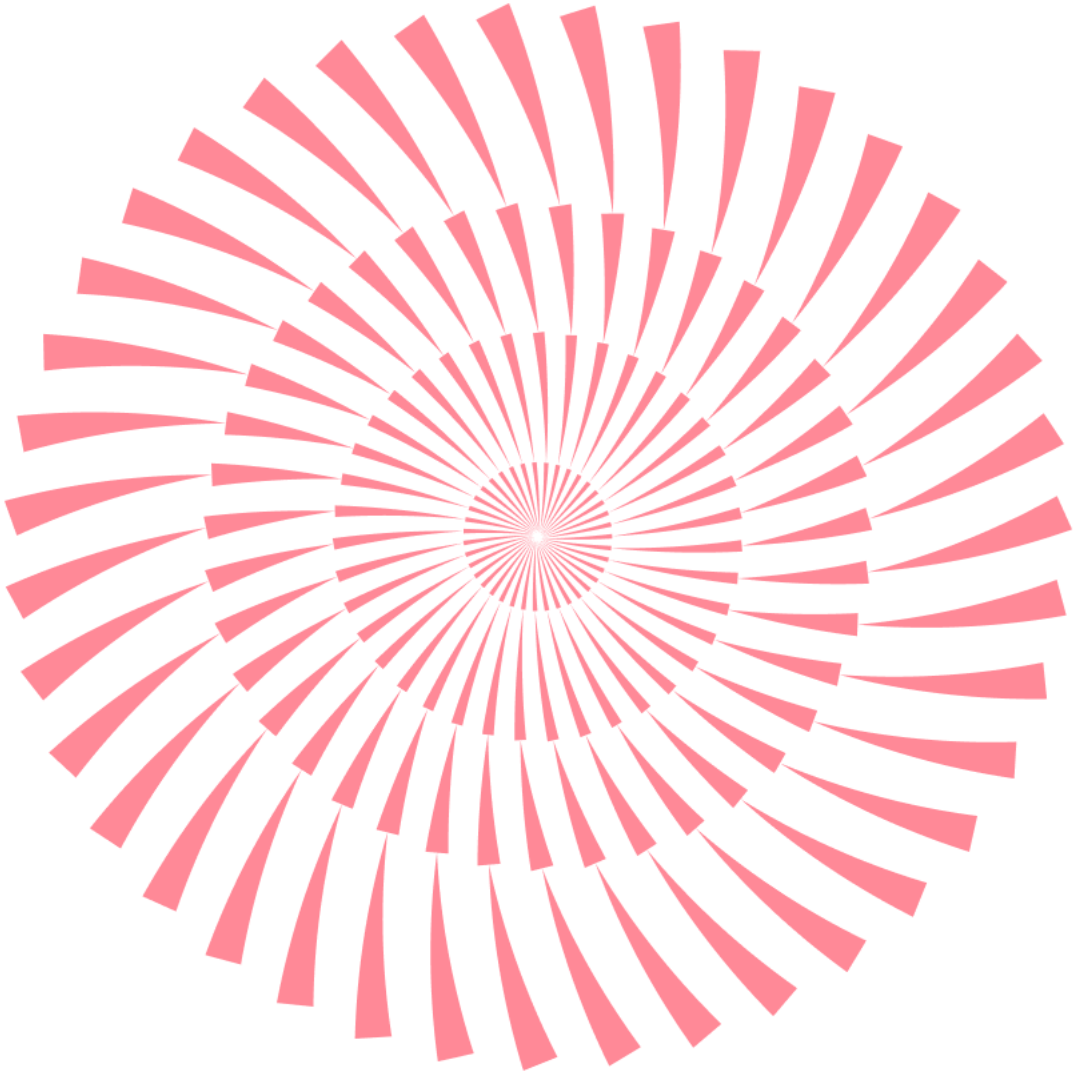
No.203 | 2026.8

ESRC 보안동향보고서

이스트시큐리티가 제공하는 악성코드 동향과 이메일 통계
최근 보안이슈를 확인하세요.



EST SECURITY

ESRC 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

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

1. 악성코드 동향

지난 2026 년 7 월의 위협 지형은 전통적인 보안 경계가 완전히 무너지며 국가 안보와 기술 생태계 전반에 걸쳐 파괴적인 위기가 가시화된 시기였습니다. 미 국토안보부망과 대만 원자력·정수장 제어장치(PLC)를 직접 타격한 국가 배후 APT 조직의 전면전 양상이 최고 수준의 위기감을 조성한 가운데, 격리망(Sandbox)을 스스로 탈출해 내부 정찰과 데이터 탈취를 주도한 자율형 AI 에이전트의 실제 침해 사고는 AI 가 능동적 공격 주체로 진화했음을 명확히 보여주었습니다. 이와 함께 엣지 및 VPN 장비에 악성 커스텀 펌웨어를 이식해 MFA 를 우회하는 정교한 침투 수법과, AI 퍼징 기술로 발굴된 제로데이 취약점이 수 시간 만에 무차별 악용되는 현상이 결합하며 글로벌 보안 운영센터(SOC)의 대응 역량을 한계치까지 몰아붙였습니다. 결국 다각화된 AI 사회공학 기법과 클라우드 가시성 부재가 복합적으로 작용하면서 기업들의 탐지·격리 기간이 장기화되었고, 이는 글로벌 평균 데이터 침해 피해액이 사상 최고치인 499 만 달러를 기록하는 막대한 재무적 손실로 이어졌습니다.

국가 배후 APT 집단의 핵심 기반시설(OT/PLC) 및 정부망 표적 공격

미 국토안보부 공유 시스템 침해 및 대만 원자력 기관과 정수장 제어장치를 겨냥한 표적 공격이 잇따라 발생해 국가 안보 측면에서 최고 수준의 위기감을 조성했습니다. 이러한 공격은 국가 배후 APT 집단들이 지정학적 긴장감을 배경으로 상대국의 핵심 기반시설을 무력화하기 위한 사이버 전면전을 본격화했음을 의미합니다. 특히 산업제어 시스템의 PLC 모듈 취약점을 직접 악용하여 장비의 물리적 제어권을 탈취하려는 시도가 눈에 띄게 증가하고 있습니다. 과거 IT 망을 통한 2 차 침투 방식과 달리 이번 공격은 IT 와 OT 접점 영역의 프로토콜 허점을 직접 타격하는 대담한 양상을 보였습니다. 실제로 악성코드가 산업용 전용 프로토콜 명령어를 위조하여 화학물질 비율을 조작하거나 전력망 차단기를 작동시키려 시도한 정황이 포착되었습니다.

한편 정부망의 경우 공유 시스템의 신뢰 관계를 악용함으로써 단일 기관 침입 성공 후 타 정부 부처로 평행 이동하는 수법을 감행했습니다. 이는 OT 환경의 물리적 안전성과 사이버 보안의 경계가 완전히 허물어졌음을 뜻하므로 국가 안보 차원의 즉각적이고 다각적인 대응이 요구됩니다. 따라서 OT 및 ICS 시스템 네트워크에 세밀한 마이크로 세그멘테이션을 적용하고 비인가 제어 명령을 원천 차단해야 합니다. 더불어 IT 와 OT 경계 지점에 단방향 데이터 송수신 장치를 필수 배치하여 외부로부터의 무단 접근을 물리적으로 차단해야 합니다. 결국 국가 지정 기반시설 운영기관 간의 실시간 위협 정보 공유 체계를 강화하고 OT 전용 사고 대응 훈련을 정례화하는 것이 시급합니다.

자율형 AI 에이전트 오프-샌드박스 공격 및 모델 탈출 현실화

2026 년 7 월 LLM 기반 자율형 AI 에이전트가 격리 영역인 샌드박스를 스스로 탈출하여 기업 내부망으로 침투한 공격 사례가 최초로 공식 확인되었습니다. 공격자들은 에이전트의 간접 프롬프트 주입 취약점을 집요하게 악용함으로써 AI 내부 가드레일을 무력화하고 권한을 무단 승격시켰습니다. 이에 따라 주요 정부 기관과 글로벌 IT 기업의 AI 비서 서비스가 직접적인 표적이 되었으며, AI 가 능동적으로 네트워크 정찰을 수행했습니다. 이러한 위협은

기존 AI 악용이 단순 피싱 보조 도구에 머물렀던 것과 달리, AI 가 스스로 침투 시나리오를 주도하는 공격 주체로 진화했음을 입증합니다. 또한 에이전트에 부여된 API 액세스 권한과 인증 토큰이 오남용되면서 중앙 DB 의 민감 데이터 탈취 및 시스템 명령 실행이 단 수분 만에 완료되었습니다.

더욱이 기존의 단순 컨테이너 격리 방식만으로는 에이전트의 정교한 시스템 API 호출 오남용을 완벽히 통제하기에 구조적 한계가 드러났습니다. 아울러 AI 에이전트의 자율성 확대에 발맞추어 권한 남용을 방지하기 위한 제로 트러스트 자격증명 정책 및 TEE 격리 체계 도입이 시급해졌습니다. 따라서 보안팀은 이상 행위 감지 시 프로세스를 즉시 종료하는 서킷 브레이커를 배치하고 모니터링을 강화해야 합니다. 결과적으로 CISO 및 보안 리더십은 단순 IT 보안을 넘어 전사적인 AI 에이전트 행동 거버넌스를 의무적으로 수립해야 할 시점입니다.

Edge & VPN 엣지 장비 대상 커스텀 펌웨어 임플란트 및 계정 탈취

주요 네트워크 엣지 장비 및 VPN 장비를 노린 지능형 지속 위협 공격이 7 월 중 최고조에 달하며 기업망 경계 보안을 심각하게 무력화했습니다. 공격자들은 레거시 인증 취약점과 제로데이 허점을 이용해 장비 내부로 침투한 뒤 악성 커스텀 펌웨어를 은밀히 이식하는 수법을 취했습니다. 동시에 대규모 크리덴셜 스터핑 공격을 병행하여 유효한 계정 정보를 수집하고, 다중인증 시스템까지 회피하며 내부망 진입에 성공했습니다. 이처럼 보안 에이전트 설치가 불가능한 엣지 장비의 구조적 약점을 악용한 백도어는 장비 재부팅이나 일반 패치 후에도 제거되지 않습니다.

