2023.9.14.

위협 헌팅 전문 기업

CQ VISTA preventive network security

씨큐리포트

국가 지원 해커그룹 및 대응방안

> **해커그룹, 그들은 누구인가**
> **해커그룹 공격 방법 및 대응방안**

CQVISTA
씨큐비스타
T. 02-565-0236
www.cqvista.com
경기도 의왕시 성고개로 53, 에이스청계타워 822호

01. 국가 차원의 지원을 받는 해커그룹, 그들은 누구인가?

국가의 지시에 따라 또는 국가의 지원을 받아 컴퓨터 네트워크 작업을 수행하는 그룹으로서, 고도로 숙련되고 자 금이 풍부하다는 특징이 있으며, 타국 정부 기관 및 중요 인프라 제공업체와 같은 높은 가치의 표적을 노리는 경 향이 있다. 이들의 공작 방식에는 간첩 행위와 사보타주(Sabotage: '비밀 파괴 공작'이란 뜻으로 비밀리에 적의 산업 시설이 나 직장에 대한 직접적인 시설 파괴를 행하는 것을 의미)가 포함되는 경우가 많으며 일반적으로 정교한 도구와 기술을 사용하여 대상 시스템에 접근한다.

그들은 자국 정부를 위해 일하는 조직이며 정부, 조직 또는 개인을 방해하거나 침해하여 귀중한 데이터나 정보에 접근하고 국제적으로 중요한 사건을 일으킬 수 있다.

02. 국가 지원을 받는 해커 그룹의 공격 방법

미국 국가 안보국 (NSA: National Security Agency) 산하의 Top 해커 그룹에 따르면, 그들은 네트워크를 구축하고 운영 하는 사람들보다도 더 네트워크를 상세히 파악함으로써 공격에 항상 성공한다고 밝혔다. NSA 산하의 Top 해커 그룹은 다음의 6단계를 통하여 자신들의 목적을 달성한다고 밝힌 바 있다. 그들의 방법을 참고하면 보다 상세히 국가 차원의 지원을 받는 해커 그룹의 공격 방법을 파악할 수 있다.

1) Initial Reconnaissance (초기 정찰)

[공격 방법]
해커는 호스트 및 운영 체제를 식별하고 취약점에 대한 조사를 수행하기 할 수 있는 수많은 네트워크 스캔 도구를 보유하고 있는데, 해커가 취약한 OS, 클라이언트 데이터베이스, 민감한 데이터를 처리하기 위한 기술을 식별할 수 있다면 이미 문제가 심각한 상황이다.

[대응 방안]
최소한 실행되고 있는 스캐닝 방법을 탐지 또는 방지할 수 있어야 한다. 중요 자산과 자산에 접촉하는 사람을 지속적으로 모니터링 하기 위한 시스템, 기술 및 절차를 확보해야 한다. 내부 네트워크내의 시스템간 통신("east-west)을 지속적으로 모니터링할 수 있는 능력을 확보해 해커보다 네트워크를 상세히 파악해 관리하는게 특히 중요하다.

2) Initial Exploitation (초기 익스플로잇)

[공격 방법]

NSA에 따르면 Zero-day 익스플로잇과 새로운 네트워크 침해 기법의 중요성은 지나치게 과장되어 있으며, 실제로는 대부분의 침입은 2가지 초기 공격 벡터 중 하나를 이용하여 공격하는데, 첫째 이메일 첨부파일 및 클릭 유도 와, 둘째 악의적인 웹사이트 접속을 통한 불법 컨텐츠를 실행하는 방법을 대부분 사용한다고 밝혔다.

[대응 방안]

네트워크를 위험에 빠뜨리는 내부 네트워크 트래픽 및 계정 사용을 모니터링 하여야 하며, 이미 감염된 사용자 계정에 의한 의심스러운 행위를 모니터링해야 한다고 밝히고 있다.

3) Establish Persistence (지속성 확립)

[공격 방법]

해커가 일단 네트워크 침입에 성공하면, 추가적인 백도어를 생성하여 보다 강력한 발판을 다지며 일반적으로 탐지나 축출을 어렵게 만든다. 지속성은 더 높은 권한에 대한 인증 정보(계정)를 탈취하고 삭제해도 재설치 되는 악성코드를 이용할 수 있다.

[대응 방안]

'정상 네트워크 행위'를 구성하는 사용자, 세그먼트, 업무 구역을 파악함으로써, 해커가 **보안요원들에게** 들키지 않고 장시간 인가**되지 않은** 접속을 유지하는 것을 어렵게 만들어야 하며, 애플리케이션 및 사용자 행위에 대한 지속 적 모니터링을 통하여 베이스라인을 수립하여 이를 기반으로 **네트워크를** 상세히 모니터링 해야 한다.

