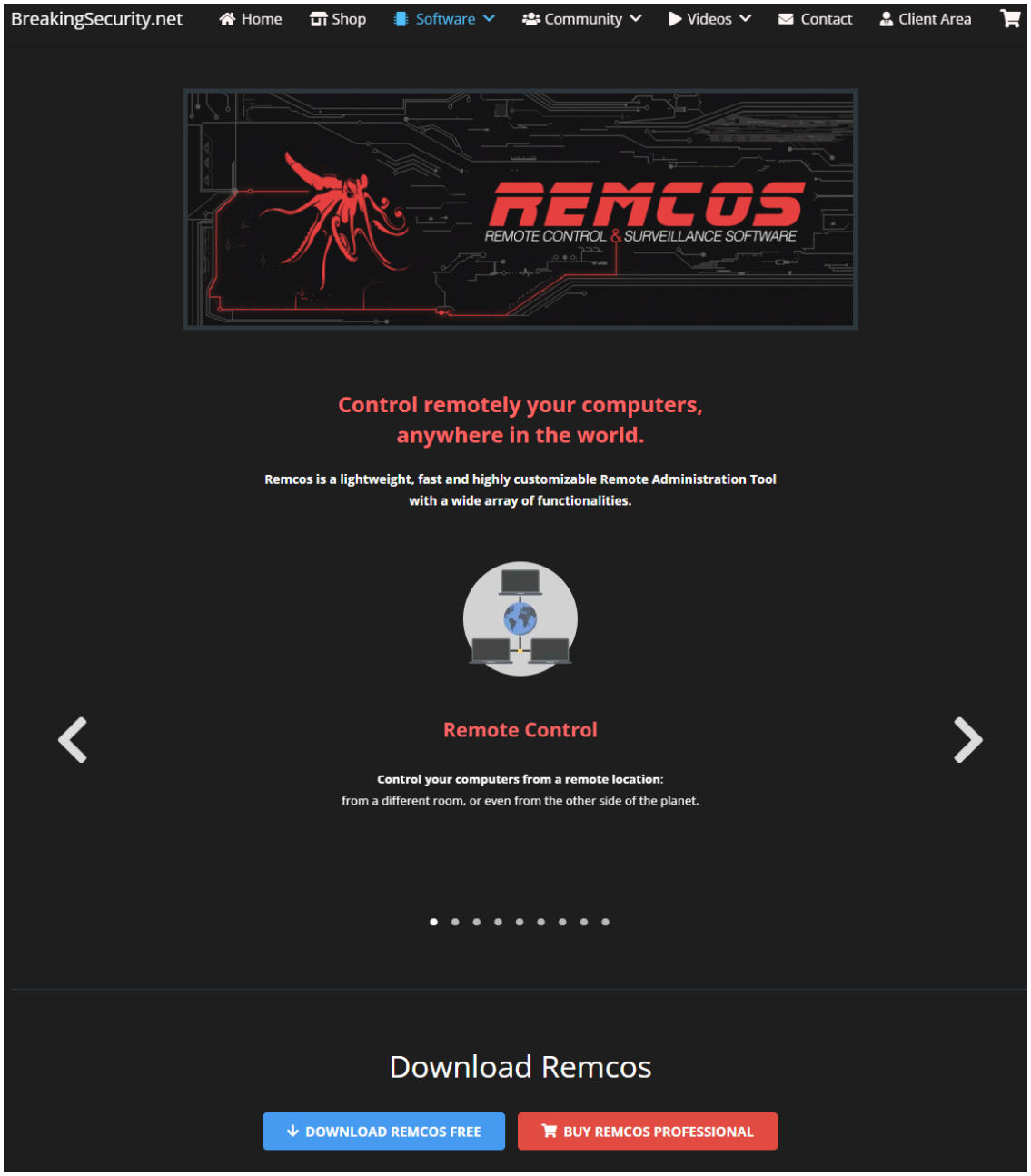
AhnLab's MDS products provide a Mail Transfer Agent (MTA) feature to block malware distributed via email. Figure 3 below shows the GuLoader malware detection report screen of AhnLab MDS. In this case, the GuLoader downloader downloaded Remcos from the threat actor's server.