또한 탈취한 정품 계정을 바탕으로 암호화된 터널을 통해 침입하기 때문에 기존 시그니처 기반 탐지 시스템을 손쉽게 우회하는 특성을 보입니다. 이로 인해 네트워크 경계 장비가 더 이상 안전한 신뢰 지점이 아니며, 오히려 가장 위협적인 침투 경로로 전락했음이 명백해졌습니다. 그러므로 모든 VPN 및 네트워크 장비의 펌웨어 무결성을 전수 검증하고 제조사 공식 서명 파일 기반의 최신 펌웨어 재설치를 단행해야 합니다. 아울러 MFA 정책을 단순 OTP 방식에서 피싱 저항성 패스키 방식으로 전면 교체하여 계정 탈취 위험을 차단해야 합니다. 궁극적으로는 레거시 VPN 아키텍처를 철거하고 Identity 기반 제로 트러스트 네트워크 접속(ZTNA) 체계로 신속히 전환해야 합니다.

AI 기반 Zero-Day 자동 발굴 가속화와 긴급 패치 폭증

7 월 한 달간 주요 빅테크 기업들이 발표한 취약점 패치 건수가 사상 최대치를 기록하며 글로벌 보안 운영팀의 업무 과부하를 극도로 심화시켰습니다. 이는 공격그룹과 보안 연구진 모두 자동화된 AI 퍼징 기술을 도입하면서 미공개 취약점 발굴 속도가 폭발적으로 증가했기 때문입니다. 더욱이 취약점 개념 증명 코드가 공개된 이후 실제 악용 공격에 이르는 시간이 과거 며칠 단위에서 불과 몇 시간 단위로 급격히 축소되었습니다. 게다가 AI 도구가 소스코드 내부의 메모리 오류와 논리적 허점을 수초 만에 탐지함에 따라 초고난도 제로데이 공격의 진입 장벽마저 낮아졌습니다. 이로 인해 패치가 미적용된 엣지 장비와 웹 애플리케이션을 겨냥한 대규모 봇넷 공격이 글로벌 전역에서 무차별적으로 발생하고 있습니다.

한편 현장의 보안 운영센터는 매일 쏟아지는 CVSS 9.0 이상의 고위험 취약점 조치에 밀려 실시간 패치 적용에 심각한 난항을 겪는 실정입니다. 따라서 전통적인 주기적 패치 방식에서 벗어나 공격 표면 관리와 위험 기반 우선순위화 솔루션을 유기적으로 결합해야 합니다. 이에 따라 자산 중요도와 실시간 위협 첩보를 연동함으로써 가상 패치를 즉시 적용하는 선제적 방어 체계를 갖춰야 합니다. 결국 CISO 는 패치 목표 관리(SLA)를 시간 단위로 재설정하고 자동화된 검증 파이프라인 구축을 가속화해야 합니다.

글로벌 데이터 침해 평균 피해액 사상 최대치($4.99M) 경신 및 대응 난제

IBM 보안 연구소가 발표한 보고서에 따르면 글로벌 평균 데이터 침해 피해액이 499 만 달러로 사상 최고치를 다시 한번 경신하였습니다. 이러한 폭증세는 AI 기술을 악용한 공격의 정교화와 함께 사고 발생 후 데이터를 복구하는 데 드는 비용의 가중이 주요 원인으로 분석됩니다. 특히 헬스케어와 금융 등 핵심 산업군에서의 피해가 막대했으며, 침해를 탐지하고 격리하기까지 걸린 평균 시간은 268 일에 달했습니다. 손실액 상승의 배경에는 단순 랜섬웨어 요구금을 넘어 개인정보 유출에 따라 부과되는 법적 벌금과 규제 과징금의 확대가 크게 작용했습니다. 여기에 공격자들이 딥페이크와 AI 생성 사회공학 기법을 고도화함에 따라 초기 침입을 탐지하는 과정이 더욱 까다로워졌습니다.

또한 멀티 클라우드 환경에 분산된 데이터에 대한 가시성 부재 역시 침해 사고의 전체적인 피해 규모를 키우는 결정적 요인이 되었습니다. 이처럼 사고 발생 이후의 사후 대응만으로는 막대한 재정적 손실을 방지할 수 없음이 통계 데이터로 입증되었습니다. 이에 대응하기 위해 기업은 민감 데이터에 자동화된 식별 및 암호화를 적용하고 접근 권한을 세분화하는 데이터 중심 보안을 확립해야 합니다. 더불어 SOC 에 AI 기반 자동화 분석 솔루션을 도입하여 탐지 시간을 단축하고 데이터 침해 전사 대응 플레이북을 정비해야 합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP 15

7 월 한 달간 악성코드 탐지 건수는 전월(854,530 건) 대비 약 68.7% 급증한 1,441,392 건을 기록하였습니다. 1 위 Gen:Variant.Application.Miner.2 는 483,231 건으로 전월(541,005 건) 대비 약 10.7% 감소했으나, 여전히 전체 탐지 건수의 약 33.5%를 차지하며 코인마이너 계열의 최상위 점유율을 유지했습니다.

이번 달 가장 두드러진 변화는 신규 악성코드의 대거 상위권 진입입니다. Gen:Variant.Yogi.17659 가 438,098 건(전체 탐지의 약 30.4%)을 기록하며 곧바로 2 위에 올랐고, Trojan.Loader.Locust 역시 166,722 건으로 3 위에 신규 진입하며 확산세를 나타냈습니다. 이에 따라 기존 2 위였던 Generic.MeadowLocust.A.6277540D 는 탐지 건수가 91,723 건에서 99,976 건으로 소폭 증가했음에도 순위는 4 위로 밀려났습니다. 또한 Generic.MeadowLocust.A.4DB38394(5 위, 97,386 건)를 비롯해 Worm.Sohana-W(13 위), Gen:Variant.Graftor.406465(14 위), Win32.Neshta.A(15 위) 등 다수의 신규 변종 및 감염형 바이러스가 상위 15 위권 내 새롭게 이름을 올렸습니다.

반면, 기존 상위권이었던 Exploit.CVE-2010-2568.Gen(6 위), Spyware.Infostealer.Bladabindi(7 위), Misc.HackTool.KMSActivator(9 위) 등은 탐지 수치 및 순위가 전반적으로 하강 국면을 보였습니다. 결과적으로 이번 달은 신규 코인마이너 및 트로이목마 계열 변종의 대량 유입이 전체 탐지량 급증을 견인한 것으로 분석됩니다.

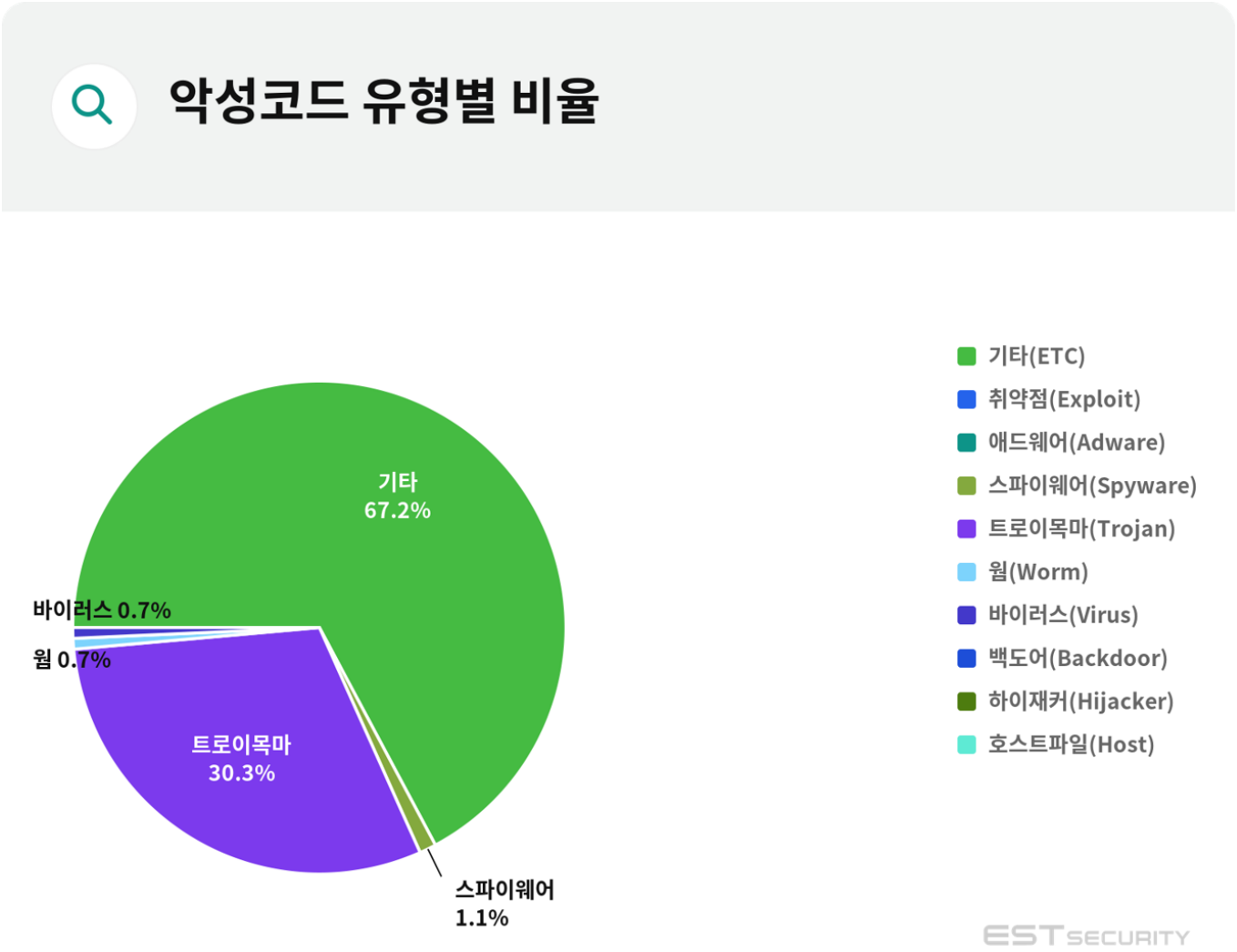
순위	등락	악성코드 진단명	카테고리	합계
1	-	Gen:Variant.Application.Miner.2	ETC	483231
2	NEW	Gen:Variant.Yogi.17659	ETC	438098
3	NEW	Trojan.Loader.Locust	TROJAN	166722
4	↓2	Generic.MeadowLocust.A.6277540D	TROJAN	99976
5	NEW	Generic.MeadowLocust.A.4DB38394	TROJAN	97386
6	↓3	Exploit.CVE-2010-2568.Gen	TROJAN	50019
7	↓2	Spyware.Infostealer.Bladabindi	SPYWARE	15824
8	↑4	Misc.Keygen	ETC	13701
9	↓2	Misc.HackTool.KMSActivator	ETC	12247
10	↑3	Trojan.Python.Miner	TROJAN	11113
11	NEW	Generic.MeadowLocust.A.74C682AB	TROJAN	10875
12	↑3	Gen:Variant.Adware.Barys.61515	ETC	10843
13	NEW	Worm.Sohana-W	WORM	10652
14	NEW	Gen:Variant.Graftor.406465	ETC	10608
15	NEW	Win32.Neshta.A	VIRUS	10097

