네트워크 현황인지를 통한 은닉공격 탐지

커넥텀® 기업망 내부의 은닉공격 탐지 장치

(주)나루씨큐리티 김혁준

소음과 신호라는 책에서 저자인 네이트 실버[1]는 정밀과 정확의 차이점을 다음과 같이 말하였다. 정확한 예측으로 둔갑한 정밀한 예측은 우리를 우롱하고 결국 잘못된 곳에 투자를 결정하게 한다. 이는 비단 저자가 말하고자 한 경제학의 영역 뿐 아니라 진화하는 공격에 올바른 대응책을 제시하지 못하는 정보보호 영역에도 적용되는 사실이다.

사이버 영역에서 발생되는 공격이 빠르게 진화하면서 방화벽, 침입차단장치, 샌드박스 등 수 많은 정보보호 장치들이 설치되고 있으나 이러한 시도들은 너무나 많은 노이즈를 생성하여 운영중인 방어체계를 우회하여 내부망에 은닉하고 있는 공격자를 효과적으로 탐지하지 못하고 있다.

(주)나루씨큐리티는 현재의 방어체계가 진행 중인 공격을 탐지할 수 없다는 것은 글로벌 기업, 공공기관 등 최고 수준의 정보보호 체계를 운영하고 있는 국내외 다수의 주요 기관의 내부망 통신 점검을 통해 증명해 왔으며 수년간의 네트워크 실망점검을 통해 축적된 경험과 기술을 타겟형 침해사고탐지 플랫폼인 **커넥텀®**에 적용하였다.

커넥텀®은 네트워크 기반의 은닉공격 탐지 장치로 현황점검, 위협인지 및 사고추적 기능을 통해 기존의 예방체계를 우회하여 오랜기간 잠복하며 내부정보 유출, 시스템파괴 등의 타겟공격에 수반되는 공격자의 행위를 정밀하고 정확하게 탐지하는 장치이다.

커넥텀®은 내부망에서 발생하는 모든 네트워크 트래픽을 분석하여 초기침해, 명령제어채널구성, 내부망이동, 정보유출 과정에서 발생하는 침해징후를 탐지하며 이러한 일련의 과정을 시간의 흐름에 따라 추적하는 기능을 제공한다. 본 백서에서는 **커넥텀®**의 주요 기능 및 실망에서 적용된 분석사례의 소개를 통해 제품의 기능과 성능 및 방어 영역을 소개한다.

> All that matter is to differentiate signal of IoC from noise in your network.

목차

[1] 네이트 실버는 미국의 저술가이자 통계학자이며 뉴욕타임즈의 정치블로그인 FiveThirtyEight.com 및 PECOTA라는 야구경기 결과 예측시스템을 만들어 정보예측에 새로운 패러다임을 제시하였으며 이러한 성과로 타임 매거진에서 선정한 세계에서 가장 영향력있는 100인에 선정되었다.

1. 개요

2009년 7월 7일 대한민국 침해사고대응에 새로운 시대가 시작되었다. 국내 정부, 금융, 포털기업 및 미국의 주요 사이트가 분산서비스거부공격을 받았으며 대부분의 국내 사이트는 정상적인 서비스를 제공하지 못했다. 이 공격이 기존에 발생한 수많은 서비스거부공격에 추가된 하나의 공격으로 생각 될 수 있으나 이 공격의 목적 및 이를 수행하기 위해 사용된 기술, 전술 및 수행절차[2]는 기존의 공격방식을 벗어난 완전히 새로운 방식이었다. 당시의 서비스거부공격은 금전적 이익을 얻기위한 목적으로 지엽적인 공격으로 치부되어 왔고 이러한 공격에 대응은 공격목표 지점으로 전송되는 트래픽을 차단하는 네트워크 대역폭소진공격 대응 관점으로 운영되었으며 따라서 사고발생 시 관성적으로 고려되던 관문 및 망간 연동구간에서의 대응은 아무런 방어효과를 내지 못하였다.

당시 공격자는 공격발생 전 최소 6개월의 기간 동안 국내 네트워크에 잠입하여 국내외 각 대역에 고르게 전파된 최소 오만대 이상의 좀비PC로 구성된 공격 인프라를 구성하였으며 공격이 시작되자 각 네트워크의 말단에서 부터 서서히 진행된 공격트래픽은 공격대상지에 도달 했을 때 당시의 방어기술로는 대응할 수 없는 수준의 공격으로 나타났다. 비록 최근 국내 네트워크를 대상으로 한 대형 서비스거부공격은 발생하고 있지않으나 또 다른 형태의 타겟공격 인 사이버테러 및 민감정보 탈취라는 새로운 형태의 사이버공격이 기존의 공격보다 더 많은 피해를 발생시키며 급격하게 증가하고 있다.

2009년을 기점으로 공격자의 행위는 점점 더 정교하게 진화하고 있으나 운영되고 있는 방어체계는 선택적인 데이터수집에 의존하여 공격의 전체그림을 보지 못하는 표면적인 대응에 머물러 왔다. 이는 기존에 체계의 기술적 문제점이라기 보다는 이를 우회하기 위한 공격자의 행위변경에 더 큰 이유가 있다. 현재 운용되는 탐지체계는 자신의 방어 영역에 해당하는 악성행위는 매우 정밀하게 탐지하나 이에 해당하지 않는 영역에서 발생하는 사고는 탐지하지 못한다. 일례로 시그니처기반의 침입탐지장치는 자신의 알고있는 공격은 매우 정밀하게 탐지하나 알려지지 않은 공격은 탐지하지 못하며 최근 대형사업장을 기준으로 도입되고 있는 샌드박스 기반의 악성코드 탐지 시스템은 시간차 실행을 통한 샌드박스 우회 혹은 사람의 개입을 통해 설치되는 PUP/PUA[3]형 악성코드를 탐지하지 못한다.

