데이터 시트

VitalQIP DNS 보안 솔루션

DNS를 보호하고 네트워크를 보호합니다.

경격격 또는 불법 사용으로부터 DNS의 방어

DNS에 대한 공격은 네트워크를 다운 시키는데 매우 효과적입니다. DNS를 이용하면 방화벽을 자유롭게 통과하기 때문에 공격은 손쉽게 명령을 보내거나 제어센터에 접근할 수 있습니다.

DNS는 실제 아주 효과적이고 확장성이 뛰어난 것으로 입증되었습니다. 대부분의 사람들이 DNS가 안정성이 입증되었다고 여깁니다. 그러나 이러한 DNS의 필수 기능과 분산형 구조는 악의적인 활동을 위해 아키텍처와 풍부한 데이터 저장소를 이용하려는 공격자를 유인하는 역할을 합니다.

DNS 인프라 공격

공격자는 통신을 방해하거나 무의식적으로 웹서버 또는 기타 대상을 속이도록 유도하여 최종 사용자를 조정할 목적으로 DNS 서버 자체를 타깃으로 삼을 수 있습니다. 익숙한 서비스 거부(DoS) 또는 분산 서비스 거부공격(DDoS)은 공격자가 거짓의 DNS 요청을 폭주 시켜 정상적인 쿼리를 처리하지 못하도록 호출합니다. PRSD(Pseudo-Random SubDomain) 공격은 일반적으로 네트워크 서비스 제공자가 가입자의 성능을 저해하기 위해 재귀적 DNS 서비스를 거부하기 위해 시도합니다.

호스트나 서버에 대한 공격은 DNS 리솔루션 처리를 방해하거나 DNS 데이터를 조작하기 위해 시도 됩니다. DNS 데이터는 리졸버 공격, 캐시 포이즈닝, 데이터 권한 조작 등과 같은 여러 방법으로 조작될 수도 있습니다.

DNS를 이용한 네트워크 공격

DNS는 광범위한 네트워크 공격에 이용될 수 있는 매개를 제공할 수 있습니다. DNS를 통해 사용자는 텍스트 기반 수신처를 IP 주소로 확인하여 웹사이트에 접속할 수 있게 하듯이, 공격자 멀웨어는 커맨드 센터 및 제어(C2) 센터를 찾거나 방화벽을 통해 정보를 터널링 할 수 있습니다. DNS는 그 특성상 잠재적으로 유용한 공격 대상 네트워크, 호스트 이름 및 IP 주소에 대한 정보를 공개적으로 게시합니다.

(R) with CygnaRadar / (G) with DDI Guard

Reflector 및 Amplification 형태의 공격은 대상 호스트의 IP 주소를 스푸핑 하여 여러 개의 쿼리로 시작하는 DoS 공격의 한 형태입니다. 호스트는 사이즈가 큰 DNS 응답 패킷을 여럿 개 수신하여 호스트를 마비시킵니다.

APT(Advanced Persistent Threats)는 C2 Center의 지침에 따라 공격을 은밀히 수행하고 재 프로그래밍하여 대상 네트워크 내에서 지속되는 멀웨어입니다. 이러한 공격에는 서비스 거부, 네트워크 중단, 데이터 유출 또는 기타 불법 활동들 포함될 수 있습니다.

Why Cygna VitalQIP?

Cygna VitalQIP는 DNS와 네트워크를 보호하는 데 도움이 됩니다. Cygna Labs는 20년 동안의 DDI 경험을 통해 수많은 산업과 제품에 혁신을 도입했으며 다음과 같은 경쟁 우위를 제공합니다:

- **완전한 IPAM** - Cygna VitalQIP는 네트워크에서 서브 넷, 개별 IP 할당, DHCP 및 DNS에 이르기까지 완벽한 IPAM 자동화를 제공합니다.
- **가시성 및 포렌식** - Cygna Radar 및 DDI Guard 소프트웨어와 함께 DHCP/DNS 트랜잭션 동향 및 포렌식에 대한 중앙 집중식 감사 및 보고 기능을 제공합니다.(R),(G)
- **유출 탐지** - Cygna Radar는 DNS 프로토콜을 통한 민감한 데이터 유출을 방지하기 위해 DNS 터널링 탐지 및 종료를 지원합니다.(R)
- **멀웨어 완화** - Cygna Labs의 DNS 방화벽 서비스는 VitalQIP 어플라이언스에서 멀웨어 도메인 쿼리 및 응답을 차단하는 기능을 제공합니다.
- **자동화** - VitalQIP는 한번 클릭 또는 REST API 호출로 IPAM 기능을 자동화합니다.
- **클라우드 DNS 지원** - VitalQIP를 사용하면 온프레미시스, 하드웨어, 소프트웨어, 가상, 클라우드 또는 Amazon Route53, Azure DNS와 같은 DNS 클라우드 서비스에서 실행 여부와 상관없이 전체 DNS 자산을 관리할 수 있습니다.

