Nimda 바이러스로부터 네트워크를 보호하는 방법

목차

소개

이 문서에서는 Nimda(님다) 지렁이 네트워크에 미치는 영향을 최소화하는 방법을 설명합니다.이 문서에서는 두 가지 주제를 다룹니다.

- 네트워크가 감염되었으며, 무엇을 할 수 있습니까?어떻게 하면 피해와 결과를 최소화할 수 있을까요?
- 네트워크가 아직 감염되지 않았거나 일부만 감염되었습니다.이 벌레의 확산을 최소화하기 위해 할 수 있는 일은 무엇인가?

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

Nimda worm에 대한 배경 정보는 다음 링크를 참조하십시오.

- http://www.cert.org/body/advisories/CA200126_FA200126.html
- http://vil.nai.com/vil/content/v_99209.htm
- http://www.sarc.com/avcenter/venc/data/w32.nimda.a@mm.html

지원되는 플랫폼

이 문서에 설명된 NBAR(Network-based application recognition) 솔루션에는 Cisco IOS® 소프트웨어 내에서 클래스 기반 마킹 기능이 필요합니다.특히 HTTP URL의 모든 부분에서 매칭하는 기능은 NBAR 내의 HTTP 하위 포트 분류 기능을 사용합니다.지원되는 플랫폼 및 최소 Cisco IOS 소프트웨어 요구 사항은 아래에 요약되어 있습니다.

플랫폼	최소 Cisco IOS 소프트웨어 버전
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(5)T

참고: NBAR(Network-Based Application Recognition)를 사용하려면 Cisco CEF(Express Forwarding)를 활성화해야 합니다.

NBAR는 릴리스 12.1E부터 일부 Cisco IOS 소프트웨어 플랫폼에서도 지원됩니다.네트워크 기반 애플리케이션 인식 문서에서 "지원되는 프로토콜"을 참조하십시오.

클래스 기반 마킹 및 DNBAR(Distributed NBAR)는 다음 플랫폼에서도 사용할 수 있습니다.

플랫폼	최소 Cisco IOS 소프트웨어 버전
7500	12.1(6)E
FlexWAN	12.1(6)E

NBAR를 구축하는 경우 Cisco 버그 ID CSCdv06207(등록된 고객만 해당)에 유의하십시오. 이 결함이 발생할 경우 CSCdv06207에 설명된 해결 방법이 필요할 수 있습니다.

ACL(Access Control List) 솔루션은 모든 최신 Cisco IOS 소프트웨어 릴리스에서 지원됩니다.

Modular QoS(Quality of Service) CLI(command line interface)를 사용해야 하는 솔루션의 경우(예: 속도 제한 ARP 트래픽 또는 CAR 대신 폴리서 속도 제한 구현), Cisco IOS 소프트웨어 릴리스 12.0XE, 12.1E, 12.1T 및 모든 릴리스에서 사용 가능한 Modular Quality of Service Command-Line Interface가 필요합니다. ...을 클릭합니다.

CAR(Committed Access Rate)을 사용하려면 Cisco IOS 소프트웨어 릴리스11.1CC와 12.0 이상의 모든 릴리스가 필요합니다.

피해를 최소화하고 결과를 제한하는 방법

이 섹션에서는 Nimda 바이러스를 확산시킬 수 있는 감염 벡터에 대해 간략하게 설명하고 바이러스 확산을 줄이기 위한 팁을 제공합니다.

- 이 worm은 MIME 오디오/x-wav 유형의 이메일 첨부 파일을 통해 전파될 수 있습니다.**팁**:SMTP(Simple Mail Transfer Protocol) 서버에 다음 첨부 파일이 있는 이메일을 차단하도록 규칙을 추가합니다.readme.exeAdmin.dll
- Javascript 실행이 활성화된 상태에서 감염된 웹 서버를 탐색하고 MS01-020 (예: IE 5.0 또는 IE 5.01(SP2 제외)에서 설명한 익스플로잇에 취약한 IE(Internet Explorer) 버전을 사용할 때 WORM이 분산될 수 있습니다.**팁:**Netscape를 브라우저로 사용하거나 IE에서 Javascript를 비활성화하거나 SP II에 IE를 패치합니다.Cisco NBAR(Network-based application recognition)를 사용하여 readme.eml 파일이 다운로드되지 않도록 필터링합니다.다음은 NBAR를 구성하는 예입니다.

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*readme.eml*"
```

트래픽을 매칭한 후에는 트래픽을 폐기하거나 Policy Based Route를 선택하여 감염된 호스트를 모니터링할 수 있습니다.전체 구현의 예는 "코드 레드" WORM 차단을 위해 네트워크 기반 애플리케이션 인식 및 액세스 제어 목록 사용을 참조하십시오.
- 이 worm은 IIS 공격의 형태로 시스템 간에 전파될 수 있습니다(주로 코드 Red II의 효과로 생성된 취약성을 악용하려고 시도하지만, 이전에 MS00-078 에서 패치한 취약성도 악용합니다).**팁**:에 설명된 코드 빨간색 구성표를 사용합니다."코드 레드(Code Red)" WORM으로 인한 악성코드 및 높은 CPU 사용률 처리네트워크 기반 애플리케이션 인식 및 액세스 제어 목록을 사용하여 "코드 레드" WORM 차단