커넥텀®은 기존의 정보보호 체계를 대신하는 장치가 아니며 기존 체계를 통해 대응하지 못하는 영역에서 발생하는 침해사고를 탐지하는 장치이다. 기존체계가 사고의 발생을 원천적으로 차단하는 예방체계라면 **커넥텀**®은 이러한 최선의 노력에도 불구하고 기존의 체계를 우회하는 고도의 공격 발생 시 이를 탐지하고 대응하기 위해 개발되었다. **커넥텀**®은 네트워크에서 발생하는 모든 통신사실을 분석하여 현황정보, 위협정보를 제공하며 사이버킬체인 기반의 위협정보의 인과관계 기반 사고추적 기능을 통해 예방체계를 우회하여 기업 내부에서 진행되고 있는 은닉공격을 탐지할 수 있는 방법을 제공한다.

2. 상황인지

상황인지는 위협대응 중심의 정보보호에서 가장 적게 주목 받아 온 분야 중 하나이다. 운영 중인 백신체계에서 10개의 악성코드가 탐지 된 경우 이를 어떻게 해석하여야 하는 가는 내부망에 유입된 바이너리 중 알려진 악성코드 몇개를 탐지하였는가에 따라 달라진다. 이렇듯 정확한 현황정보가 없다면 정보보호 팀 구성원 중 몇몇은 이를 매우 심각한 상황으로 받아들일 수 있고 동시에 나머지 구성원들은 동일한 상황을 그저 일상적인 현실로 받아들일 수 있을 것이다. 이는 정보보호 조직 나아가서는 기업전반의 정보보호 수준에 대한 불확실성을 가중시키게 된다. 이러한 불확실성은 측정하기 어려우며 따라서 정보보호 조직의 방향성

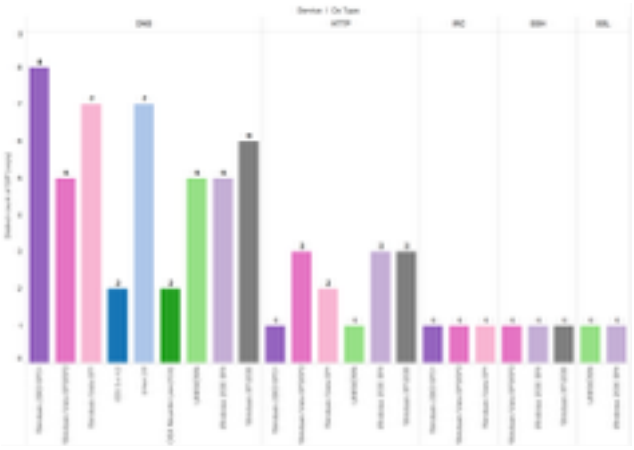


그림 1. 내부망 호스트 운영체제 및 어플리케이션 분포

[2] Technique, Tactics and Procedures

[3] Potentially Unwanted Program e, Potentially Unwanted Software의 약자로 애드웨어, 스파이웨어 등이 포함된다.

을 제시할 수 없다.

커넥텀®은 내부망에서 동작 중인 호스트의 수, 서브넷 분포, 설치된 운영체제, 활성화된 네트워크 서비스 포트, 프로토콜, 어플리케이션 및 HTTP/SMTP/FTP 프로토콜을 통해 전송된 모든 바이너리 파일의 정보를 실시간 추적하여 내부 시스템의 변화를 인지할 수 있도록 하며 시그니처와 무관하게 내부망에 존재하는 모든 지속성 통신을 추적하는 기능을 갖추고 있다. 그림 1은 **커넥텀**®을 활용한 내부망 보안현황 점검 리포트의 일부이며 내부망에 존재하는 호스트 운영체제 분포 및 운영 중인 네트워크 서비스를 나타낸다.

내부 네트워크에 대한 현황인지가 없다면 보안조직은 언제 발생할 지 모르는 사고에 대한 막연한 불안감만을 가지고 있게되며 기업의 정보보호 위험수준을 측정할 수 없다. 측정된 위험은 정보보호 조직을 움직이게 하는 힘이되지만 측정될 수 없는 불확실성은 정보보호 조직을 멈춰서게한다.

3. 위협인지

커넥텀®의 위협인지는 네트워크에서 발생한 비정상 행위를 탐지하는 방법으로 상황인지 단계에서 습득된 지식을 기반으로 수행된다. 위협인지는 다시 사이버 킬체인[4] 기반의 초기침해, 명령제어, 내부이동, 목적달성의 단계로 나누어 진다.