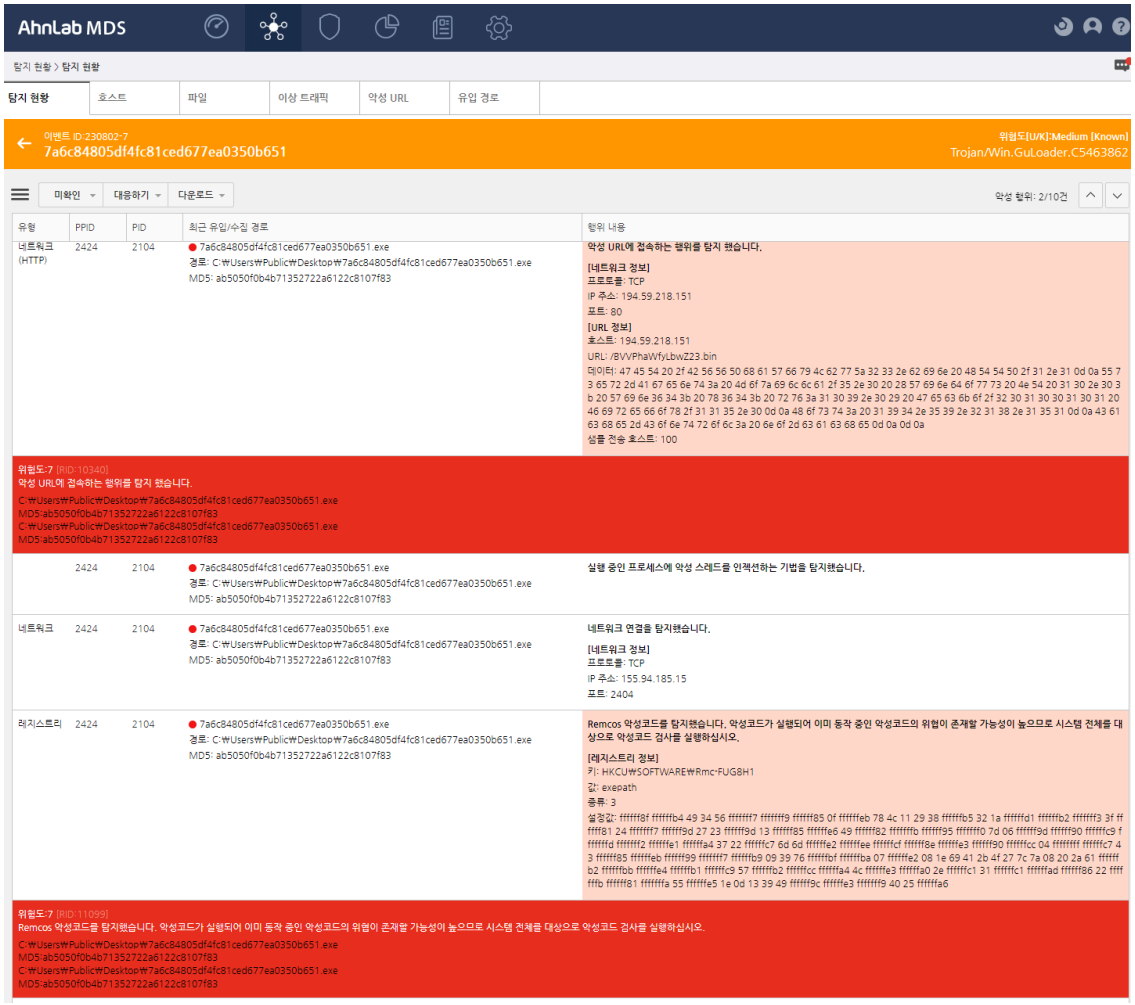
Remcos is a known RAT (Remote Administration Tool) distributed via spam emails and MS-SQL vulnerabilities. The malware has been covered on the ASEC Blog.

