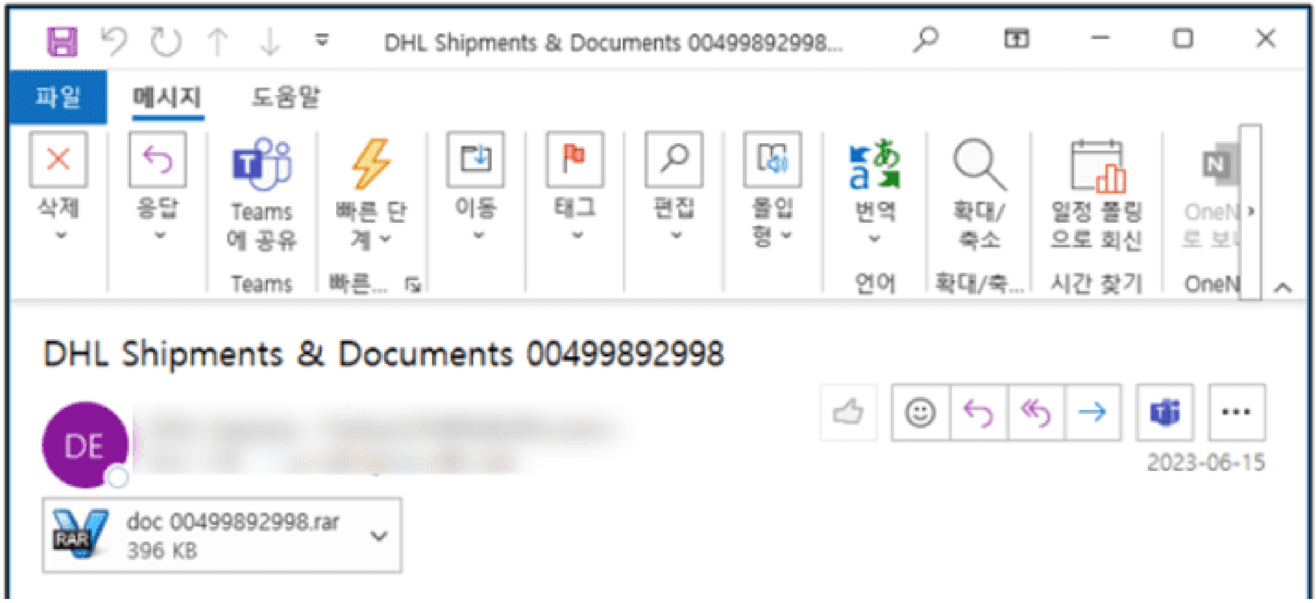
GuLoader Malware Disguised as Tax Invoices and Shipping Statements (Detected by MDS Products)

asec.ahnlab.com/en/55978/

By AhnLab_en

August 10, 2023

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.