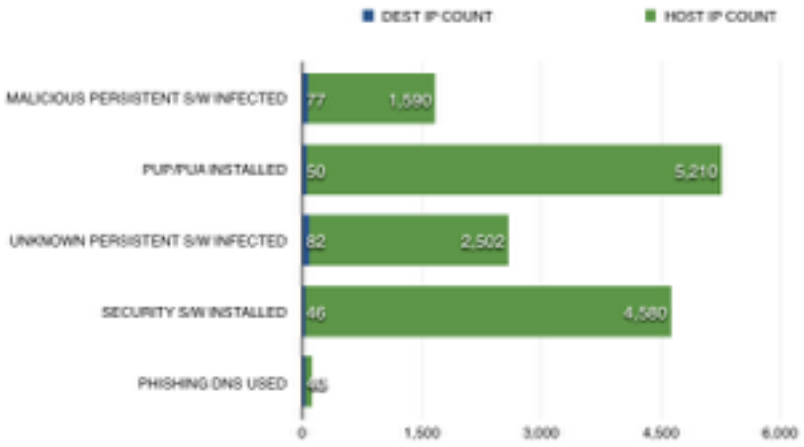


그림 2. 명령제어채널의 형태와 이와 통신중인 호스트의 수

초기침해 단계는 현재의 방어모델에서 대부분의 대응이 이루어지는 부분으로 침입탐지장치, 바이러스백신 그리고 가상머신 기반의 샌드박스 등의 대응장치 등이 포함된다. **커넥텀**®은 초기침해 단계에서 HTTP, FTP 혹은SMTP 프로토콜을 통해 내부망에 전송되는 모든 바이너리 파일을 재조합하여 해당파일의 해시값을 생성하고 이를 알려진 좋은 바이너리파일, 알려진 악성 바이너리 파일 및 알려지지 않은 바이너리 파일로 분류한다. 이러한 기능은 현재 운영되고 있는 백신체계의 정확성(탐지율)을 측정하는 방법으로 사용될 수 있다. 또한 직접 다운로드 된 바이너리 파일과 URL 변경을 통해 다운로드 된 간접 바이너리 파일의 구별 기능을 이용한 원 접속치 추적 등 초기침입 시 발생할 수 있는 다양한 징후를 탐지한다.

위협인지의 두번째 단계는 명령제어채널 탐지 기능으로 여기에는 주기적 외부행 통신을 수행하는 비콘형 통신탐지 기능과 지속형 통신을 이용한 백도어형 통신탐지 기능이 포함된다. 동시에 다수의 에이전트를 통제하고자 하는 공격자는 외부에서 직접접근이 차단된 내부망에 접근하기 위해 비콘형 통신채널을 구성하며 보다 상세한 비정형 작업을 수행하는 공격자는 백도어형의 명령제어채널을 사용하나 다수의 사례에서 나타난 것과 같이 공격자는 자신의 공격 목적을 달성하기 위해 이러한 두가지 형태의 명령제어채널을 혼용하여 사용한다.

전통적으로 명령제어채널의 구성은 시스템 혹은 소프트웨어의 취약점을 공격하는 공격코드(exploit code)에 의해 수행되어 왔으나 최근 공격에는 사용자 설치유도, 기 설치된 소프트웨어의 명령제어채널 가로채기 등 다양한 공격방법이 사용되고 있다. 명령제어채널은 공격대상 내부망에 은닉하며 지속적인 작업을 수행하기 위해 반드시 필요한 구성요소로 **커넥텀**®은 자체 개발된 통신분석 기능을 이용하여 알려진 정보에 의존하지 않은 범용 명령제어채널 탐지방법을 사용한다. 그림 2는 현장분석을 통해 탐지된 명령제어채널의 형태와 각 채널별 목적지 및 내부망 호스트 수를 나타낸 것으로 탐지된 명령제어채널은 악성코드, PUP/PUA 소프트웨어, 보안프로그램 그리고 알려지지 않은

[4] 사이버킬체인은 침해의 단계를 기술하며 대응 가능한 정보보호 인텔리전스 기반의 모델링을 통해 구성된다. 이 모델을 이용하여 방어자는 공격행위를 모델링 하여 공격진행 단계에 따른 선택적 대응을 가능하게 한다.

