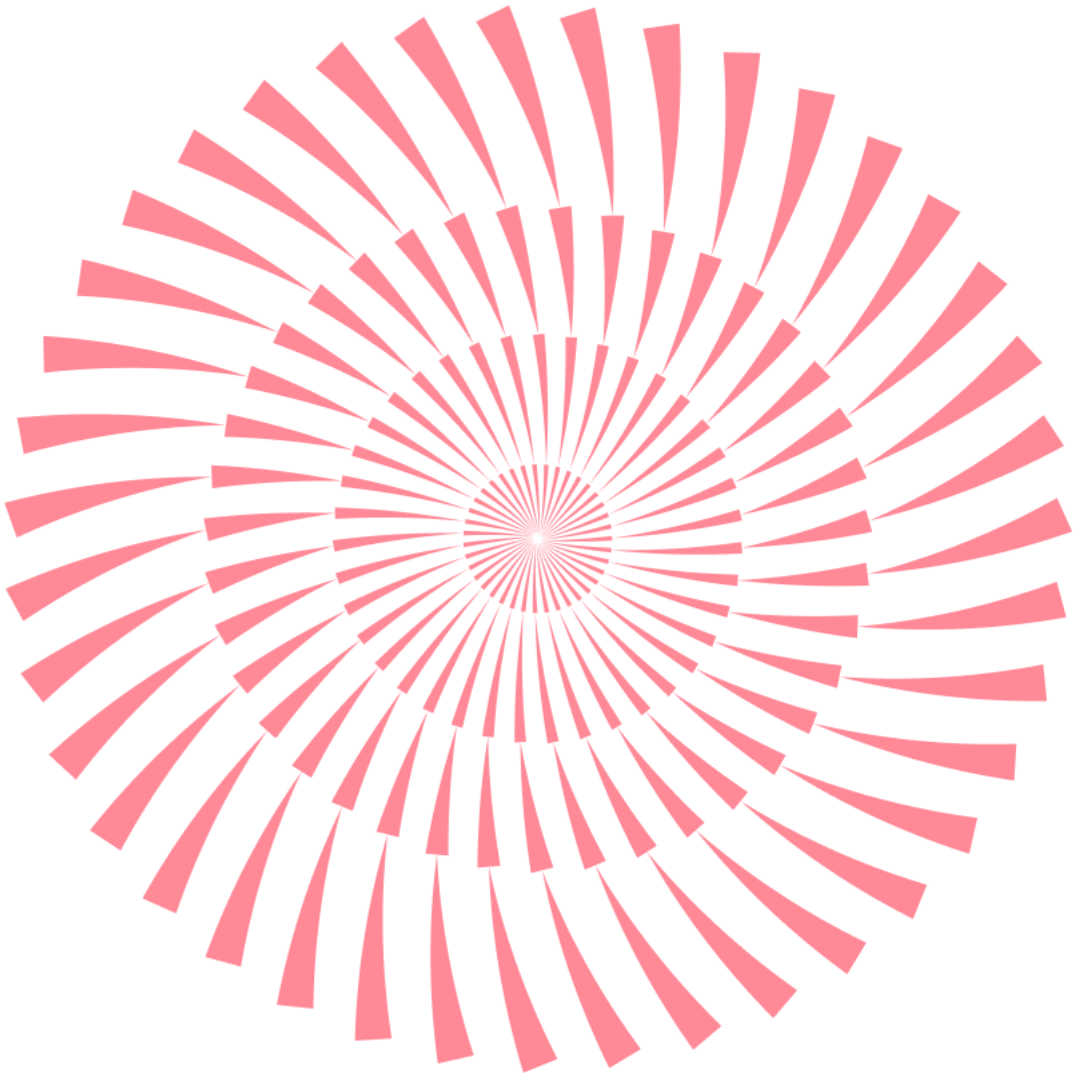
No.196 | 2026.1

ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



Copyright©2025 ESTsecurity Corp. All rights reserved.

EST SECURITY

ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지 URL 통계

2 최신 보안 동향 06-13

코인 선물 트레이딩 비법서를 위장한 LNK 파일 주의!

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지 URL 통계

1. 악성코드 동향

최근 보안 위협은 기술적 진보와 관리적 허점을 동시에 파고들며 더욱 정교해지고 있습니다.