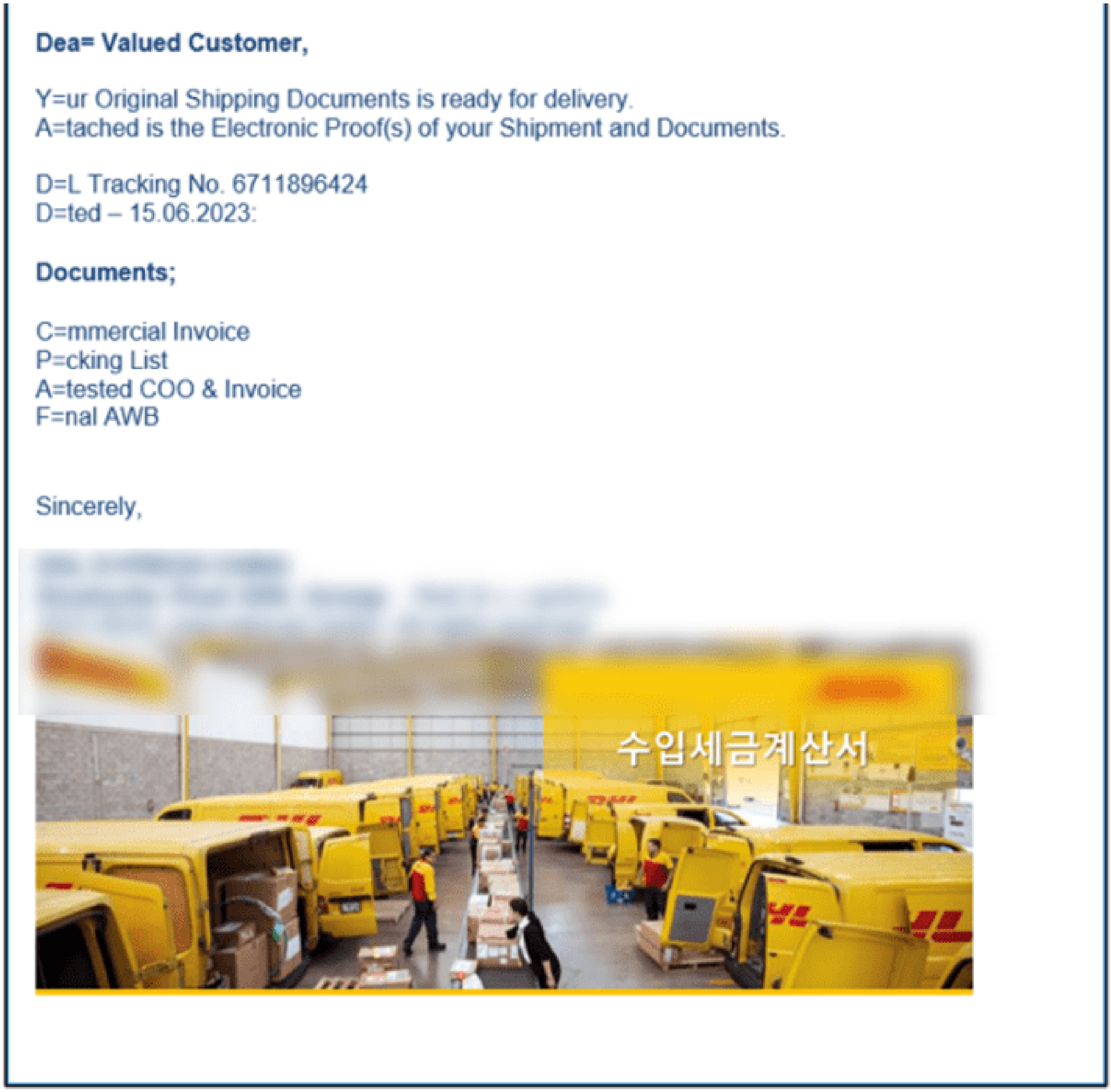


DHL Shipments & Documents 00499892998

DE [redacted]

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:

