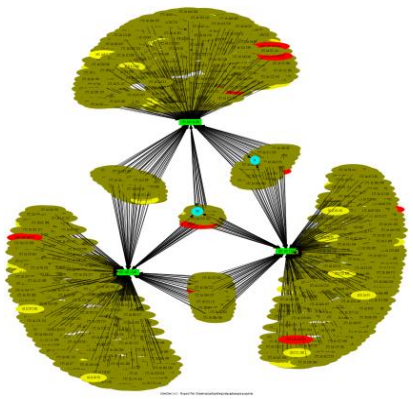
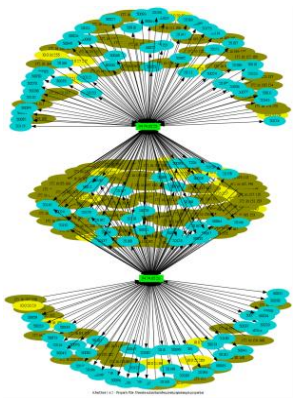
ConnecTome®

Knows Who Owns Your Network

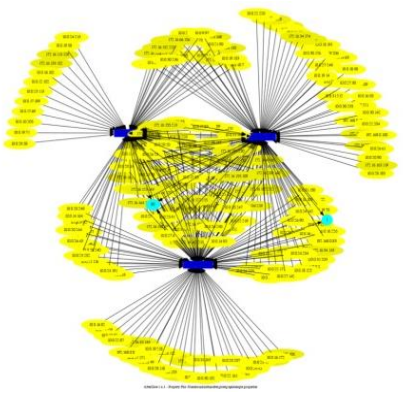
운영중인 방어체계를 우회하여 기업내부에서 진행중인 사이버 공격탐지



Multi-Tiered Command and Control



Double-Tiered Command and Control



Triple-Tiered Command and Control

문제점

어느 누구도 자신이 방어중인 네트워크에서 발생하는 사실을 정확하게 인지하지 못함.

해결방안

정보유출, 시스템파괴 등의 목적으로 내부에 침투한 공격자의 행위 탐지 및 대응.

커넥텀으로 침해사고대응의 패러다임 전환이 이루어집니다.

네트워크에서 수집된 데이터 기반의 위협탐지 기능을 통해 안티바이러스, 샌드박스 등 기존의 방어체계를 우회한 공격을 탐지합니다.

명령제어채널 탐지

내부망에 침투하여 외부에 접근하기 위해 구성된 명령제어채널 및 백도어를 통신사실 분석을 통해 탐지합니다.

사이버킬체인기반 공격탐지

내부망에서 발생하는 이상징후를 사이버킬체인 기반으로 공격진행을 단계별로 추적하여 사고발생 가능성이 높은 공격에 우선적으로 대응이 가능하게 합니다.

Making Sense of the Unknown

NARUSECURITY

Key Features

상황인지

내부 호스트 및 네트워크 분포, 사용중인 운영체제, 네트워크세션, 활성화된 내부 네트워크 서비스 등의 정보 실시간 탐지 기능

위협인지

내부유입 바이너리, 명령제어채널, 내부망이동, 정보유출, 비인가장치 설치 등 내부망 위협 탐지 기능

사고추적

사이버킬체인 기반의 초기침해, 명령제어채널수립, 추가도구다운로드, 내부망이동, 공격목적 달성의 단계별 공격자의 움직임 추적기능

www.narusec.com

Naru Security, Inc.

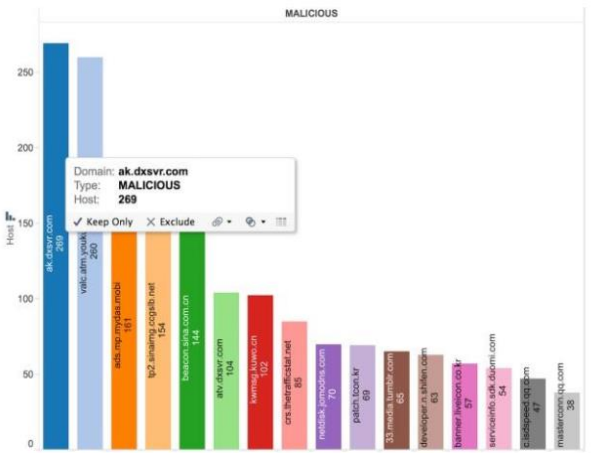
02-522-7912

서울시 강남구 영동대로 621, 9층
(삼성동 621빌딩)
(주)나루씨큐리티

Pervasive Security Intelligence with ConnecTome®

Persistent Connection and Nr. of Binding Hosts

Geographic Location of C2 Channel



Malicious Domain and Number of Compromised Hosts

커넥텀은 진행중인 공격이 정보유출 시스템파괴 등의 사고로 발전하기 전 대응이 가능하게 합니다.

커넥텀은 물리적으로 분리된 다수의 지역에 설치된 센서에서 수집된 데이터를 논리적으로 하나의 장소에서 통합 분석 할 수 있는 환경을 제공합니다. 또한 (주)나루씨큐리티의 특허기술인 명령제어탐지 기술을 이용하여 기 설치된 대응체계를 우회하여 내부망 자원을 성공적으로 침해한 공격을 탐지하며 이를 사이버킬체인 기반의 공격단계별로 연계분석하여 정보유출, 시스템파괴 등에 사용되는 은닉공격에 대응할 수 있도록 합니다.