생성형 AI 를 활용한 공격이 지속적으로 발견되고 있는 가운데 금융 사기 영역에서도 AI 기반 악성코드가 발견되어 각별한 주의가 필요합니다. 이번에 발견된 악성코드는 사용자 스마트폰에 침투하여 NFC 결제 데이터를 실시간으로 중계하거나 가로챌 수 있습니다. 이렇게 가로챈 결제데이터를 사용하여 온라인 구매를 시도하거나 ATM 에서 무단 인출을 수행하는 등의 악성행위가 가능합니다. 특히 악성코드 제작 단계부터 AI 를 활용해 탐지 회피 기술을 고도화 하고 있어 각별한 주의가 필요합니다.

기업들을 타깃으로 한 공격 및 공격 시도도 지속되고 있습니다.

OTT 플랫폼 티빙은 최근 타 사이트에서 유출된 계정 정보를 무차별적으로 대입하는 크리덴셜 스터핑 공격을 탐지하여 선제적 방어 조치를 취했음을 알렸습니다.

G 마켓에서는 60 여명의 고객 계정이 도용되어 무단으로 결제가 이루어진 사고가 발생했으며, 신세계 그룹은 내부 인트라넷에 저장되어 있던 약 8 만명의 임직원 및 협력사 직원 정보가 유출되었습니다. 써클차트에서도 6 만 건의 개인정보가 유출되어, 이에 대한 보상으로 피해자들에게 공연 티켓을 지급하기도 했습니다.

외부의 침입만큼이나 치명적인 내부자에 의한 위협도 현실화되었습니다.

신한카드에서 발생한 가맹점 대표 정보 등 약 20 만 건의 유출 사건은 조사 결과 내부 직원의 소행으로 밝혀졌습니다. 해당 직원은 자신의 영업 실적을 올리기 위해 고객 정보를 무단으로 조회하고 활용한 것으로 드러났는데, 비록 유출된 정보의 판매 등 2 차 범죄 정황은 아직 확인되지 않았으나 가장 신뢰받아야 할 내부 인력에 의한 위협이 얼마나 심각한 보안 사각지대인지를 여실히 보여주었습니다.

국가배후 해킹조직의 해킹이 지속되고 있는 가운데, 금융보안원이 위협 인텔리전스 보고서 '다크프리즘 캠페인'(Campaign Dark Prism)을 공개했습니다. 보고서에서는 작년 1 월부터 올해 9 월까지 수집된 200 여개 LNK 악성코드를 심층 분석한 결과, 공격 초기 단계에서 정찰을 통해 선별된 목표를 정밀하게 노리며, 전술·기술·절차(TTP)가 빠르게 고도화되고 탐지 회피를 위한 구조 개선이 지속되고 있다고 설명하였습니다.

한국인터넷진흥원(KISA)은 국내 최초로 '운영기술(OT) 환경의 제로트러스트 적용 안내서'를 발간함으로써, 산업 현장의 특수성을 반영한 제도적 보안 대응 체계의 기틀을 마련하였습니다. 이는 현장 장비의 가용성과 실시간성을 요구하는 OT 환경의 특성을 고려한 국내 최초 OT 특화 제로트러스트 적용 방안을 제시한 안내서로, 국내 OT 보안에 대한 인식을 제고하고, 산업 현장의 운영 기술(OT) 보안 수준을 한 단계 높이는데 기여할 것으로 예상됩니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

12 월에는 Trojan.GenericKD.71882277 이 1 위를 차지하였습니다. 또한 불법 라이선스 우회 도구(크랙툴) 탐지명인 Misc.HackTool.AutoKMS, Application.Keygen-Crack-Patcher.17 와 가상화폐 채굴 악성코드인 Gen:Variant.Application.Miner.2, Misc.Riskware.BitCoinMiner 악성코드도 순위권에 이름을 올렸습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑3	Trojan.GenericKD.71882277	Trojan	49372
2	-	Exploit.CVE-2010-2568.Gen	Exploit	47827
3	NEW	Trojan.Generic.38743459	Trojan	45609
4	↑1	Gen:Variant.Tedy.675091	ETC	30433
5	↑6	JS:Trojan.Cryxos.14392	Trojan	27898
6	↑4	Gen:Variant.Application.Ulise.127573	ETC	20990
7	NEW	Gen:Variant.Tedy.827134	ETC	20839
8	↑1	Misc.HackTool.AutoKMS	ETC	12652
9	NEW	Application.Keygen-Crack-Patcher.17	ETC	9562
10	↑1	JS:Trojan.Cryxos.15301	Trojan	9236
11	↑4	Gen:Variant.Application.Miner.2	ETC	9184
12	NEW	Gen:Variant.Jaik.292533	ETC	8860
13	↓1	Spyware.Infostealer.Bladabindi	Spyware	7128
14	NEW	Gen:Variant.Graftor.406465	ETC	7038
15	NEW	Misc.Riskware.BitCoinMiner	ETC	7028