CYGNA LABS

- **더 적은 비용** - Cygna VitalQIP는 단일 통합 솔루션으로 IPAM/DDI, Discover, Report 등의 모든 기능이 하나의 GUI와 단일 소스입니다. Discover, Report, Microsoft 지원, DNS 방화벽, 클라우드 자동화, GeoDNS 등을 위해 추가 어플라이언스와 추가 라이선스가 필요한 경쟁업체와 다릅니다.
- **Flexibility** - Cygna Labs는 소프트웨어, 어플라이언스, 가상 및 매니지드 서비스를 통해 최대한의 유연성을 제공하는 포괄적인 제품을 제공하는 유일한 DDI 공급업체입니다.
- **IP 인벤토리 보장** - IP 주소, 주소 bock, 주소 pool과 IP 회수에 대해 선택적으로 가져오기를 통해 계획된 불일치와 실제의 불일치를 확인하여 IP 인벤토리를 보장합니다.
- **구성 우위** - Cygna VitalQIP는 서버 옵션 및 RRType을 포함한 ISC/BIND 구성을 지원하지만, 다른 제품들은 RRType의 하위 옵션만을 지원합니다.
- **Scalabilitiy** - Cygnalabs 솔루션은 지구상에서 가장 큰 IP 네트워크를 관리합니다.
- **다중 관리자 제어** - Cygna VitalQIP는 타의 추종을 불허하는 관리자 정책 세분화 와 계층화된 관리 위임 기능을 제공합니다.

VitalQIP DNS 보안 특징 요약

VitalQIP는 DDI 프로세스를 자동화하고 네트워크를 보호할 수 있는 포괄적인 솔루션을 제공합니다. 다음 표에는 주요 DNS 및 네트워크 위협과 하드웨어 및 가상 VitalQIP DNS 어플라이언스, Cygna Radar 및 DDI Guard 제품을 포함하여 CygnaLabs VitalQIP 솔루션을 사용하여 구현할 수 있는 완화 접근 방식이 요약되어 있습니다.

	위협	위협 요약	VitalQIP 완화 접근법
서비스 거부	서비스 거부 (Dos)	공격자가 대량의 TCP, UDP, DNS 또는 기타 패킷을 DNS 서버로 전송하여 리소스를 고갈시킵니다	• 인바운드 속도 제한 • 애니캐스트 적용
	분산서비스거부(DDoS)	공격자가 여러 소스에서 대량의 TCP, UDP, DNS 또는 기타 패킷을 DNS 서버로 전송하여 리소스를 고갈시킵니다	• 인바운드 속도 제한 • 애니캐스트 직용
	가짜 쿼리	공격자가 대량의 가짜 쿼리를 전송하여 재귀 서버가 신뢰할 수 있는 서버를 무의미하게 만듭니다	• 클라이언트당 미결 쿼리 제한
Cache Poisoning	패킷 Interception/ 스푸핑	공격자는 캐시를 감염시키기 위해 재귀 DNS 서버에 DNS 응답을 전송하여 DNS의 무결성에 영향을 미칩니다.	• 자동화된 트러스트 앵커 관리를 사용하여 캐싱 서버에 대한 DNSSEC 유효성 검사 • 소스포트및 XID 랜덤화 • ACLs – allow-query, allow- query-on, allow-query-cache, allow-query-cache-on, allow-recursion, allow-recursion-on • 응답 무결성 검증
	ID 추측/ 쿼리 예측	공격자는 예상하거나 다양한 XID 값을 사용하여 예측된 쿼리에 DNS 응답을 전송합니다.	• 자동화된 트러스트 앵커 관리를 사용하여 캐싱 서버에 대한 DNSSEC 유효성 검사 • 소스포트및 XID 랜덤화 • 응답 무결성 검증