4) Install Tools (공격 도구 설치)

[공격 방법]
공격자는 시스템에 소프트웨어 도구를 설치함으로써 데이터를 유출하거나 또는 공격 행위를 확고히 하는데 도움 이 될 수 있는 추가적인 소프트웨어를 다운로드 하도록 하는 것이 일반적이다.

[대응 방안]
파일 평판 서비스를 활용하면, 알려진 실행파일에 대한 클라우드 기반 데이터베이스를 이용하여 해당 프로그램이 스팸, 악성코드, 피싱 행위를 하는 지를 검사할 수 있다. 일부 평판 서비스는 특정 소프트웨어가 호출하는 도메인 이름도 확인하기 때문에 클라이언트가 특정 도메인을 호출하는 경우 멀웨어 "C&C"(명령 및 제어)일 수 있다는 경 고를 확보할 수 있다. NSA는 파일 평판 및 도메인 평판을 활용할 것을 권고하고 있다.

5) Move Laterally (내부망 이동)

[공격 방법]
공격자는 침입하기 쉬운 지점에 우선 침입한 후, 민감한 네트워크 공유 또는 데이터베이스로 이동하기 때문에 네트워크는 언제든지 침해될 수 있다고 생각하여야 하며, 따라서 네트워크에서 의심스러운 측면 이동(Lateral Mov.)을 탐지할 수 있어야 한다.

[대응 방안]
이미 네트워크가 침해되었다고 가정하고, 침입자가 네트워크 내에서 무엇을 하는지 파악 알 수 있어야 공격자를 방해할 수 있는데, 특히 내부 동서(East-West)간의 트래픽을 감시하는 것이 중요하다.

6) Collect, Exfil, and Exploit (수집, 유출 및 추가 해킹)

[공격 방법]
이 단계까지 진행되었다면 이미 사고가 발생한 상황이므로 보안 담당자가 할 수 있는 것은 거의 없다. 하지만 이미 어려운 상황이지만 포기할 수는 없다.

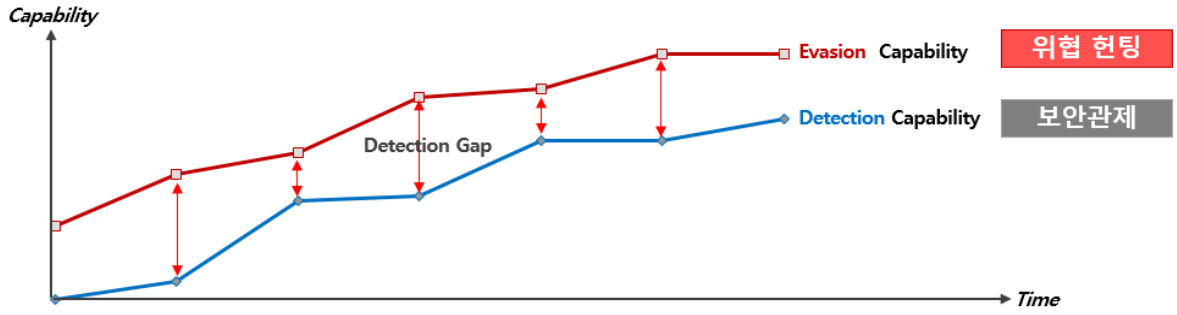
[대응 방안]
이미 침해 사고를 당한 상황보다 더 악화될 수 있으므로 대응 계획이 수립이 필요하다. 데이터 손상, 데이터 조작, 데이터 파괴를 어떻게 처리할 것인가에 대한 사전계획 수립을 통하여 피해를 최소화 해야 한다.

또 실시간으로 네트워크 활동을 모니터링하여 해커가 이용하고 있는 목표 시스템 및 대상을 파악하여야 한다. 특히, 해커가 노릴 만한, '중요 자산'에 접근을 실시간에 상세히 모니터링함으로써 해커의 접근을 잠재적으로 차단하여야 한다.

지능형 해커의 네트워크 침입 과정을 요약하면, 2) 및 4) 단계는 악성코드 탐지와 관련이 있으며, 1), 3), 5) 및 6) 단계는 네트워크 통신 세션 분석과 관련이 있다. 즉, 효과적으로 기존 보안관제에서 놓칠 수 있는 위협을 관리하기 위해서는 2) 및 4) 단계 악성코드 위협 탐지를 보강할 필요가 있으며, 1), 3), 5) 및 6) 단계의 네트워크 통신 세션을 고속으로 정확하게 분석할 필요가 있다.

03. 국가지원 해커그룹, 통합보안관제로 관리할 수 없을까?