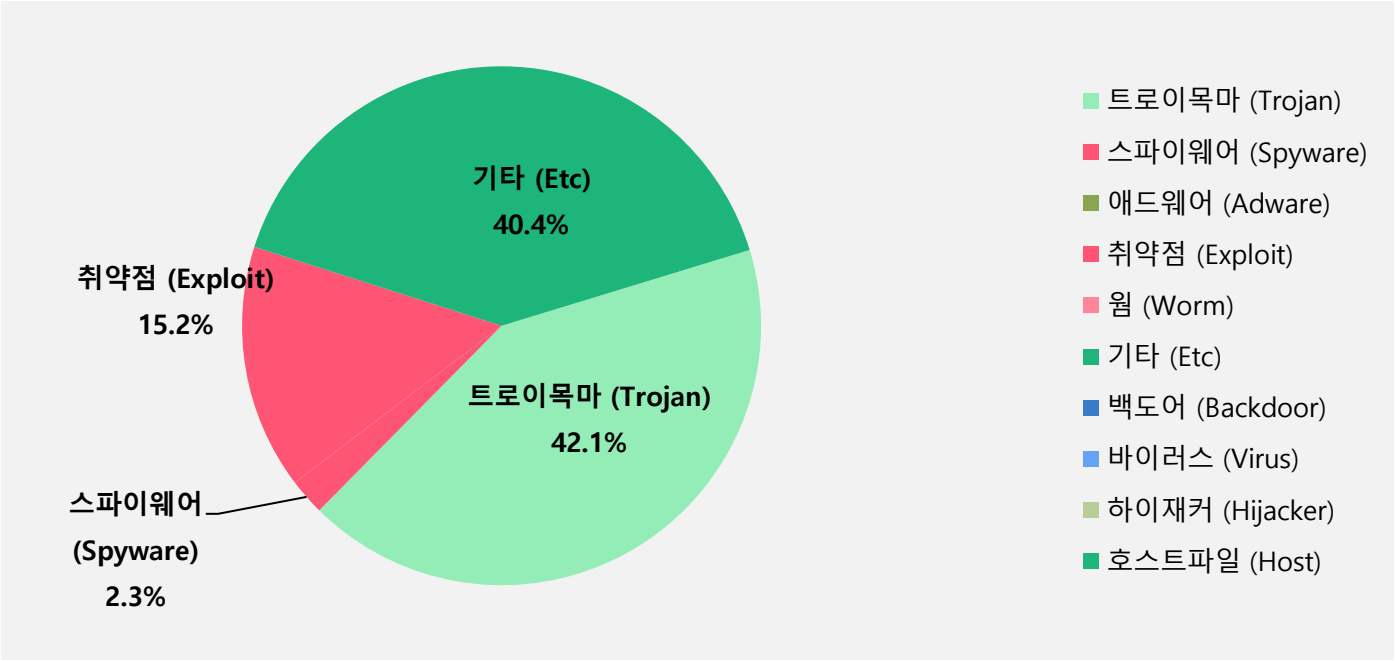
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 12 월 1 일 ~ 2025 년 12 월 31 일

