May
2025
Vol.10

CQ VISTA

2025 씨큐비스타 CQREPORT

네트워크 위협헌팅 보안보고서

차세대 NDR 기반 Stealth 위협 대응 전략

CQVISTA
씨큐비스타

- 02-565-0236
- sales@cqvista.com
- WWW.CQVISTA.COM
- 경기도 성남시 분당구 판교로 255번길 9-22, 5F 511호.

CONTENTS

VISTA

주제

차세대 NDR 기반 Stealth 위협 대응 전략

목차

01 서론

2025 년 4 월, 국내 대형 통신사의 홈 가입자 서버(HSS) 해킹을 통한 대규모 유심(USIM) 정보 유출과, 고객센터 운영 전문기업의 인사시스템 해킹으로 약 3 만 6 천여 명의 개인정보가 유출되는 사고가 연이어 발생했다. 이로 인해 국민적 사이버 보안 불안이 급격히 증대되고 있다.

특히, 유심 인증 정보와 주민등록번호, 주소, 이력서 등 개인식별정보가 결합될 경우, 명의 도용, 금융사기, 본인 인증 체계 무력화 등의 심각한 2 차 피해로 이어질 위험성이 높아진다. 보안 전문가들은 통신, 금융, 의료, 고용정보 등 핵심 민감 정보를 다루는 기관들의 취약성이 한계에 달했음을 경고하고 있으며, 정부와 민간의 긴밀한 협력과 보안 인프라의 근본적 강화가 필요하다고 촉구하고 있다.

본 보고서는 기존 보안 기술로는 탐지가 어려운 리눅스 및 윈도우 기반 스텔스 악성코드를 상세히 분석하고, 이에 대한 탐지 및 대응 전략을 제시하고자 한다.

1-1. 리눅스 및 윈도우 기반 스텔스(Stealth) 악성코드의 부상

최근 사이버 위협 환경에서는 리눅스와 윈도우 시스템을 모두 대상으로 하는 스텔스형 악성코드가 급속히 진화하고 있다. 이들 악성코드는 장기간 은닉할 수 있는 능력을 갖추고 있으며, 통신 인프라, 클라우드 서버, 엔드포인트를 위협하는 주요 수단으로 부상하고 있다.

대표적인 사례로 BPFdoor, Symbiote, LummaC2 를 들 수 있다.

1-2. BPFdoor, Symbiote, LummaC2 위협 개요

위협명	주요 특징
BPFdoor	리눅스/BSD 대상, eBPF 활용 네트워크 레벨 은닉형 백도어, 포트리스 통신
Symbiote	리눅스 대상, LD_PRELOAD 기반 기생형 루트킷, 시스템 호출 조작
LummaC2	윈도우 대상, 다단계 암호화 및 C2 기반 인포스틸러, 광범위 정보 탈취

1) BPFdoor

최근 사이버 위협 환경은 고도화된 은닉성과 지속성을 가진 공격 형태로 빠르게 진화하고 있다. 특히 커널 레벨에서 은밀히 동작하는 eBPF(Extended Berkeley Packet Filter) 기반 스텔스 위협은 전통적인 사용자 공간(User Space) 보안 체계의 감시를 우회하며, 네트워크 및 시스템 수준에서 장기간 탐지되지 않고 활동할 수 있는 심각한 보안 리스크를 초래하고 있다.

본 보고서에서는 eBPF 기술의 기본 원리, 악용 방식, 스텔스 위협으로의 발전 경로를 분석하고, 이에 따른 보안상의 문제점과 대응 방향을 심층적으로 고찰한다.

eBPF 는 리눅스 커널에서 사용자 정의 프로그램을 안전하게 실행할 수 있도록 허용하는 가상 머신(VM) 기반 기술이다. 원래는 네트워크 패킷 필터링(BPF) 용도로 개발됐으나, 이후 시스템 추적, 성능 모니터링, 보안 제어 등 다양한 용도로 확장됐다.

특징

- 커널 코드를 수정하거나 리부팅 없이 새로운 로직 삽입 가능.
- 이벤트 기반 트리거(예: 네트워크 패킷 수신, 시스템 콜 호출 등)에 따라 실행.
- 높은 성능(네이티브 실행에 가까운 속도)과 안정성 확보.
- 사용자 공간과 커널 공간 간 안전한 인터페이스 제공.

eBPF 의 강력한 시스템 제어 기능은 공격자에게도 매력적인 공격 수단을 제공한다. 특히 다음과 같은 방식으로 악용될 수 있다.

커널 레벨 트래픽 조작 및 은폐

- eBPF 프로그램을 네트워크 스택에 삽입하여 특정 패킷을 가로채거나 조작.
- 포트리스(Portless) 통신 구현: 포트를 열지 않고도 외부 트리거 패킷 수신 시만 연결 활성화.
- IDS/IPS, 방화벽 등의 전통적인 네트워크 보안 장비 우회.

시스템 호출 감시 및 변조

- 파일 접근, 프로세스 생성, 네트워크 연결 등 주요 시스템 호출을 후킹.
- 악성 행위나 파일 존재를 숨김으로써 EDR, SIEM 등 사용자 공간 보안 솔루션 무력화.

은닉형 백도어 구축

- 정상 프로세스에 삽입되어 존재를 감추면서 원격 명령어 실행, 데이터 탈취 수행.
- 로그 기록, 감시 활동 자체를 변조하여 포렌식 분석조차 어렵게 만듦.

eBPF 기반 스텔스 위협의 특징

항목	내용
운영 계층	커널 공간(Kernel Space)
탐지 회피	사용자 공간 보안 제품(EPP/EDR) 우회
은닉성	포트리스 통신, 시스템 콜 조작, 트래픽 조작
지속성	서버/시스템 재시작 후에도 유지 가능 (특정 설정 시)
공격 용도	장기 은닉, 명령 제어(C2), lateral movement 지원

실제 사례: BPFdoor

BPFdoor 는 eBPF 기반 백도어 기술을 이용해 구현된 대표적인 악성코드 사례로, 다음과 같은 특징을 보인다.

- 포트리스 통신: 열린 포트 없이 매직 패킷을 통한 비밀 통신 경로 생성.
- 정상 프로세스 위장: 시스템 상에서 정체를 숨기며 활동.
- 전통적 보안 솔루션 우회: IDS, IPS, 방화벽을 무력화.

BPFdoor 는 통신사, 정부 기관, 금융 기관 등을 표적으로 하여 장기 침투 및 기밀 탈취 목적으로 사용된 것으로 분석됐다.

2) Symbiote

사이버 공격 기술이 지속적으로 고도화되면서, 단순한 악성코드 탐지로는 대응이 어려운 은닉형 위협(Stealth Threat)이 급증하고 있다. 특히 Symbiote 와 같은 고급 스텔스 루트킷은 정상 프로세스에 기생(parasitic)하여 존재를 철저히 숨기면서도, 내부 시스템을 장기적으로 조작하고 탈취할 수 있는 심각한 위협을 초래하고 있다.

