No.186 | 2025.3

ESRC 보안동향보고서

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

ESTsecurity

ESRC 보안동향보고서

CONTENTS

1

악성코드 통계 및 분석

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

1. 악성코드 동향

2 월달에는 대규모 가상화폐 해킹 사건이 발생했습니다.

가상화폐 거래소 바이비트에서 24 억 6000 만달러 규모의 가상화폐가 해킹을 통해 탈취가 되었습니다. 이는 한화로 환산하면 약 2 조 1000 억원 규모로 역사상 피해액이 가장 큰 탈취 사건이 되었습니다.

이번 해킹에는 고소득 일자리 제안 등을 위장하여 악성코드가 포함된 가상화폐 애플리케이션 등을 다운로드하도록 유도하는 '트레이더트레이터'라는 공격 기법이 사용된 것으로 확인되었습니다.

조사 결과, 이번 공격은 북한의 해킹조직인 라자루스의 소행인 것으로 확인되었습니다.

국내에서도 북한 해커의 위협이 지속되었습니다.

서울시 시민메일 계정으로 서울시 공무원 명의로 '대북전달 살포'회의와 관련하여 비대면 회의 가능 여부를 묻는 이메일이 불특정 다수에게 발송되었는데 확인결과 계정이 도용된 것으로 확인되었습니다.

해당 메일에는 악성코드가 포함되어 있는 파일이 첨부되어 있었으며, 사용된 IP 주소 분석 결과 북한의 해커 조직인 '김수키'가 사용했었던 이력이 존재했습니다.

서울시는 공식 업무 시는 공식 업무 메일(@seoul.go.kr)이 아닌 시민메일(@citizen.seoul.kr)로 발송된 이메일은 절대 열람하지 말고 즉시 삭제할 것을 당부하였습니다.

대규모 개인정보 유출사건도 발생하였습니다.

GS 리테일에서 개인정보가 대량으로 유출되었습니다.

해킹 공격으로 GS25 편의점 홈페이지에서 9 만여명의 개인정보가 유출되었으며, 홈쇼핑 GS 샵 웹사이트에서도 158 만건의 개인정보가 유출되었습니다.

이번에 유출된 개인정보에는 이름, 성명, 생년월일, 주소, 연락처 등 뿐만 아니라 개인통관 고유분호, 기혼 여부 등도 포함되어 있는 것으로 확인되었습니다.

뿐만 아니라 교육기업 대교에서도 학부모, 교사, 학생 등 회원들의 개인정보가 유출되었으며 규모는 아직 정확히 확인되지 않았다고 밝혔습니다.

이렇게 개인정보가 유출되었을 경우, 유출된 개인정보를 기반으로 2 차, 3 차 피해가 발생할 수 있는 만큼 사용자여러분들께서는 자신의 개인정보가 유출되었는지 확인하고, 만약 유출되었을 경우 동일한 계정정보를 사용하시는 사이트들의 비밀번호를 변경하시어 추가 피해를 최소화 해야 겠습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2025 년 1 월에는 Gen:Variant.Graftor.927510, Trojan.GenericKD.71231591, Worm.IM-VB.as, Win32.Grenam.Dam.G 악성코드가 새롭게 Top 15 에 진입하였습니다.

루트킷 악성코드 탐지명인 Gen:Variant.TDss.49 이 지난 10 월 이후로 여전히 최상위권을 유지하고 있으며, Microsoft Windows 및 Office 제품의 라이선스 인증을 우회하는 데 사용되는 KMS 기반 불법 인증 도구에 대한 탐지명 Misc.HackTool.AutoKMS, Application.Hacktool.BBJ, Misc.HackTool.KMSActivator 도 Top15 에 포함되었습니다.

