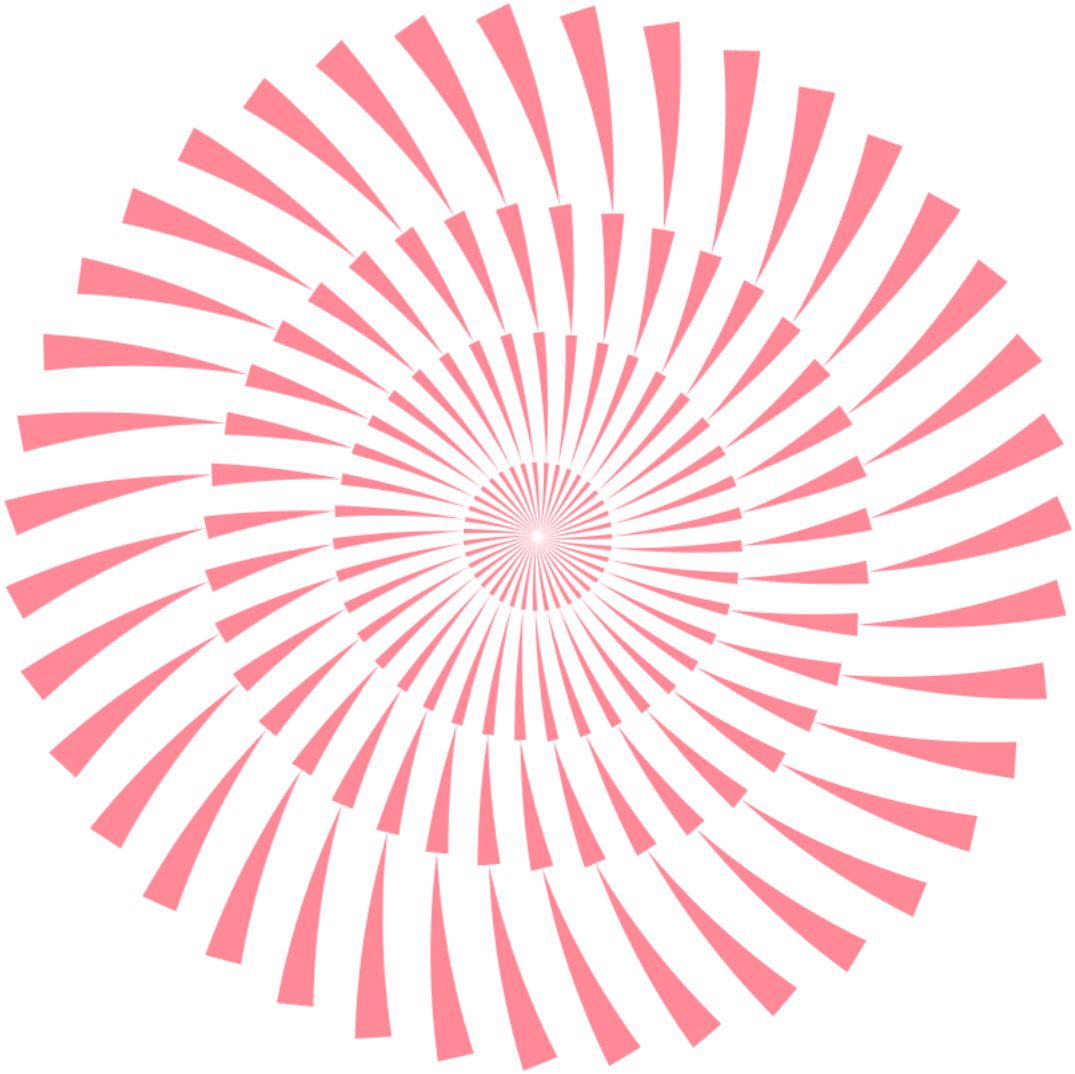
No.195 | 2025.12

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/경유지 URL 통계

2 최신 보안 동향 08-13

.hta 파일로 유포중인 KimJongRAT 주의!

1

악성코드 통계 및 분석

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

1. 악성코드 동향

11 월에는 국내 가상자산 거래소, 게임사, 대형 이커머스 기업에서 거의 동시에 대형 보안 사고가 발생하며 연쇄 침해 사례가 발생했습니다.