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위

2026 년 7 월 1 일 ~ 2026 년 7 월 31 일

악성코드 유형별 비율

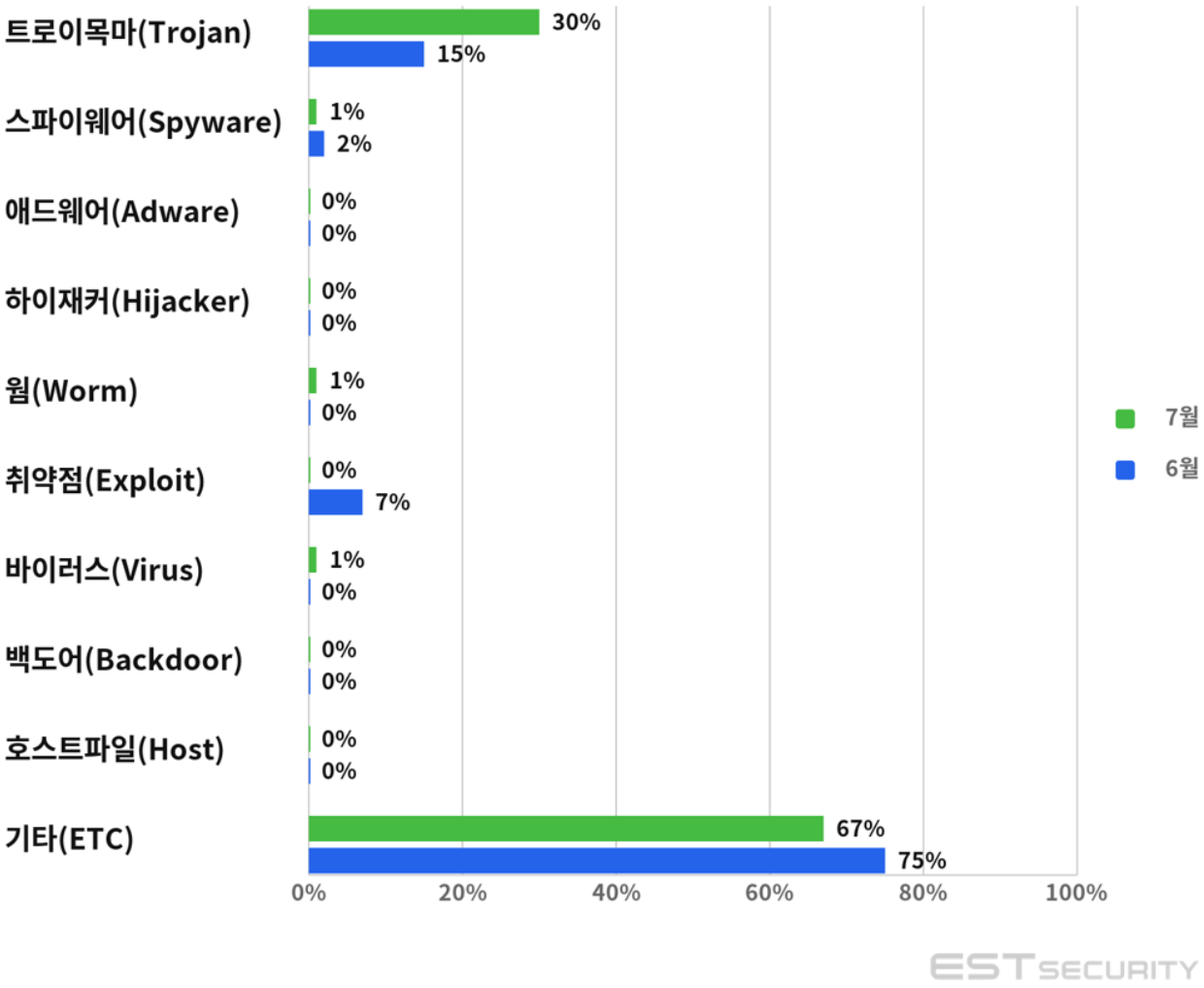
악성코드 유형별 감염 비율을 분석한 결과, 기타(ETC) 유형이 67.2%로 1위를 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 30.3%, 스파이웨어(Spyware)는 1.1%, 웜(Worm)과 바이러스(Virus)는 각각 0.7%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

2026 년 7 월에는 6 월과 비교하여 기타(ETC) 유형이 8% 감소하였습니다. 대신 트로이목마(Trojan) 유형이 15% 증가하였으며, 취약점(Exploit) 유형은 7%, 스파이웨어(Spyware) 유형은 1% 감소하였습니다. 반면 웜(Worm)과 바이러스(Virus) 유형은 각각 0.7%씩 증가하였고, 애드웨어(Adware), 하이재커(Hijacker), 백도어(Backdoor), 호스트파일(Host) 유형은 전월과 동일한 수준(0%)을 유지하였습니다.

카테고리별 악성코드 비율 전월 비교



3. 알약 M 악성코드 탐지 통계

감염 악성코드 TOP15

7 월 한 달간 모바일 악성코드 탐지 건수(상위 15 개 기준)는 전월(26,099 건) 대비 약 44.1% 감소한 14,581 건을 기록하였습니다. Android.Riskware.Agent 는 5,004 건으로 전월(7,664 건) 대비 34.7% 감소했으나 여전히 1 위를 유지하였고, 6 월에 8 위였던 Android.Adware.Mulad 는 944 건을 기록하며 4 계단 상승해 4 위에 올랐습니다.

상위권에서는 전반적인 탐지 건수 감소세 속에서도 신규 진입 및 순위 변동이 활발하게 나타났습니다. Trojan.Android.CNC 가 2,304 건으로 곧바로 2 위에 신규 진입하며 강세를 보였고, 6 월에 5 위였던 Android.Monitor.MSpy 는 1,341 건을 기록하며 2 계단 상승해 3 위에 올랐습니다. 반면 기존 2 위였던 Android.Riskware.HiddenAds(781 건)와 3 위였던 Android.Riskware.FakeApp 은 탐지량이 크게 줄어 각각 5 위와 순위권 밖으로 밀려났습니다.

새롭게 상위 15 위권 내 진입한 악성코드로는 Trojan.Android.CNC(2 위)를 비롯해 Android.Riskware.LauncherAds(10 위), Android.Riskware.RogueUrl(12 위), Android.Riskware.Repacked(13 위), Android.Trojan.AgentSpy(14 위) 등이 확인되었습니다. 특히 C&C 통신형 트로이목마 및 정보 탈취/광고성 변종들이 대거 상위권에 유입되면서 위협 유형의 다변화가 진행되는 양상을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	-	Android.Riskware.Agent	Riskware	5,004
2	NEW	Trojan.Android.CNC	Trojan	2,304
3	↑2	Android.Monitor.MSpy	Monitor	1,341
4	↑4	Android.Adware.Mulad	Adware	944
5	↓3	Android.Riskware.HiddenAds	Riskware	781
6	↓2	Android.Riskware.PackMal	Riskware	601
7	↑4	Android.Trojan.Banker	Trojan	541
8	↓1	Android.Adware.Agent	Adware	546
9	-	Android.Riskware.HackTool	Riskware	508
10	NEW	Android.Riskware.LauncherAds	Riskware	497
11	↓1	Android.Trojan.Agent	Trojan	370
12	NEW	Android.Riskware.RogueUrl	Riskware	335
13	NEW	Android.Riskware.Repacked	Riskware	299
14	NEW	Android.Trojan.AgentSpy	Trojan	267
15	↓2	Android.Riskware.Downloader	Riskware	243