본 보고서는 Symbiote 악성코드의 기술적 특성과 위협 모델을 심층 분석하고, 이로 인한 보안 리스크와 대응 전략을 구체적으로 제시한다.

Symbiote 는 리눅스 시스템을 대상으로 설계된 고급 스텔스 루트킷(Stealth Rootkit)이다. 단독 실행 파일 형태가 아니라, 정상 시스템 프로세스에 동적으로 삽입되어 활동하며, 파일 시스템, 프로세스 목록, 네트워크 통신 정보를 조작하여 자신의 존재를 철저히 숨긴다.

주요 특징

항목	내용
대상 플랫폼	Linux 기반 서버 및 엔터프라이즈 시스템
감염 방식	LD_PRELOAD 를 이용한 사용자 공간 라이브러리 삽입
은폐 기법	시스템 콜 후킹, 프로세스/파일/네트워크 연결 은폐
공격 기능	관리자 권한 탈취, 네트워크 조작, 데이터 탈취, 백도어 구축
탐지 회피	독립 실행 파일 없이 정상 프로세스 내부에 은폐

Symbiote 의 동작 원리

① 감염 단계

• LD_PRELOAD 이용
- 시스템 환경 변수에 악성 공유 라이브러리(.so)를 등록해 정상 프로세스가 실행될 때 함께 로드되도록 설정.

• 프로세스 기생
- 별도 프로세스를 생성하지 않고, 정상 프로세스 내부에 자신을 주입하여 탐지를 회피.

② 은폐 및 변조

• 시스템 콜 후킹(System Call Hooking)
- open, getdents, read, netstat 등 주요 시스템 콜을 변조.
- 자신과 관련된 파일, 디렉터리, 네트워크 세션 정보를 사용자에게 숨김.

• 네트워크 조작
- 특정 포트나 IP 주소의 트래픽을 은폐하거나 변조.
- 공격자에게만 비공개 백도어 연결을 허용.

• 권한 탈취 및 백도어 설치
- 관리자 계정 비밀번호 탈취.
- 지속적인 시스템 장악을 위한 백도어 통신 구축.

Symbiote 기반 위협의 특징

구분	내용
기생성(Parasitism)	별도 프로세스 없이 정상 프로세스 내부에 은닉
시스템 변조 범위	파일 시스템, 프로세스 관리, 네트워크 스택
탐지 회피성	안티바이러스, EDR, IDS/IPS 로부터 은폐
지속성(Persistence)	시스템 재부팅 이후에도 감염 상태 유지 가능(특정 설정 시)
APT 연계성	장기 은닉 침투 및 수평 이동(Lateral Movement) 지원

3) LummaC2

디지털 전환과 원격 근무 환경 확산으로 인해 윈도우 기반 시스템을 표적으로 한 사이버 위협이 급증하고 있다. 특히 최근 확산 중인 LummaC2 는 고속화, 경량화, 암호화된 통신을 특징으로 하는 고급 정보 탈취형 인포스틸러(Infostealer) 로, 기존 탐지 체계를 어렵게 만들며 대규모 개인정보 및 인증정보 유출 사고를 초래하고 있다.

본 보고서는 LummaC2 악성코드의 구조와 특성을 심층 분석하고, 이를 통해 발생할 수 있는 주요 위협 시나리오와 효과적인 탐지·대응 방안을 제시한다.

LummaC2 는 윈도우 환경을 표적으로 한 정보 탈취형 악성코드로, 암호화된 C2(Command and Control) 채널을 통해 민감 데이터를 수집 및 탈취하는 데 최적화되어 있다. 특히 브라우저 저장 정보, 암호화폐 지갑 데이터, 인증 토큰을 주요 탈취 대상으로 삼는다.

주요 특징

항목	내용
대상 플랫폼	Microsoft Windows 운영체제
주요 기능	자격 증명 탈취, 세션 쿠키 수집, 암호화폐 지갑 데이터 탈취
감염 경로	피싱 이메일, 악성 광고(Adware), 불법 소프트웨어 배포
통신 방식	다단계 암호화된 HTTPS C2 채널
탐지 회피 기법	코드 난독화, 프로세스 인젝션, 무작위화된 통신 경로 사용

LummaC2 의 동작 원리

① 초기 감염 및 로딩

• 사용자가 악성 파일(스크립트, 실행파일 등)을 실행하면, LummaC2 는 정상 프로세스(예: explorer.exe, svchost.exe 등)에 자신을 인젝션하여 탐지를 회피한다.

② 정보 수집 및 탈취

• 브라우저(Chrome, Edge, Firefox 등)의 저장된 아이디/비밀번호, 세션 쿠키를 수집.
• 암호화폐 지갑(Exodus, MetaMask 등) 관련 파일 및 키를 검색하고 탈취.
• Discord, Telegram, Steam 등 주요 플랫폼의 인증 토큰을 추출.

③ 암호화된 C2 통신

• 수집한 데이터를 다단계로 암호화(AES, RC4 등)한 후, HTTPS 기반 C2 서버로 전송.
• 매 감염 시마다 C2 경로를 무작위(randomized paths)로 변경하여 트래픽 분석을 회피.

④ 확장 및 업데이트

• 공격자가 명령을 내려 추가 페이로드(예: 키로거, 스크린샷 모듈)를 설치하거나, 악성 행위를 업데이트할 수 있도록 설계됨.

LummaC2 기반 위협의 특징

구분	내용
경량성 및 속도	감염 및 정보 탈취까지 수 분 내에 완료
암호화 통신 위장	정상 HTTPS 트래픽과 구별이 어려움
다단계 은폐	프로세스 인젝션, 코드 난독화, 통신 무작위화
광범위 정보 수집	단일 침투로 다수 인증정보 및 금융 데이터 탈취 가능
다크웹 연계성	탈취된 데이터가 즉시 거래·악용되는 구조와 연결

02 스텔스(Stealth) 악성코드 위협 분석

2-1. BPFdoor: eBPF 기반 네트워크 스텔스(Stealth) 백도어

BPFdoor 는 리눅스 및 일부 BSD 시스템을 표적으로 하는 고급 스텔스(Stealth) 백도어 악성코드로, 기존 악성코드들과 달리 네트워크 계층에서 매우 은밀하게 통신을 제어할 수 있도록 설계됐다.

1) 핵심 특징

항목	설명
기반 기술	BPF (Berkeley Packet Filter) 또는 eBPF
주요 기능	패킷 레벨에서 직접 네트워크 통신 가로채기
은닉 방식	포트 리스닝 없음, 프로세스 명/파일 이름 위장
통신 방식	특정 '매직 패킷' 수신 시만 활성화 (기본은 무반응)
명령 기능	셸 명령 실행, 파일 업로드/다운로드, 포트 포워딩
탐지 회피	IDS/IPS, 포트 스캐닝, 네트워크 로깅 모두 회피 가능

2) 동작 원리

• 패킷 가로채기
- BPF/eBPF 를 이용해 커널 수준에서 직접 네트워크 패킷을 스니핑한다. 일반적인 방화벽 룰이나 IDS 에 의해 탐지되지 않는 '은닉 채널'을 만들어낸다.