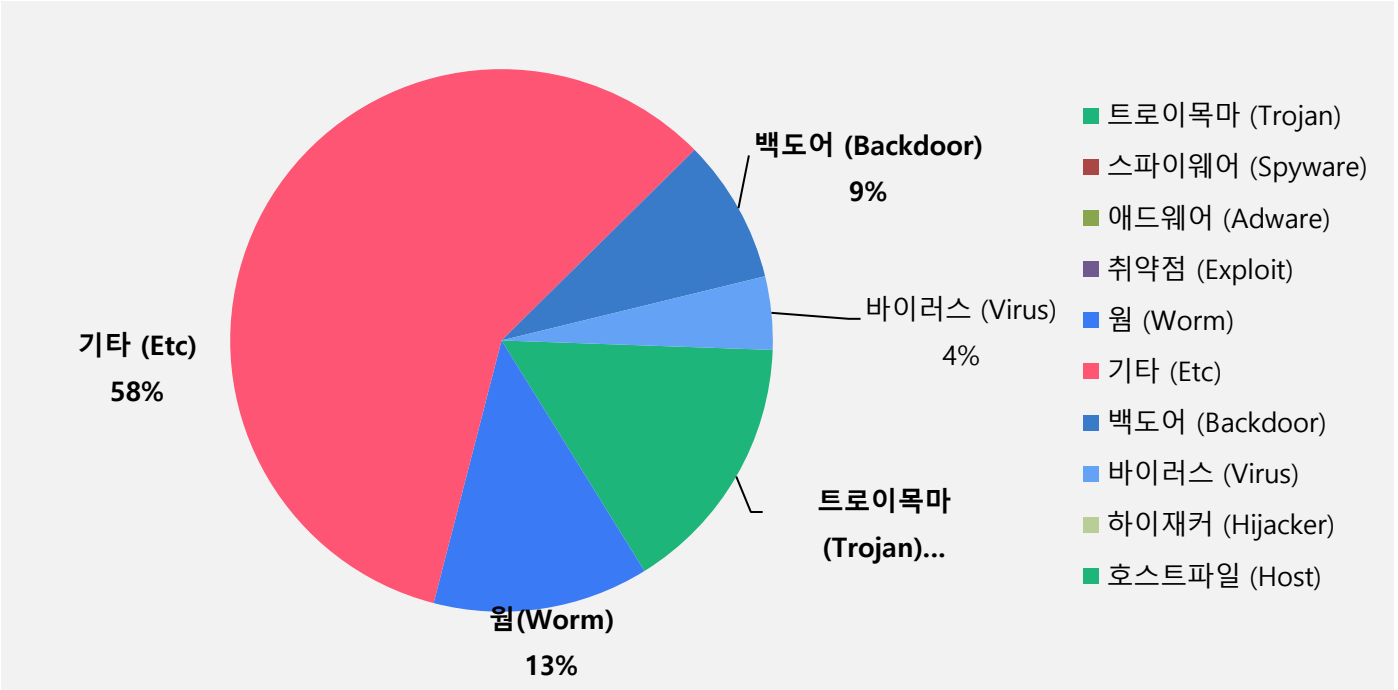
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	↑1	Gen:Variant.Lazy.266772	ETC	79,224
2	↑1	Gen:Variant.Tedy.675091	ETC	28,714
3	↑1	Misc.HackTool.AutoKMS	ETC	28,322
4	↑3	Backdoor.Generic.792814	Backdoor	27,354
5	-	Trojan.DDoS.Nitol.gen	Trojan	22,992
6	NEW	Worm.Autorun.TUD	Worm	17,166
7	↑3	Application.Hacktool.BBJ	ETC	16,023
8	NEW	Trojan.Generic.36498051	Trojan	13,915
9	NEW	Win32.Neshta.A	Virus	13,872
10	NEW	Worm.ACAD.Bursted	Worm	13,530
11	↓2	Trojan.Acad.Bursted.AK	Trojan	12,766
12	↓6	Gen:Variant.Graftor.927510	ETC	12,277
13	↓1	Gen:Variant.Lazy.20522	ETC	11,469
14	↓13	Gen:Variant.TDss.49	ETC	10,343
15	↓4	Worm.IM-VB.as	Worm	10,232

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 2 월 1 일 ~ 2025 년 2 월 28 일

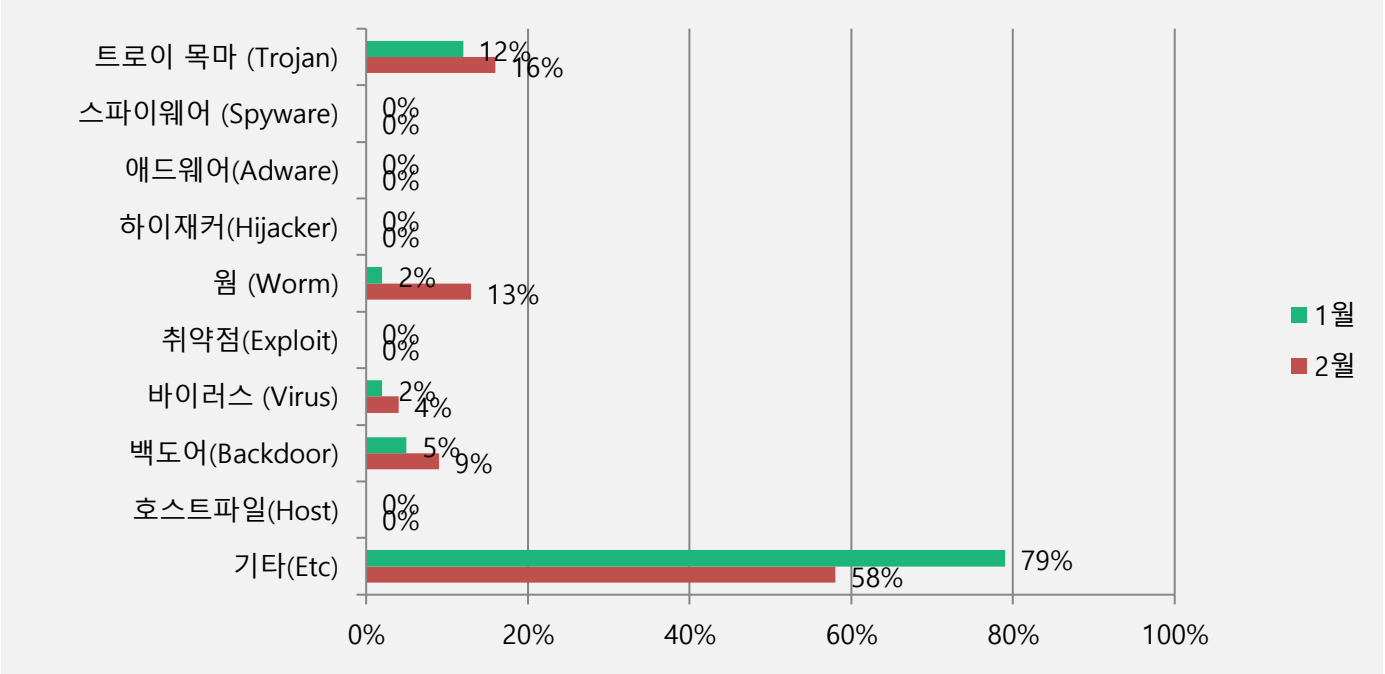
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 58%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 16%, 웜(Worm) 유형이 13%, 백도어(Backdoor) 유형이 9%, 바이러스(Virus) 유형이 2%로 확인되었습니다. 2025 년 1 월과 비교하여 전체 감염 건수는 20.9% 감소하였습니다.