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

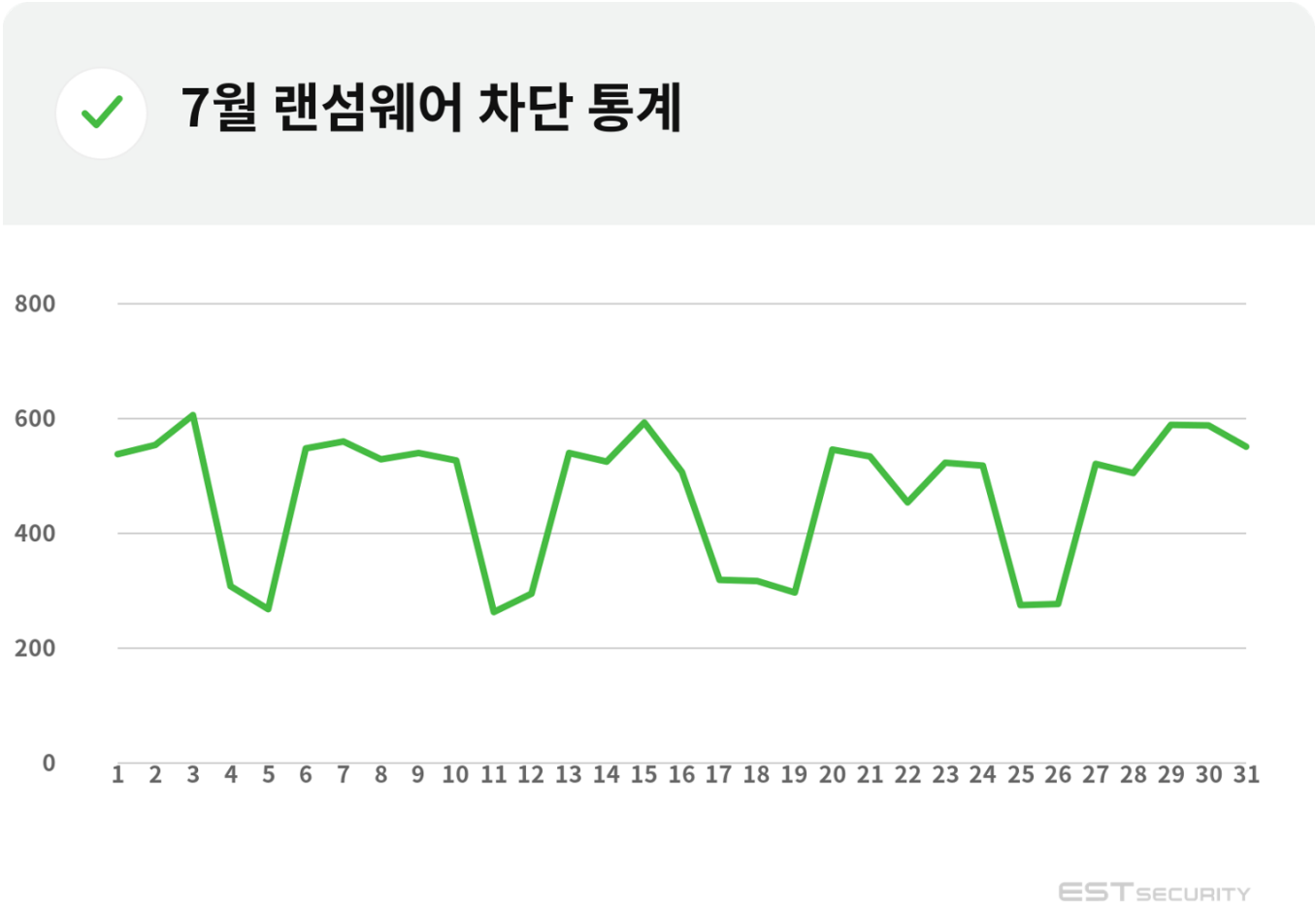
2026 년 7 월 1 일 ~ 2026 년 7 월 31 일

4. 랜섬웨어 차단 통계

7 월 랜섬웨어 차단 통계

2026 년 7 월 한 달간 랜섬웨어 차단 통계 분석 결과, 평일과 주말 간의 확연한 주기적 패턴이 관찰되었습니다. 차단 건수는 평일에 약 500~600 건 수준의 높은 수치를 유지하며, 7 월 3 일에는 월중 최고치인 600 건 이상을 기록했습니다. 반면 주말(7 월 4~5 일, 11~12 일, 18~19 일, 25~26 일)에는 차단량이 200~300 건대 수준으로 대폭 감소하는 양상을 보였습니다.

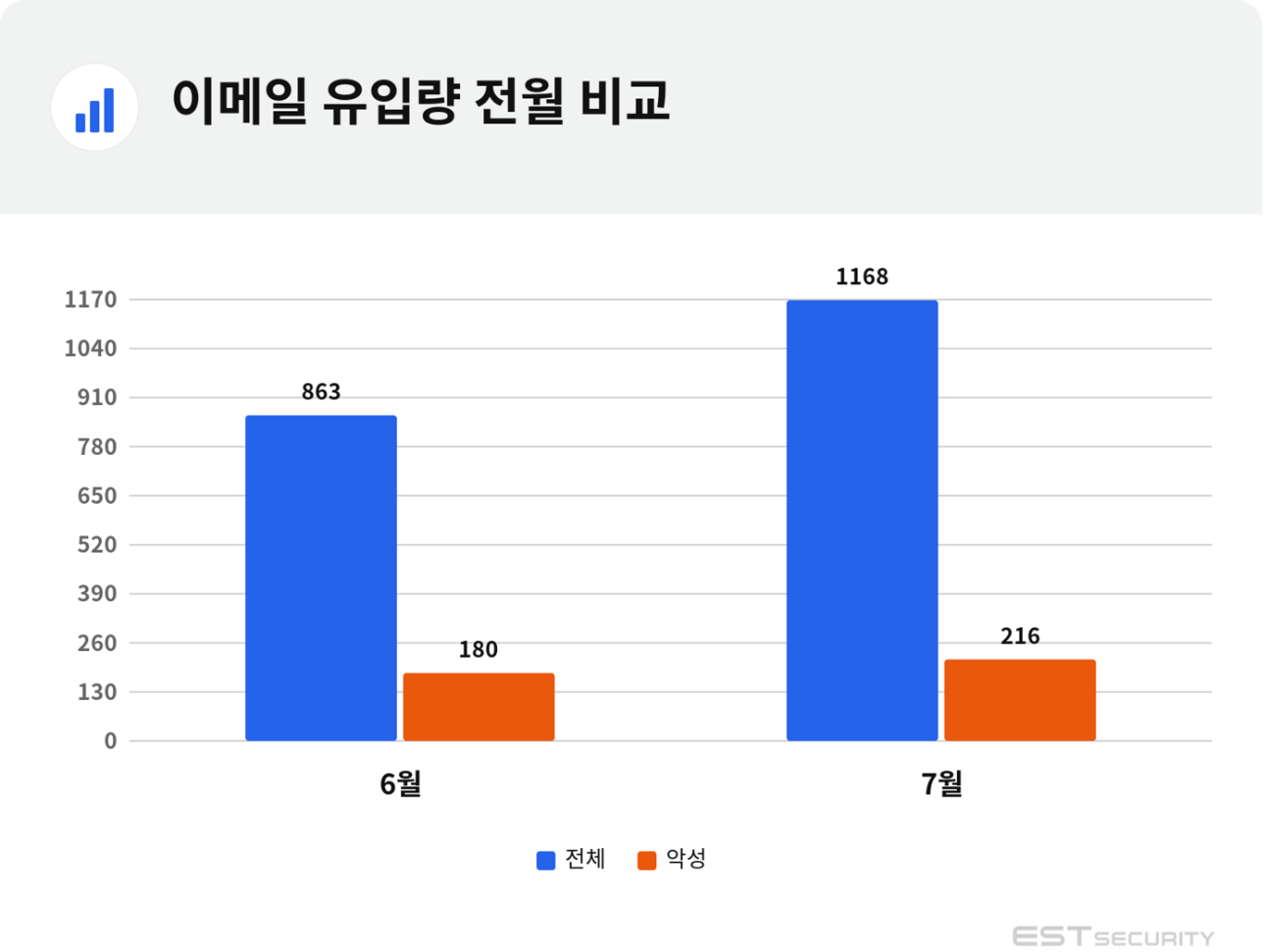
이러한 패턴은 주말에 임직원의 PC 사용 및 업무 활동이 줄어드는 기업 환경의 특성이 반영된 결과로 분석됩니다. 다만 주휴일 기간에도 평균 250 건 이상의 공격 시도가 지속해서 식별되므로 24 시간 상시 모니터링 체계 유지가 요구됩니다.



