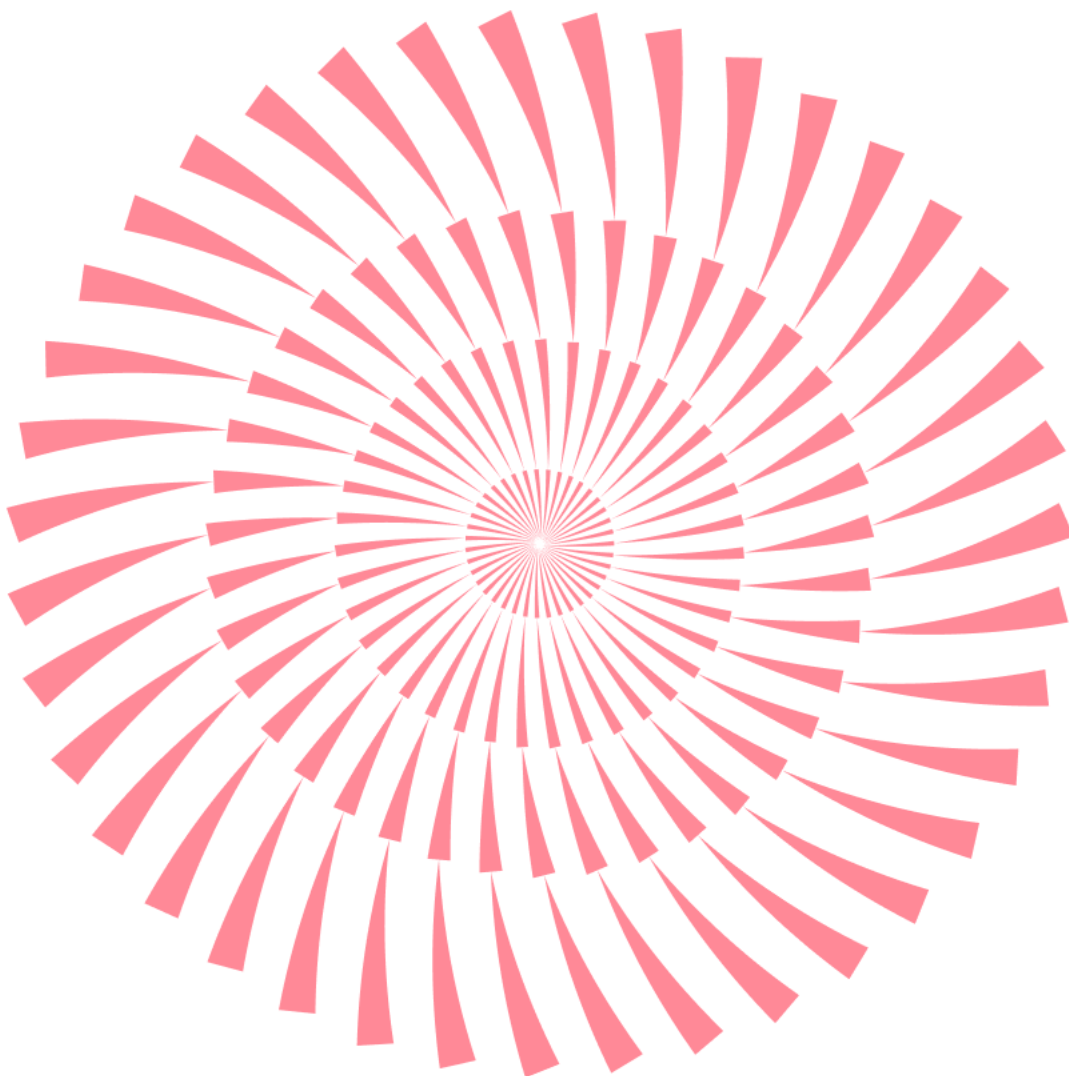


No.188 | 2025.5

ESRC 보안동향보고서

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



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

08-12

BPF 필터를 악용하는 BPFDoor 리눅스 악성코드 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

2025년 4월 18일, 국내 통신사 역사상 최대 규모의 개인정보 유출 사건이 발생했습니다.