카테고리별 악성코드 비율 전월 비교

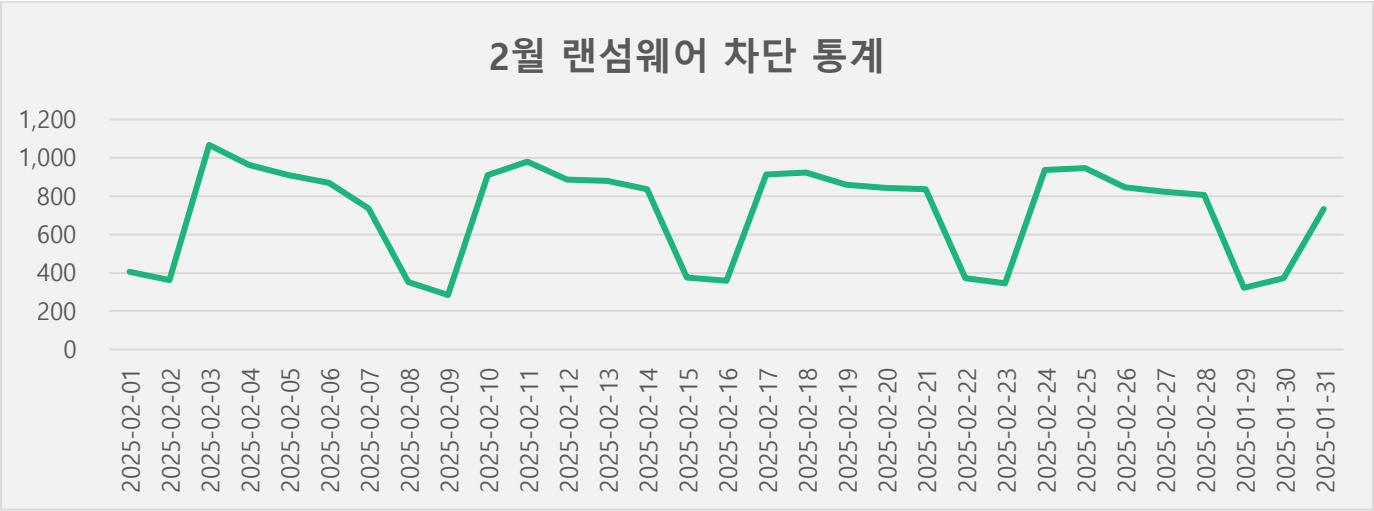
2025 년 2 월에는 1 월과 비교하여 트로이목마(Trojan) 유형이 4%, 바이러스(Virus) 유형이 2%, 웜(Worm)유형이 11%, 백도어(Back door) 유형이 4% 증가하였으며, 기타(ETC)유형은 21% 감소하였습니다.



3. 랜섬웨어 차단 통계

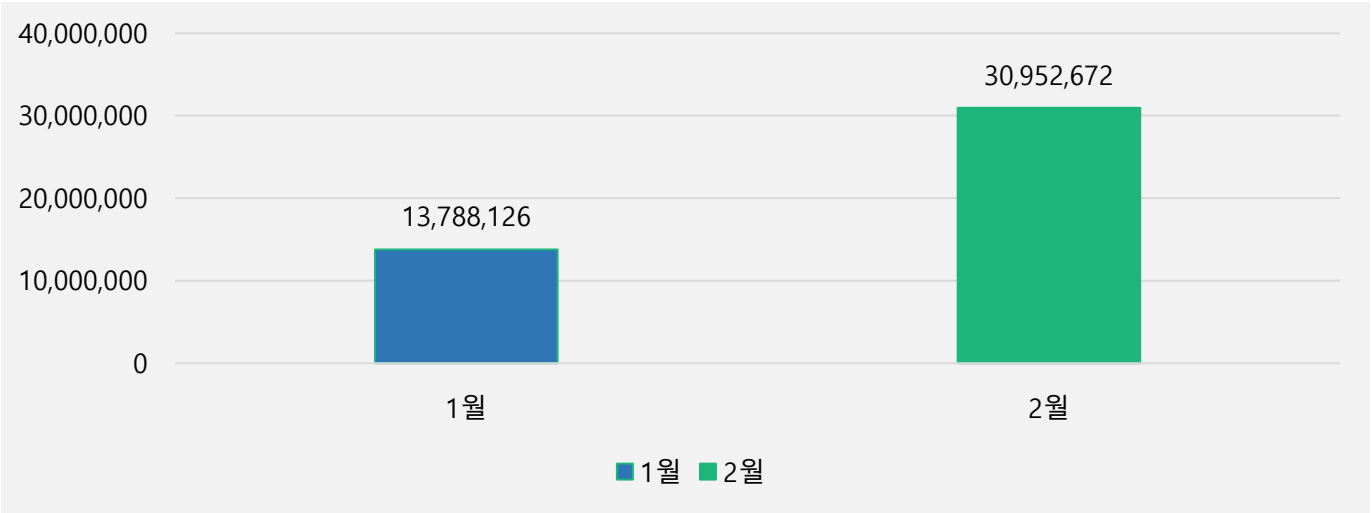
2 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 2 월 1 일부터 2 월 28 일까지 총 19,480 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 URL 에 대한 통계로, 25 년 2 월 한 달간 총 30,952,672 건의 URL 이 확인되었습니다. 이 수치는 25 년 1 월 한 달간 확인되었던 13,788,126 건의 악성코드 경유지/유포지 URL 수에 비해 약 124.48% 가량 증가한 수치입니다. 악성코드 URL 의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