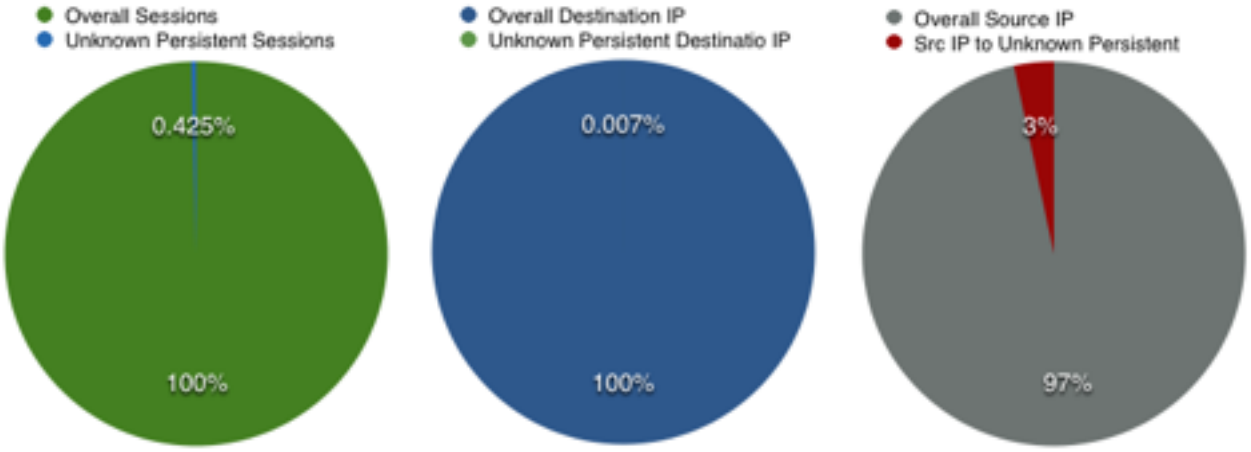


그림 3. 글로벌 대형 사업장에서의 네트워크 세션 수와 형태 별 지속통신 비율

명령제어채널 등이 포함되어 있다. 또한 **커넥텀**®은 기존 명령제어채널의 변화 발생 시 이를 사용자에게 전달하여 보안프로그램, 업무용소프트웨어의 업데이트 채널 가로채기 공격탐지 기능을 제공한다. 그림 3은 약 2기가비트의 외부행 대역폭과 약 만대의 내부망호스트로 구성된 대형 글로벌 네트워크에서의 분석사례를 나타내며 이 경우 최소 10억건 이상의 외부행 통신세션이 발생하나 이중 0.425%인 5십만 건의 지속통신 세션이 발생하며 이중 알려지지 않은 명령제어채널을 목적지 IP 기준으로 분류하면 그림 중앙에 나타난 것과 같이 전체 외부통신 IP의 0.007%인 26개의 목적지로 나타나며 전체 내부망호스트의 약 3%가 탐지된 26개의 호스트와 지속적인 통신을 수행하는 것을 나타낸다.

커넥텀®이 제공하는 사이버킬체인기반 공격탐지 기능 중 세번째는 내부망이동 탐지 기능이다. **커넥텀**®은 물리적으로 분산된 센서에서 수집된 정보를 하나의 논리적 분석장치를 통해 처리하도록 구성되어 있으며 센서 설치구간에 망간 통신이 이루어지는 경우 내부망 호스트간의 통신시도, 실 통신발생 등의 행위를 차별적으로 탐지하며 이를 기반으로 내부망 호스트 간 통신 자유도(Order of degree) 검사를 통해 내부망호스트간 통신변화를 추적하여 수평적, 수직적 연결시도 신규통신발생, 내부정보이동 등의 이상징후를 탐지하는 기능을 갖추고 있다. 이러한 기능은 높은 수준의 통신보안이 요구되는 폐쇄망 등의 환경에서 정상통신 화이트리스팅 기반의 정책 수립 및 이상징후 탐지를 가능하게 한다.

위협인지기능의 마지막 단계는 정보유출 탐지기능으로 이 단계에서는 망내 정보이동 및 망간 정보이동 트래픽을 분석하여 정보유출 징후를 탐지한다. 이를 위해 **커넥텀**®은 프로토콜 기반 및 통신량 기반의 이상징후 탐지 기능을 제공한다. 프로토콜 기반 탐지 시 발생하는 통신 중 HTTP, FTP, SMTP를 이용하는 통신의 경우 비정규 통신포트사용, 비정규프로토콜 사용등의 방법을 사용한다. 통신량 기반의 탐지는 시간에 흐름에 따른 누적 통신량 추적을 통해 한 시점에서는 적은량의 통신으로 보이나 지속적인 정보유출을 통해 궁극적으로 대량의 정보유출을 발생시키는 통신을 탐지하며 이를 위해 통신주체간 바이트비율, 절대값검사, 누적값 검사등의 방법을 제공한다. 외부행 정보유출을 탐지시 사용하는 방법 중 하나로는 내부호스트와 외부서버와의 통신량 검사 기능을 사용한다. 일반적으로 내부호스트는 외부에서 정보를 받아오는 클라이언트로 동작하며 외부 서버는 정보를 제공하는 서버 역할을 수행한다. 지속적인 누적통신 검사를 통해 서버와 클라이언트의 통신비율이 일정수준 이상 역전되는 경우 이를 이상징후로 탐지하는 방법 등을 사용하여 내부망에서의 정보유출 징후를 탐지한다.

내부망에 은닉한 공격자를 탐지하기 위해 위협인지 단계에서 사용된 사이버킬체인에서는 공격자의 연속적 움직임을 추적하기 보다는 각 단계에서 발생하는 이벤트에 중점을 두었다. 이 문서의 다음부분에서 소개될 사고추적 기능은 각 단계별 발생한 이벤트를 시간과 통신연계정도를 기반으로 내부망에서 발생한 이상징후를 연속적인 행위로 재구성하여 침해사고 원인분석에 사용할 수 있도록 하였다.

4. 사고추적

사고추적 단계는 인지된 위협행위가 내부의 적법한 사용자에 의해 수행된 것인지 아니면 외부의 공격자에 의해 수행된 것인 가를 구분하기 위해 사용되며 또한 동일 시점에 다수의 공격이 진행되는 경우 가장 중요한 자산에 가장 가깝게 접근한 사고를 먼저 처리할 수 있도록 한다.

여기서 각 단계에서 발생한 침해징후에 대한 인과관계 분석을 통해 시간에 흐름에 따른 공격자의 움직임을 추적한다. (주)나루씨큐리티는 수년간의 현장분석 경험을 바탕으로 기존의 선형적 사이버킬체인 모델을 **커넥텀®**을 통해 그림 4와 같은 원형 모델로 재구성하였다. 정보유출 시스템 파괴 등의 목적을 가지고 내부망에 침투한 공격자는 다양한 방법의 초기침해를 통해 내부시스템에 불법접근권한을 획득하고 망 외부에 공격자가 내부망 자원에 접근할 수 있도록 명령제어채널을 구성한다. 그러나 이 단계이후 공격자는 추가도구 다운로드, 내부이동, 공격목적달성 등의 단계를 순차적으로 진행하지 않는다. 하나의 호스트를 점유한 공격자는 해당 호스트의 정보를 유출할 수 있으며 또한 내부망에 위치한 다른 호스트에 대한 초기침해를 수행 할 수 있다. 이러한 과정은 결국 각 상황에서 공격의 목적을 달성하기 위해 공격자의 자유의지에 따라 이루어 진다. 그러나 공격이 진행됨에 따라 각 단계 별 이벤트 발생은 증가하며 이 과정에서 그림 4와 같이 항상 명령제어채널을 중심으로 사이버킬체인의 다른 요소들이 존재하게 된다. 이러한 요소들 간의 상호작용이 커질 수록 내부망에서 진행되는 공격이 활발하게 움직이는 것으로 볼 수 있으며 사고추적 과정에서는 사이버킬체인 요소 중 하나의 단계에서 발생하는 사건의 중복은 전체 위험도에 큰 영향을 미치지 못하나 명령제어채널을 중심으로 각 요소간 다수의 상호작용이 탐지 된 경우 이에 대한 사고 가능성을 높게 계산하여 침해사고 대응시 위협정도에 따라 차등적인 대응이 가능하도록 구성하였다.