11 월 22 일, 넷마블 PC 게임 포털에서 약 611 만여 건의 개인정보가 유출되었습니다.
유출된 정보에는 일반 회원 정보뿐 아니라 PC 방 가맹점 데이터와 임직원 정보까지 포함된 것으로 확인되었습니다.
특히 이번에 유출된 정보 중에는 휴면계정 정보와 2015 년 이전 PC 방 가맹점 정보까지 포함되어 있어, 데이터 수명주기 관리가 장기간 제대로 이행되지 않았다는 점이 드러났습니다.

11 월 27 일에는 가상자산 거래소 업비트에서 해킹 사고가 발생했습니다.
핫월렛에 보관 중이던 자산 일부가 외부 지갑으로 대량 유출되었으며, 규모는 약 445 억 원 상당의 솔라나 계열 자산으로 파악되었습니다. 이번 사고는 운영 편의를 위해 유지되던 핫월렛 기반 구조와 키 관리 체계의 허점이 주요 원인으로 지적됩니다.
사고 직후 회사는 핫월렛 내 자산을 즉시 콜드월렛으로 전면 이관해 추가 비정상 출금을 차단했고, 고객 피해 자산은 회사 자산으로 전액 보전하겠다는 입장을 밝혔습니다.

11 월 30 일에는 이커머스 업체 쿠팡에서 대규모 개인정보 유출 사고가 발생했습니다.
쿠팡에서 근무했던 중국 국적의 전직 직원이 정보를 유출한 것으로 알려졌으며, 해당 직원은 이미 퇴사 후 한국을 떠난 상황으로 파악됩니다.
이번 사고로 약 3,370 만 건의 고객 정보가 유출되었고, 이름, 이메일, 배송지 주소, 전화번호 등 기본 개인정보뿐 아니라 공동현관 비밀번호까지 포함된 것으로 확인되어 2 차 피해 우려가 커지고 있습니다.

이번 보안사고들은 단순히 짧은 기간에 여러 사고가 우연히 발생한 것이 아니라, 서로 다른 산업 분야의 기업들이 오랜 기간 유지된 시스템·계정·키·권한의 방치, 상시 모니터링 체계 미흡, 침해 사고 인지·공지 지연, 불완전한 보안 거버넌스라는 공통된 구조적 취약점을 드러냈다는 데 있습니다. 최근에는 국가 기반 공격자나 전문화된 범죄 조직이 한국을 테스트베드로 활용하고 있다는 분석까지 제기되며, 기업 차원의 대응만으로는 한계가 있다는 지적도 늘고 있습니다. 또한 기업 내부자에 의한 정보 유출 가능성이 재차 확인되면서, 계정 관리와 퇴직자 권한 회수 등 내부 보안 정책의 중요성 역시 강조되고 있습니다.

대규모 개인정보 유출이 발생하면, 이를 악용한 정교한 피싱 및 스미싱 공격이 증가할 수 있습니다. 따라서 실제 사용 중인 서비스에서 온 문자나 이메일처럼 보이더라도, 열람 전 반드시 한 번 더 확인하는 것이 필요합니다. 또한 유출된 서비스와 동일한 계정 정보를 다른 플랫폼에서도 사용하고 있다면, 해당 플랫폼들의 비밀번호를 즉시 변경하고 2 단계 인증을 설정하여 크리덴셜 스터핑 등 연계 공격을 예방해야 하겠습니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

Gen:Variant.Symmi.49795 탐지명 악성코드가 전월과 동일한 1 위를 차지하였습니다. 2010 년에 발견된 취약점을 악용하는 Exploit.CVE-2010-2568.Gen 악성코드의 탐지순위가 전월대비 3 단계 상승했으며, 불법 라이선스 우회 도구(크랙툴) 탐지명인 Misc.HackTool.AutoKMS 도 여전히 순위권에 올라와 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.Symmi.49795	ETC	546472
2	↑3	Exploit.CVE-2010-2568.Gen	Exploit	55335
3	↓1	Trojan.GenericKD.71882277	Trojan	50142
4	NEW	Gen:Variant.Ulise.585667	ETC	44492
5	↑1	Gen:Variant.Tedy.675091	ETC	33532
6	NEW	Gen:Variant.Application.Barys.63612	ETC	31387
7	↑5	Trojan.Generic.38743459	Trojan	26074
8	NEW	Gen:Variant.Tedy.830187	ETC	17407
9	-	Misc.HackTool.AutoKMS	ETC	15489
10	NEW	Gen:Variant.Application.Ulise.127573	ETC	14361
11	NEW	JS:Trojan.Cryxos.14392	Trojan	14110
12	↑1	Spyware.Infostealer.Bladabindi	Spyware	11453
13	NEW	Trojan.Generic.39162720	Trojan	11328
14	NEW	Trojan.Generic.6257285	Trojan	9695
15	NEW	Gen:Variant.Application.Miner.2	ETC	9437