2

최신 보안 동향

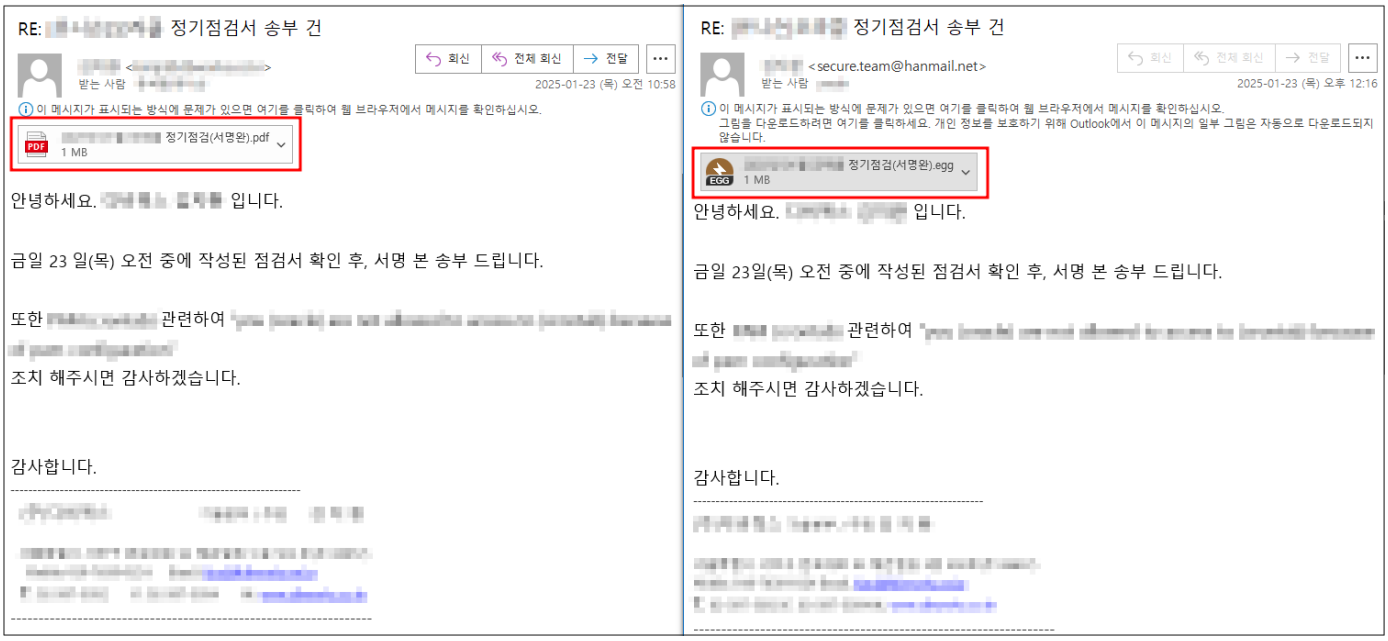
北 해킹 조직, 거래처 업무 메일로 위장한 스피어 피싱 공격 주의!

최근 거래처 업무메일을 위장한 스피어 피싱 공격이 발견되어 기업 사용자분들의 각별한 주의가 필요합니다.

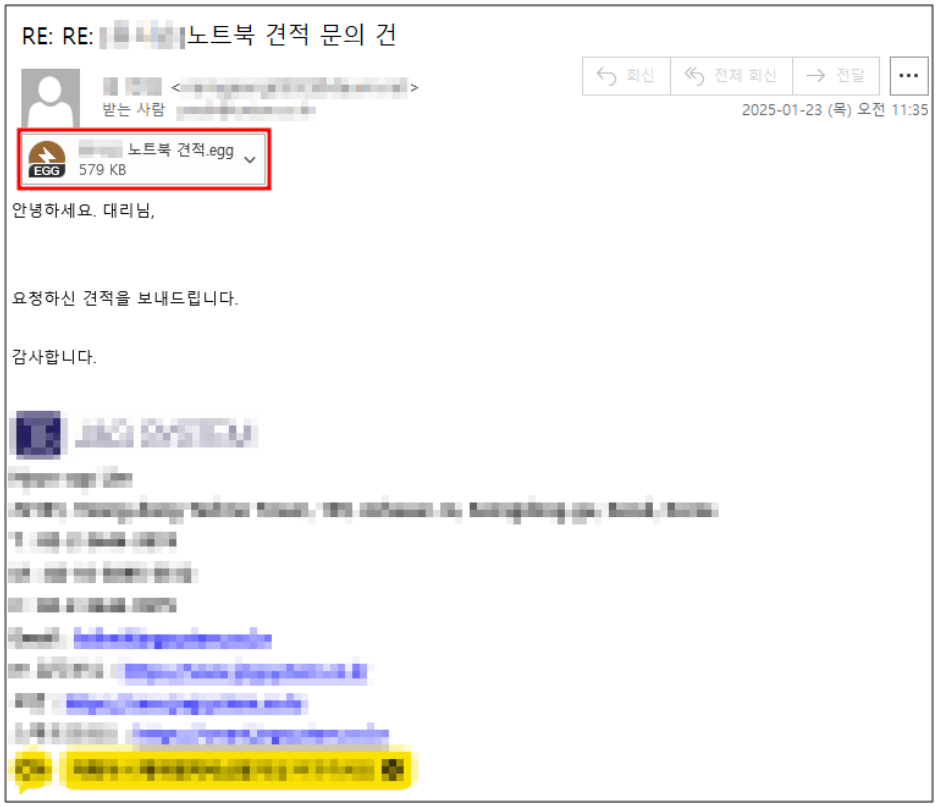
이번 공격은 이메일 수신자가 거래처와 업무상 메일을 주고 받는 과정 중에 공격자가 회신메일을 보냄으로써 사용자가 의심하지 못하도록 교묘하게 속이는 수법을 사용했습니다. 이를 위해 공격자는 사전에 메일 수신자의 계정을 탈취한 뒤 이메일 수신내역을 확인하는 작업을 진행했을 것으로 유추됩니다.