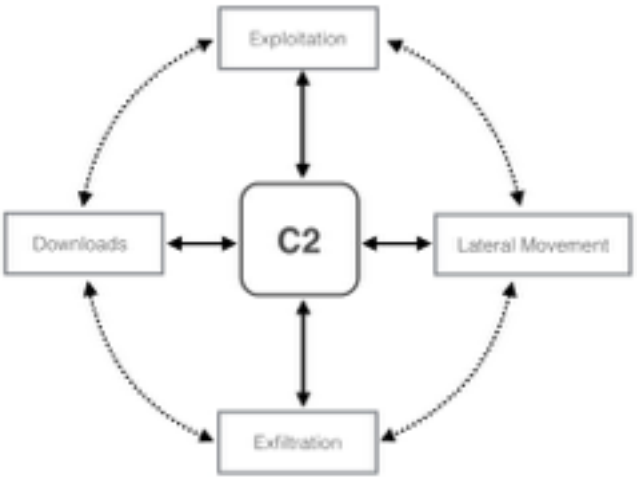


그림 4. 원형 사이버킬체인 추적 프로세스

앞서 언급된 것과 같이 **커넥텀®**은 다수의 분산된 지점에서 수집된 정보를 센서간 클러스터링 기능을 이용하여 최적화하고 수집된 정보를 이용하여 내부망에서 발생하는 공격자의 행위를 보다 정밀하게 추적하여 비록 공격자가 성공적인 초기침해와 명령제어채널을 구성 했다고 해도 정보유출 혹은 시스템 파괴 등의 행위가 발생하기 전 이를 탐지하고 대응할 수 있도록 한다. 표 1은 사이버킬체인 기능을 이용한 공격추적과 각 단계에 해당하는 위협정도를 표시한 예로 **커넥텀®**의 위협값 계산 방법을 나타낸다.

커넥텀®을 이용한 침해사고 탐지 시나리오

공격단계	침해사고탐지 징후	위협수준
1	사용자 PC에서 알려지지 않은 바이너리 파일 다운로드	0%
2	바이너리 파일이 다운로드 된 뒤 외부행 비콘 통신 발생	30%
2	비콘 발생 수일 후 외부행 백도어 통신 발생	60%
3	백도어 발생 PC에서 내부망 주변 PC에 다수의 실패한 접속시도 탐지	70%
3	백도에 발생 PC와 내부망 주변 PC에 존재하지 않던 네트워크 세션 탐지	80%
4	내부망 호스트에서 외부망 호스트로 지속적인 정보유출징후 탐지	90%

표1. **커넥텀®**을 이용한 위협탐지 및 사이버킬체인 기반 위협 수준

5. 결론

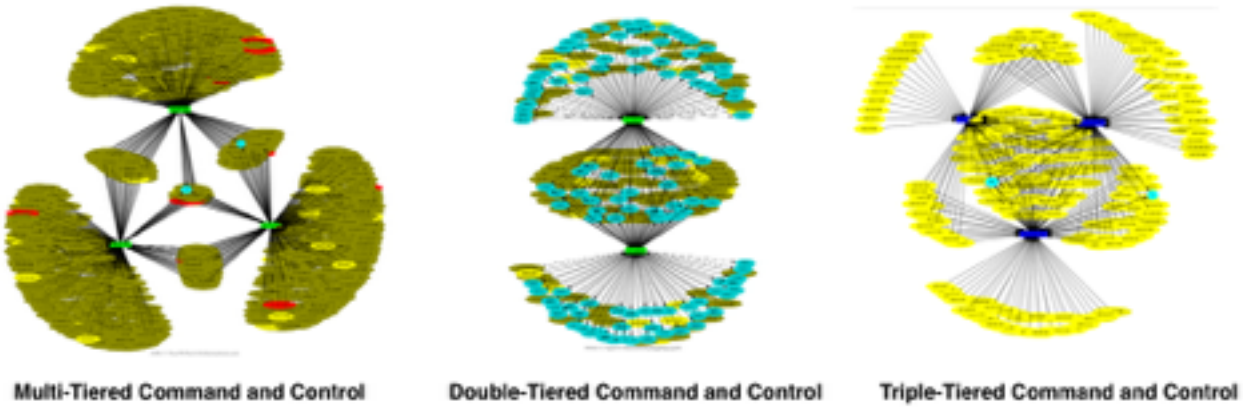


그림 5. **커넥텀**®을 이용해 탐지된 명령제어채널

현재 미국 파이어아이 사의 CSS(Chief Security Strategist)인 리차드 베이트릭(Richard Bejtlich)은 2004년 자신의 저서 Tao of Network Security에서 “예방체계는 결국 우회된다.” 라고 말했다. 하지만 아직 많은 기관에서는 예방체계의 강화로 침해사고를 완벽하게 예방 할 수 있다고 믿고있다. (주)나루씨큐리티는 다수의 침해사고 현장분석 경험을 통해 다양한 사례의 우회모델을 분석해 왔으며 모든 분석대상 기관이 일정 수준이상의 정보보호 체계를 운영하고 있음에도 불구하고 이를 우회한 공격자가 수십에서 수백대의 내부 호스트를 점유하고 있다는 것을 탐지하였다. 그림 5는 분석과정에서 탐지된 명령제어채널과 공격 목적에 따른 구성형태의 차이점을 나타낸다.