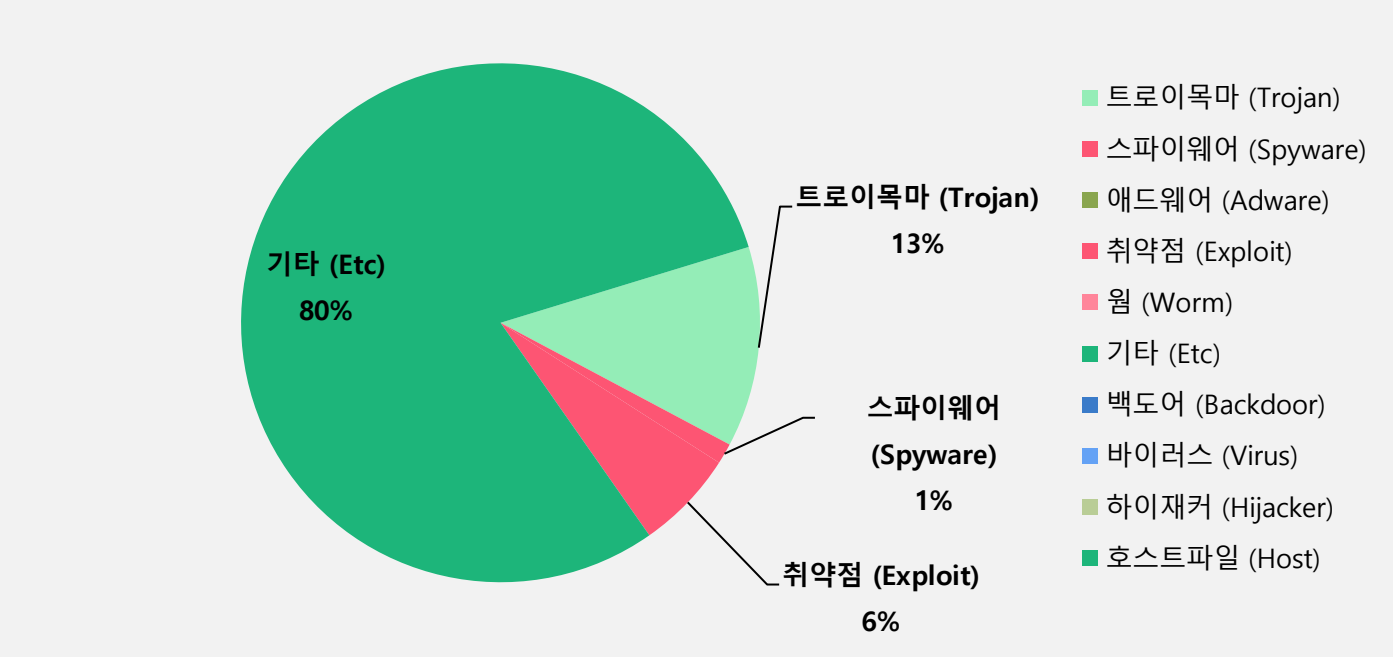
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 11 월 1 일 ~ 2025 년 11 월 30 일