악성 메일은 '정기점검서 송부 건' 과 '노트북 견적 문의' 에 대한 회신메일에 도용된 계정을 사용하여 발신자명 조작 후 동일한 수신자에게 발송되었습니다.

첫 번째 메일의 경우 먼저 발송된 정상 회신메일과 동일한 내용으로 첨부파일만 교체하여 다시 발송한 것으로 확인되었습니다.

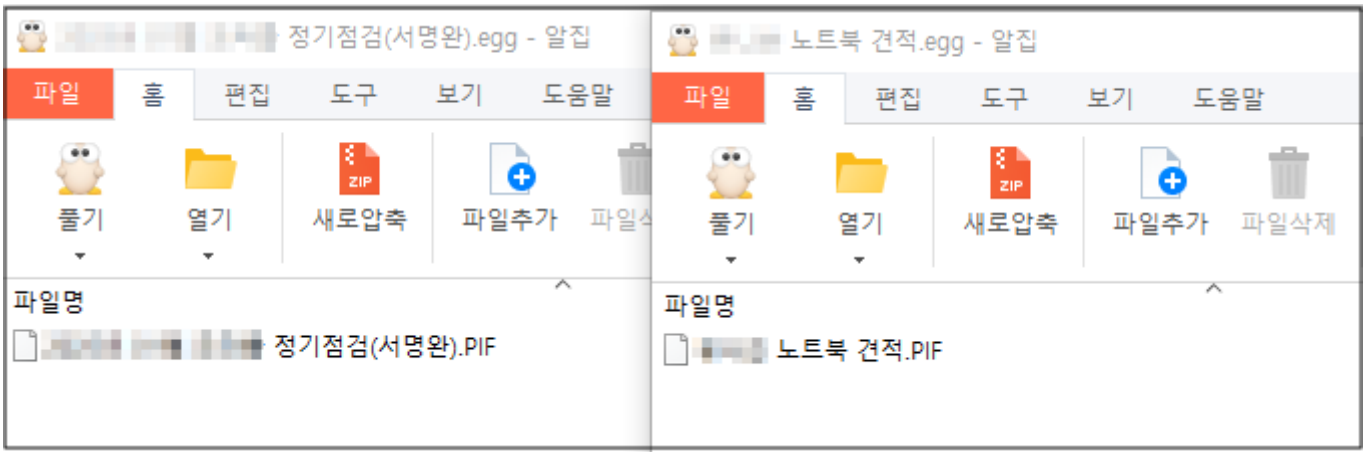


[그림 1] 정상 회신 메일 (좌) / 악성 회신 메일 (우)



[그림 2] 견적 문의에 대한 회신 메일 (악성)

위의 두 가지 악성메일에는 동일하게 내부에 악성 PIF 파일이 있는 EGG 포맷의 압축파일이 첨부되어 있습니다.



[그림 3] 첨부된 압축파일

PIF(Program Information File) 파일은 MS-DOS 프로그램 실행을 위한 정보를 담은 파일이며, EXE 확장자와 같은 실행 가능한 파일입니다. 현재는 거의 사용되지 않는 파일이나 탐지 회피를 위해 공격에 사용한 것으로 판단됩니다.

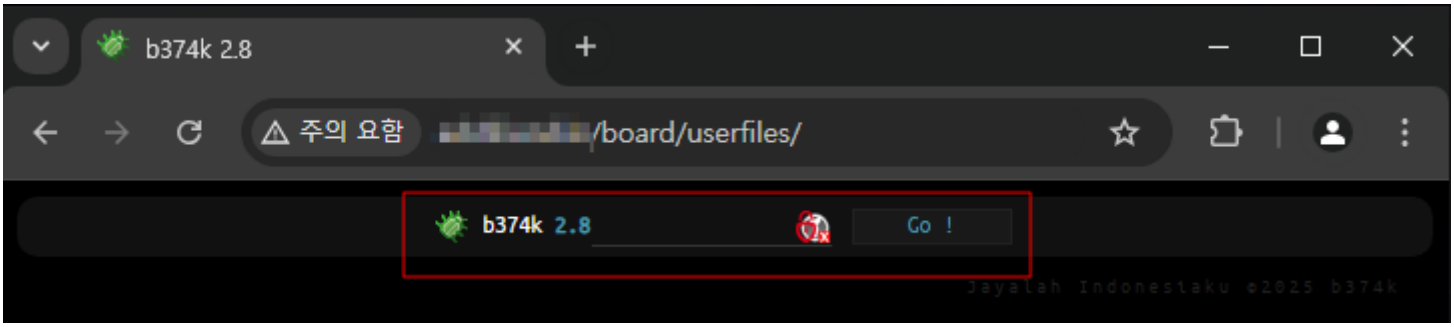
사용자가 첨부파일의 압축을 해제 한 후 내부의 PIF 파일을 실행하면 각각 정기점검서와 노트북 견적서에 해당하는 정상 PDF 파일을 띄워 사용자의 의심을 피하고, 백그라운드에서는 IconCashe.tmp.pif 파일을 생성 및 실행합니다.