민관합동조사단의 1차 조사 결과, SK 텔레콤의 가입자 인증 서버(HSS)가 외부 해킹 공격을 받아 약 2,500만 명의 가입자 유심(USIM) 정보가 유출된 것으로 확인됐습니다.

유출된 유심 정보에는 가입자 전화번호, 가입자 식별번호(IMS), 기본키, 사업자 인증키 등이 포함되어 있으며, 이는 통신사가 가입자를 식별하고 서비스 제공에 활용하는 핵심 데이터입니다.

이로 인해 온라인에서는 '심스와핑(SIM Swapping)' 공격에 대한 우려가 제기됐습니다.

심스와핑(또는 SIM Hijacking)은 공격자가 피해자의 유심 정보를 복제해 타 기기에서 인증을 시도하는 방식으로, 금융 계좌나 가상자산 계정 등에 무단 접근할 수 있는 위험이 있습니다.

다만, 이 공격이 성공하려면 유심 정보 외에도 사용자 개인정보, 인증서 비밀번호, 패턴 등 추가 인증 정보가 필요하므로, 공격자가 사전에 이 정보를 확보하지 못한 경우 실행 가능성은 낮은 편입니다.

불안감이 커지면서 유심을 교체하려는 고객들이 대리점에 몰려 혼란이 발생했고, SK 텔레콤은 고객 보호와 불안 해소를 위해 타 기기에서의 유심 사용 차단, 타 기기 이용 시 실시간 알림, 해외 로밍 제한 기능 등을 포함한 '유심 보호 서비스' 전 고객 자동 가입과 유심 무료 교체 서비스를 시행했습니다.

5월 19일 발표된 2차 조사 결과, 감염 서버가 기존 5대에서 23대로, 악성코드는 4종에서 총 25종으로 크게 늘어났습니다. 또한 1차 조사 당시 유출되지 않았던 것으로 알려졌던 IMEI(단말기 고유번호) 등 개인정보가 추가로 유출됐을 가능성도 제기됐습니다. 특히 IMEI 29만여 건이 저장된 서버가 악성코드에 감염된 사실이 확인됐으며, 해당 기간(2022년 6월부터 2023년 12월까지)에는 자료 유출 여부를 확인할 수 없는 상황입니다.

SK 텔레콤 해킹에 사용된 악성코드는 대부분 BPFDoor 계열과 그 변종으로, 리눅스 시스템을 타깃으로 하며 매직시퀀스(Magic Sequence)가 포함된 패킷이 탐지될 때만 활성화되어 장기간 시스템에 은닉될 수 있는 특징이 있습니다.

이 사건은 아직 조사가 진행 중이며, 유출된 데이터가 추가로 확인될 가능성이 있어 지속적인 관심이 필요합니다.

기업 보안 담당자라면 시스템 내 BPF 필터를 조회하고, 공개된 BPFDoor 악성코드의 매직 시퀀스(0x7255, 0x5293, 0x39393939)를 검색해보는 것이 필요합니다. 또한, 지속적으로 프로세스와 네트워크를 모니터링해 비정상 파일이나 트래픽을 분석하고, 불필요한 서비스와 포트를 주기적으로 점검해 비활성화하는 등 선제적 보안 조치를 취해야 합니다.

개인 사용자는 주요 플랫폼의 비밀번호를 변경하고 2단계 인증(2FA)을 설정하시는 것을 권고드립니다. 또한 유출된 개인정보를 활용한 맞춤형 공격이나 사회적 이슈를 이용한 피싱 시도가 증가할 수 있으므로, SMS에 포함된 링크 클릭을 자제하고, 출처가 불분명한 이메일은 반드시 발신자를 확인한 뒤 첨부파일 실행 전 확장자를 확인하는 등 각별한 주의가 필요합니다.

기본적인 보안 수칙을 지키는 것이 2차 피해 예방에 가장 효과적인 점을 반드시 기억해주시기 바랍니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2025 년 4 월에는 애드웨어 Adware.Generic.3184910 이 1 위를 차지하였습니다. 다양한 악성행위를 하는 악성코드 탐지명인 Gen:Variant.Tedy.675091 도 많이 탐지되었으며, 불법 인증툴 탐지명인 Application.Hacktool.BHM 도 새롭게 순위에 진입하였습니다.