	카민스키공격/ NameChaining 공격	공격자는 추가 섹션에서 위조된 답변과 함께 DNS 응답을 전송합니다. 이 공격은 결정적 쿼리를 생성해서 다음 공격을 용이하게 합니다.	• 자동화된 트러스트 앵커 관리를 사용하여 캐싱 서버에 대한 DNSSEC 유효성 검사
Authoritative Poisoning	불법 동적 업데이트	공격자는 DNS 업데이트 메시지를 마스터 DNS 서버로 전송하여 대상 영역에서 리소스 레코드를 추가, 수정 또는 삭제합니다	• ACL들 allow-update, allow-notify, notify-source 사용합니다. • ACL은 추가 원본 인증을 위해 트랜잭션 서명을 요구하는 것으로 정의할 수도 있습니다.
	서버 공격/Hijack	공격자는 서버 기능 중에서 DNS 데이터를 조작할 수 있는 DNS 서버를 해킹합니다	• Host ACL 구성 • 마스터 숨김 사용 • 강화된 Red Hat OS • 격리 DNS 서비스 • SSH 인증 필요 • 포트 또는 콘솔 액세스 제한 • VitalQIP 및 DDI Guard로 서버 모니터링
	DNS 서비스 오류 설정	구성 오류에 대한 취약성으로 인해 DNS 서비스가 부적절한 구성에 노출됩니다	• VitalQIP DNS 오류 검사 • Checkzone 과 checkconf 유틸리티 사용 • 재로드가 필요한 경우를 위해 데이터 백업
서버/OS공격	버퍼 오버플로 및 OS 레벨 공격	공격자가 서버 운영 체제 취약성을 이용함	• 강화된 Red Hat 운영 체제 • 보안 패치 적용
	제어채널 공격	공격자가 DNS 서비스 제어 채널에 액세스하여 DNS 서비스를 방해	• 제어채널 ACL 사용 • 제어채널 키 인증
	DNS 서비스 취약점	공격자가 DNS 서비스 취약성을 이용함	• 보안 패치 적용 • DNS 버전 노출 금지
리졸버/호스트 공격	재귀적 DNS 리디렉션	공격자가 불법적 재귀 DNS 서버를 가리키도록 리졸버의 구성을 변경함	• DHCP를 통해 레졸버 DNS 서버 구성 • 미허가 DHCP 서버 모니터링 • 각 클라이언트의 잘못된 구성이나 이상 여부를 주기적으로 감사
	리졸버 설정 공격	공격자 어떤 장치를 해킹하여 다른 장치의 기능 중 리졸버 기능의 구성을 조작할 수 있습니다	• Host ACL 구성 • 보안 패치 적용

CYGNA LABS

네트워크 인식	이름 추측	공격자가 추가 공격을 하기위해 정당한 DNS 쿼리를 실행합니다	• 알기 쉬운 이름으로 호스트이름 지정 금지
	불법 Zone Transfer	공격자가 잠재적인 공격 대상을 식별하기 위한 영역 리소스 레코드를 얻기 위해 권한 있는 DNS 서버로 영역 전송 요청을 실행합니다	• 전송 허용 시 TSIG와 함께 ACL을 사용하고, 전송 소스 IP 주소 및 포트를 사용하여 zone transfer에 비표준 포트를 사용합니다
리플렉터 스타일 공격	리플렉터 공격	공격자는 타킷 IP 주소를 스푸핑하고 하나 이상의 권한 있는 DNS 서버에 수많은 쿼리를 발행하여 대상을 고갈시킵니다	• 라우터에서 스푸핑을 완화하기 위한 입력 필터링 구현합니다 • DNS 응답률 제한
	증폭(Amplification) 공격	공격자는 쿼리당 대상에 대한 데이터 흐름을 늘리기 위해 "대규모" 리소스 레코드를 쿼리하여 리플렉터 공격을 증폭합니다	• 라우터에서 스푸핑을 완화하기 위한 입력 필터링 구현합니다 • DNS 응답률 제한
자료유출	(R)DNS 터널링	공격자는 DNS를 전송 프로토콜로 사용하여 방화벽을 통해 데이터를 전송합니다	• Cygna Radar로 DNS 터널 차단 및 포렌식 수행 • 터널 이벤트 및 DDI Guard 포렌식 사용
	(G)리소스 로케이터	공격자는 DNS를 사용하여 Command & Control 센터를 찾는 내부 장치를 감염시킵니다	• Cygna Labs DNS 방화벽 서비스 피드를 사용한 DNS 방화벽 사용 • DDI Guard를 사용한 DNS 방화벽 이벤트 감사
APT	(R)Advanced Persistent threats	공격자는 네트워크 내에 적응형 멀웨어를 배포하여 통신을 방해하거나 정보를 탈취하는 악의적인 기능을 수행합니다	• Cygna Labs DNS 방화벽 서비스 피드를 사용한 DNS 방화벽 사용 • Cygna Radar로 DNS 터널 차단 및 포렌식 수행

For more information about Cygna Labs products and services, please contact us at
Toll Free: **(844) 442-9462** | International: **+1 (305) 501-2430** | Email: **sales@cygnalabs.com**
Cygna Labs Corp. | 1111 Lincoln Road, Suite 760 | Miami Beach, FL 33139 | United States