실행된 IconCache.tmp.pif 파일은 백도어 악성코드인 PebbleDash 악성코드로 확인되었으며, 공격자가 지정해둔 C2 로 접속하여 공격자의 파일 다운로드/업로드, 실행 등의 명령을 수행하게 됩니다. C2 로 사용된 서버는 해킹을 통해 웹쉘을 삽입하여 사용한 것으로 추정됩니다.

ESRC 에서는 이번 공격에서 다음과 같은 두 가지 특징을 발견했습니다.

첫 번째, 공격에 사용된 PebbleDash 악성코드는 과거 라자루스(Lazarus)라는 조직에서 사용했었으나 최근에는 김수키(Kimsuky)그룹의 공격에서 자주 발견되고 있는 것으로 알려져 있습니다.

두 번째, IconCache.tmp.pif 파일을 통해 접속된 C2 에서 웹쉘이 발견되었는데, 해당 웹쉘이 과거 김수키(Kimsuky)그룹이 사용했던 웹쉘과 동일한 것으로 확인되었습니다.



[그림 4] C2 에서 확인된 웹쉘

해당 웹쉘이 사용된 사례는 지난 블로그 포스팅을 통해서 확인할 수 있습니다.

[스페셜 리포트] APT 캠페인 'Konni' & 'Thallium(Kimsuky)' 조직의 공통점 발견

이러한 정보들을 바탕으로 이번 공격이 북한 배후의 김수키(Kimsuky)그룹과 연관된 공격으로 추정하고 있으며, 추가적인 연관성 분석을 진행하고 있습니다.

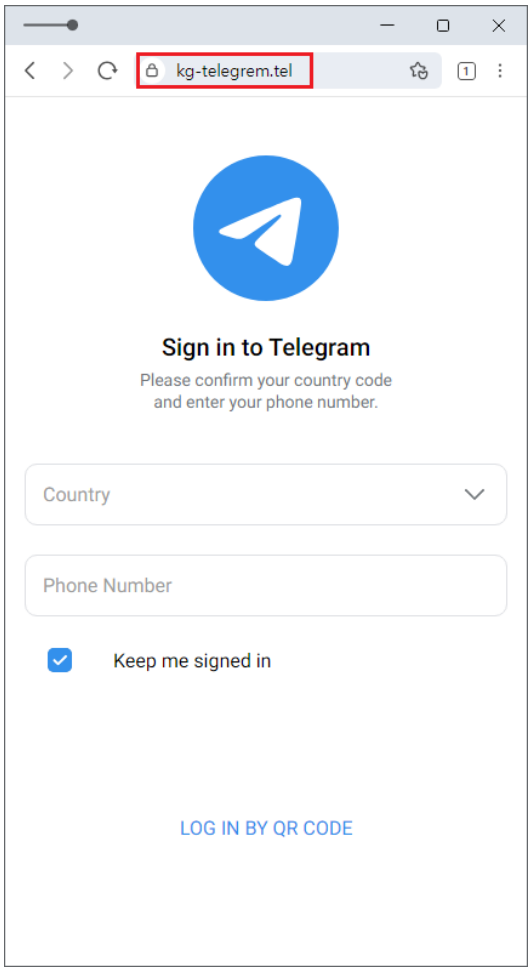
텔레그램 계정을 노리는 스미싱 주의!

텔레그램 계정탈취를 목적으로 하는 스미싱이 지속적으로 유포되고 있어 사용자들의 각별한 주의가 필요합니다.
스미싱 문자는 다음과 같은 내용들과 함께 피싱 링크가 포함된 형태로 유포됩니다.

[국외발신]telegram 계정보안활동이발견됩니다. 계정보완을위해, 다시로그인하세요 피싱링크
[국외발신] Telegram 정책상 탈퇴예정이니 6 시간내 인증바랍니다. 피싱링크
Telegram 정책상 탈퇴예정이니 6 시간내 인증바랍니다. 피싱링크
[국외발신] Telegram 정책에따라 탈퇴될 예정이니 6 시간이내 인증을 완료바랍니다. 피싱링크
해외기기의 로그인 접촉. 홈페이지 접속후 재연동해주세요 피싱링크