• 트리거 기반 활성화
- 일반적인 포트 열림 없이, 특정 매직 패킷(미리 설정된 값 포함)을 수신할 때만 활성화된다. 이로 인해 평상시에는 '아무것도 안 하는 정상 프로세스처럼' 보인다.

• C2 제어 및 명령 수행
- 매직 패킷을 수신한 후, 공격자와 비밀리에 세션을 생성해 쉘 명령을 실행하거나, 파일을 탈취하거나, 역방향 포트 포워딩을 설정할 수 있다.

3) 탐지의 어려움

• 네트워크 상에서 포트가 열려 있지 않음.
• 악성 프로세스가 정상적인 시스템 프로세스처럼 위장됨.
• 통신 흐름이 일반적인 TCP 세션 패턴과 다름.

기존 네트워크/호스트 보안 솔루션으로 탐지가 거의 불가능하다.

2-2. Symbiote: 리눅스 스텔스(Stealth) 루트킷

Symbiote 는 리눅스 시스템을 표적으로 한 고급 스텔스(Stealth) 루트킷(Stealth Rootkit)이다. 다른 일반적인 악성코드와 달리, Symbiote 는 단독 실행되지 않고 기존 정상 프로세스에 기생(parasitic)해 시스템 활동을 은닉하고 공격자의 권한을 장기적으로 유지하기 위해 설계됐다.

1) 핵심 특징

항목	설명
대상 플랫폼	리눅스 (특히 엔터프라이즈 서버 환경)
은닉 방법	LD_PRELOAD 환경 변수 기반 동적 라이브러리 삽입
은닉 대상	프로세스 목록, 네트워크 연결, 파일 시스템 활동, 시스템 호출 결과
악성 기능	관리자 인증 정보 탈취, 백도어 접근, 시스템 명령 변조, 네트워크 트래픽 조작
탐지 회피	독립 실행 파일 없음, 정상 프로세스 내부에 은닉, EDR 및 보안 모듈 우회

2) 동작 방식

① LD_PRELOAD 를 이용한 라이브러리 삽입

• Symbiote 는 시스템 환경 변수 LD_PRELOAD 를 통해 악성 공유 라이브러리(.so 파일)를 정상 프로세스에 강제로 삽입한다.
• 이 기법은 리눅스에서 프로그램이 시작될 때 특정 라이브러리를 먼저 로드 하도록 하는 표준 메커니즘이다.

② 시스템 호출(System Calls) 변조

• 파일 열람(open), 프로세스 조회(getdents), 네트워크 연결 조회(netstat) 같은 시스템 콜을 후킹한다.
• Symbiote 자신이나 공격자가 설치한 악성 프로세스, 파일, 네트워크 세션을 보이지 않게 숨긴다.

③ 네트워크 통신 은닉

• 특정 포트, 소켓 연결을 감춘다.
• 악성 통신 트래픽도 '정상 트래픽'처럼 위장해 IDS/IPS 를 우회한다.

④ 백도어 기능

• 공격자는 Symbiote 가 설치된 시스템에 은밀히 로그인하거나 명령어를 실행할 수 있다.
• 추가로 시스템 내부 사용자 인증 정보를 탈취하여 장기적 권한 확보도 가능하다.

⑤ 탐지 및 제거 어려움

• Symbiote 는 별도의 독립 실행 파일이 존재하지 않고, 오직 메모리에 정상 프로세스에 은닉돼 있다.
• 일반적인 파일 기반 안티바이러스나 EDR 솔루션은 이를 탐지하기 매우 어렵다.

3) Symbiote 만의 고유한 위협성

• 기생적 특성(Parasitic)
- 별도 프로세스가 없기 때문에, 활동을 추적하거나 정지시키기가 거의 불가능하다.

• 전체 시스템 후킹(System-wide Hijacking)
- 파일 시스템, 프로세스 관리, 네트워크 레이어를 통째로 변조할 수 있어, 루트킷 탐지 솔루션까지도 속일 수 있다.

• 네트워크 및 시스템 통제권 탈취
- 감염된 서버를 통해 내부망 침투, lateral movement(수평 이동)가 가능하다.

• APT(지능형 지속 위협) 연계 용이성
- Symbiote 는 특히 장기 은닉 침투와 APT 그룹의 '지속성 유지' 수단으로 주로 활용된다.

2-3. BPFdoor 와 Symbiote 결합에 따른 위협 가능성 및 시나리오

현재까지 BPFdoor 와 Symbiote 가 동시에 사용된 공식 해킹 사례는 보고되지 않았다. 그러나 두 악성코드의 기능적 특성과 상호 보완성을 고려할 때, 향후 복합 운용이 현실화될 경우 기존 방어 체계로는 탐지 및 대응이 극히 어려운 초장기 은닉 침투 위협으로 발전할 수 있다.

BPFdoor 와 Symbiote 는 각각 독립적으로도 고도의 은닉성과 지속성을 갖춘 악성코드로 평가받는다. 그러나 이 두 위협이 결합할 경우, 단순한 결합을 넘어 탐지가 극히 어려운 장기 침투형 복합 공격 체계가 구축될 수 있다.

우선, BPFdoor 는 네트워크 계층에서 흔적을 남기지 않고 통신을 제어하는 능력을 제공한다. 이 악성코드는 특정 매직 패킷을 수신하기 전까지는 어떠한 네트워크 세션도 열지 않기 때문에, IDS/IPS 및 방화벽을 통한 탐지를 회피할 수 있다. 동시에 Symbiote 는 리눅스 시스템 내부에서 정상 프로세스에 기생하여, 프로세스 목록, 파일 시스템 접근, 네트워크 연결 정보 등을 변조함으로써 시스템 감시 도구 및 EDR 의 탐지를 무력화한다.

이러한 네트워크 및 호스트 계층 양면의 은닉 조합은, 침해가 발생한 사실조차 인지하지 못한 상태로 공격자가 수개월 또는 수년간 시스템에 상주하며 활동할 수 있게 만든다. 공격자는 Symbiote 를 통해 시스템 관리자 권한을 탈취하고, 내부 정보에 접근하거나 인증 정보를 지속적으로 수집할 수 있으며, BPFdoor 를 이용해 외부 C2(Command and Control) 서버와 은밀히 통신하며 명령어를 실행하거나 추가 악성 모듈을 배포할 수 있다.

특히, 이 조합은 APT(Advanced Persistent Threat) 공격에 최적화되어 있다. 조직 내부망에 장기 은닉 침투 후, lateral movement 를 통해 추가 시스템으로 확장하거나, 중요 데이터 및 계정 정보를 탈취하여 대규모 피해를 야기할 수 있다. Symbiote 가 서버 내부의 보안 로깅 기능 자체를 조작하는 동안, BPFdoor 는 외부와의 비인가 통신 경로를 비밀리에 유지함으로써 보안 관제 및 사고 대응을 극도로 어렵게 만든다.