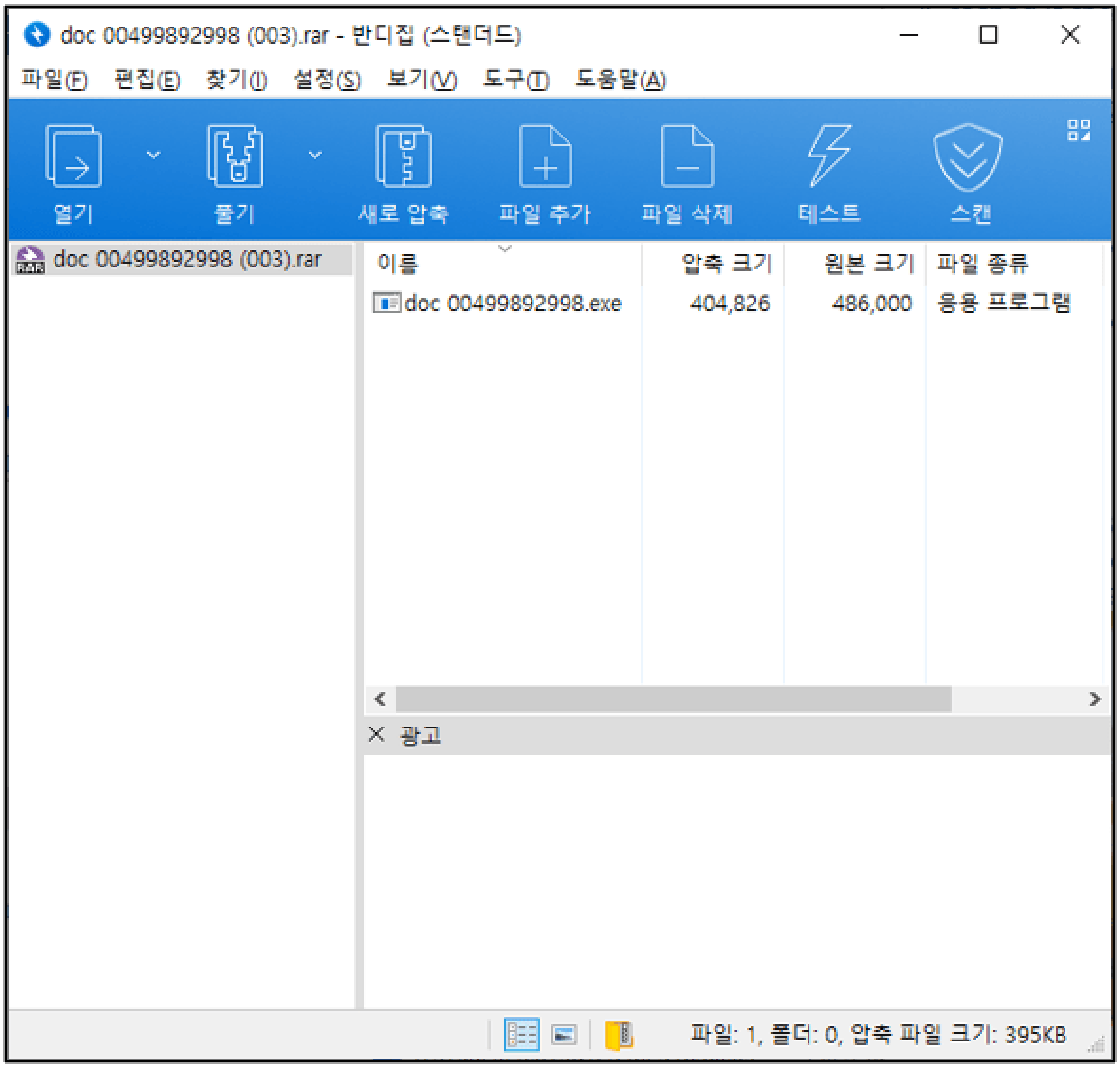
Documents;

C=mmercial Invoice
P=cking List
A=tested COO & Invoice
F=nal AWB

Sincerely,

[redacted]

Figure 1. An email disguised as a tax invoice (GuLoader)