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

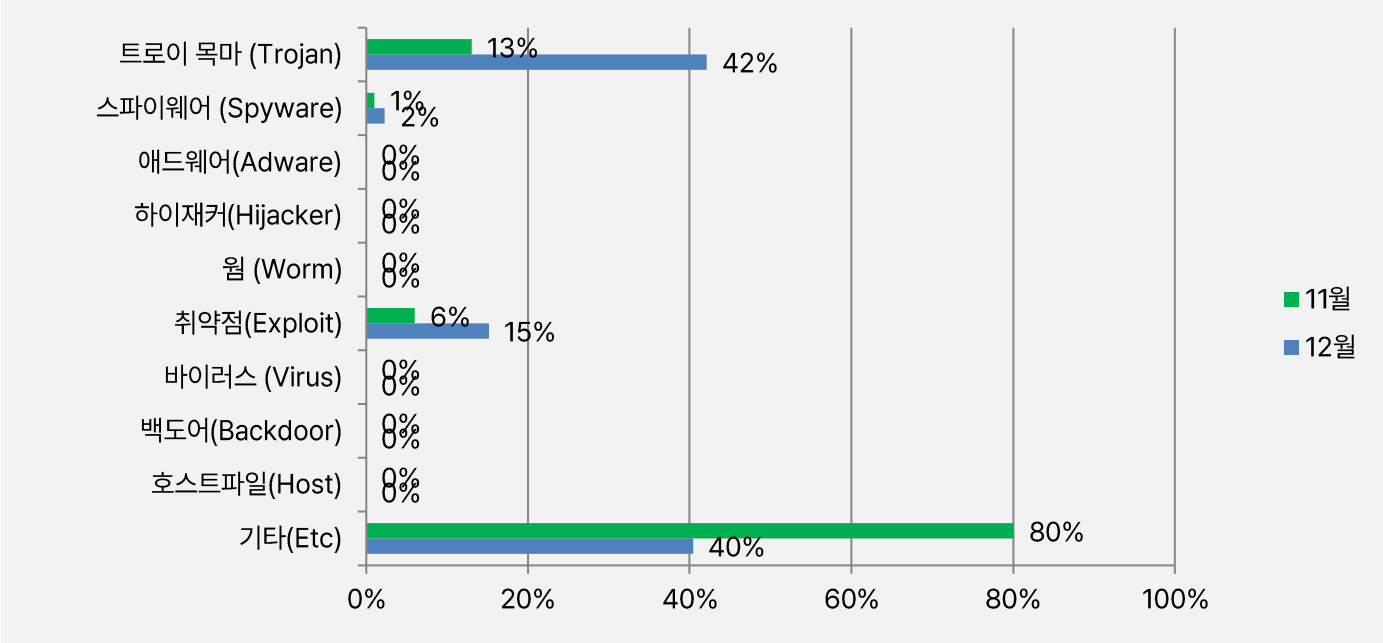
악성코드 유형별 감염 비율을 분석한 결과, 트로이목마(Trojan)가 40.4%로 1 위를 차지하였으며, 그 뒤를 이어 기타(Etc) 유형이 40.4%, 취약점(Exploit)이 15.2%, 스파이웨어(Spyware)가 2.3%를 차지하였습니다.



카테고리별 악성코드 비율 전월 비교

카테고리별 악성코드 비율의 경우 비교를 용이하게 하기 위하여 반올림된 수치를 사용합니다.

2025 년 12 월에는 지난 11 월과 비교하여 기타(ETC) 유형이 40% 큰 폭으로 감소하였습니다. 대신 트로이목마(Trojan) 유형이 29% 큰 폭으로 증가하였으며, 스파이웨어(Spyware) 유형은 1%, 취약점(Exploit)유형은 9% 증가하였습니다.