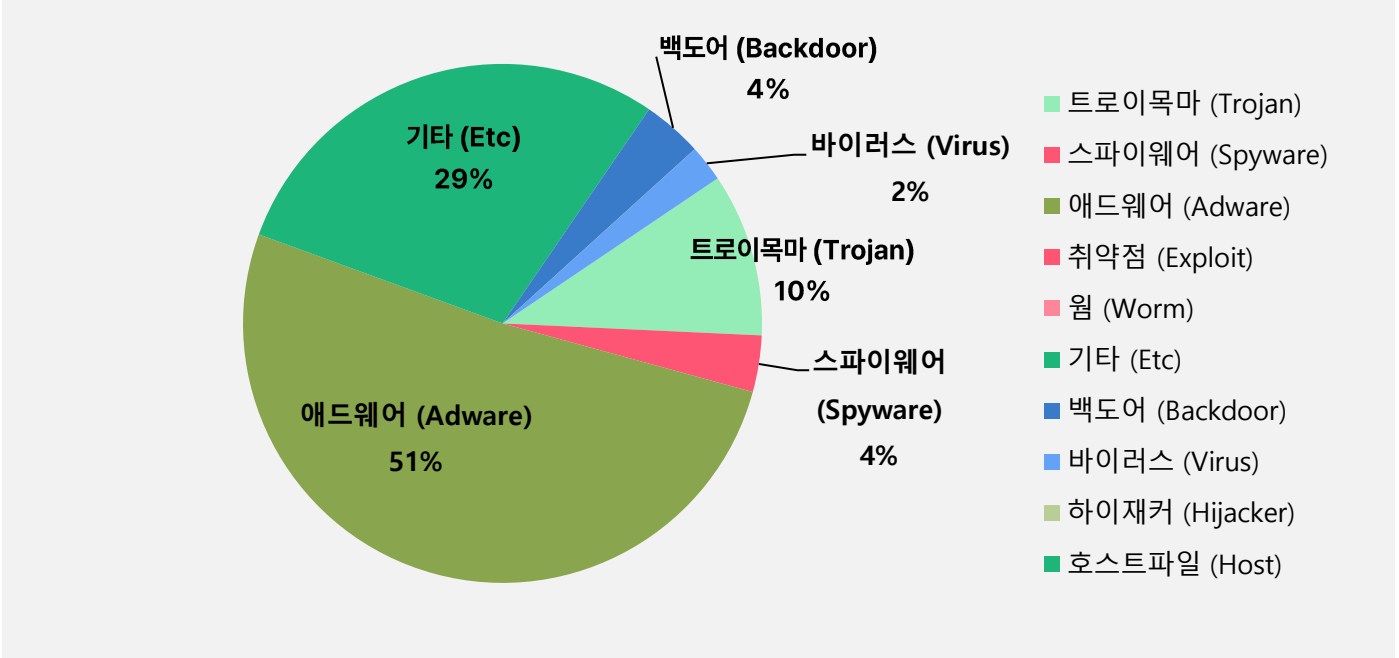
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Adware.Generic.3184910	Adware	215,840
2	↑1	Gen:Variant.Tedy.675091	ETC	39,790
3	↑2	Trojan.DDoS.Nitol.gen	Trojan	27,437
4	-	Misc.HackTool.AutoKMS	ETC	26,170
5	↑6	Gen:Variant.TDss.49	ETC	24,691
6	NEW	Adware.GenericKD.61044978	Adware	18,185
7	↓1	Backdoor.Generic.792814	Backdoor	16,989
8	↓1	Spyware.Infostealer.Bladabindi	Spyware	16,052
9	↓1	Application.Hacktool.BBJ	ETC	14,788
10	NEW	Application.Hacktool.BHM	ETC	11,200
11	NEW	Trojan.Acad.Bursted.AK	Trojan	10,487
12	-	Win32.Neshta.A		10,390
13	NEW	Trojan.GenericKD.72973669	Trojan	8,519
14	NEW	Gen:Variant.Ulise.144799	ETC	7,833
15	↓1	Misc.HackTool.KMSActivator	ETC	7,676