결국 BPFdoor 와 Symbiote 의 결합은 탐지 우회, 장기 은닉, 네트워크 및 시스템 통제권 장악이라는 세 가지 위협 요소를 통합하는 결과를 초래하며, 이는 단일 서버 감염을 넘어 전체 조직의 보안 체계가 붕괴될 위험성을 내포하고 있다.

2-4. LummaC2: 암호화 C2 기반 정보 탈취형 악성코드

LummaC2 는 주로 윈도우 환경을 대상으로 동작하는 정보 탈취형(Infostealer) 악성코드로, 암호화된 C2(Command and Control) 통신을 기반으로 공격자와 비밀리에 데이터를 주고받으며, 다양한 민감 정보를 대량 수집하는 데 최적화되어 있다.

1) 핵심 특징

항목	설명
대상 플랫폼	Windows 운영체제
주요 기능	로그인 자격 증명, 브라우저 세션 쿠키, 암호화폐 지갑 정보, 인증 토큰 탈취
통신 방식	암호화된 HTTPS C2 통신, 무작위 경로(Randomized Paths)
감염 경로	피싱 이메일, 악성 웹사이트, 크랙된 소프트웨어, 드라이브 바이 다운로드
탐지 회피 기법	코드 난독화, 다단계 암호화, 프로세스 인젝션, API 변조

2) 동작 방식

① 감염 및 초기 로딩

• 사용자가 악성 파일을 실행하면 LummaC2 는 프로세스 인젝션을 통해 정상 프로세스(EX: explorer.exe, svchost.exe)에 자신을 삽입하여 실행된다.
• 초기 단계에서는 시스템 정보를 수집하여 공격자 C2 서버에 전송한다.

② 정보 탈취

• 다양한 브라우저(Chrome, Edge, Firefox, Opera 등)의 저장된 비밀번호, 세션 쿠키를 수집한다.
• 암호화폐 지갑 프로그램(Exodus, MetaMask, Electrum 등)과 관련된 파일을 찾아 탈취한다.
• Discord, Telegram, Steam 등 주요 애플리케이션의 인증 토큰을 추출하여 추가 계정 탈취를 시도한다.

③ C2 통신

• 수집한 정보를 AES 등으로 암호화한 후 HTTPS 프로토콜을 통해 공격자의 C2 서버로 전송한다.
• 통신 경로는 실행할 때마다 무작위로 생성되며, 트래픽 패턴 분석을 어렵게 만든다.

④ 자체 업데이트 및 확장 기능

• 공격자는 C2 를 통해 추가 모듈을 내려 보내 기능을 확장할 수 있다. (예: 키로깅, 스크린샷 캡처, 파일 업로드)

3) 암호화 및 은닉 기술

• 다단계 암호화(Multi-layer Encryption)
- 악성코드 자체는 여러 단계로 암호화되어 분석을 어렵게 하며, 동적 디코딩을 통해 런타임에만 활성화된다.

• 코드 난독화(Obfuscation)
- API 호출, 문자열, 제어 흐름을 난독화하여 정적 분석 및 시그니처 탐지를 우회한다.

• C2 트래픽 위장
- 정상 HTTPS 트래픽처럼 위장하여 방화벽 및 IDS/IPS 탐지를 회피한다. 일부 변종은 CDN(Cloudflare 등)을 경유하여 C2 를 은닉하기도 한다.

03 기존 방어 수단의 한계

3-1. 스텔스(Stealth) 통신 탐지 실패 사례

최근 발생한 다수의 침해 사고는 기존 보안 솔루션(방화벽, IDS/IPS, EDR, 게이트웨이 기반 탐지 체계)의 한계를 극명히 드러냈다. 특히 스텔스(Stealth) 통신 기반 악성코드인 BPFdoor, Symbiote, LummaC2 는 탐지 회피 기술을 통해 장기간 은닉 활동을 수행하면서도 보안 솔루션의 탐지를 완벽히 우회했다.

1) BPFdoor 탐지 실패 사례

① 2025 년 4 월 대한민국 통신 대기업 해킹 사건

• 대한민국 통신 대기업의 HSS 서버에 침입하여 유심(USIM) 인증정보, IMEI, ICCID 등을 탈취한 공격에 BPFdoor 기반 백도어가 사용된 것으로 분석됨.
• 공격자는 평상시 통신 흔적을 남기지 않다가 매직 패킷을 통해 활성화 후 데이터 탈취를 수행한 것으로 보고됨.

② 2024 년 중동·아시아 통신 인프라 공격

• 중국계 APT 그룹(레드멘션 추정)이 중동, 아시아 지역 통신사업자 대상 장기간 침투에 BPFdoor 변종 사용.
• 침입 후 수개월 동안 은닉 상태를 유지하며 기밀 데이터 탈취.

2) Symbiote 탐지 실패 사례

① 2024 년 브라질 금융권 침해

• 대형 은행의 리눅스 기반 백엔드 서버에 Symbiote 가 설치.
• 사용자 계정 탈취 및 보안 로그 조작이 수개월간 지속됐음.

② 2023 년 북미 에너지 인프라 침투

• SCADA 제어 서버에 침투한 Symbiote 변종이 발견.
• 에너지 거래 기록과 계정 인증 데이터를 변조 시도한 정황이 확인됨.

3) LummaC2 탐지 실패 사례

① 2025 년 초 글로벌 인증정보 대량 유출 사건

- LummaC2 기반 인포스틸러가 다크웹에서 대규모로 유포됨.
- 전 세계 주요 금융사, 기업 포털 사용자 계정 50 만건 이상 탈취.
- 특히 OTP 인증 정보, 암호화폐 지갑 키 정보까지 유출된 것이 확인되어 피해 심각.

② 2024 년 국내 기업 내부망 감염 사례

- 국내 유명 전자상거래 기업 내부 PC 수십 대가 LummaC2 에 감염.
- 고객 개인정보와 내부 인증 서버 접근 토큰이 외부로 유출된 정황이 포렌식 분석에서 확인됨.

이러한 사례들은 전통적인 시그니처 기반 탐지와 포트 중심의 정책 관리 체계, EDR 만으로는 고도화된 스텔스(Stealth)형 통신 위협에 대응할 수 없음을 명확히 보여준다. 특히, 암호화된 C2 트래픽과 커널·라이브러리 수준의 은닉 기술은 기존 보안 수단들의 탐지 범위를 벗어난다.

3-2. 암호화 트래픽 내 위협 탐지의 한계

오늘날 네트워크 통신의 상당 부분이 TLS(Transport Layer Security) 기반으로 암호화되면서, 정보 보호는 강화되었지만 동시에 보안 위협 탐지의 새로운 한계가 드러나고 있다. 특히 공격자는 암호화된 트래픽을 적극적으로 악용하여 기존 보안 체계를 우회하고 있다.