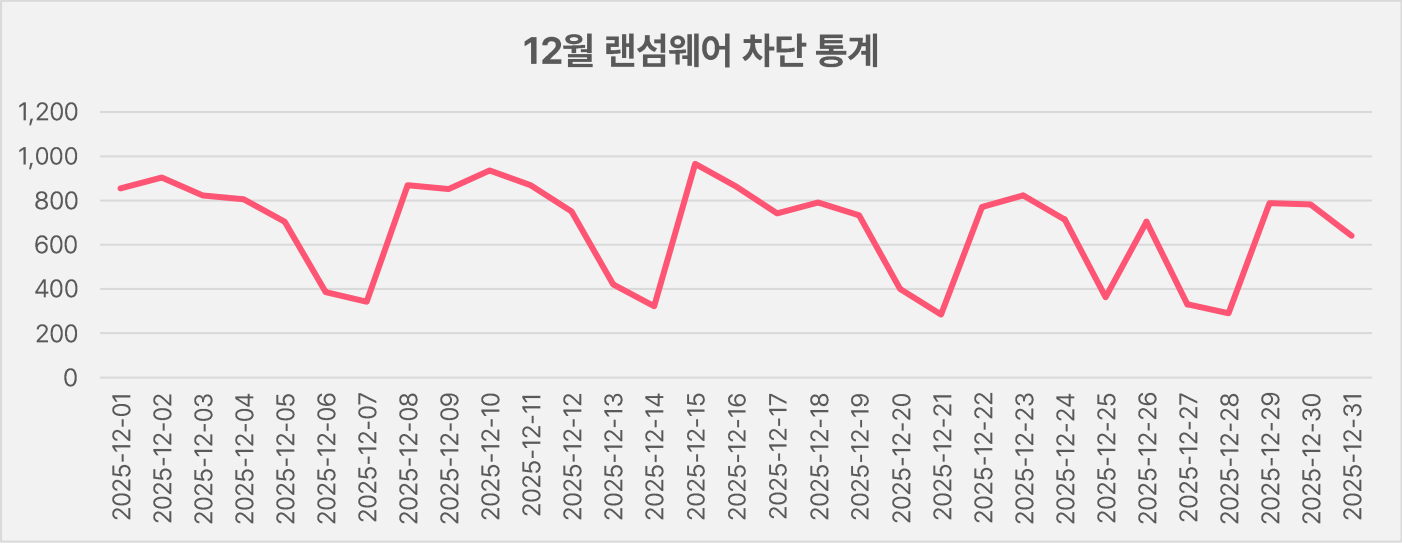


ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

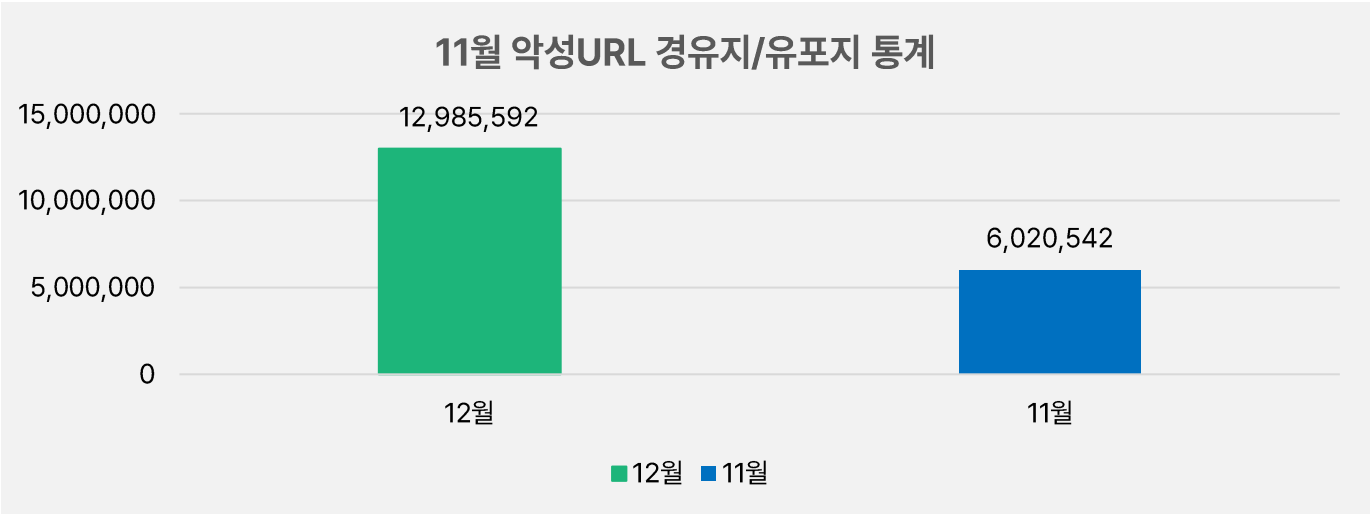
12 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 12 월 1 일부터 12 월 31 일까지 20,833 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 25 년 12 월 한 달간 총 12,985,592 건의 URL 이 확인되었습니다. 이 수치는 11 월 한 달간 총 6,020,542 건의 악성코드 유포지 URL 수에 비해 약 115.7% 가량 증가한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

2

최신 보안 동향

코인 선물 트레이딩 비법서를 위장한 LNK 파일 주의!