커넥텀®은 네트워크 기반의 침해사고 탐지 장치로 지엽적 정밀성에 함몰되지 않고 현재 방어자의 네트워크에서 진행 중인 공격을 정확하게 탐지 할 수 있는 방법을 제공하며 이를 위해 현황인지, 위협인지 및 사고추적의 기능을 갖추고 있다. 현황인지 기능을 통해 정보보호 현황정보를 제공하여 이상징후 탐지를 위한 베이스라인을 제공한다. 위협인지 기능은 사이버킬체인 기반의 공격행위모델링 기법을 사용하여 내부망에 침투한 공격자의 행위를 단계별로 탐지한다. 마지막으로 사고추적 기능은 위협인지 기능에서 탐지된 이벤트 간의 인과관계 분석을 통해 내부망에 성공적으로 침투한 공격자가 민감정보유출, 시스템파괴등의 공격목적을 달성하기 전 이를 저지 할 수 있는 방법을 제시한다.

㈜나루씨큐리티

내부망 인텔리전스

사이버인텔리전스 어떻게 활용할 것인가

9 월 15 일 데일리시큐에서 주최하는 사이버인텔리전스 컨퍼런스 관련 기고문입니다.
사이버인텔리전스와 내부망 보안의 관계와 우리가 나아가야 할 방향을 정리했습니다.

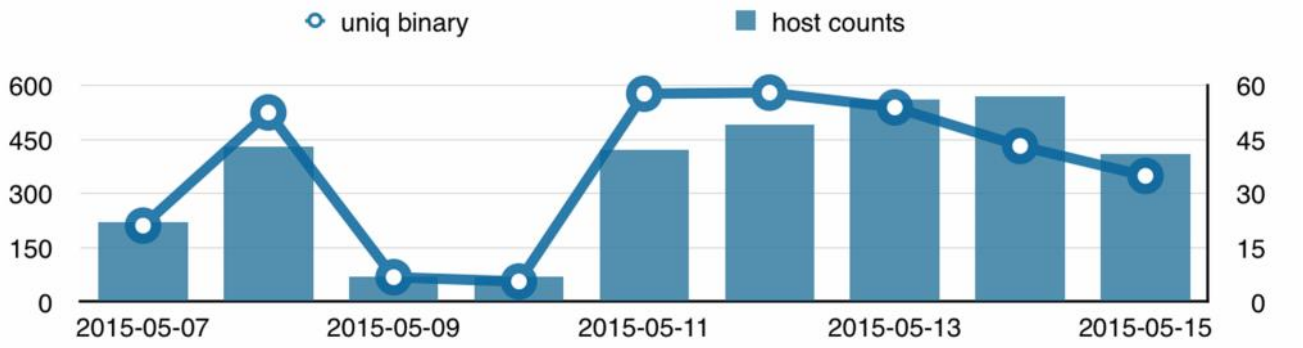
㈜나루씨큐리티 김혁준

1988 년 23 살의 코넬대학교 대학원생이자 당시 미국 NSA 의 수석 컴퓨터 과학자의 아들인 로버트 모리스는 자신의 행위를 은닉하기 위해 하버드대학교에서 컴퓨터 웜을 최초 전파하였다. 자칭 "인터넷의 크기 측정"을 위한 실험이라는 변명으로 집행유예를 받았으나 모리스웜은 당시 인터넷의 삼분의 일에 해당하는 시스템을 감염시켰으며, 인터넷 침해사고를 대응하기 위한 정보공유 및 공동대응기구의 필요성을 정보보호 커뮤니티에 인지시켰다. 이후 연쇄적으로 발생한 멜리사(Melissa), 님다(Nimda), 코드레드(Code Red) 그리고 국내에 1.25 인터넷 대란을 발생시킨 슬래머(Slammer), 블래스터(Blaster), 님다(Nimda), 사서(Sasser) 등은 모두 불특정 다수의 대상으로 하는 넓은 형태의 공격이었다.

그러나 2009 년 발생한 7.7 분산서비스거부공격은 이러한 패러다임을 따르지 않고 국내외 주요 웹사이트를 대상으로 한 명확한 공격목표에 대해 3 일동안 매우 효과적인 사이버테러를 수행하였다. 기존의 공격이 특정 취약점 혹은 특정 형태의 시스템을 목표로 하였다면, 이 공격은 특정 시스템이 아닌 국가 주요 서비스를 목표로 하였고 다수의 공격목표에 효과적인 공격을 수행하기 위해 최소 오십만대 이상의 봇넷을 동원하였다. 또한 기존의 공격자들은 유사한 공격을 수행하기 위해 상대적으로 오랜 시간 충분한 공격력을 갖춘 봇넷을 양생하기 위한 시간을 보내거나 제 3 자의 봇넷을 대여 형태로 사용하였지만, 7.7 서비스거부공격을 수행한 공격자는 이미 충분한 수의 사용자를 확보하고 있는 정상 인터넷 서비스를 하이재킹하여 매우 효과적인 대형 일회성 봇넷을 구성하였으며 이러한 전술은 농협전산망해킹, 3.20 사이버테러 등 기존의 신뢰관계를 이용한 해킹의 형태로 자리잡았다.