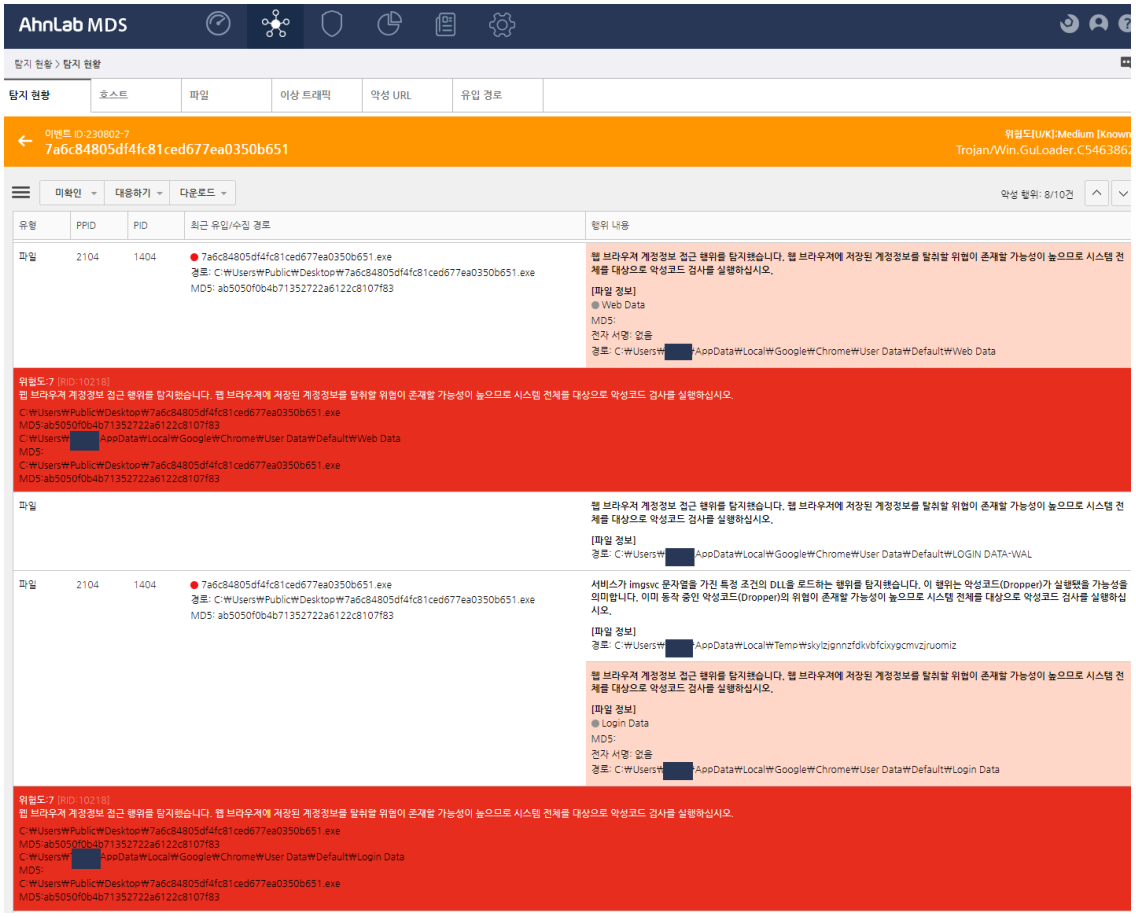
- (Nov 23, 2020) Remcos RAT Malware being Distributed as Spam Mail

There is an official sales page for Remcos. Following the initial release of version 1.0 in July 2016, version 4.9.0 was released on July 26th, 2023. It seems the creator is constantly updating the features of this malware and selling copies for commercial purposes.



When an email is received, MDS uses the virtual machine-based dynamic analysis to detect malware strains based on GuLoader's behavior of downloading malware types and Remcos' behavior of exfiltrating information as well as their characteristics.