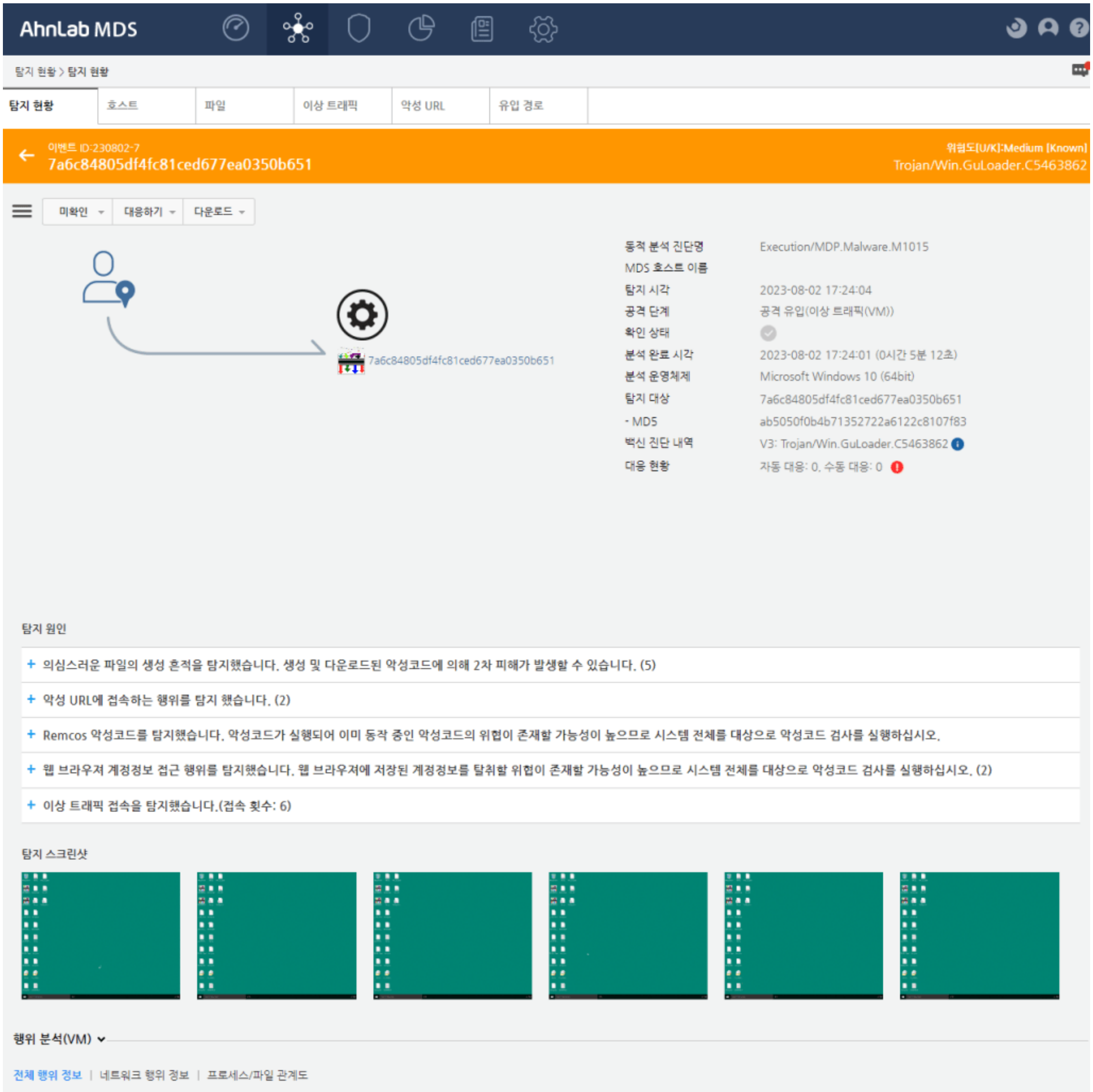
이름	압축 크기	원본 크기	파일 종류
doc 00499892998.exe	404,826	486,000	응용 프로그램

파일: 1, 폴더: 0, 압축 파일 크기: 395KB

Figure 2.

An executable file within the doc 00499892998.exe compressed file (GuLoader)

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.



이벤트 ID:230802-7
7a6c84805df4fc81ced677ea0350b651

위협도[U/K]:Medium [Known]
Trojan/Win.GuLoader.C5463862

동적 분석 진단명	Execution/MDP.Malware.M1015
MDS 호스트 이름	
탐지 시각	2023-08-02 17:24:04
공격 단계	공격 유입(이상 트래픽(VM))
확인 상태	✓
분석 완료 시각	2023-08-02 17:24:01 (0시간 5분 12초)
분석 운영체제	Microsoft Windows 10 (64bit)
탐지 대상	7a6c84805df4fc81ced677ea0350b651
- MD5	ab5050f0b4b71352722a6122c8107f83
백신 진단 내역	V3: Trojan/Win.GuLoader.C5463862
대응 현황	자동 대응: 0, 수동 대응: 0

탐지 원인

- + 의심스러운 파일의 생성 흔적을 탐지했습니다. 생성 및 다운로드된 악성코드에 의해 2차 피해가 발생할 수 있습니다. (5)
- + 악성 URL에 접속하는 행위를 탐지 했습니다. (2)
- + Remcos 악성코드를 탐지했습니다. 악성코드가 실행되어 이미 동작 중인 악성코드의 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.
- + 웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오. (2)
- + 이상 트래픽 접속을 탐지했습니다.(접속 횟수: 6)