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

악성코드 유형별 비율

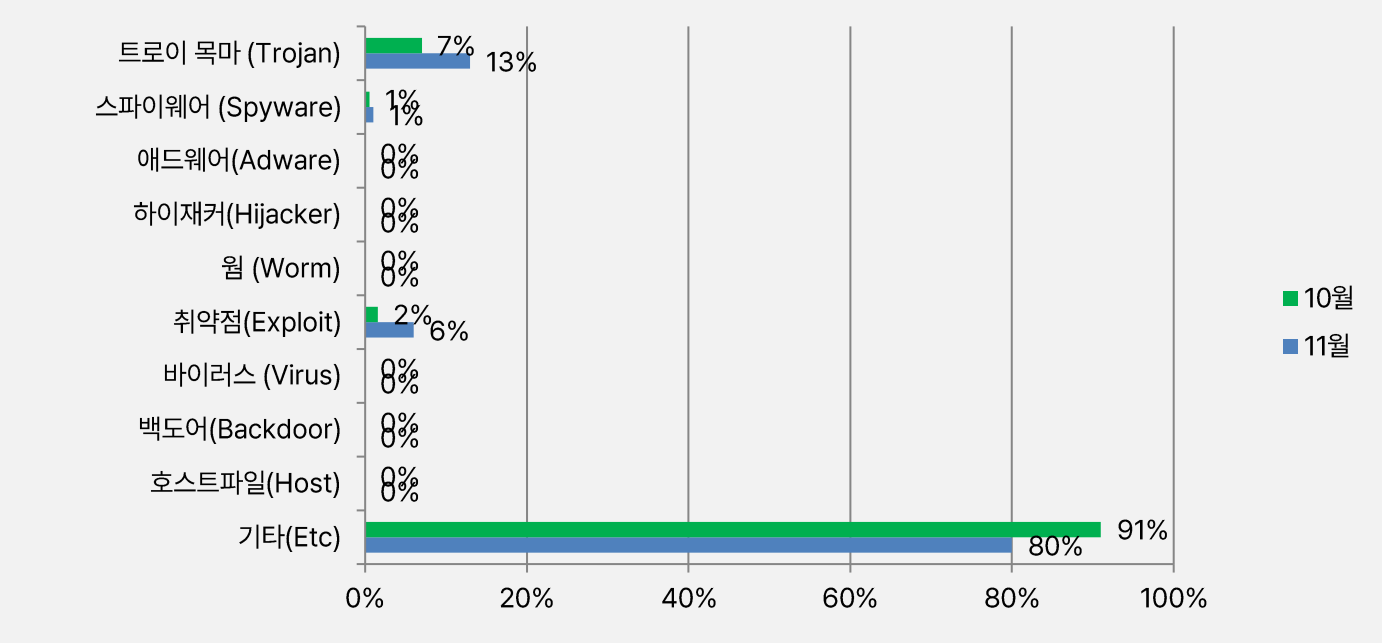
악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 80%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 13%, 취약점(Exploit)dl 6%, 스파이웨어가 1%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

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

2025 년 11 월에는 지난 10 월과 비교하여 트로이목마(Trojan) 유형이 6%, 취약점(Exploit) 유형이 4% 증가하였습니다. 기타(Etc)유형은 11% 감소하였습니다.