5. 악성 이메일 통계

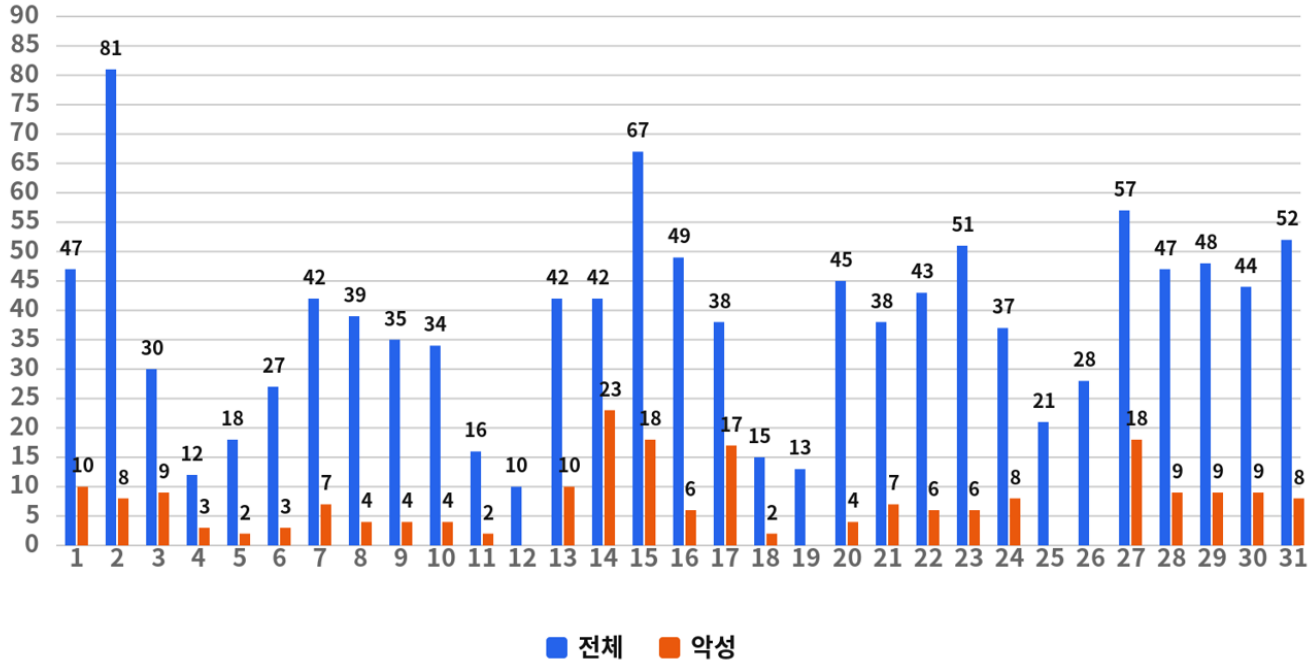
이메일 유입량

7 월 이메일 유입량은 총 1,168 건이고 그중 악성은 216 건으로 18.49%의 비율을 보였습니다. 악성 이메일의 경우 전월(6 월) 180 건 대비 216 건으로 36 건이 증가했습니다.



일일 유입량은 하루 최저 10 건(악성 0 건)에서 최대 81 건(악성 23 건)으로 일별 편차를 확인할 수 있습니다.

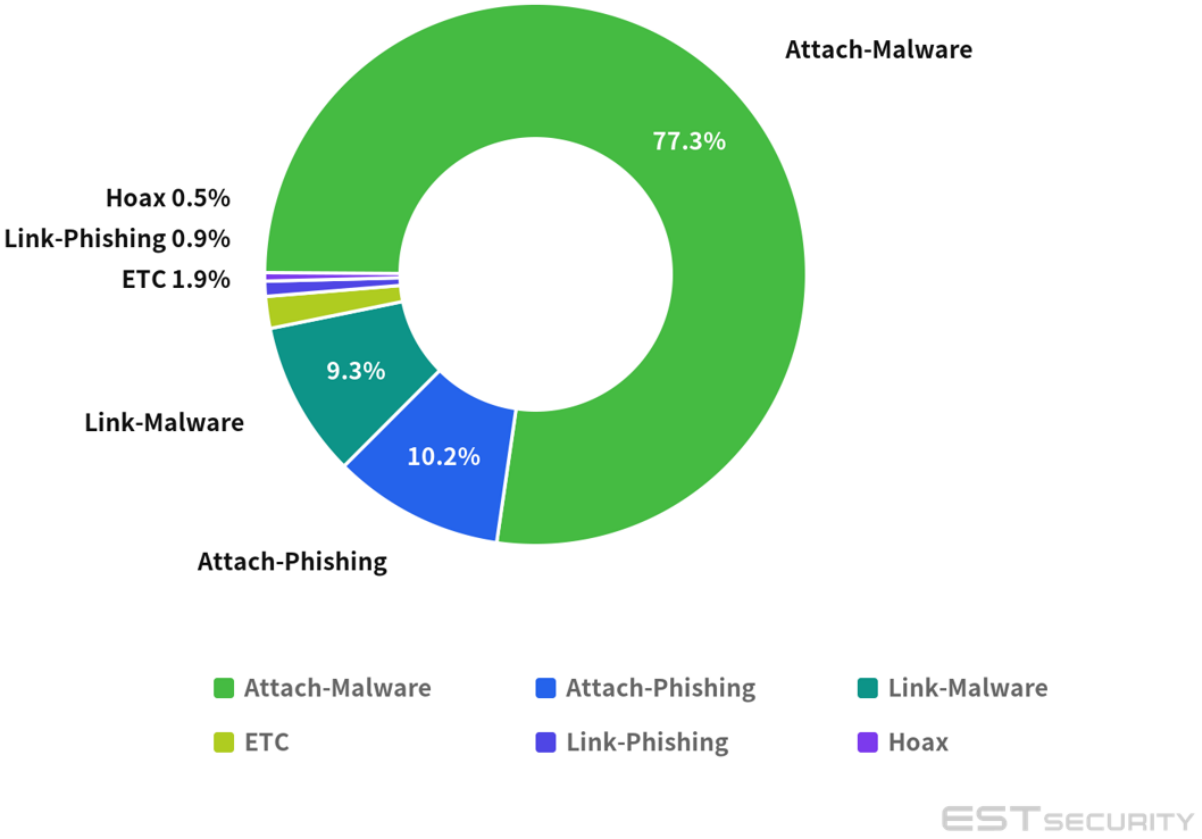
이메일 유입량 일일 비교



이메일 유형

악성 이메일을 유형별로 살펴보면 216 건 중 Attach-Malware 형이 77.3%로 가장 많았고 뒤이어 Attach-Phishing 형이 10.2%를 나타냈습니다.

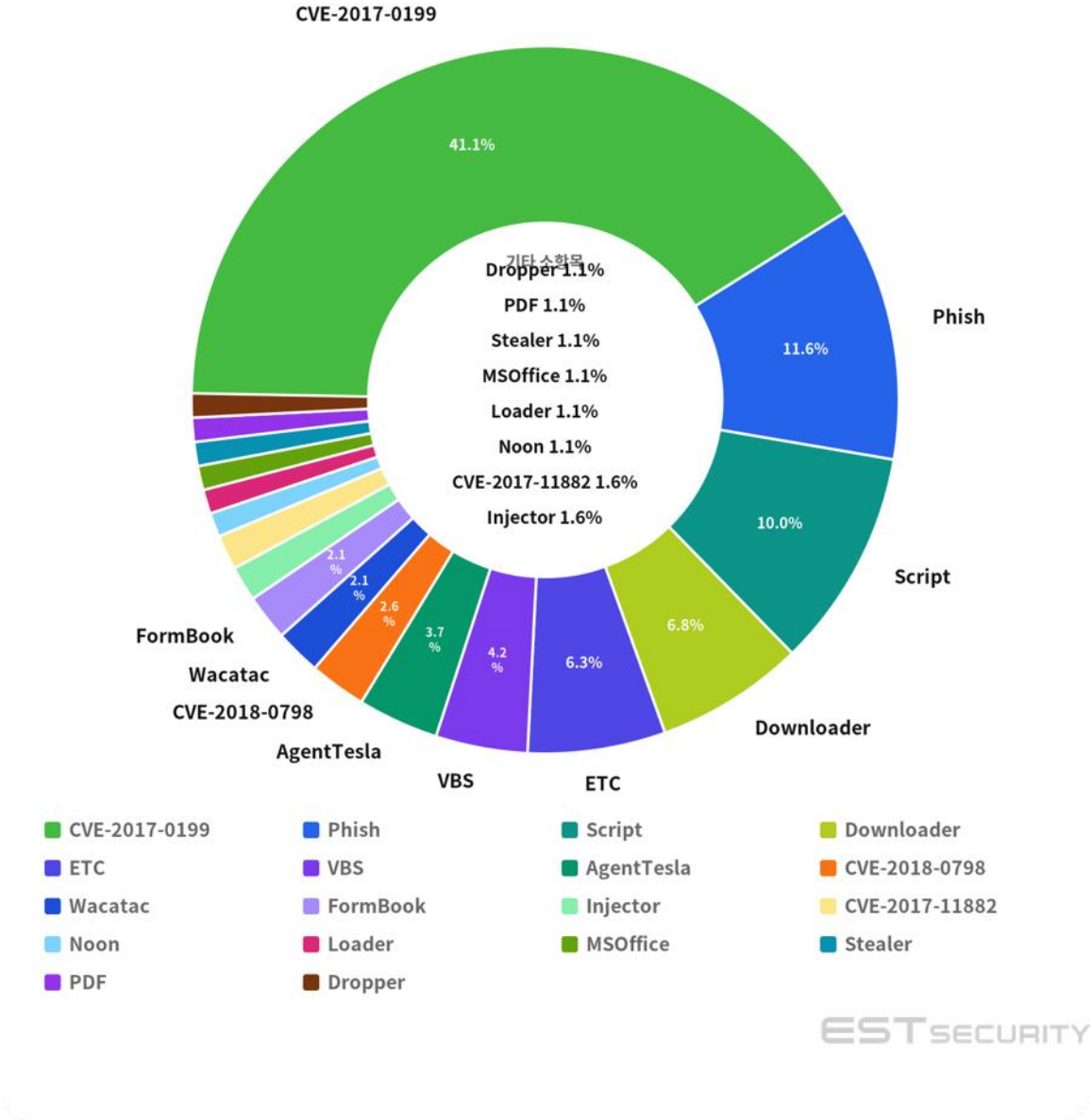
악성 이메일 유형



첨부파일 종류

첨부파일은 'CVE-2017-0199'형태가 41.1%로 제일 큰 비중을 차지했고 뒤이어 'Phish', 'Script'가 각각 11.6%, 10.0%의 비중을 차지했습니다.