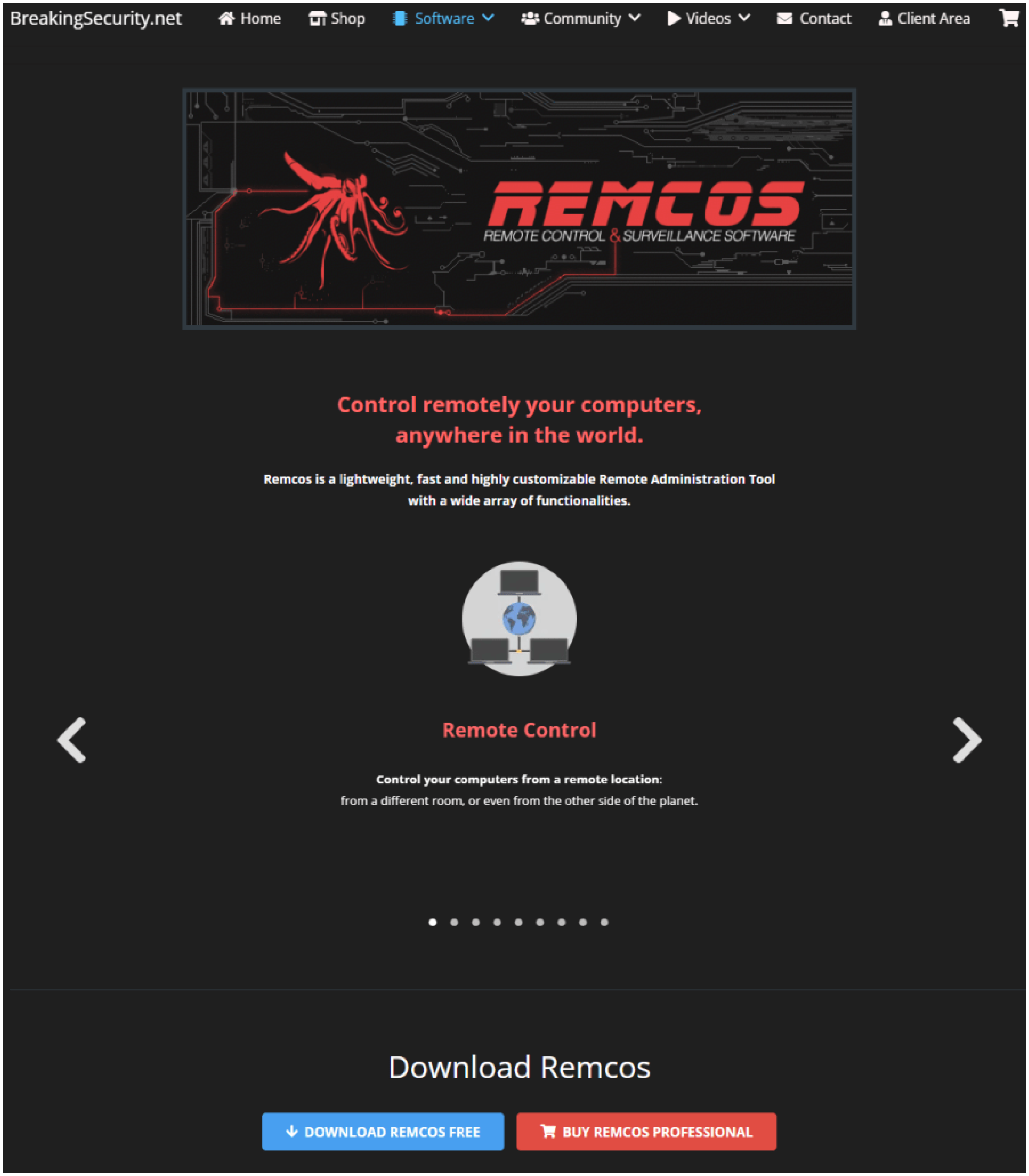
탐지 스크린샷

Figure 3. AhnLab MDS GuLoader malware detection screen

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.



Control remotely your computers, anywhere in the world.

Remcos is a lightweight, fast and highly customizable Remote Administration Tool with a wide array of functionalities.