1) 암호화 트래픽 확산 현황

• 2025 년 현재 인터넷 트래픽의 90% 이상이 암호화되어 있다.
• 기업 내부망에서도 이메일, 파일 전송, SaaS 애플리케이션 접근 등 거의 모든 데이터 흐름이 HTTPS, TLS 기반으로 이뤄진다.
• 악성코드 제작자들도 C2 통신, 데이터 탈취 경로를 암호화 채널에 숨기는 것이 기본 전략이 됐다.

2) 기존 보안 솔루션의 한계

구분	내용
방화벽/IPS/IDS	패킷 내용(payload)을 분석할 수 없어, 암호화 트래픽은 포트/프로토콜 수준에서만 제한적으로 제어 가능
프록시/게이트웨이	HTTPS Proxy(SSL Inspection)로 복호화 가능하나, 속도 저하 및 프라이버시 침해 우려로 전면 적용이 어려움
EDR/NDR 솔루션	암호화된 트래픽 자체를 분석하거나 메타데이터(Flow, SNI 등)만을 기반으로 제한적 탐지만 가능

3) 공격자가 암호화 트래픽을 악용하는 방식

• C2 통신 은닉
- 악성코드는 암호화된 HTTPS 를 이용해 명령어를 수신하거나 탈취 데이터를 전송한다.
(예: LummaC2, Cobalt Strike, BazarLoader)

• 악성 파일 다운로드
- 감염된 시스템은 암호화 채널을 통해 추가 악성 페이로드를 다운로드한다.
- 이 과정은 일반 사용자 웹 트래픽과 구별이 어렵다.

• 피싱 사이트 위장
- 피싱 공격자들도 정식 인증서가 적용된 HTTPS 사이트를 구축하여 사용자를 속인다.
(예: Let's Encrypt 무료 인증서 악용)

• 멀웨어 배포 서버 위장
- 공격자는 합법적 도메인(Cloudflare, AWS 등)을 활용해 암호화된 서버를 운영하고, 보안 장비의 도메인 필터링을 우회한다.

4) SSL/TLS 복호화(SSL Inspection)의 적용시 보안 문제

• 속도 및 성능 저하
- 전 구간 복호화를 적용하면 트래픽 분석 부하가 급증하여 사용자 경험 저하, 서비스 중단 위험이 발생할 수 있다.

• 프라이버시 및 법적 문제
- 개인 이메일, 의료정보, 금융 데이터까지 복호화하는 것은 프라이버시 침해 이슈와 법적 제약(예: GDPR 위반) 위험을 초래할 수 있다.

• 기술적 한계
- TLS 1.3 과 QUIC 은 핸드세이크부터 전면 암호화를 적용하기 때문에, 네트워크 중간에 위치한 복호화 장비가 트래픽을 복호화하거나 검사할 수 있는 기존 방식(Man-in-the-Middle Inspection)이 사실상 무력화된다.

5) 메타데이터 기반 탐지의 제약

• SSL/TLS 통신에서 사용 가능한 메타데이터(SNI, JA3, 트래픽 패턴)만으로는 악성 여부를 명확히 판별하기 어렵다.

• 정상 사이트와 악성 사이트 모두 비슷한 트래픽 특성을 보이기 때문에 오탐(false positive)과 미탐(false negative) 문제가 심각하다.

• 예를 들어, 정상적인 클라우드 서비스 통신(예: Google Drive)과, 악성코드가 탈취 데이터를 보내는 HTTPS 통신은 트래픽 양상만 봐서는 거의 구분할 수 없다.

04 네트워크 관점 대응 전략

4-1. 통신 세션 메타데이터 기반 이상 탐지 방안

암호화 트래픽이 보편화된 최신 네트워크 환경에서는 패킷 내용(payload)을 분석하는 전통적인 탐지 기법만으로는 보안 위협을 효과적으로 식별하는 데 한계가 존재한다. 이에 따라, 암호화 여부와 관계없이 네트워크 통신 과정에서 생성되는 통신 세션 메타데이터(session metadata)를 활용하여 이상 행위를 탐지하는 전략이 중요성이 부각되고 있다.

1) 통신 세션 메타데이터의 정의

통신 세션 메타데이터는 개별 세션을 식별하고 특성을 요약할 수 있는 데이터로, 패킷의 실제 내용이 아닌 세션 속성 정보로 구성된다. 일부 항목의 예를 들면 다음과 같다.

주요 메타데이터 항목	설명
Source IP / Destination IP	통신 시작지 및 목적지 IP 주소
Source Port / Destination Port	통신 포트 번호
Protocol	사용된 네트워크 프로토콜 (TCP/UDP/ICMP 등)
세션 지속시간(Duration)	세션이 유지된 시간
송수신 바이트 수(Bytes Sent/Received)	전송된 데이터 크기
송수신 패킷 수(Packets Sent/Received)	전송된 패킷 수
서버 이름 표시(SNI)	TLS 핸드셰이크 시 서버 식별 정보
암호화 핑거프린트(JA3/JA3S)	TLS 핸드셰이크 기반 클라이언트/서버 지문
세션 주기성(Periodicity)	세션 재연결 주기 또는 빈도 패턴

2) 통신 세션 메타데이터 기반 이상 탐지

① 트래픽 특성 기반 탐지

• 비정상 세션 지속시간 감지 ➔ 지나치게 짧거나 비정상적으로 긴 연결을 탐지.
• 비대칭 트래픽 패턴 감지 ➔ 송신량과 수신량이 과도하게 불균형한 세션은 명령 제어(C2) 통신이나 데이터 탈취 징후일 수 있음.

② 포트 및 프로토콜 이상 탐지

• 표준 포트를 사용하지 않는 암호화 트래픽(예: HTTPS 통신이지만 포트 443 이 아님)을 식별.
• UDP 기반 암호화 통신(예: QUIC)을 사용하는 비정상 호스트 탐지.

③ SNI 및 JA3/JA3S 기반 탐지

• TLS 통신 시 SNI 필드가 누락되었거나 비정상 값일 경우 악성 가능성 추정.
• 클라이언트 핑거프린트(JA3) 또는 서버 핑거프린트(JA3S)가 알려진 악성 도구와 일치하는지 비교해 탐지.

④ 주기적 통신(Beaconing) 탐지

• 일정한 주기로 통신을 시도하는 세션은 명령 제어(C2) 통신 징후일 수 있음.
• 세션 간 시간 간격(Time Delta) 분석을 통해 비콘 패턴을 식별.