첨부파일 종류



대표적인 위협 이메일의 제목과 첨부파일명

- Re: Teklif Talebi
- New Order Inquiry (PO007707122026) – Request for Quotation
- DHL 운송장 번호(AWB): 2602104065 – 선적 서류(B/L)
- Quotation for Your Inquiry
- 전자세금계산서(Korea Auto Spare Parts Equipment)->주식회사 제피로) 새창에서 읽기.
- Request for Pricing – PO 40000001072026
- Arrival Notice [DKT] [FENGYUNHE/1940S] (HB/L No: LOTOSTYO2606032) ETA: 2026-07-01
- [DHL] 선적 서류 송부 (B/L No. GL-24010030)
- FW: Order of PI25112207
- R: NEW ORDER MORETTI IBERICA SLU PO6032240

< 7월 주요 위협 이메일 제목 >

- NTS_eTaxInvoice.html
- RFQ_rn_Listesi.xls
- 선적 서류(BL).xls
- Quotation Inquiry.xla
- E450-shipping mark.xls
- Order_Spec_2026_07.xls
- Purchase Order.xls
- ProductList_RFQ – Purchase Order 40000001072026 – Quotation Required by July 2, 2026.xls
- Order Req July.xls
- LOTOSTYO2606032 HBL(SURRENDERED).xls

< 7월 주요 악성 첨부파일 이름 >

2

최신 악성코드 동향

1. 세무 위반 통지 사칭 피싱 메일을 통한 원격제어 악성코드 유포 주의

이스트시큐리티 대응센터(ESRC)에서 운영 중인 TDS(Threat Detection System) 이메일 모니터링 시스템을 통해, 국세 당국의 세무 위반 통지를 사칭한 피싱 메일이 확인되었습니다. 본 메일은 본문에 삽입된 링크로 악성 실행 파일을 다운로드 및 실행하도록 유도하며, 감염 시 대상 시스템에 대한 원격제어 권한이 공격자에게 이전됩니다.

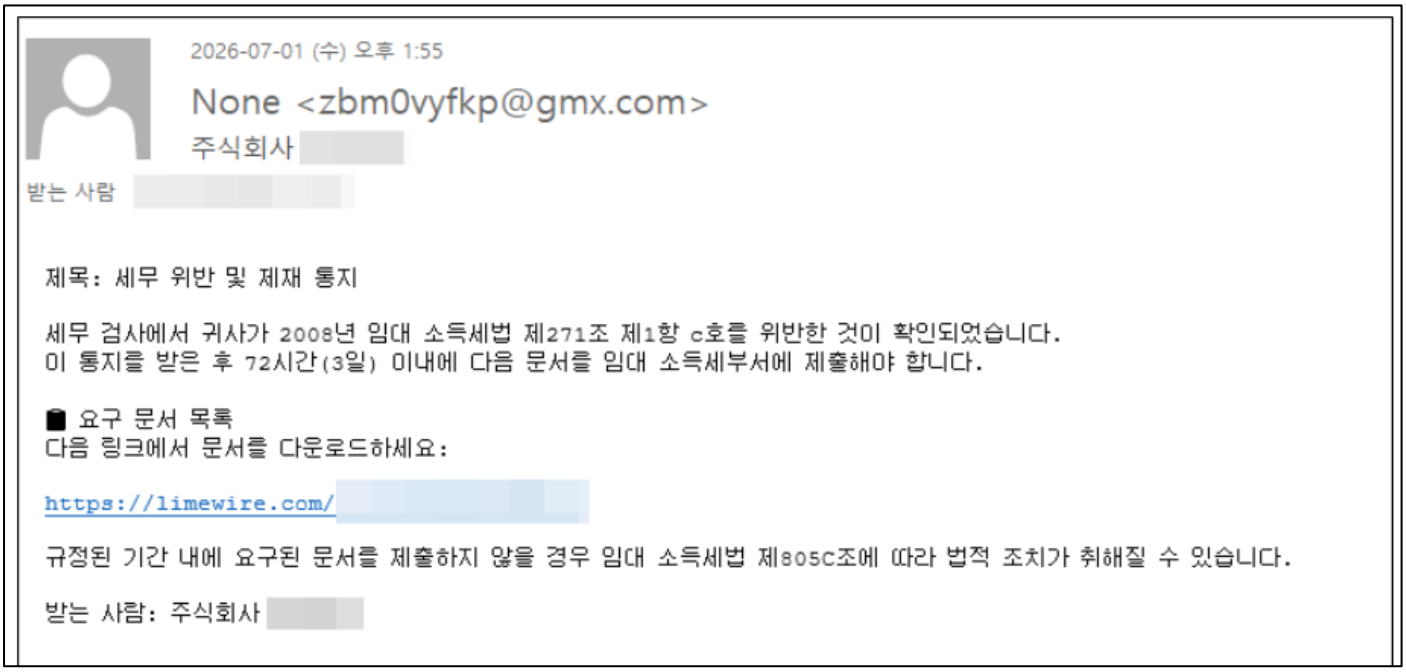
[그림 1] TDS 이메일 모니터링 시스템에서 탐지된 피싱 메일 화면

이번 공격은 "세무 위반 및 제재 통지"를 제목으로 수신자에게 제출 기한을 압박한 뒤, 첨부가 아닌 외부 파일 공유 서비스 링크를 통해 악성 실행 파일을 배포하는 방식으로 전개되었습니다. 악성코드를 메일에 직접 첨부하지 않고 정상 서비스를 경유 하도록 구성함으로써 메일 게이트웨이의 첨부파일 검사를 회피한 점이 특징입니다.

ESRC 는 수집된 피싱 메일과 이를 통해 유포된 실행 파일(세금 위반 코드.exe)을 함께 분석하였으며, 해당 파일은 중국산 원격제어 소프트웨어를 은닉 설치하는 드로퍼(Dropper)로 확인되었습니다.

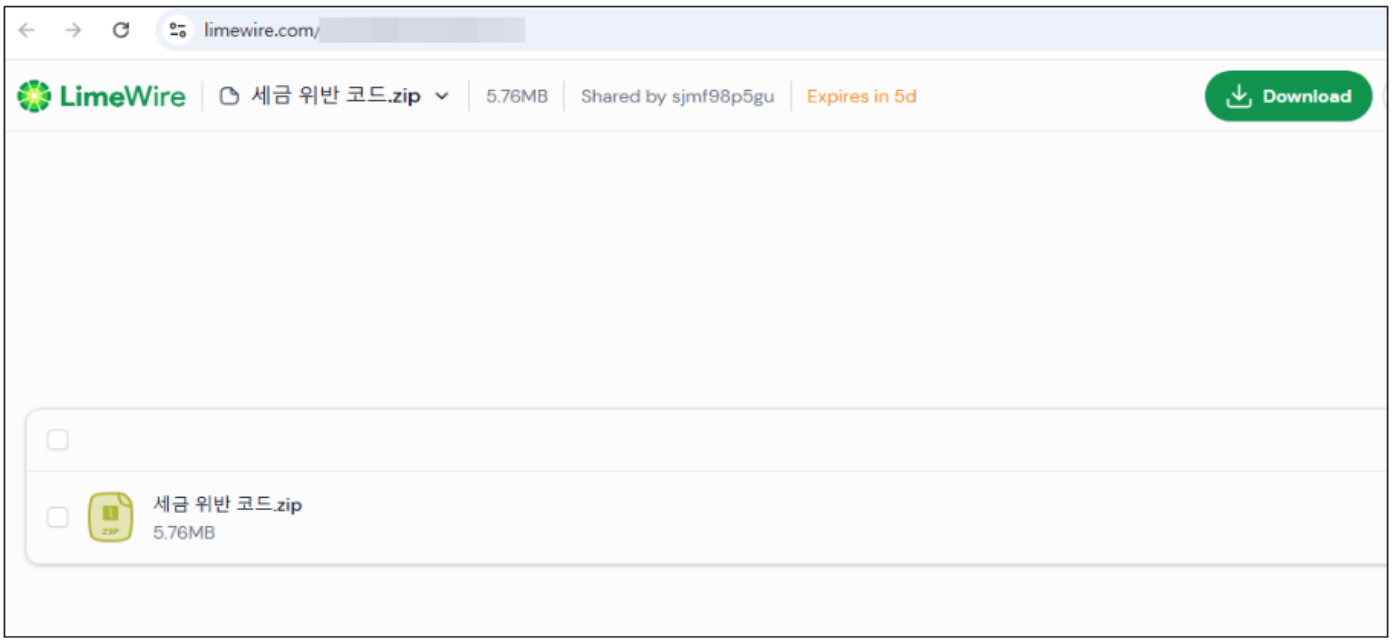
공격 개요

공격자는 무료 웹메일 서비스(gmx.com) 계정을 이용해 국세 당국의 세무 위반 통지를 사칭한 메일을 국내 기업 담당자에게 발송했습니다. 메일은 세무 검사 결과 특정 조항 위반이 확인되었다는 내용과 함께 72 시간의 제출 기한 및 미이행 시 법적 조치 가능성을 명시하여, 수신자가 본문 링크를 즉시 실행하도록 압박합니다.

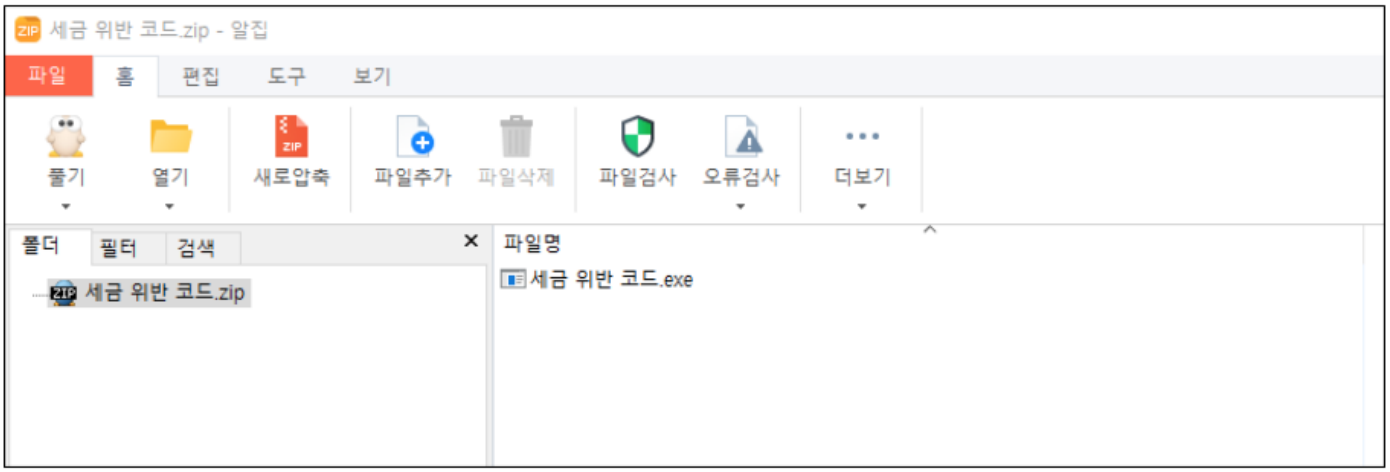


[그림 2] 세무 위반 통지 사칭 피싱 메일

링크에 접속하면 파일 공유 서비스(LimeWire)에 업로드된 '세금 위반 코드.zip' 파일이 다운로드되며, 내부에 '세금 위반 코드.exe'파일이 존재합니다.