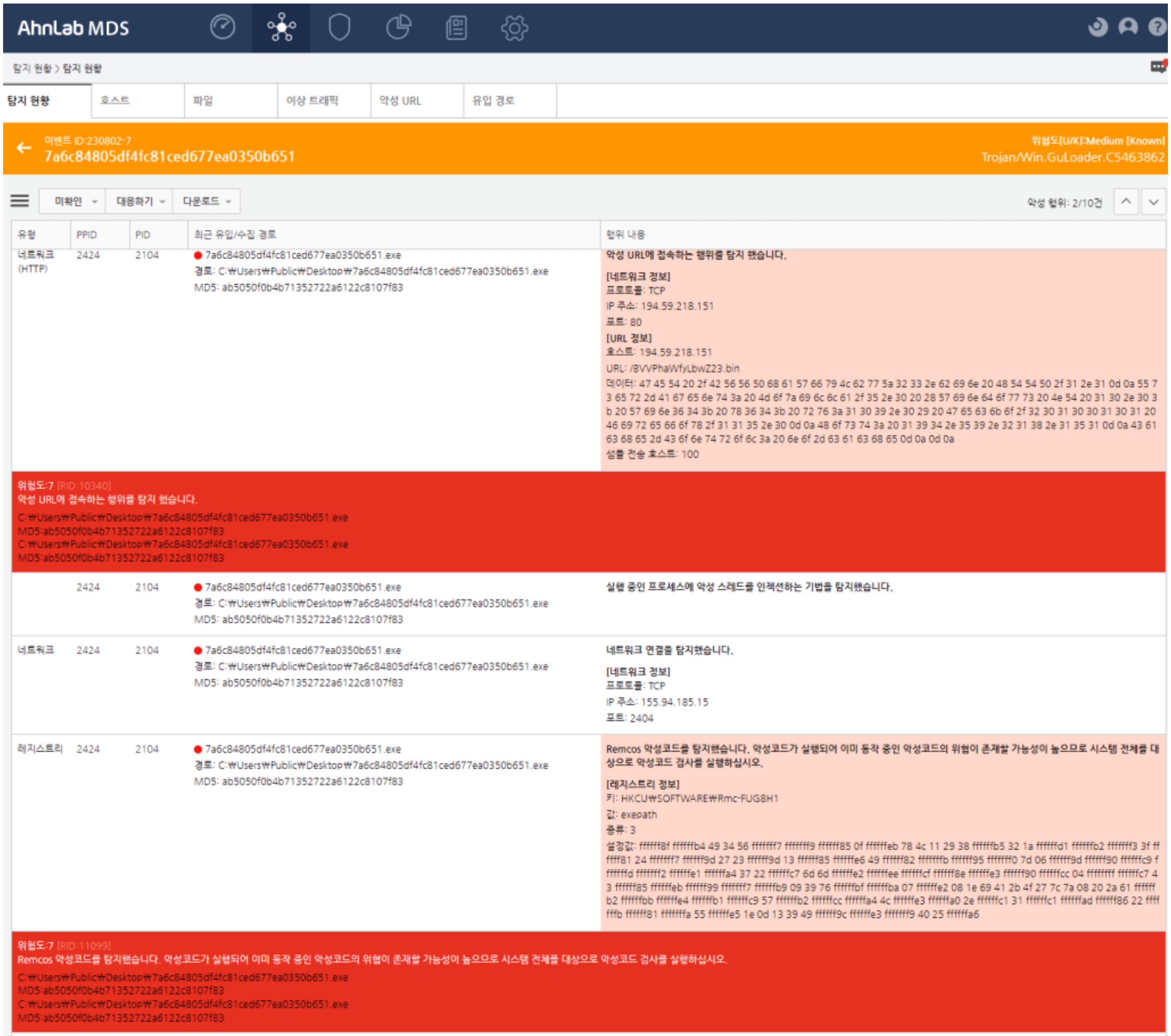
Remote Control

Control your computers from a remote location:
from a different room, or even from the other side of the planet.

Download Remcos

Figure 4. Remcos sales page

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.