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025 년 4 월 1 일 ~ 2025 년 4 월 30 일

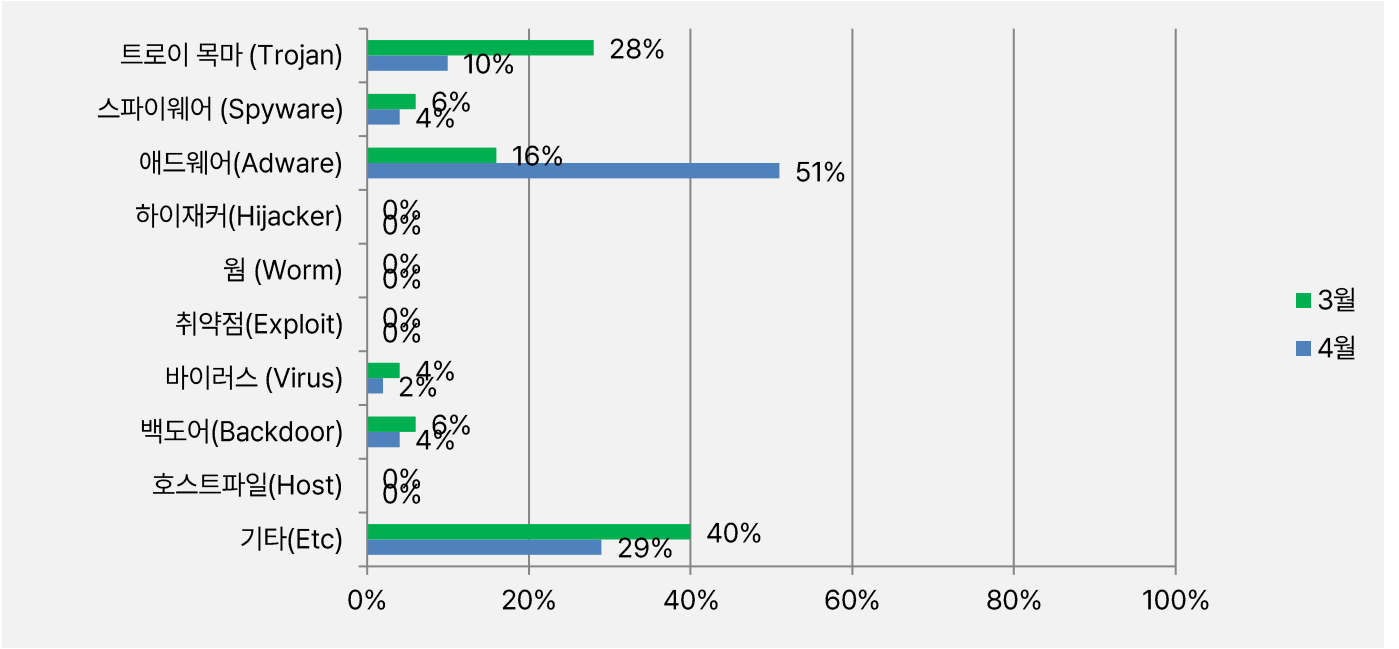
악성코드 유형별 비율

악성코드 유형별 비율에서 애드웨어(Adware)유형이 51%로 가장 높은 비율로 탐지되었으며, 그 다음으로 기타 (ETC) 29%, 트로이목마(Trojan) 10%, 백도어(Backdoor)와 스파이웨어(Spyware)가 각각 4%, 바이러스(Virus)가 2%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