3) 통신 세션 메타데이터 수집 및 분석 프로세스

① 트래픽에서 통신 세션 메타데이터 추출
(네트워크 미러링, TAP 장비, 스팸 포트 등을 통해 세션 메타정보 수집)

② 정규화 및 저장
(통일된 포맷으로 정리하여 대량 저장 – 예: 로그 서버, 고속 컬럼형 데이터베이스)

③ 기준(Profiling) 구축
(업무 서버, 사용자 그룹별 정상 통신 패턴 수집 및 학습)

④ 이상 패턴 탐지 및 경보 생성
(행위 탐지 규칙 기반 탐지 + 이상 탐지 모델(Machine Learning) 적용)

⑤ 이상 징후 분석 및 대응 조치
(수집된 메타데이터를 기반으로 위협 유무를 신속히 판별하고 조치)

4) 통신 세션 메타데이터 기반 탐지의 기대 효과와 제약사항

구분	내용
기대 효과	암호화 여부에 상관없이 비정상 통신 패턴을 조기에 식별 가능
프라이버시 보호	패킷 내용 복호화 없이 탐지 가능, 개인정보 침해 위험 없음
적용 유연성	클라우드, 온프레미스, 하이브리드 네트워크 모두 적용 가능
제약 사항	- 정상·비정상 경계가 모호할 경우 오탐(False Positive) 발생 가능성 - APT 공격자가 정상 트래픽 패턴을 모방할 경우 탐지 난이도 증가

4-2. 세션 행동 기반 패턴 분석

암호화 트래픽 환경 및 고도화된 스텔스(Stealth) 위협에 대응하기 위해, 단순한 플로우 통계 분석을 넘어 세션 행동(session behavior) 기반 패턴 분석이 중요한 탐지 전략으로 부상하고 있다. 세션 행동 기반 분석은 개별 네트워크 세션이 보이는 다양한 동작 특성을 포착하고, 이를 정형화하여 정상/비정상 패턴을 식별하는 방식이다. 이 접근법은 단일 플로우 특성만 보는 것이 아니라, 세션이 시간에 따라 어떻게 행동하는지, 세션들이 어떤 집합적 양상을 보이는지를 분석하는 데 초점을 맞춘다.

1) 세션 행동 기반 패턴 분석의 핵심 요소

분석 요소	설명
세션 생성 빈도(Session Frequency)	특정 호스트 또는 IP 가 일정 시간 동안 생성한 세션 수
세션 지속시간(Session Duration)	개별 세션이 유지된 시간 분포
송수신 바이트 및 패킷 수 (Byte/Packet Volume)	세션당 송수신 트래픽 양
전송 방향성(Traffic Directionality)	송신과 수신의 비율 변화 (ex. 단방향 vs 양방향 통신)
통신 주기성(Periodicity)	특정 주기(interval)로 발생하는 세션 여부
목적지 다양성(Destination Diversity)	세션이 향하는 목적지 IP/도메인 수
세션 내 이벤트(Embedded Events)	연결 시도 실패율, 세션 재시도, 인증 절차 발생 여부 등

2) 세션 행동 분석 방안

① 세션 단위 시계열 분석

• 개별 호스트 또는 IP 주소 기준으로 세션 수, 바이트 전송량, 평균 세션 길이 등의 지표를 시간 순으로 기록하고 ➔ 시간별 패턴 변동을 탐지한다.
• 정상 업무 흐름과 비교하여 ➔ 과도한 세션 급증, 트래픽 피크, 비정상 지속시간 세션 발생 등을 조기에 감지할 수 있다.

② 다차원 메타데이터 집계 및 분포 분석

• 송수신량, 패킷 수, 지속시간, 목적지 포트를 다차원적으로 집계한 후,
• 통계적 이상치(Outlier)를 검출하거나, 정상 분포에서 벗어난 세션 집합을 탐지한다.
• 예를 들어, 통상 1 분 내 종료되는 웹 세션에서 10 시간 이상 지속되는 세션이 발견될 경우 이상 징후로 판단한다.

③ 주기성(Beaconing) 및 재시도 패턴 탐지

• 일정 간격으로 반복 연결하거나, 실패 후 재시도하는 패턴이 포착되면 명령 제어(C2) 통신 또는 자동화된 공격 스크립트 가능성을 의심할 수 있다.
• 세션 간 인터벌(Interval) 분포를 분석하여 비정상적 주기성을 탐지한다.

④ 통신 경로 및 목적지 행동 프로파일링

• 정상적인 세션은 목적지 IP/도메인 군이 일정하고 통신 패턴이 예측 가능하다.
• 반면, 공격자는 다수의 목적지로 분산 연결하거나, 예상치 못한 포트/프로토콜을 사용할 수 있다.
• 이탈 정도를 수치화하여 이상 패턴을 감지한다.

3) 세션 행동 데이터 수집 및 처리 방안

① 네트워크 관문 또는 센서에서 세션 메타데이터 수집

• 수집 항목: 5-Tuple, 지속시간, 송수신 바이트, 패킷 수, TLS 정보 등.

② 고속 메타데이터 저장 및 쿼리 최적화

• 대용량 세션 로그를 실시간 또는 준실시간으로 집계할 수 있는 구조 필요.
• 집계 및 필터링에 최적화된 분석형 데이터베이스 사용.

③ 시간/행동 기준 데이터 모델링

• 호스트/IP 별 세션 행동 이력을 시계열 및 집계 형태로 저장.
• 세션 특성 기반 통계 지표(평균, 분산, 백분위 등) 자동 생성.

④ 이상 행동 탐지 로직 적용

• 룰 기반, 이상치 감지, 머신러닝 기반 모델 등을 활용하여 이상 행동 탐지.
• 이상 탐지 결과는 추가 세션 상세 분석 및 경보(Alarm)로 연계.

4) 기대 효과 및 주의사항

구분	내용
기대 효과	단일 세션 특성 분석보다 더 정교한 이상 징후 탐지 가능
장점	패킷 복호화 없이 암호화 트래픽 내부의 위협 행위 식별 가능
주의사항	- 정상 서비스의 복잡성에 따른 오탐 가능성 - 통상적인 네트워크 동작의 변동성을 감안한 기준선 설정 필요

05 차세대 NDR 기반 스텔스(Stealth)위협 대응전략

디지털 전환 가속화와 복합화된 사이버 위협 환경에서, 기존 시그니처 기반 보안 체계는 심각한 한계에 직면하고 있다. 특히 암호화 트래픽 비율 증가, 고도화된 스텔스(Stealth)형 공격, 내부망을 통한 수평 이동 공격(lateral movement) 등을 고려할 때, 보다 정교하고 지속적인 위협 탐지를 지원하는 차세대 네트워크 탐지 및 대응(Network Detection and Response, NDR) 프레임워크가 필수적이다.

차세대 NDR 기반 위협 탐지 및 대응 프레임워크는 네트워크 전 구간에서 실시간으로 메타데이터를 수집, 분석하고, 이상 행위 기반 탐지를 수행함으로써 보이지 않는 위협을 가시화하는 것을 목표로 한다.