이러한 형태의 공격은 공격자의 의도와 능력에 의해 긴 시간 동안 공격의 목적을 달성하기 위한 다양한 형태의 기술적 행위의 집합으로 발생하며 이를 정상 혹은 악성의 기술적 이분법으로 대응하는 과정에서 하나의 목적을 가진 공격행위가 수백 가지의 기술적 행위로 해체되고 방어자는 쏟아지는 정보 속에서 침해사고대응이라는 원래의 목적은 망각되고 단편적 기술적 대응만이 이루어진다. 이러한 현실 속에서 정보보호 현장은 기술적 정보(Information)의 과잉으로 인한 피로감이 증가하고 있는 현실이다. 또한 기존의 공격자는 기술적 목표를 달성하기 위한 단편적인 공격을 수행하였으나 최근 발생하는 공격은 보다 현실적인 공격목적을 달성하기 위한 일련의 과정으로 이루어지며, 각각의 과정에 사용되는

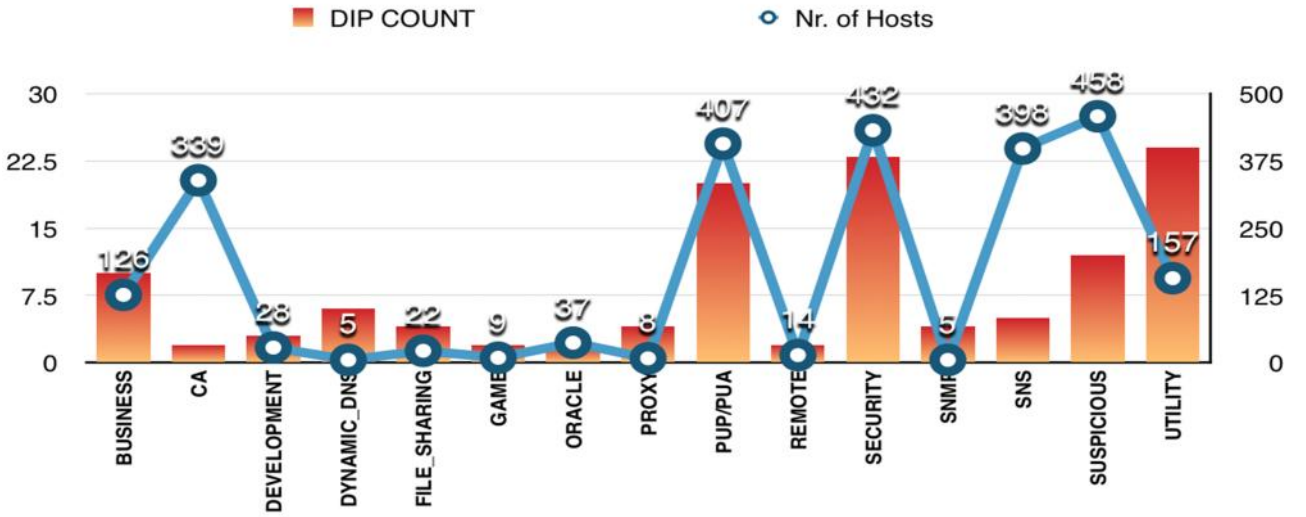
기술은 각 단계별 목표를 달성하기 위해 독립적으로 사용된다. 사이버인텔리전스는 공격자의 행위과정에서 발생하는 겉으로 보이기에 연관성이 없어 보이는 대량의 정보 속에서 패턴을 탐지하고 이를 기반으로 데이터 기반의 정보보호 의사결정을 이끌어내는 역할을 수행한다.



[그림1] 네트워크를 통해 유입되는 실행 바이너리

사이버인텔리전스를 활용한 정보보호가 효과적으로 동작하기 위해서는 방어자는 내부 인텔리전스와 외부 인텔리전스에서 획득되는 정보를 구분하고, 상호간 의미 있는 접점을 구성하여야 한다. 먼저 내부 인텔리전스란 내부망 호스트, 어플리케이션, 운영중인 네트워크 서비스 정보 등 전통적인 자산현황 정보 및 진화하는 공격에 보다 효과적으로 대응하기 위한 내부유입 바이너리, 지속통신 및 내부이동(Lateral Movement) 정보 등이 포함된다. 이에 상응하는 외부 인텔리전스는 바이러스토탈 등에서 제공하는 악성 URL 정보, 바이너리 정보 및 통신정보 등이 포함된다. 여기서 지속통신이란 내부망에서 외부로 지속적으로 발생하는 비콘(beacon) 혹은 백도어 형 통신으로 여기에는 애드웨어, 보안프로그램, 악성코드, 비즈니스소프트웨어 등 다양한 형태가 존재한다.