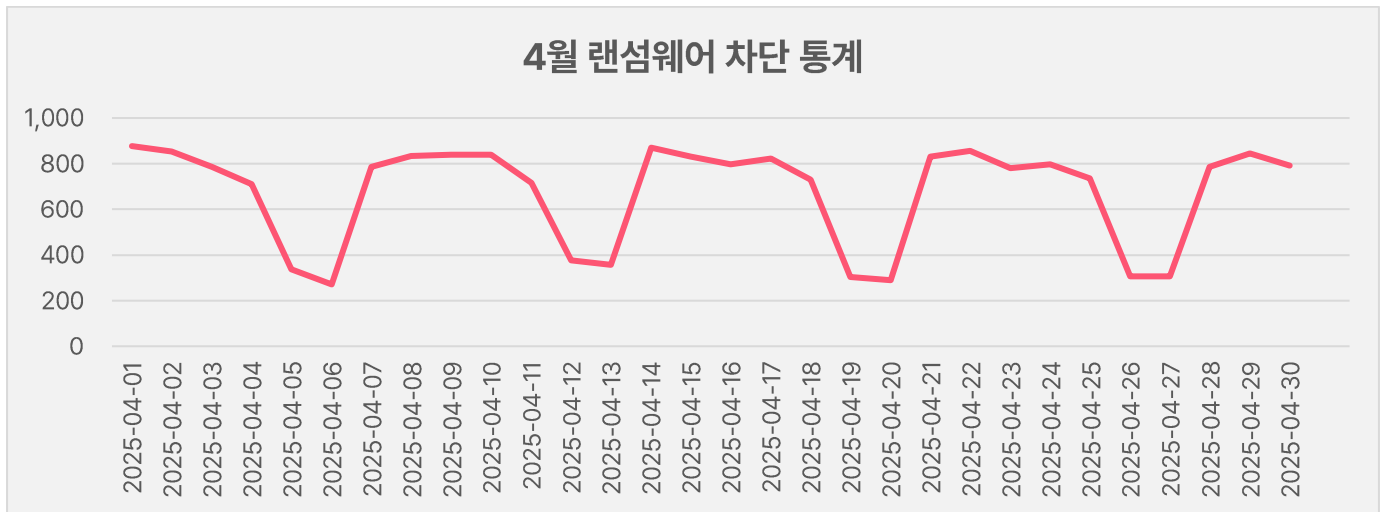
2025년 4월에는 지난 3월과 비교하여 트로이목마(Trojan) 유형이 18% 감소하였고, 백도어(Backdoor) 유형이 2%,스파이웨어(Spyware) 2%,기타(ETC) 유형이 11% 감소하였습니다. 또한, 애드웨어(Adware) 유형이 35% 큰 폭으로 증가하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

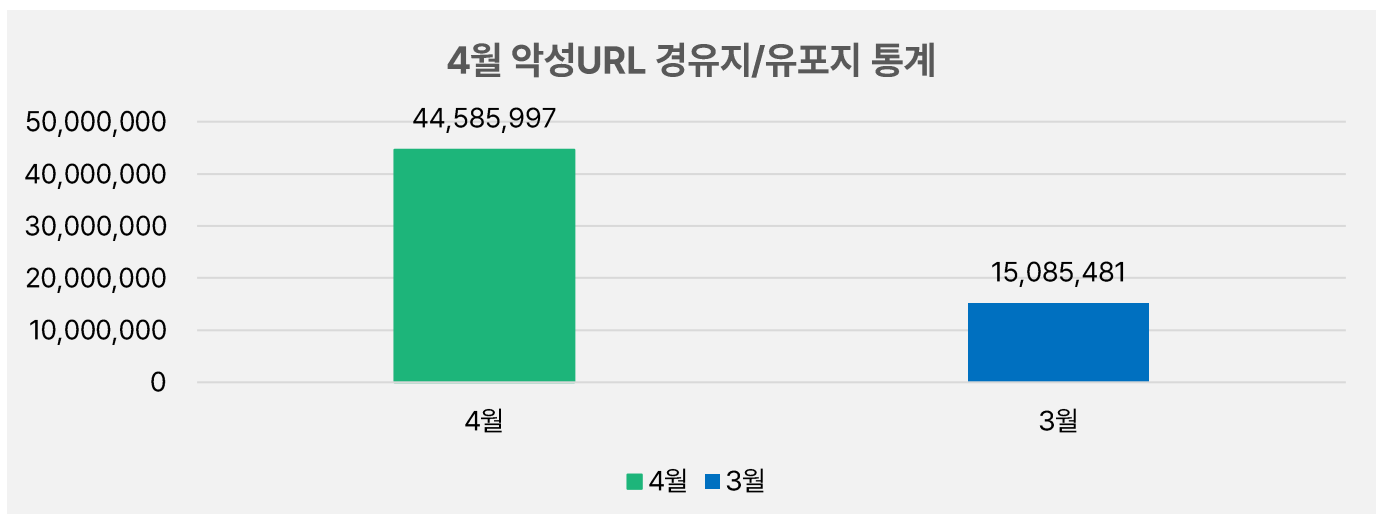
4 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 4월 1일부터 4월 30일까지 11,084건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 4월 한 달간 총 44,585,997건의 URL이 확인되었습니다. 이 수치는 25년 3월 한 달간 총 15,085,481건의 악성코드 경유지/유포지 URL 수에 비해 약 195.5% 가량 증가한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