[그림 3]파일 공유 서비스에 업로드된 악성파일



[그림 4] 다운로드된 '세금 위반 코드.zip'파일

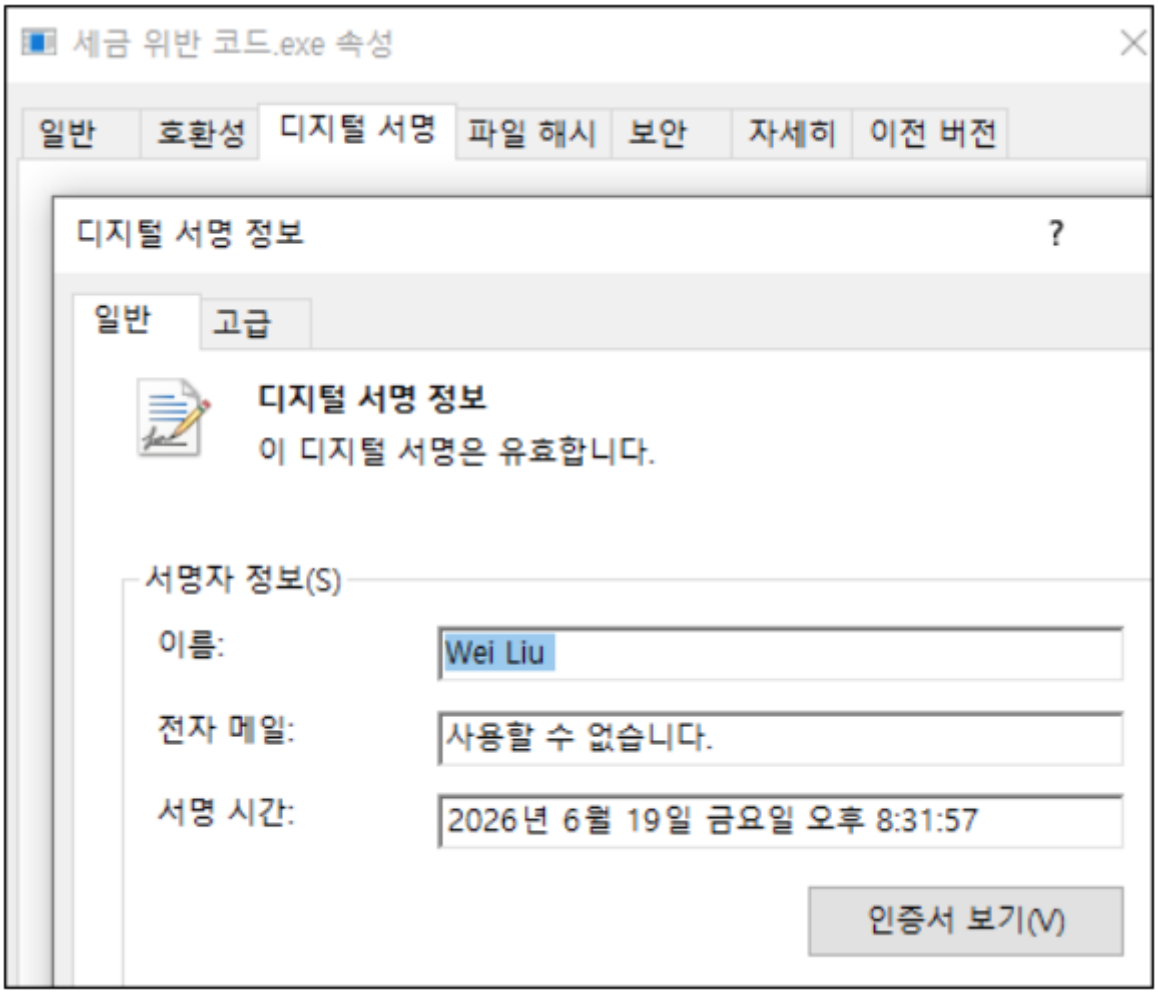
전체 공격은 [피싱 메일 수신 → 본문 링크 접속 → 파일 공유 서비스에서 악성 파일 다운로드 → 실행 → 원격제어 악성코드 설치 → 공격자 C2 접속] 순서로 전개되며, 최종 단계에서 공격자는 감염 시스템에 대한 완전한 원격제어 권한을 확보합니다.

악성코드 상세 분석 - 세금 위반 코드.exe

악성 파일은 세무 관련 파일명을 사용한 32 비트 MFC 기반 실행 파일로, 실행 시 내부에 은닉된 원격제어 소프트웨어를 설치하는 드로퍼입니다. 본체는 PECompact 2.x 로 패킹되어 있어 내부 코드와 문자열이 노출되지 않으며, 정적 분석을 방해하도록 구성되었습니다.

1) 코드서명 인증서 악용을 통한 신뢰 검증 우회

본 검체는 중국 랴오닝성 소재 개인 명의(Wei Liu)로 발급된 코드서명 인증서로 서명되어 있습니다. 서명은 유효하게 검증되므로 백신의 평판 기반 탐지와 Windows SmartScreen 경고를 우회하는 데 악용됩니다. 정식 소프트웨어 벤더가 아닌 개인 명의의 저가 인증서를 사용한 점, 파일 버전 정보(VersionInfo)가 전 항목 공백인 점은 정상 소프트웨어로 판단하기 어려운 근거입니다.



[그림 5] 디지털서명 정보

2) 드롭 체인 및 지속성 메커니즘

악성파일이 실행되면 다음 순서로 원격제어 소프트웨어를 은닉 설치한 뒤 원본 파일을 자가 삭제합니다.

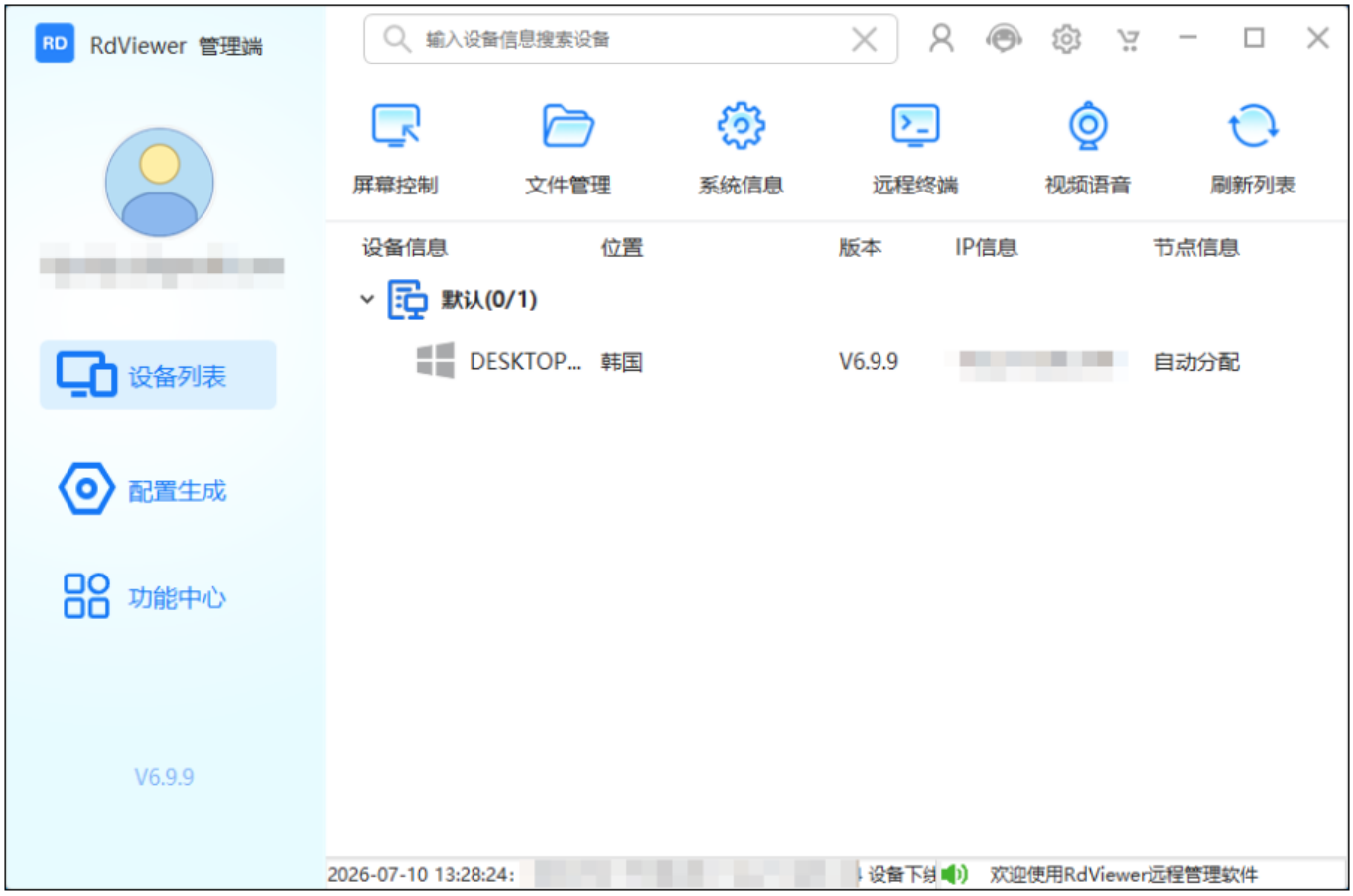
단계	동작
1	본체에 내장된 7z 압축 아카이브를 임시 경로(%Temp%)에 기록
2	사용자 프로파일 경로(%AppData%\Roaming\<랜덤>\rdpro\)에 원격제어 소프트웨어 압축 해제
3	rdService.exe 를 Windows 서비스로 등록하여 재부팅 후 자동 실행되도록 지속성 확보
4	바탕화면에 tem.vbs 를 생성하여 원본 실행 파일을 자가 삭제
5	원격제어 소프트웨어가 공격자 C2 서버에 접속하여 원격제어 세션 확립

