

『Tech-Biz Korea 2017』 ETRI 기술소개 자료

◆ SDN 기반 동적 망 은닉 기술

<p>담당자</p>	<p>이현진 책임 (초연결통신연구소 네트워크연구본부 / 042-860-5386)</p>
<p>기술개요</p>	<p>악의의 사용자로부터 해킹의 대상이 되는 망을 숨기는 기술로써, 서버까지 연결된 경로를 주기적으로 변경하거나, IP 주소/ 포트 번호와 같은 서버 정보를 위장하기도 하고, 망을 복제하여 어느 망이 진짜인지 혼란스럽게 하는 기술이다.</p> <p>RRM : Random Route Mutation (망 경로 은닉) RHM : Random Host Mutation (서버 정보 은닉) VNC : Virtual Network Cloning (네트워크 은닉)</p>
<p>기술특징</p>	<ul style="list-style-type: none"> ○ 방화벽(Firewall), 침입탐지시스템(IDS) 등 기존 경계 기반 네트워크 보안 개념을 벗어나, 공격자의 타겟인 서버, 서버로 구성된 네트워크, 그리고 서버로의 경로를 동적으로 은닉시키는 변혁적 기술 ○ 서비스를 제공하는 서버를 은닉시키고, 서버까지의 경로를 은닉시킴으로써, 공격 확률을 이중 삼중으로 낮출 수 있음 ○ SDN 기반으로 의심 트래픽을 탐지할 수 있으며, 단순 차단 뿐만 아니라 격리/추적까지 가능한 구조임
<p>응용 및 활용분야</p>	<ul style="list-style-type: none"> ○ APT 등 다양한 위협 요소로부터 네트워크를 방어할 수 있으므로, 은행망이나 국방망에 활용 가능 ○ 엔터프라이즈나 데이터 센터 등 주요 지점 네트워크의 방어 장비 및 공격자 탐지용으로 활용 가능