최근 코인 선물 트레이딩 비법서를 위장한 LNK 파일이 발견되어 사용자 여러분의 각별한 주의가 필요합니다.

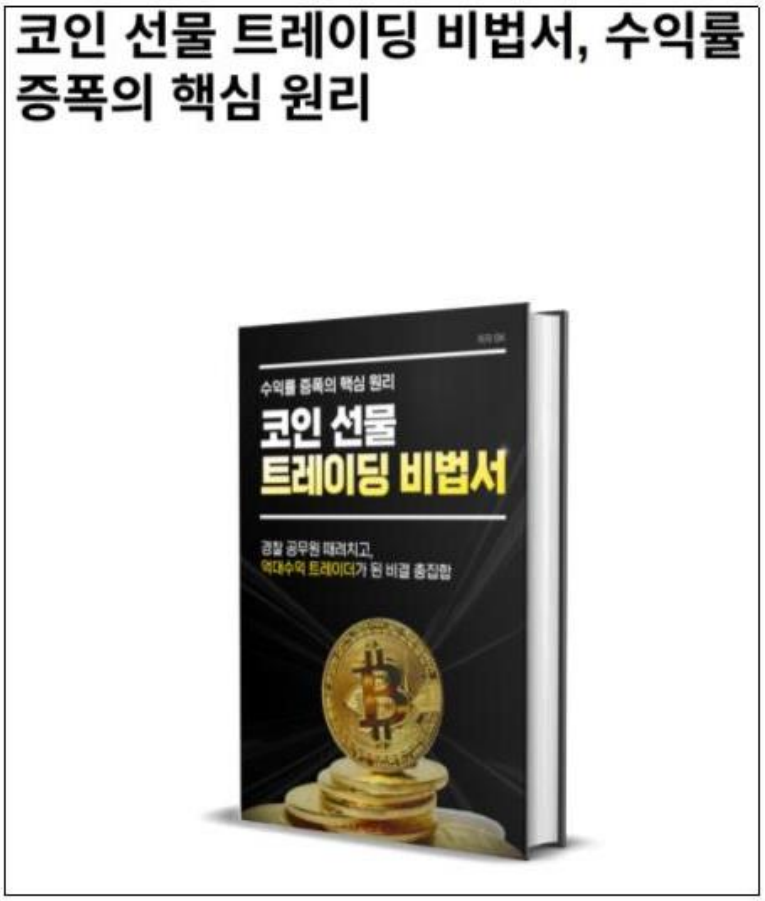
이 파일은 실전 트레이딩 핵심 비법서.lnk 파일명으로 유포되어 사람들의 실행을 유도합니다. LNK 파일 실행 시 내부에 포함되어 있던 파워쉘 명령어가 실행됩니다.



[그림 1] LNK 파일 속성

파워쉘 명령어는 실행 후 '실전 트레이딩 핵심 비법서.pdf' 파일명을 가진 디코이 파일을 실행하여 사용자가 정상 파일로 오인하도록 유도함과 동시에 백그라운드에서 '[랜덤].ps1' 파일을 실행합니다.

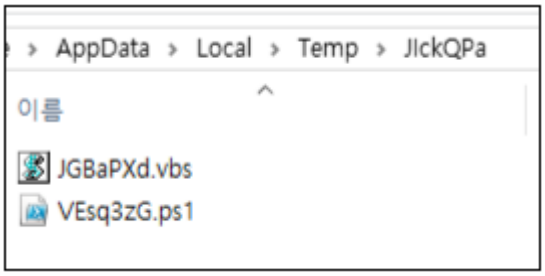
ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



[그림 2] 디코이 파일

'[랜덤].ps1' 파일은 난독화가 되어 있으며, 사용자의 실행중인 프로세스 체크 후, 공격자가 미리 지정해 놓은 악성코드 분석툴 관련 프로세스가 존재하면 스크립트를 실행하지 않고 종료합니다.