[그림 1]은 내부망에 네트워크를 통해 유입되는 모든 실행 바이너리 파일 현황을 나타낸 것으로 분석 대상 네트워크에는 일별 수 백 개의 바이너리파일이 수십 개의 호스트에 지속적으로 유입되는 현상이 나타나 있다. 사이버인텔리전스를 적용하지 않은 경우 일반적으로 유입되는 실행 바이너리 파일은 내부에서 운영중인 백신 프로그램에 의해 악성으로 탐지되는 것과 그렇지 않은 것 두 가지로 분류된다. 그러나 내부망에 유입되는 실행 바이너리 파일은 먼저 유입 경로에 따라 네트워크를 통해 유입되는 것과 그렇지 않은 것으로 나뉘며 네트워크를 통해 유입되는 파일은 알려진 악성, 알려진 정상, 알려지지 않은 정상, 알려지지 않은 악성의 네 가지로 분류된다. 이 단계에서 내부 및 외부 인텔리전스를 통해 대응 가능한 것은 내부 백신에 의해 악성으로 탐지된 실행파일과 외부 인텔리전스와의 연동을 통해 악성으로 탐지된 실행파일이 있다.



[그림 2] 내부망에서 탐지되는 지속통신의 형태와 통신 호스트 수

명확한 공격의도를 가진 공격자는 비록 몇 가지 악성 바이너리 전송/설치 시도가 내부 및 외부 인텔리전스에 의해 탐지되었다고 해도 결국 자신의 목적을 달성하기 위해 지속적인 시도를 할 것이며, 결국 전송시점에 알려지지 않은 악성실행파일을 네트워크 혹은 기타경로로 내부 시스템에 전달하게 된다. [그림 2]는 내부망에서 발생하는 모든 지속통신에 대한 정보이며 여기에는 게임, 애드웨어, 알려진 악성코드 및 알려지지 않은 프로세스에 의해 발생하는 모든 지속통신이 나타나 있다. 아래의 분류에서는 외부 인텔리전스를 통해 악성으로 분류된 지속통신과 목적지 및 해당 통신을 발생시키는 프로세스 정보가 불분명한 경우 이를 모두 의심(SUSPICIOUS)로 분류되어 있다.

만약 [그림 1]의 단계에서 내부망 호스트에 실행파일이 전송된 뒤 [그림 2]의 단계에 기존에 존재하지 않던 불명확한 프로세스가 새롭게 탐지된다면, 방어자는 해당 이벤트에 보다 많은 시간과 노력을 들여야 하는 당위성을 확보 할 수 있다. 따라서 방어자는 새로운 지속통신을 발생시킨 프로세스를 직접 수집하여 바이너리 분석을 수행하거나 혹은 외주업체와의 협업을 통해 해당 프로세스에 대한 대응수준을 결정할 수 있다.

앞에서 나타난 2 가지 과정을 통해 내부망 호스트에 성공적으로 악성 실행파일을 설치하고 외부에서 제어가 가능한 명령제어채널을 수립한 공격자는 초기침해가 발생한 호스트 정보를 수집한 뒤 목표정보 수집 및 목표시스템 파괴 등 공격의 목적을 달성하기 위해 초기침해 호스트를 교두보로 삼아 보다 많은 내부망 호스트에 대한 접근을 시도한다. 만약 공격자가 내부망 특정 호스트에 저장된 민감정보를 목표로 한 공격을 수행한 경우 처음 침투한 시스템에 관련정보가 존재하지 않는다면 결국 이러한 정보가 수집된 시스템으로 이동하고자 할 것이며, 이 과정에서 내부 네트워크에 대한 접속시도가 발생하며 접근시도가 성공하는 경우 기존에 존재하지 않던 내부 시스템 간의 새로운 통신형태가 발생한다. [그림 3]은 내부망 호스트간 연결시도 및 연결을 추적하는 것으로 이 단계에서는 단지 내부망 현황에 대한 인텔리전스 및 시간의 흐름에 따른 변화추적을 통해 내부망에 침투한 공격자를 탐지하게 된다.

㈜나루씨큐리티

번호	날짜	SRC IP	목적지 호스트 수	로그 수	연결 호스트 수 ▾	비연결 호스트 수	로그 확인
1	20150806	192.168.1.146	13	1483	10	4	로그보기 그래프보기
2	20150804	192.168.1.146	13	1410	9	6	로그보기 그래프보기
3	20150807	192.168.1.151	12	7038	8	7	로그보기 그래프보기
4	20150806	192.168.1.151	12	6672	8	8	로그보기 그래프보기
5	20150807	192.168.1.146	12	2817	7	7	로그보기 그래프보기
6	20150805	192.168.1.127	7	7175	6	3	로그보기 그래프보기
7	20150804	192.168.1.107	7	1216	6	3	로그보기 그래프보기
8	20150807	192.168.1.141	12	1306	5	9	로그보기 그래프보기
9	20150807	192.168.1.107	7	2111	5	2	로그보기 그래프보기
10	20150804	192.168.1.141	12	1649	5	10	로그보기 그래프보기

[그림3] 내부망 호스트간 연결도(Order-of-connectivity) 추적정보

이러한 일련의 과정은 복잡하고 어려운 기술적 용어 없이 쉽게 경영층에 전달 될 수 있으며 만약 공격목표가 기업 혹은 기관의 민감정보인 경우 정보보호 담당자는 정보보호가 비즈니스의 걸림돌이 아닌 비즈니스 연속성 보장에 필수불가결한 요소임을 명확하게 전달할 수 있으며, 이러한 과정을 통해 불편함을 가중시킨다는 이미지에서 벗어나 조직에서 존경 받는 구성원으로서의 자리잡을 수 있을 것이다. 사이버인텔리전스는 주관적 경험과 직관을 넘어 객관적인 데이터와 분석을 통해 측정 가능한 정보보호 의사결정을 이끌어내며 이를 통해 정보보호 산업이 비즈니스 연속성 보장을 위한 필수 요소로 자리잡을 수 있도록 할 것이다.