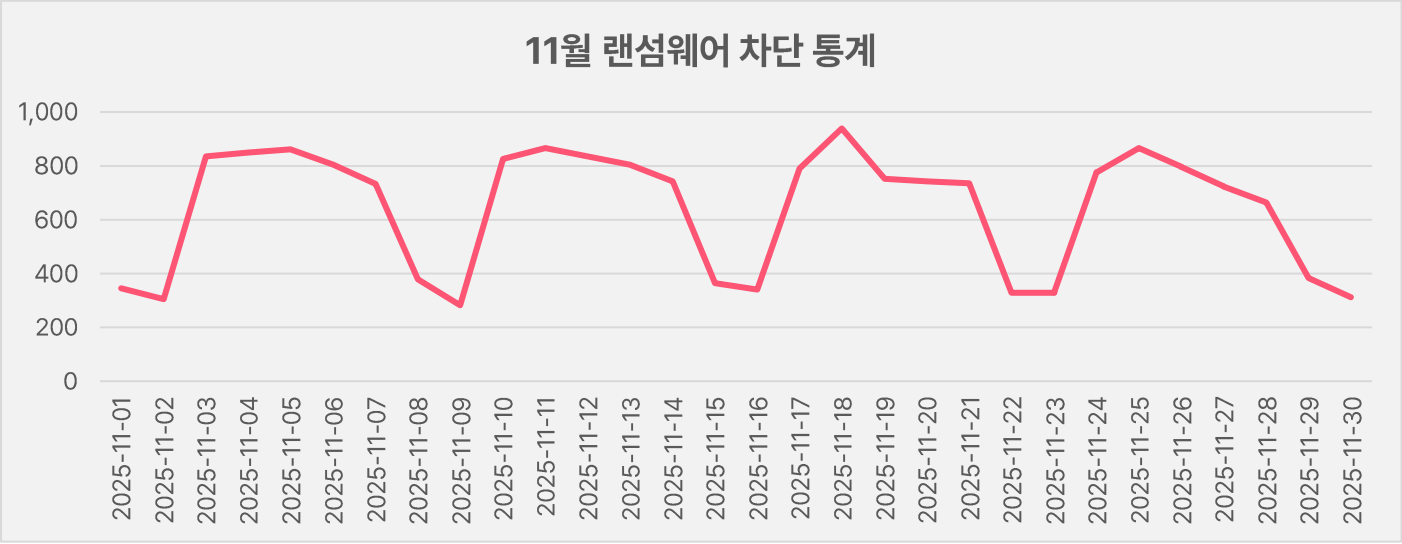


ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

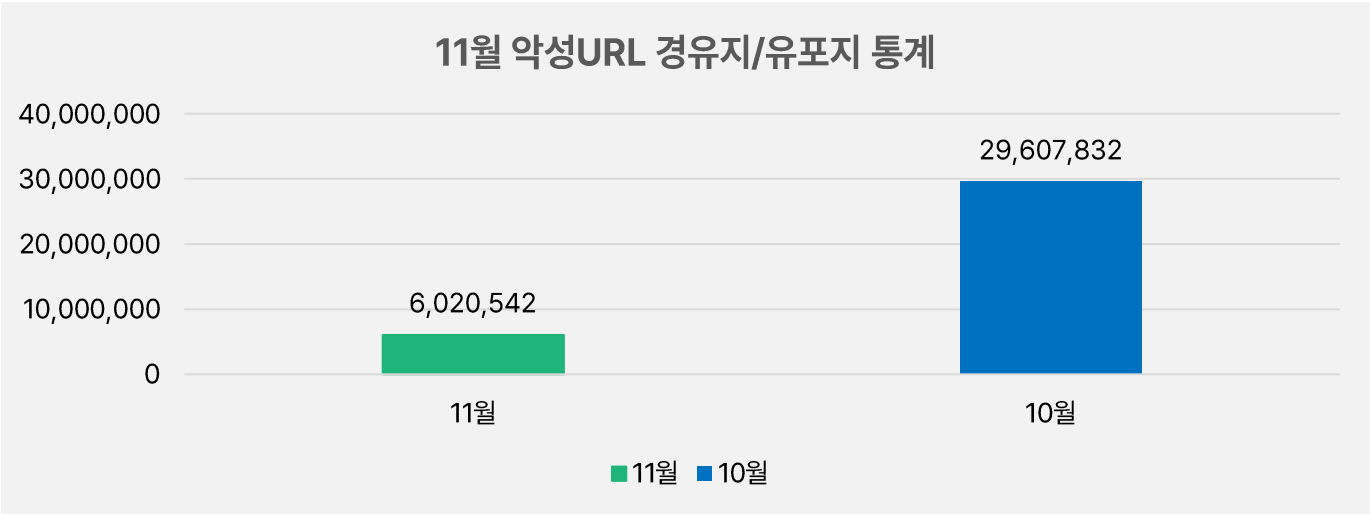
11 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 11 월 1 일부터 11 월 30 일까지 19,308 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 25 년 11 월 한 달간 총 6,020,542 건의 URL 이 확인되었습니다. 이 수치는 10 월 한 달간 총 29,607,832 건의 악성코드 경유지/유포지 URL 수에 비해 약 79.6% 가량 감소한 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