이벤트 ID:230802-7
7a6c84805df4fc81ced677ea0350b651

위험도[U/K]:Medium [Known]
Trojan/Win.GuLoader.C5463862

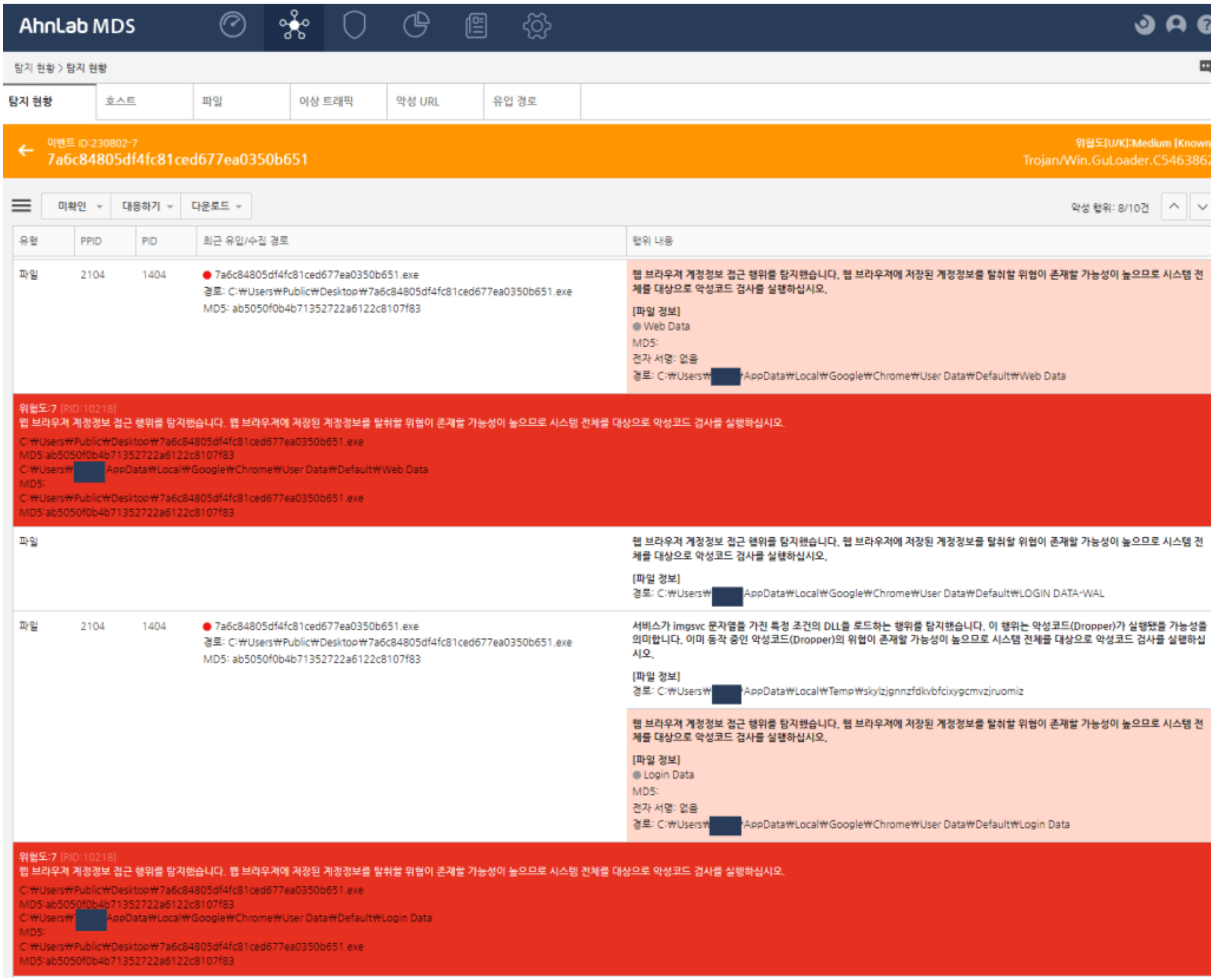
유형	PPID	PID	최근 유입/수집 경로	행위 내용
네트워크 (HTTP)	2424	2104	● 7a6c84805df4fc81ced677ea0350b651.exe 경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe MD5: ab5050f0b4b71352722a6122c8107f83	**악성 URL에 접속하는 행위를 탐지 했습니다.** **[네트워크 정보]** 프로토콜: TCP IP 주소: 194.59.218.151 포트: 80 **[URL 정보]** 호스트: 194.59.218.151 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 7 3 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 3 b 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