정교한 위협은 자동화된 사이버 보안 및 보안 관제를 우회할 수 있다. IBM에 따르면 자동화된 보안 도구들 및 Tier1~2 보안 운영 센터(SOC) 보안관제 요원들이 약 80%의 위협은 처리할 수 있지만, 나머지 20%는 처리하기 힘들다. 즉 기존 보안관제 방법으로는 **최선을 다한다면 최대 80%의 위협을 관리할 수 있으나**, 정교한 20% 위협 및 공격 행위는 관리**하기 힘들다**.



04. 기존 보안이 처리할 수 없는 20%에 대한 위협 관리

위협 대응 측면에서 사이버보안은 공격자의 유입 경로를 파악하는 일과 함께 잠복기에 있는 위협의 진행과 흔적을 사전에 파악, 제거하고, 보안 사고 발생 또는 징후를 파악한 후에도 잔여 흔적과 잠복기에 해당하는 여러 징후들을 파악하여 선제적으로 대응하는 것이 중요하다.

Wikipedia에 따르면 위협 헌팅의 정의는 '기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 능동적이고 반복적으로 검색하는 프로세스'이다. "잠재적인 위협에 대한 경고가 발생하거나 사고가 발생한 후에 조사를 수행하는 방화벽, 침입탐지시스템 (IDS), 멀웨어 샌드박스 및 SIEM 시스템 등과 같은 기존 보안관리 방법과는 대조적이다" 라고 밝히고 있다. 즉, 기존 보안방법으로는 관리할 수 없는 20%의 위협과 기존 보안관제에서 인지할 수 없는 현재 진행 중인 침해 활동을 능동적으로 탐지하여 관리하기 위한 방법이다.

즉, 보안관제에서 놓치는 20%의 위협을 피해가 발생하기전에 탐지하여 대응하기 위한 위협 헌팅 활동을 수행하여야 하는데, 위협 헌터들은 보안 관제요원들이 사용하는 도구와는 완전히 다른 별도의 풍부한 네트워크 데이터 및 엔드포인트 데이터를 제공하는 도구가 필요하다.

[네트워크 기반 데이터]

네트워크 기반 데이터는 여러가지가 있을 수 있다. 일단은 탐지 이벤트는 보안 관제에서 SIEM을 기반으로 이미 관리하고 있으며, 탐지 이벤트는 연속적인 데이터가 아니라 이산적(discrete) 데이터이다. 즉, 다수의 보안솔루션이 탐지한 침해 징후들만 이벤트로 만들어지기 때문에 탐지하지 못한 침해 징후는 이벤트로 생성되지 않으므로 위협 헌팅에는 크게 도움이 되지 않는다.

효과적인 위협 헌팅을 위해서는 탐지한 침해 징후들과 탐지하지 못한 침해 징후를 모두 포함하는 연속적(continuous)인 데이터가 필요하다. Netflow는 연속적인 데이터이기는 하지만 전송 계층 세션 데이터에 대한 통계 정보로서, 보안 요원에게는 충분한 데이터 및 문맥을 제공하지는 못한다.

풀 패킷(Full Packet) 정보는 데이터 충실도 측면에서는 가장 유리한 방식이지만 높은 저장 비용과 더불어 분석에 많은 노력과 시간이 소요되는 문제가 있다. 따라서 '기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 능동적이고 반복적으로 검색하는 프로세스' 인 위협헌팅 수행목적으로는 활용하기 힘들다.

따라서 위협 헌팅 목적으로 가장 유리한 정보는 양방향 전송 및 응용 계층의 통신 세션 정보와 유/출입 되는 모든 파일 정보이다. 즉, 응용 계층의 세션 정보, 컨텐츠 정보, 인덱스 정보를 기반으로 고속 분석이 가능하며, 보안 요원에게 문맥과 더불어 필요한 정보를 제공할 수 있으며 고속의 교차 세션 분석이 가능하므로 '기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 능동적이고 반복적으로 검색하는 프로세스' 인 위협 헌팅에 가장 유리한 정보이다.

[엔드포인트 기반 데이터]

엔드포인트 관점에서는 프로세스 실행 데이터, 레지스트리 접근 데이터, 파일 데이터, 네트워크 통신 데이터 및 파일 사용 빈도 등의 정보가 필요하다.

프로세스 실행 데이터는 특정 호스트에서 실행되는 프로세스에 대한 정보와 프로세스 실행과 관련된 핵심 메타 데이터로 명령 및 인자와 프로세스 파일이름 및 ID를 포함하여야 한다.

레지스트리 접근 데이터는 키 및 값 메타 데이터를 포함하는 레지스트리 오브젝트와 관련된 데이터가 필요하다.