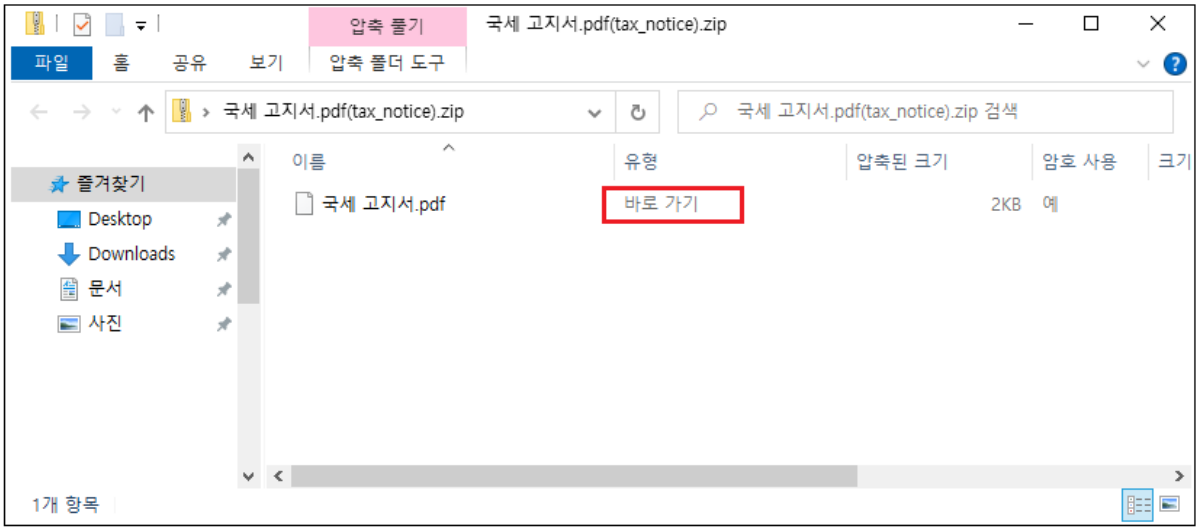
최신 보안 동향

.hta 파일로 유포중인 KimJongRAT 주의!

KimJongRAT 은 북한 배후로 추정되는 Kimsuky 그룹과 연관된 것으로 알려진 원격 액세스 트로이 목마(RAT) 로, 최근 .hta 파일을 통해 KimJongRAT 이 유포되고 있는 것을 확인하였습니다.

이번에 발견된 파일은 국세 고지서.pdf(tax_notice).zip 파일명으로 유포되었으며, 피싱 메일을 통해 최초 유포된 것으로 추정되고 있습니다.

국세 고지서.pdf(tax_notice).zip 내에는 국세고지서.pdf 파일을 위장한 lnk 파일이 포함되어 있습니다.



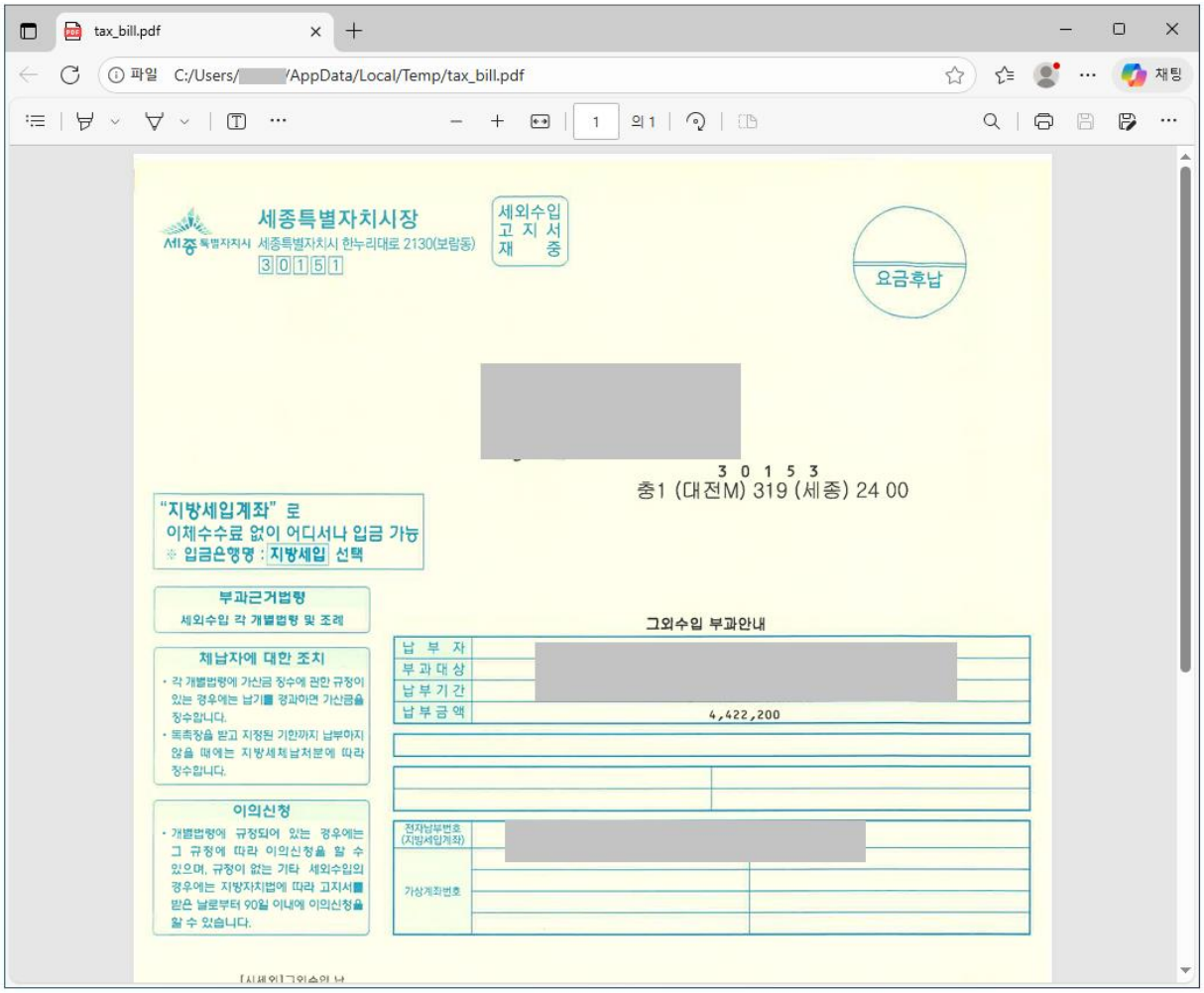
[그림 1] 국세 고지서.pdf(tax_notice).zip 파일 내 lnk 파일