이후 'Selling CoinBoruhde Whistling NOprobnl{BD234234324-1243324ADVE}' 이름의 스케줄이 있는지 확인 후 없으면 실행이 안된 것으로 보고 base64 로 인코딩된 문자열을 디코딩하여 %temp%\[랜덤 7 글자]경로에 [랜덤 7 글자].ps1, [랜덤 7 글자].vbs 파일을 생성한 후 30 분마다 [랜덤 7 글자].vbs 파일을 실행하는 스케줄을 등록합니다. 이 vbs 파일은 추가로 생성된 [랜덤 7 글자].ps1 파일을 실행하는 역할을 합니다.

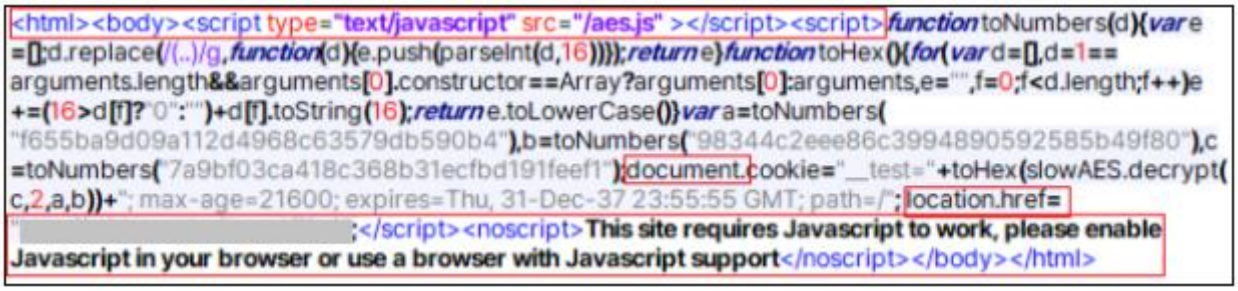


[그림 3] 생성되는 파일 목록

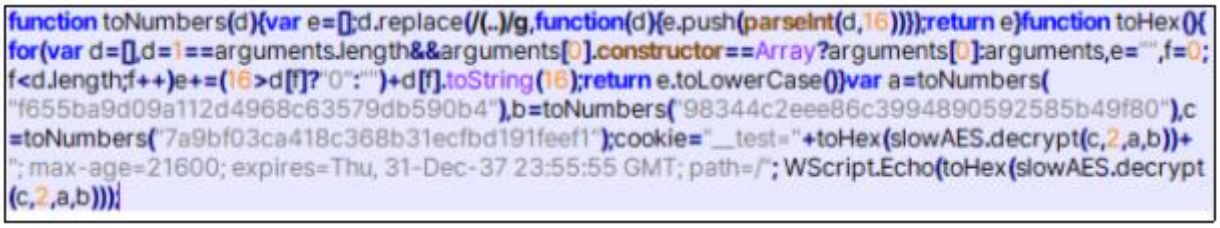
ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

스케줄 등록 후, WMI(Windows Management Instrumentation) 쿼리를 이용하여 사용자 시스템 정보를 수집하여 POST 형식으로 공격자 C2 에 전송합니다. 정보 전송 시 User Agent 및 쿠키값을 공격자가 설정한 값으로 설정하는데, 헤더의 쿠키값 생성 시 aes.js(slowAES 라이브러리)와 메인페이지에 접속하여 내용을 하나의 스크립트로 만든 후 실행결과를 쿠키값으로 사용합니다.

이때, 메인 페이지의 html 문자열을 replace 매서드를 통해 js 로 변환하는 독특한 방법을 사용합니다.



[그림 4] replace 전



[그림 5] replace 후

vbs 파일이 30 분마다 실행하는 [랜덤 7 글자].ps1 파일은 c2 에 접속하여 내용을 %temp% 경로에 [랜덤].ps1 에 저장한 다음 실행 후 삭제합니다. 이를 통해 공격자는 주기적으로 c2 에서 원하는 명령을 하달 할 수 있습니다.

현재 알약에서는 해당 악성파일에 대해 Trojan.Agent.LNK.Gen 로 탐지중에 있습니다.

사용자 여러분들께서는 파일 탐색기 내 파일 확장자명 보기 기능을 활성화 하시고, 파일을 실행하기 전 반드시 확장자를 확인하시기 바랍니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616
(주)이스트시큐리티

www.estsecurity.com