파일 데이터는 로컬 호스트에 저장된 파일 및 아티팩트에 대한 정보가 필요하다. 즉, 파일 생성 및 수정 시각, 크기, 유형 및 저장 위치 정보가 필요하다.

엔드포인트 네트워크 통신 데이터는 네트워크 연결을 수행하는 프로세스의 부모 프로세스를 식별하는 것이 필요하며, 파일 빈도 데이터는 사용자 환경에서 해당 파일이 얼마나 일반적으로 사용하는 파일인가에 대한 정보가 필요하다.

05. 국가 지원을 받는 해커그룹 대응 방안

네트워크 관점 데이터 및 엔드포인트 관점 데이터가 취합되어 있더라도 위협 헌팅이 용이한 것은 아니다. 위협 헌터는 보안 위협 동향 등에 대해서 정통하여야 하며, 분석 도구 개발능력 보유 등 고급인력이지만, 현실적으로는 보안 전문인력은 매우 부족하며, 특히 전문성 있는 보안 인력은 찾아보기 힘든 실정이다. 위협 헌팅의 가장 기초적인 단계는 타 기관이 만든 위협 헌팅 절차를 준수하는 것이다. 그러나 타 기관이 만든 위협 헌팅 절차를 준수하는 것은 예산 문제, 인력 문제 등으로 인하여 실현 불가능에 가깝다.

이러한 위협 헌팅을 단순화/자동화하는 것이 필요한데, MITRE의 ATT&CK는 선도적인 EDR 솔루션에서 일부 구현하고 있다. MITERE ATT&CK는 유용하지만 방대하며, 주로 단말 관점에서 공격자 TTP를 다루고 있다. 따라서 선도적인 EDR 도입 및 운영을 통해서 MITERE ATT&CK에서 제시하는 엔드포인트 관점에서의 공격자 TTP의 일부를 자동으로 탐지할 수 있다.

하지만 MITRE ATT&CK는 엔드포인트 관점이므로 네트워크 관점에서의 위협 헌팅에는 적용하기 어려우므로, 별도의 절차가 필요하다.

유용한 네트워크 관점의 위협 헌팅 방안은 앞서 언급한 미국 국가 안보국(NSA)의 6단계 해킹 플레이 북이며, 일부 선도적인 NDR에서 이러한 공격자 TTP(Tactics, Techniques & Procedure) 탐지를 제공하고 있다.

효과적인 위협 헌팅을 위해서는 네트워크 기반 탐지 및 대응과 엔드포인트 기반 탐지 및 대응 솔루션을 동시에 활용하여야 하며, 위에서 언급한 '풍부한' 데이터를 제공하는지 여부와, 고속 분석이 가능한지 여부, 그리고 TTP에 대한 자동화된 분석을 얼마나 지원하는 지 여부 등을 확인하여야 한다.

이러한 도구들을 잘 활용하여 능동적이고 적극적인 위협 헌팅 활동을 수행함으로써 기존 보안관제에서 놓치는 20% 위협, 즉 국가 지원을 받는 해커의 공격을 관리할 수 있을 것이다. (끝)

◆ 씨큐비스타

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

최근 차세대 네트워크 위협 헌팅 플랫폼 '패킷사이버 v2.5'를 발표해 보안업계의 다크호스로 급부상하고 있다.
전덕조 대표는 네트워크 위협헌팅, 네트워크 포렌식, 악성코드 분석 전문가로 세계 2대 침해사고 대응 센터 SANS Institute GSEC 한국 멘토 등을 지낸 보안업계 스페셜리스트로 손꼽힌다.

◆ 패킷사이버

'패킷사이버'(PacketCYBER)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 6단계' 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 유 출 등 네트워크 이상 행위를 실시간으로 탐지하는게 특징이다. 최근 FDR 기술을 접목시켜, 모든 파일을 추출/분석· 탐지하는 등 '파일'이 아닌 통신 기록만 탐지하는 국내외 기존 NDR과는 차별화된 네트워크 위협 탐지 및 대응(NDR) 플랫폼이다.

이 제품은 한국 및 일본의 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 대 응 솔루션을 제공하는 차세대 NDR 보안관리 플랫폼이다. 소프트웨어 품질인증(GS인증) 1등급 획득 및 조달 상품에 등록됐다.

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 IP주소를 확인 가능하며, 탐지를 회피하기 위해 암호화된 데이터의 관련 이상 징후를 탐지할 수 있는 강력한 보안 솔루션이다.

2023.9.14.

네트워크 기반 위협헌팅
보안기술 전문기업

CQVISTA
씨큐비스타
T. 02-565-0236
www.cqvista.com
경기도 의왕시 성고개로 53, 에이스청계타워 822호