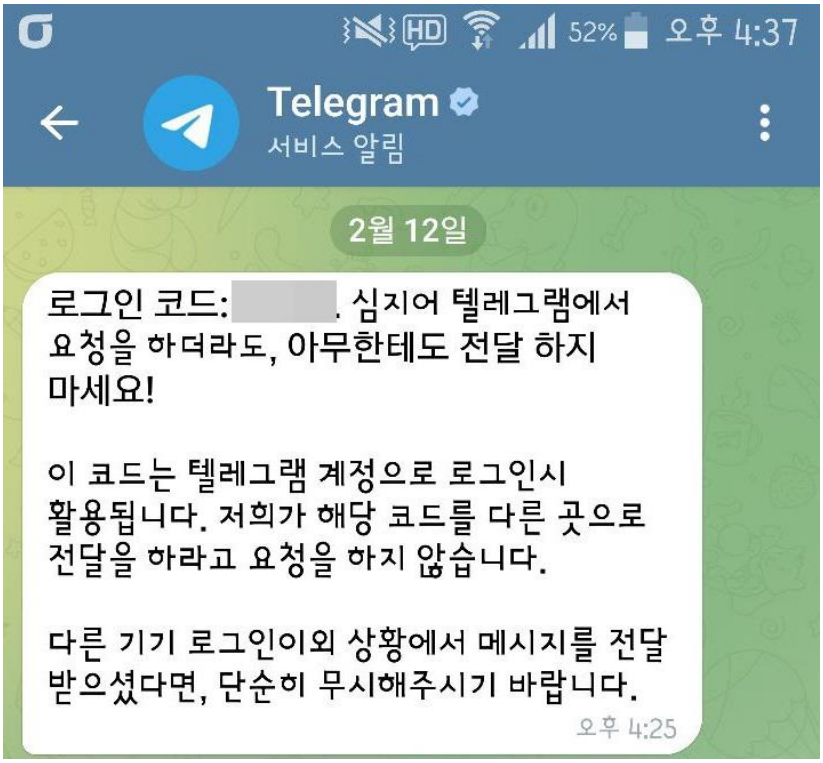
스미싱 문자의 내용과 형식은 조금씩 다르지만, 공통적으로 사용자로 하여금 Telegram 재인증 혹은 재로그인을 유도한다는 점 입니다.

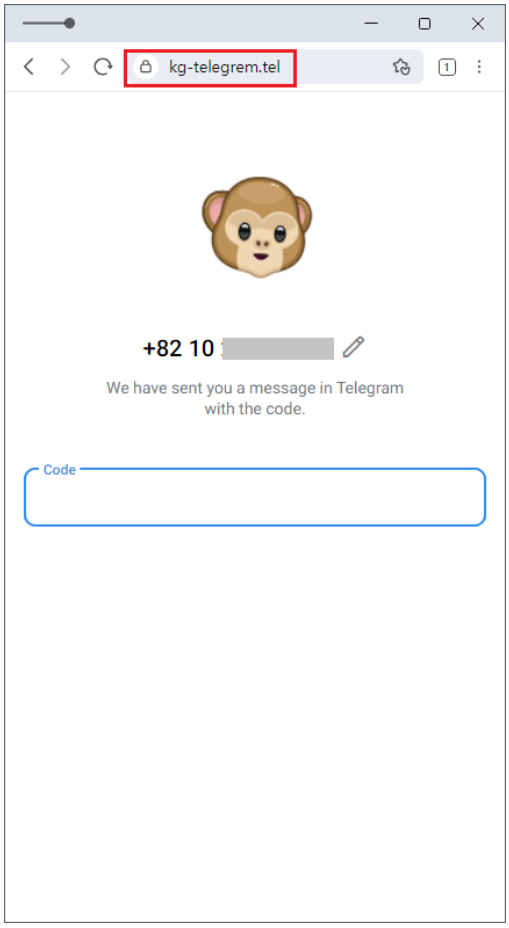
사용자가 스미싱 문자 내에 포함된 피싱 링크를 클릭하면 텔레그램 로그인 페이지와 유사하게 제작된 피싱 페이지로 접속됩니다.



[그림 1] 피싱 페이지 메인화면

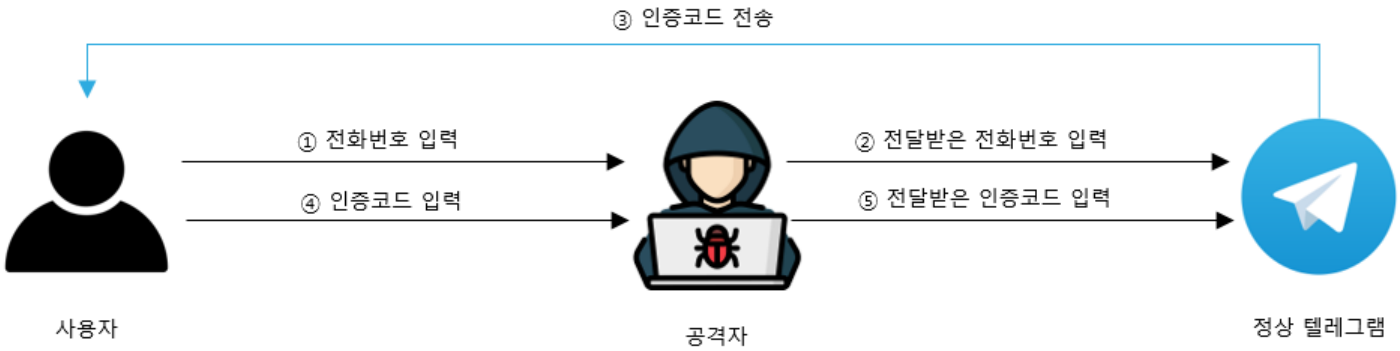
피싱페이지에 접속한 사용자가 로그인을 위해 자신의 휴대폰 정보를 입력하면 실제 텔레그램서버에서 로그인을 위한 인증번호이 발송됩니다.