유형	PPID	PID	최근 유입/수집 경로	행위 내용
	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 fffffff3 3f ff ffff81 24 fffffff7 ffffff9d 27 23 ffffff9d 13 ffffff85 ffffffe6 49 ffffff82 fffffffb ffffff95 fffffff0 7d 06 ffffff9d ffffff90 ffffffc9 f ffffffd fffffff2 ffffffe1 ffffffa4 37 22 ffffffc7 6d 6d ffffffe2 ffffffee ffffffcf ffffff8e ffffffe3 ffffff90 ffffffcc 04 ffffffff ffffffc7 4 3 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 ffffff b2 ffffffbb ffffffe4 ffffffb1 ffffffc9 57 ffffffb2 ffffffcc ffffffa4 4c ffffffe3 ffffffa0 2e ffffffc1 31 ffffffc1 ffffffad ffffff86 22 ffff fffb ffffff81 fffffffa 55 ffffffe5 1e 0d 13 39 49 ffffff9c ffffffe3 fffffff9 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

Figure 5. Screen showing MDS detection of Remcos (behaviors of downloading malware strains and modifying registry keys)



이벤트 ID:230802-7
7a6c84805df4fc81ced677ea0350b651

위험도[U/K]:Medium [Known
Trojan/Win.GuLoader.C546386

악성 행위: 8/10건

유형	PPID	PID	최근 유입/수집 경로	행위 내용
파일	2104	1404	● 7a6c84805df4fc81ced677ea0350b651.exe 경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe MD5: ab5050f0b4b71352722a6122c8107f83	웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오. [파일 정보] ● Web Data MD5: 전자 서명: 없음 경로: C:₩Users₩[redacted]₩AppData₩Local₩Google₩Chrome₩User Data₩Default₩Web Data

위험도:7 [RID:10218]
웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83
C:₩Users₩[redacted]AppData₩Local₩Google₩Chrome₩User Data₩Default₩Web Data
MD5:
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83

유형	PPID	PID	최근 유입/수집 경로	행위 내용
파일				웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오. [파일 정보] 경로: C:₩Users₩[redacted]AppData₩Local₩Google₩Chrome₩User Data₩Default₩LOGIN DATA-WAL
파일	2104	1404	● 7a6c84805df4fc81ced677ea0350b651.exe 경로: C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe MD5: ab5050f0b4b71352722a6122c8107f83	서비스가 imgsvc 문자열을 가진 특정 조건의 DLL을 로드하는 행위를 탐지했습니다. 이 행위는 악성코드(Dropper)가 실행됐을 가능성을 의미합니다. 이미 동작 중인 악성코드(Dropper)의 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오. [파일 정보] 경로: C:₩Users₩[redacted]AppData₩Local₩Temp₩skylzjgnnzfdkvbfcixygcmvzjruomiz 웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오. [파일 정보] ● Login Data MD5: 전자 서명: 없음 경로: C:₩Users₩[redacted]AppData₩Local₩Google₩Chrome₩User Data₩Default₩Login Data

위험도:7 [RID:10218]
웹 브라우저 계정정보 접근 행위를 탐지했습니다. 웹 브라우저에 저장된 계정정보를 탈취할 위협이 존재할 가능성이 높으므로 시스템 전체를 대상으로 악성코드 검사를 실행하십시오.
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83
C:₩Users₩[redacted]AppData₩Local₩Google₩Chrome₩User Data₩Default₩Login Data
MD5:
C:₩Users₩Public₩Desktop₩7a6c84805df4fc81ced677ea0350b651.exe
MD5:ab5050f0b4b71352722a6122c8107f83

Figure 6. Screen showing MDS detection of Remcos (accessing account credential files)

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.

[IoC]

[MD5]

– ab5050f0b4b71352722a6122c8107f83

[File Detection]

– Trojan/Win.Guloader.C5463862 (2023.08.02.00)

[Behavior Detection]
– Execution/MDP.Remcos.M11099
– Infostealer/MDP.Credential.M10218

AhnLab MDS detects and responds to unknown threats through sandbox-based dynamic analysis. For more information about the product, please visit our official website.

AhnLab MDS
We Stop All Threats
No Ransomware No APT No Phishing
Our powerful sandboxing solution AhnLab MDS effectively detect, fend off and respond to APTs
MAX

Categories:AhnLab Detection

Tagged as:MDS,Remcos