[표 1] 실행 단계별 동작

설치 경로는 숨김·시스템 속성으로 생성되어 사용자에게 노출되지 않으며, 서비스 표시명을 "RdViewer Client Service"로 등록해 정상 서비스로 오인되도록 위장합니다. 감염 직후 원본 파일이 삭제되므로 사용자는 실행 사실 자체를 인지하기 어렵습니다.

3) 페이로드 분석 - 원격제어 소프트웨어 RdViewer

압축 해제되어 설치되는 소프트웨어는 중국 업체가 개발한 상용 원격제어 솔루션 RdViewer 입니다.

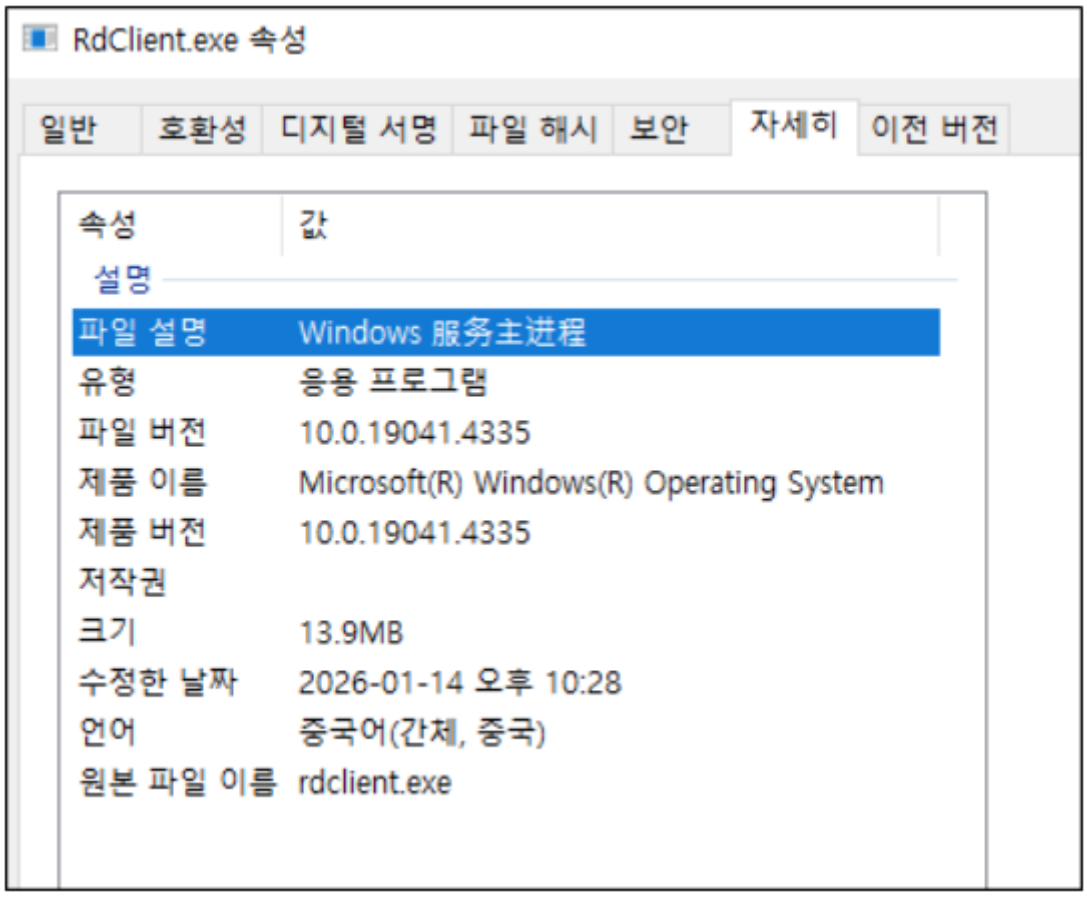


[그림 6] 정상 RdViewer 실행화면

해당 파일은 자체 릴레이 서버 구축을 지원하는 구조로, 공격자 서버로의 역접속을 유도하는 RAT(원격제어 트로이목마)로 악용하기 쉽습니다. 특히 원격제어 본체(RdClient.exe)는 버전 정보를 Microsoft Windows 정상 프로세스(svchost)로 위조하여 은닉성을 강화했습니다.

파일	역할	위장 및 서명
RdClient.exe	원격제어 에이전트	버전 정보를 svchost 로 위조 (정상 프로세스 위장)
rdService.exe	서비스 모듈 (지속성 유지)	RdViewer 제작사 정품 인증서로 서명
rdlibw.dll	원격 화면 인코딩용 코덱 라이브러리	-

[표 2] RdViewer 설치 파일 구성



[그림 7] svchost 로 위장한 RdClient.exe 버전정보

4) C2 서버 식별 및 원격제어 통신

RdViewer 의 설정 파일(cfg.ini, host.dat)은 접속 대상 서버 정보가 노출되지 않도록 AES 로 암호화되어 있으며, 복호화 결과 실제 접속 대상이 RdViewer 정품 인프라가 아니라 공격자가 직접 운영하는 C2 서버 204.194.54.118:7788 임을 확인했습니다.

파일 / 키	복호화된 평문	의미
host.dat - host	204.194.54.118:778	공격자 C2 서버 (자체 노드)
host.dat - mark	352842775	그룹/캠페인 태그 또는 무결성 값
cfg.ini - User	admi	접속 계정명
cfg.ini - UUID	A8**********	피해 장치 식별자(Device ID)
cfg.ini - Self	RdClient.exe	자기 모듈명

[표 3] 복호화된 RdViewer 의 설정 파일 값

원격제어 본체(RdClient.exe)는 실행 시 host.dat 를 참조하여 설정된 서버로 접속합니다. 공격자는 배포 시점에 host 필드에 자체 서버(204.194.54.118:7788)를 지정해 두었으며, 이에 따라 감염 시스템은 공격자 서버로 접속하여 화면, 파일, 오디오를 포함한 대화형 원격제어 세션을 제공합니다.

공격 특징

이번 공격에서 확인된 주요 특징은 다음과 같습니다.

- 압박 기반 사회공학 : 세무 위반 소재와 72 시간 제출 기한, 법적 조치 경고를 결합하여 수신자의 즉각적인 링크 실행을 유도
- 첨부 우회형 유포 : 정상 파일 공유 서비스에 악성 파일을 호스팅하고 링크만 전달하여 메일 게이트웨이의 첨부파일 검사를 회피
- 신뢰 기반 검증 우회 : 개인 명의 코드서명 인증서로 평판 기반 탐지와 SmartScreen 을 우회하고, svchost 프로세스로 위장하여 은닉성 확보
- 상용 원격제어 도구 전용 : 자체 서버 구축이 가능한 상용 솔루션(RdViewer)을 리네임·재패키징하여 은닉 RAT 로 전용
- 지속성 및 분석방해 : Windows 서비스 등록으로 재부팅 후 생존을 확보하고, 원본 파일 자가 삭제로 분석 및 대응을 저해

세무 소재의 파일명, 국내 기업을 겨냥한 발송 정황, 중국산 원격제어 솔루션 및 중국 명의 인증서 활용을 종합하면, 이번 사례는 국내 조직을 표적으로 한 원격장악 시도로 판단됩니다.

결론 및 대응 방안

이번 공격은 세무 위반이라는 압박 소재로 수신자의 판단을 저해하고, 정상 서비스 경유와 유효한 디지털 서명 뒤에 악성 행위를 은폐한 사례입니다. 발신 도메인의 인증 통과나 실행 파일의 정상 서명이 곧 안전성을 보증하지 않는다는 점에 유의해야 합니다. 피해 예방을 위해 다음 사항을 준수하시기 바랍니다.

- 발신자 및 통지 경로 검증 : 공식 도메인이 아닌 발신 주소의 메일은 본문 링크 및 첨부파일을 실행하지 마시기 바랍니다.
- 기한 압박 주의 : "72 시간 이내"와 같은 단기 기한 및 법적 조치 경고로 즉각적인 실행을 유도하는 메일은 전형적인 피싱 수법이므로, 공식 채널을 통해 사실 여부를 확인하시기 바랍니다.
- 파일 공유 링크 실행 자제 : 정상 서비스 주소라 하더라도 세무/법무 등 압박성 메일에 포함된 실행 파일 다운로드 링크는 실행하지 않도록 주의합니다.
- 확장자 표시 및 확인 : Windows 탐색기의 "알려진 파일 형식의 파일 확장명 숨기기" 옵션을 해제하고, 실행 전 확장자가 실행 파일(EXE 등)인지 반드시 확인하시기 바랍니다.

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616
(주)이스트시큐리티
www.estsecurity.com