5-1. 차세대 NDR 기반 위협 탐지 및 대응 프레임워크

1) 탐지 프레임워크

항목	처리 메커니즘
데이터 중심 수집	전체 패킷이 아닌, 경량화된 통신 세션 및 통신 메타데이터 중심 수집
구조화된 분석	비정형 패킷 대신 정형화된 통신 세션 데이터를 중심으로 분석
고속 대용량 처리 (유사 실시간 위협 탐지)	초당 수십만 세션 생성 환경을 감안한 고성능 저장/쿼리 아키텍처
실시간 이상 징후 탐지	실시간 행위 탐지 규칙 및 행동 기반(anomaly-based) 탐지의 병행 운영
확장성 및 유연성	멀티사이트, 멀티센서 환경을 고려한 분산 구조 적용

2) 주요 구성 요소

① 네트워크 트래픽 수집 및 통신 세션화

• L2/L3 미러링, 가상 TAP(VTAP), 클라우드 네이티브 트래픽 미러링 등을 통해 네트워크 트래픽을 수집한다.
• 수집한 트래픽에서 세션 단위로 재구성하고, 5-Tuple 정보, 세션 지속시간, 바이트 및 패킷 수, TLS 관련 정보 등 구조화된 통신 세션 메타데이터를 생성한다.

② 세션 메타데이터 저장 및 관리

• 초당 수만 건 이상의 세션 메타데이터를 고속으로 처리할 수 있도록 대규모 병렬 처리 및 컬럼 기반 저장 구조를 채택한다.
• 시간 순서에 따른 데이터 삽입 및 고속 조회를 지원하여, 실시간 분석과 장기 추적을 모두 가능하게 한다.

③ 실시간 이상 탐지 엔진

• 통신 세션 메타데이터를 기반으로 실시간 행위 탐지 규칙 기반 탐지(known TTPs)와 이상 행동 기반 탐지(unknown threats)를 병행한다.
• 주요 탐지 로직 예시:
- 비정상 포트/프로토콜 사용
- 비정상 세션 지속시간
- 주기적 Beacon 통신 탐지
- TLS SNI 누락 또는 비정상 JA3 핑거프린트 탐지
- 송수신 트래픽 비대칭성 이상 징후

④ 위협 인텔리전스 연계

• 외부 위협 인텔리전스(Threat Intelligence)와 통합하여, 수집된 세션 메타데이터와 상호 교차 매칭을 수행한다.
• 악성 IP, 도메인, JA3 시그니처 등과의 매칭 결과를 통해 탐지 정확도를 향상시킨다.

⑤ 대응 및 연계 인터페이스

• 이상 세션 탐지 시 즉각적으로 경보를 생성하고, EDR, SOAR 등 외부 보안 시스템과 연동하여 자동화된 대응 조치를 지원한다.
• 예를 들어, 탐지된 악성 통신 세션 차단, 사용자 세션 강제 종료, 포렌식 세션 덤프 수행 등을 연계할 수 있다.

3) 차세대 NDR 의 기대 효과

구분	설명
암호화 트래픽 탐지 강화	패킷 복호화 없이 세션 행동 기반 이상 탐지 가능
실시간 가시성 확보	네트워크 전구간의 세션 흐름을 실시간 가시화
스텔스(Stealth) 위협 조기 감지	C2 비콘, lateral movement 등 스텔스(Stealth) 공격 탐지 가능
대응 속도 향상	탐지-분석-대응 자동화 연계를 통한 신속 대응 가능
운영 비용 절감	전체 패킷 저장 부담 없이 경량화된 통신 메타데이터 기반 분석 운영

06 차세대 NDR 에서 스텔스형 위협 탐지 및 방안
– BPFdoor, Symbiote, LummaC2 대응 전략

스텔스(stealth)형 위협은 기존의 시그니처 기반 탐지 체계를 우회하며, 통신 세션 내 이상 징후를 교묘하게 은닉한다. 이에 따라 차세대 NDR 은 통신 세션 메타데이터를 실시간으로 분석하는 TTP 탐지 모듈과 대규모 세션 데이터의 정밀 분석 체계를 병행하여 운영해야 한다. 특히 BPFdoor, Symbiote, LummaC2 와 같은 위협은 각각 고유한 통신 특성과 패턴을 가지며, 이를 조합하여 탐지 로직을 구성할 필요가 있다.

6-1. 실시간 TTP 탐지 모듈을 통한 세션 기반 위협 탐지 방안

① BPFdoor 대응: 스텔스(Stealth) 백도어 통신 탐지 방안

• 포트리스(portless) 통신 탐지
- 세션이 일반적인 TCP 3-way 핸드셰이크 없이 비정상적으로 수립되는지 확인한다.
(예: SYN 없이 ACK 로 응답하거나, 특정 소량 패킷 이후 연결이 활성화)

• 비표준 패킷 플래그 조합 감지
- 정상 세션과 다른 희귀 플래그 조합(SYN+FIN 등)을 가진 트래픽을 식별한다.

• 수신 후 Outbound 통신 활성화 탐지
- 내부 서버가 외부에서 소량 트래픽을 수신한 직후, 비정상적인 Outbound 세션을 생성하는지 모니터링한다.

② Symbiote 대응: 스텔스(Stealth) 프로세스 기반 위협 탐지 방안

• 프로세스/서비스 불일치 감지
- 서버 내 정상 프로세스명과 세션이 연결된 포트/프로토콜 간의 상관성을 분석하여, 불일치 사례를 식별한다.
(예: SSH 프로세스가 HTTP 통신을 수행하는 경우)

• 정상 통신 프로파일 이탈 분석
- 정상 서버 역할에 비추어 예상치 못한 외부 통신(예: DB 서버가 외부 웹사이트로 연결)을 탐지한다.

• 비정상 트래픽 패턴 감지
- 일정 주기로 반복되는 비정상 트래픽 재시도나 비대칭 송수신 트래픽 양상을 분석한다.

③ LummaC2 대응: 암호화된 정보 탈취 통신 탐지 방안

• 주기적 통신(Beaconing) 패턴 탐지
- 통신 세션 간 발생 간격(Time Delta)을 분석하여, 일정한 주기로 세션을 생성하는 패턴을 포착한다.

• TLS 핸드셰이크 이상 탐지
- 세션 메타데이터 내 JA3/JA3S 핑거프린트 값을 분석하여, 정상 브라우저와 다른 특이한 암호화 핸드셰이크를 식별한다. 또한, TLS SNI 필드가 비어 있거나 비정상 도메인 이름을 사용하는 세션을 주목한다.

• 송수신 트래픽 비대칭성 탐지
- 세션 송수신 바이트 비율을 분석하여, 주로 데이터가 일방향으로 전송(Exfiltration)되는 패턴을 탐지한다.

6-2. 대규모 세션 데이터 분석 기반 심층 탐지 방안

실시간 TTP 탐지로 놓칠 수 있는 스텔스(Stealth) 또는 장기 지속형 위협을 보완하기 위해, 대규모로 저장된 세션 메타데이터를 주기적으로 분석하여 위협을 추적한다.

• 비정상 세션 연결 패턴 분석
- 세션 생성 빈도, 목적지 다양성, 포트 사용 이력 등을 종합 분석하여 평상시 패턴과 다른 비정상 연결을 식별한다.

• Beaconing 패턴 대량 분석
- 동일 Source IP 가 유사한 간격으로 다수의 세션을 생성하는 경우 이상 통신으로 분류한다.