2

최신 보안 동향

BPF 필터를 악용하는 BPFDoor 리눅스 악성코드 주의!

BPFDoor은 리눅스 시스템을 공격 타깃으로 하는 백도어(Backdoor) 악성코드로, 2021년 PWC사의 [보고서](#)를 통해 최초 발견되었습니다.

BPFDoor은 중동 및 아시아 전역의 통신업체, 정부, 교육 등의 분야를 공격 타깃으로 삼고 있으며, 공격 타깃에는 대한민국도 포함되어 있습니다.

최근 한국 인터넷진흥원(KISA)에서는 "최근 해킹공격에 악용된 악성코드·IP 등 위협 정보 공유 및 주의 안내" 공지를 공개하기도 했습니다.

보안공지

🏠 > 알림마당 > 보안공지

최근 해킹공격에 악용된 악성코드, IP 등 위협정보 공유 및 주의 안내

☐ 개요

- o 최근 주요 시스템을 대상으로 해킹 공격하는 사례가 확인되어 위협정보 공유

☐ 침해사고 위협정보

1. 공격 IP : 165.232.174[.]130

2. 악성코드 해시값 및 파일정보

o hpsasmld

- size : 2,265KB

- SHA256 : c7f693f7f85b01a8c0e561bd369845f40bff423b0743c7aa0f4c323d9133b5d4

- MD5 : a47d96ffe446a431a46a3ea3d1ab4d6e

o smartadm

- size : 2,067KB

- SHA256 : 3f6f108db37d18519f47c5e4182e5e33cc795564f286ae770aa03372133d15c4

- MD5 : 227fa46cf2a4517aa1870a011c79eb54

o hald-addon-volume

- size : 2,071KB

- SHA256 : 95fd8a70c4b18a9a669fec6eb82dac0ba6a9236ac42a5ecde270330b66f51595

- MD5 : f4ae0f1204e25a17b2adbbab838097bd

o dbus-srv-bin.txt

- size : 34KB

- SHA256 : aa779e83ff5271d3f2d270eaed16751a109eb722fca61465d86317e03bbf49e4

- MD5 : 714165b06a462c9ed3d145bc56054566

[그림 1] KISA 보안공지 화면

BPFDoor은 root 권한으로 BPF 소켓을 생성하여 특정 조건에 맞는 패킷을 감지할 준비를 하며, 조건을 만족하는 패킷 (매직 넘버)이 감지되면 패킷을 열어 다음과 같은 공격자의 명령을 실행합니다.

- Reverse Shell 실행
- 새로운 접속을 특정 포트의 셸로 연결
- 백도어가 활성화 되었는지 확인

이때 공격자가 전송하는 패킷이 방화벽에 탐지가 되지 않는데, BPF는 운영체제의 커널 레벨에서 동작하는 패킷 필터링 메커니즘으로, 방화벽보다 먼저 패킷을 수신하기 때문입니다. 그렇기 때문에 사용자가 미리 정의해 둔 방화벽 네트워크 정책이 적용되지 않을 뿐만 아니라, 방화벽에 의해 차단이 되어도 공격자가 원하는 명령어를 성공적으로 실행할 수 있습니다.

BPF란?