사용자가 해당 lnk 파일을 실행하면, 내부에 Base64 로 인코딩된 URL 값을 복호화한 뒤 mshta 를 사용해 해당 링크에 접속하고, 이후 추가 페이로드를 다운로드합니다.

최종 리디렉션 된 URL 에서는 tax.hta 파일을 다운로드 받은 후 실행합니다.

.hta 파일은 VBScript 구현된 로더로, 실행 후에는 디코이 파일과 함께 추가 악성파일을 다운받습니다. 이 과정에서 Google Drive URL 을 사용하여 보안프로그램의 탐지 우회를 시도합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.



[그림 2] 디코이 파일

이번 공격은 Windows Defender의 상태를 체크하고, Windows Defender에 따라 각기 다른 페이로드를 내려주는 특징이 있습니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

```
ss = ss & chr(-59727+CLng("&He9b3"))
Set exec = oShell.Exec(ss)

output = exec.StdOut.ReadAll
If InStr(output, "STOPPED") > 0 Then
   ss = chr(CLng("&H9b23")-39616)
   ss = ss & chr(CLng("&H17d63")-97526)
   ss = ss & chr(-7553+CLng("&H1de5"))
   ss = ss & chr(747424/CLng("&H5b3d"))
   ss = ss & chr(-23614+CLng("&H5c6d"))
   ss = ss & chr(CLng("&H15434")-86993)
   ss = ss & chr(1703136/CLng("&Hcfe7"))
   ss = ss & chr(-56071+CLng("&Hdb6a"))
   ss = ss & chr(CLng("&H1355f")-79099)
   ss = ss & chr(CLng("&Hacff")-44255)
   ss = ss & chr(2099349/CLng("&Hae7b"))
   ss = ss & chr(CLng("&H44ea")-17542)
   ss = ss & chr(-73803+CLng("&H1206b"))
```

[그림 3] 윈도우 디펜더 실행여부에 따라 분기하는 코드

사용자 PC 의 Windows Defender 가 비활성화 상태일 경우,v3.log 파일을 내려받습니다. 이 파일은 최종적으로 net64.log 파일을 내려받아 실행하며, 해당 파일은 시스템 정보 및 브라우저 저장 데이터, 브라우저 암호화 키, 암호화폐 지갑 정보, 텔레그램(특정 계정), 디스코드, NPKI/GPKI 인증서등 다양한 정보를 수집합니다. 뿐만 아니라, run 레지스트리에 등록하여 지속성을 확보하여 주기적으로 사용자 정보를 수집하여 전송합니다.