• TLS 통신 프로파일 이상치 탐지
- 수집된 TLS 통신의 핸드셰이크 프로파일(JA3/JA3S, TLS 버전, Cipher Suites 등)을 정상 프로파일과 비교하여 이탈 여부를 판단한다.

• 단기/장기 세션 비율 분석
- 정상 업무에 비해 지나치게 짧거나 긴 세션 비율이 비정상적으로 증가하는 경우 이상 징후로 인식한다.

6-3. 통합 위협 탐지 체계 구성 방안

구성 요소	설명
실시간 TTP 탐지 모듈	네트워크 흐름 중 이상 징후를 즉시 포착하여 초기 경고 생성
대규모 세션 데이터 심층 분석	저장된 세션 메타데이터를 주기적으로 검토하여 스텔스 위협 추적
경보 및 대응 시스템 연계	탐지된 이상 세션 기반으로 자동화된 대응 프로세스(SOAR, NAC) 연동

07 결론

최신 사이버 위협 환경은 비약적으로 고도화되고 있으며, 특히 BPFdoor, Symbiote, LummaC2 와 같은 스텔스(Stealth)형 악성코드의 부상은 전통적 보안 체계의 한계를 명확히 드러냈다.

기존의 경계선 방어만으로는 이러한 고도화된 위협을 탐지하고 대응하기에 부족하며, 암호화 통신 환경에서는 더욱 심각한 가시성 저하가 발생하고 있다.

이에 따라 본 기술보고서에서는 비암호화 및 암호화 트래픽을 통합적으로 수집, 분석, 대응할 수 있는 차세대 NDR 프레임워크를 제시하였다. 특히, 세션 메타데이터 기반 실시간 TTP 탐지 모듈과 대규모 세션 데이터 분석 체계를 결합함으로써,

- **포트리스 백도어 통신**
- **은닉형 루트킷 기반 비정상 통신**
- **암호화된 탈취 통신**

등 다양한 스텔스(Stealth) 위협에 효과적으로 대응할 수 있는 방안을 구체적으로 기술했다.

이러한 대응 전략은 단순한 패턴 매칭이 아닌,

- **세션 행동 패턴 분석**
- **통신 주기성 탐지**
- **TLS 핸드셰이크 프로파일링**
- **정상 프로파일 이탈 탐지**

등 다차원적인 이상 행위 분석 기법을 중심으로 구성됐다.

또한, 암호화된 트래픽 환경에서도 프라이버시를 침해하지 않고 위협을 탐지할 수 있도록, 구조화된 세션 메타데이터 중심의 경량화된 분석 체계를 적용함으로써 실제 운영 환경에서도 높은 성능과 확장성을 보장할 수 있다.

결론적으로, 차세대 NDR 은 더 이상 선택이 아니라 필수이며, 지능화·은닉화·암호화되는 위협에 대응하기 위해서는 실시간 TTP 탐지와 대규모 데이터 기반 심층 분석을 유기적으로 통합한 방어 체계가 반드시 필요하다.

앞으로도 스텔스(Stealth)형 위협은 지속적으로 진화할 것이므로, 본 보고서에서 제시한 통합 대응 전략을 기반으로 탐지 체계의 지속적인 고도화와 자동화 대응 체계 구축이 병행되어야 할 것이다.

씨큐비스타

씨큐비스타는 20 여년간의 네트워크 보안 기술개발 노하우와 실시간 트래픽 처리 및 머신러닝 기반 원천기술을 보유 한 사이버 보안 소프트웨어 전문기업으로, 아시아 최초 월드클래스 네트워크 위협 헌팅(NTH) 플랫폼을 개발 및 보급하고 있는 보안업계 선도기업이다.

씨큐비스타는 NDR·FDR 원천기술 기반 실시간 네트워크 위협헌팅 시스템 '패킷사이버'(PacketCYBER v2.0)와 국내 최초 패시브 방식 IoT 보안솔루션 'IoTCYBER v2.0' 등 차별화된 보안솔루션으로 보안시장을 선도하고 있다.

씨큐비스타의 차세대 NDR·FDR 보안솔루션 'PacketCYBER v2.0'은 네트워크 탐지 및 대응(NDR) 유형 최초로 2024 년에 국가용 보안가능확인서 인증을 획득했으며, 전덕조 대표는 네트워크 위협헌팅, 네트워크 포렌식, 악성코드 분석 전문가로 세계 2 대 침해사고 대응 센터 SANS Institute GSEC 한국 멘토 등을 지낸 보안업계 스페셜리스트로 손꼽힌다.

패킷사이버

'패킷사이버'(PacketCYBER v2.0)는 기존 보안에서 놓친 위협에 의해 '모든 시스템이 해킹 됐다'는 전제로 시스템 전반에서 능동적으로 해킹 공격 행위를 찾아 제거하는 업계 최고 수준의 강력한 NDR·FDR 기반 보안솔루션이다.

'패킷사이버'는 美 국가안보국이 발표한 '해커 조직의 표적 침입 6 단계' 중 초기 감염, 추가 공격 도구 설치 단계를 집중 탐지하며, 고도화된 악성코드 탐지 엔진 'RIMA'를 탑재해, 정찰, 명령·제어(C&C) 서버 접속, 내부망 확산, 정보 유출 등 네트워크 이상 행위를 실시간으로 탐지하는 것이 특징이다. FDR 기술을 접목시켜, 모든 파일을 추출·분석·탐지하는 등 '파일'이 아닌 통신 이상만 탐지하는 국내외 기존 NDR 과는 차별화된 네트워크 위협 탐지 및 대응(NDR) 플랫폼이다.

이 제품은 한국과 일부 아시아 국가의 공공기관 및 금융기관 등에 채택돼 최고의 보안솔루션으로 인정받고 있으며, 고도화된 지능형 공격에 대비한 '수집·탐지·분석·헌팅·대응' 프로세스를 통해 트래픽을 분석, 효과적인 네트워크 위협 헌팅 대응 솔루션을 제공하는 차세대 NDR 보안관리 플랫폼이다. 소프트웨어 품질인증 (GS 인증) 1 등급 획득 및 조달 상품에 등록됐으며, 네트워크 탐지 및 대응(NDR) 유형으로는 국내 최초로 보안기능확인서 인증을 획득했다.

HTTP·DNS·SSL·파일 전송 메타데이터를 분석해 다운로드된 악성 파일의 크기, 유형 및 원본 URL, 악성 다운로드 시도 여부를 확인할 수 있고, 랜섬웨어가 통신하기 위해 접촉한 C&C 서버의 도메인과 IP 주소를 확인 가능하며, 탐지를 회피하기 위해 암호화된 데이터의 관련 이상징후를 탐지할 수 있는 강력한 보안솔루션이다.

CQ VISTA

네트워크 위협헌팅
보안솔루션 전문기업

CQVISTA

CQVISTA
씨큐비스타

- 02-565-0236
- sales@cqvista.com
- WWW.CQVISTA.COM
- 경기도 성남시 분당구 판교로 255번길 9-22, 5F 511호.