AhnLab MDS
탐지 현황 > 탐지 현황
탐지 현황
호스트
파일
이상 트래픽
악성 URL
유입 경로
이벤트 ID:230802-7
7a6c84805df4fc81ced677ea0350b651
위험도[U/K]:Medium [Known]
Trojan/Win.GuLoader.C5463862
미확인
대응하기
다운로드
악성 행위: 2/10건
유형
PPID
PID
최근 유입/수집 경로
행위 내용
네트워크 (HTTP)
2424
2104
7a6c84805df4fc81ced677ea0350b651.exe
경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5: ab5050f0b4b71352722a6122c8107f83
악성 URL에 접속하는 행위를 탐지 했습니다.
[네트워크 정보]
프로토콜: TCP
IP 주소: 194.59.218.151
포트: 80
[URL 정보]
호스트: 194.59.218.151
URL: /BVVPhaWfyLbwZ23.bin
데이터: 47 45 54 20 2f 42 56 56 50 68 61 57 66 79 4c 62 77 5a 32 33 2e 62 69 6e 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 31 35 2e 30 0d 0a 48 6f 73 74 3a 20 31 39 34 2e 35 39 2e 32 31 38 2e 31 35 31 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a
샘플 전송 호스트: 100
위험도:7 [RID:10340]
악성 URL에 접속하는 행위를 탐지 했습니다.
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83
2424
2104
7a6c84805df4fc81ced677ea0350b651.exe
경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5: ab5050f0b4b71352722a6122c8107f83
실행 중인 프로세스에 악성 스레드를 인젝션하는 기법을 탐지했습니다.
네트워크
2424
2104
7a6c84805df4fc81ced677ea0350b651.exe
경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5: ab5050f0b4b71352722a6122c8107f83
네트워크 연결을 탐지했습니다.
[네트워크 정보]
프로토콜: TCP
IP 주소: 155.94.185.15
포트: 2404
레지스트리
2424
2104
7a6c84805df4fc81ced677ea0350b651.exe
경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5: ab5050f0b4b71352722a6122c8107f83
Remcos 악성코드를 탐지했습니다. 악성코드가 실행되어 이미 동작 중인 악성코드의 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.
[레지스트리 정보]
키: HKCU₩SOFTWARE₩Rmc-FUG8H1
값: exepath
종류: 3
설정값: ffffff8f ffffffb4 49 34 56 fffffff7 fffffff9 ffffff85 0f ffffffeb 78 4c 11 29 38 ffffffb5 32 1a ffffffd1 ffffffb2 ffffff3 3f ffffff81 24 fffffff7 ffffff9d 27 23 ffffff9d 13 ffffff85 ffffffe6 49 ffffff82 ffffffb ffffff95 ffffff0 7d 06 ffffff9d ffffff90 ffffffc9 fffffffd ffffff2 ffffffe1 ffffffa4 37 22 ffffffc7 6d 6d ffffffe2 ffffffee ffffffcf ffffff8e ffffffe3 ffffff90 ffffffcc 04 fffffff ffffffc7 43 ffffff85 ffffffeb ffffff99 fffffff7 ffffffb9 09 39 76 ffffffbf ffffffba 07 ffffffe2 08 1e 69 41 2b 4f 27 7c 7a 08 20 2a 61 ffffffb2 ffffffeb ffffffe4 ffffffb1 ffffffc9 57 ffffffb2 ffffffcc ffffffa4 4c ffffffe3 ffffffa0 2e ffffffc1 31 ffffffc1 ffffffad ffffff86 22 ffffffb ffffff81 ffffffa 55 ffffffe5 1e 0d 13 39 49 ffffff9c ffffffe3 ffffff9 40 25 ffffffa6
위험도:7 [RID:11099]
Remcos 악성코드를 탐지했습니다. 악성코드가 실행되어 이미 동작 중인 악성코드의 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83



Besides Remcos, GuLoader also downloads and runs malware strains being sold on the Internet such as Formbook and Lokibot. Such malware strains offered for sale are called commodity malware. The threat actor likely uses downloaders such as GuLoader to propagate commercial malware instead of distributing them directly to bypass signature-based detection of security products. In the past, GuLoader was compiled in VisualBasic, and nowadays, it is compiled in NSIS and .NET. Whatever the case may be, its form is constantly being changed during distribution to evade static detection. However, the malware strains being executed in the memory area are commercial malware types such as Remcos, so even if the forms are different, each variant performs the same malicious behaviors. Thus, corporate security managers must implement not only endpoint security products (V3) but also sandbox-based APT solutions such as MDS to prevent damage from cyber attacks.

[File Detection]

– Trojan/Win.Guloader.C5463862 (2023.08.02.00)

[Behavior Detection]

– Execution/MDP.Remcos.M11099

– Infostealer/MDP.Credential.M10218

MD5

ab5050f0b4b71352722a6122c8107f83

Additional IOCs are available on AhnLab TIP.

To learn more about **AhnLab MDS**'s sandbox-based behavioral analysis, please click the banner below.

Source: https://asec.ahnlab.com/en/55978/