사용자 PC 의 Windows Defender 가 활성화 상태일 경우, pipe.log 파일을 내려받습니다. 이 파일은 최종적으로 1.log 파일을 내려받아 실행하며, net64.log 파일과 동일하게 시스템 정보 및 브라우저 저장 데이터, 브라우저 암호화 키, 암호화폐 지갑 정보, 텔레그램(특정 계정), 디스코드, NPKI/GPKI 인증서등 다양한 정보를 수집합니다. 뿐만 아니라, run 레지스트리에 등록하여 지속성을 확보하여 주기적으로 사용자 정보를 수집하여 전송합니다.

ESTsecurity Copyright©2025 ESTsecurity Corp. All rights reserved.

이름	확장 ID	이름	확장 ID
meta	nkbihfbeogaeaoehlefnkodbefgpgknn	bybit	pdliaogehgdbhbnmkklieghmmjkpigpa
trust	egjidjbpglichdcondbcbdnbeeppgdph	rabby	acmacodkjbdgmoleebolmdjonilkdbch
tron	ibnejdfjmmkpcnlpebklmnkoeoihofec	backpa	aflkmfhebedbjioipglgcbcmnbpgliof
exod	aholpfdialjgjfhomihkjbmgjidlcdno	ronin	fnjhmkhhmkbjkkabndcnnogagogbneec
binan	fhbohimaelbohpjbbldcngcnapndodjp	unisat	ppbibelpcjmhbdihakflkdcoccbgbkpo
okx	mcohilncbfahbmgdjkbpemcciiolgcge	compas	anokgmphncpekkhclmingpimjmcooifb
phant	bfnaelmomeimhlpmgjnjophhpkkoljpa	argent	dlcobpjiigpikoobohmabehhmhfoodbb
emeta	ejbalbakoplchlghecdalmeeeajnimhm	martia	efbglgofoippbgcjepnhiblaibcnclgk
eokx	pbpjkcldjiffchgbbndmhojiacbgflha	petra	ejjladinnckdgjemekebdpeokbikhfci
rainb	opfgelmcmbiajamepnmloijbpoleiama	leacos	fcfcfllfndlomdhbehjjcoimbgofdncg
pontem	phkbamefinggmakgklpkljjmgibohnba	braav	jnlgamecbpmbajjfhmmmlhejkemejdma
keplr	dmkamcknogkgcdfhhbddcghachkejeap	talis	fijngjgcjhjmmpcmkeiomlglpeiijkld
ton	nphplpgoakhhjchkkhmiggakijnkhfnd	magic	mkpegjkblkkefacfnmkajcjmabijhclg
iwal	jbppfhkifinbpinekbahmdomhlaidhfm	coin98	aeachknmefphepccionboohckonoeemg
stati	aiifbnbfobpmeekipheeijimdpnlpgpp	xverse	idnnbdplmphpflfnlkomgpfbpcgelopg
solf	bhhhlbepdkbapadjdnnojkbgioiodbic	unisw	nnpmfplkfogfpmcngplhnbdnnilmcdcg
kaia	jblndlipeogpafnldhgmapagcccfchpi	sui	opcgpfmipidbgpenhmajoajpbobppdil
cosmos	fpkhgmpbidmiogeglndfbkegfdlnajnf	cobas	hnfanknocfeofbddgcijnmhnfnkdnaad
subwal	onhogfjeacnfoofkfgppdlbmlmnplgbn	enkr	kkpllkodjeloidieedojogacfhpaihoh

[그림 4] 악성코드가 탈취하는 암호화폐 지갑 목록

국내에 특화된 정보들을 탈취하는것으로 보아, 국내 타깃으로 정밀하게 제작된 악성코드로 볼 수 있습니다.

최근 HTA 파일을 활용한 공격 시도가 지속되고 있습니다.

HTA 파일은 정상 윈도우 프로세스인 mshta.exe 를 사용하여 인터넷에서 원격의 hta 를 직접 실행할 수 있는 특징을 갖고 있어 공격자들이 자주 사용하는 공격방식 중 하나입니다.

Microsoft 가 보안을 강화하고 있지만, 레거시 시스템이나 보안이 약하게 설정된 환경에서는 여전히 매우 효과적인 공격수단인 만큼, 사용자 여러분들께서는 사용하시는 윈도우 및 sw 를 항상 최신버전으로 유지하시기 바라며, 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