유저 모드 프로그램이 커널 레벨에서 네트워크 패킷을 빠르게 캡처하고 필터링할 수 있게 하는 기술

BPFDoor 악성코드는 이 필터링 기능을 악용해 네트워크 패킷을 모니터링 하고 특정 패턴의 패킷이 들어오면 동작 되는 방식입니다.

BPFDoor는 2021년 처음 발견된 이후 지금까지 지속적으로 고도화 되고 있으며 다양한 기능과 명령어가 추가되고 있습니다. 이는 BPFDoor를 활용한 공격이 지속되고 성공률이 높아지고 있다는 반증으로도 볼 수 있어 기업 보안 담당자 여러분들의 각별한 주의가 필요합니다.

[대응 방안]

1) 파일 및 프로세스 모니터링

/dev/shm/kdmtmpflush, /dev/shm/kdumpflush, /dev/shm/kerneldump, /var/run/haldrund.pid 등의 비정상 파일을 감시합니다.

find /proc -lname '*' (deleted)' 2>/dev/null 명령어로 삭제된 실행 파일을 가진 프로세스를 식별합니다. ls -alR /proc/*/exe 2> /dev/null | grep deleted 명령어로 삭제된 프로세스를 식별합니다.

/dev/shm에서 실행 중인 프로세스나 환경 변수가 없는 프로세스를 확인하며, ps auxc 또는 /proc/PID/environ 을 통해 환경 변수 유무를 점검합니다.

2) 네트워크 활동 감시

BPFDor는 iptables 규칙을 조작해 42391~43390 포트로 트래픽을 리디렉션하므로, 정기적으로 방화벽 설정을 점검하고 BPFDor가 주로 사용하는 포트의 비정상 트래픽을 분석합니다.

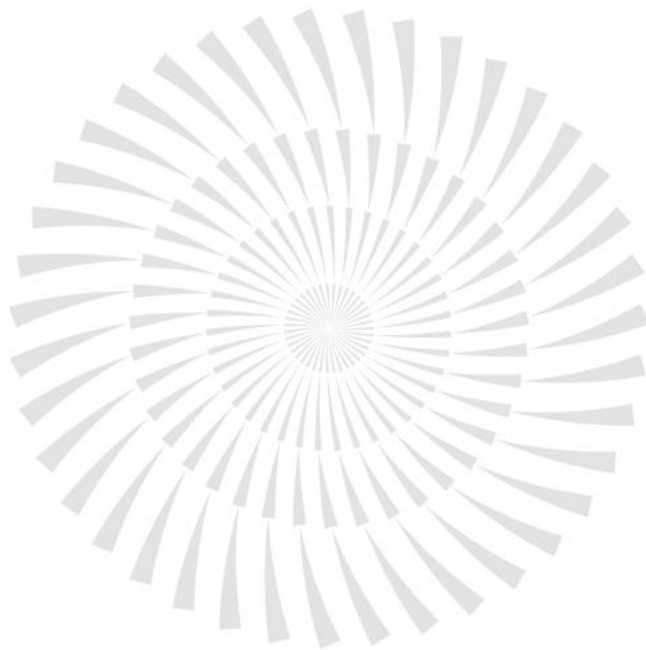
BPFDor는 매직 바이트 (예: 0x5293, 0x7255)가 포함된 패킷을 수신하면 활성화되므로, 네트워크 IDS/IPS에 시그니처 룰을 등록해 매직 패킷을 탐지하거나, 명령어를 통해 패킷 내 매직 바이트 검색합니다.

(명령어 예시) `ss -Opb | grep -EB1 --color "$((0x7255))|$((0x5293))|$((0x39393939))"`

3) 시스템 및 운영 환경 강화

BPF 관련 권한(CAP_BPF, CAP_NET_ADMIN)을 SELinux 또는 AppArmor로 최소화하며, 불필요한 서비스와 포트는 ss 또는 netstat으로 주기적으로 점검해 비활성화합니다.

알약에서 해당 악성코드에 대해 Backdoor.Linux.BPFDor로 탐지중에 있으며, 추가 변종 대한 모니터링과 신속한 대응을 진행하고 있습니다.



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

www.estsecurity.com