[그림 2] 수신된 인증번호와 인증번호 입력을 유도하는 피싱 페이지

피싱 페이지에 인증번호를 입력하게되면 공격자는 성공적으로 계정을 탈취하게 됩니다.



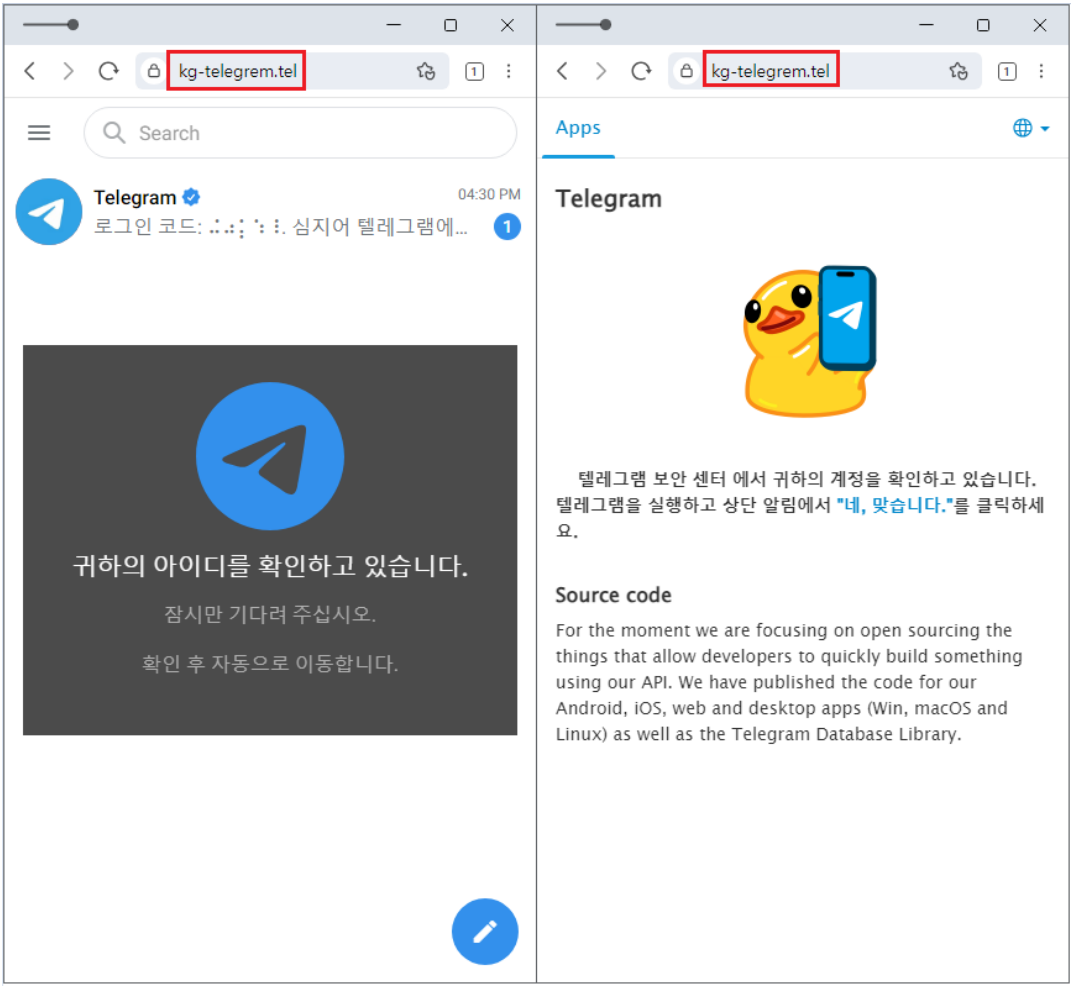
[그림 3] 공격 흐름도

해당 공격에서 공격자는 사용자와 정상 텔레그램 사이에서 데이터를 전달해 주는 전달자 역할이며, 공격자가 사용자로부터 전달받은 입력값으로 사용자 계정에 접근이 가능하게 됩니다.

Name	Value
Content-Disposition: form-data; name="userAuthId"	
Content-Disposition: form-data; name="userAuthDate"	
Content-Disposition: form-data; name="phone"	
Content-Disposition: form-data; name="pwd"	
Content-Disposition: form-data; name="userAuthDcId"	
Content-Disposition: form-data; name="dcServerSalt"	
Content-Disposition: form-data; name="dcAuthKey"	
Content-Disposition: form-data; name="stateId"	
Content-Disposition: form-data; name="url"	
Content-Disposition: form-data; name="domain"	

[그림 4] 공격자에게 전송되는 사용자 정보

전달된 후에는 공격자가 추가로 제작해 둔 페이지를 보여주는데, 이는 수집한 계정정보로 로그인을 시도할 시간을 벌기 위한 의도로 추정됩니다.



[그림 5] 추가 안내를 가장한 피싱 페이지

이런 공격을 통하여 공격자는 사용자의 휴대폰번호를 포함한 개인정보 탈취뿐만 아니라 이렇게 장악한 사용자 계정을 통해 대화내용을 열람하고 모니터링 할 수도 있어 각별한 주의가 필요합니다.

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com