```
Router(config)#class-map match-any http-hacks
Router(config-cmap)#match protocol http url "*.ida*"
Router(config-cmap)#match protocol http url "*cmd.exe*"
Router(config-cmap)#match protocol http url "*root.exe*"
Router(config-cmap)#match protocol http url "*readme.eml*"
```

트래픽을 매칭한 후에는 트래픽을 폐기하거나 Policy Based Route를 선택하여 감염된 호스트를 모니터링할 수 있습니다.전체 구현의 예는 "코드 레드" WORM 차단을 위해 네트워크 기반 애플리케이션 인식 및 액세스 제어 목록 사용을 참조하십시오.속도 제한 TCP 동기화/시작(SYN) 패킷이렇게 하면 호스트가 보호되지는 않지만, 네트워크를 성능이 저하된 방식으로 실행하고 계속 작동할 수 있습니다.SYN을 속도 제한함으로써 특정 속도를 초과하는 패킷을 버리기 때문에 일부 TCP 연결은 통과하지만 전부는 아닙니다.컨피그레이션 예는 Using CAR During DOS Attacks(DOS 공격 중 CAR 사용)의 "Rate Limiting for TCP SYN Packets(TCP SYN 패킷 속도 제한)" 섹션을 참조하십시오.ARP 스캔의 양이 네트워크에서 문제를 일으키는 경우 속도 제한 ARP(Address Resolution Protocol) 트래픽을 고려하십시오.ARP 트래픽을 rate-limit 하려면 다음을 구성합니다.

```
class-map match-any arp
   match protocol arp
!
!
policy-map ratelimitarp
   class arp
      police 8000 1500 1500 conform-action transmit exceed-action drop violate-action drop
```

그런 다음 이 정책을 관련 LAN 인터페이스에 출력 정책으로 적용해야 합니다.네트워크에서 허용할 초당 ARP 수를 적절히 수정합니다.
- Active Desktop이 활성화된 탐색기에서 .eml 또는 .nws를 강조 표시하여 WORM을 분산할 수

있습니다(기본적으로 W2K/ME/W98). 그러면 THUMBW.DLL이 파일을 실행하고 IE 버전 및 영역 설정에 따라 README.EML을 다운로드하려고 시도합니다.**팁:** 위에서 권장하는 대로 NBAR를 사용하여 readme.eml을 다운로드하지 않도록 필터링합니다.

- WORM은 매핑된 드라이브를 통해 확산될 수 있습니다.네트워크 드라이브를 매핑한 감염된 시스템은 매핑된 드라이브와 하위 디렉터리에 있는 모든 파일을 감염시킬 수 있습니다**팁:**감염된 시스템에서 TFTP를 사용하여 감염되지 않은 호스트로 파일을 전송할 수 없도록 TFTP(Block Trivial File Transfer Protocol)(포트 69).라우터에 대한 TFTP 액세스를 계속 사용할 수 있는지 확인합니다(코드 업그레이드 경로가 필요할 수 있음). 라우터에서 Cisco IOS 소프트웨어 버전 12.0 이상을 실행하는 경우 Cisco IOS 소프트웨어를 실행하는 라우터로 이미지를 전송하기 위해 항상 FTP(File Transfer Protocol)를 사용할 수 있습니다.NetBIOS를 차단합니다.NetBIOS는 LAN(Local Area Network)을 벗어날 필요가 없습니다. 통신 사업자는 포트 137, 138, 139 및 445를 차단하여 NetBIOS를 필터링해야 합니다.
- 이 지렁이는 다른 시스템을 감염시키기 위해 이메일을 보내는 데 자체 SMTP 엔진을 사용합니다.**팁:** 네트워크 내부 부분의 SMTP(Block Port 25).POP(Post Office Protocol) 3(포트 110) 또는 IMAP(Internet Mail Access Protocol)(포트 143)을 사용하여 전자 메일을 검색하는 사용자는 포트 25에 액세스할 필요가 없습니다. 네트워크용 SMTP 서버를 향하도록 포트 25만 열 수 있습니다.Eudora, Netscape 및 Outlook Express를 사용하는 사용자는 자체 SMTP 엔진을 가지고 있고 포트 25를 사용하여 아웃바운드 연결을 생성하므로 이 작업을 수행할 수 없습니다. 프록시 서버 또는 기타 메커니즘의 사용 가능성에 일부 조사를 적용해야 할 수 있습니다.
- Cisco CallManager/애플리케이션 서버 정리**팁:** 네트워크에 통화 관리자 및 Call Manager 애플리케이션 서버가 있는 사용자는 바이러스 확산을 중지하려면 다음을 수행해야 합니다.Call Manager에서 감염된 시스템을 찾아서는 안 되며 Call Manager 서버에서 드라이브를 공유해서는 안 됩니다.Nimda 바이러스를 청소하기 위해 Cisco CallManager 3.x 및 CallManager Applications Server에서 Nimda Virus를 청소하는 지침을 따릅니다.
- CSS 11000에서 Nimda 바이러스 필터링**팁:** CSS 11000을 사용하는 사용자는 NIMDA 바이러스를 지우려면 CSS 11000에서 Nimda 바이러스 필터링에 제공된 지침을 따라야 합니다.
- Nimda 바이러스에 대한 Cisco CS IDS(Secure Intrusion Detection System) 응답**팁:** CS IDS에는 두 가지 구성 요소가 있습니다.하나는 호스트 센서가 있는 HIDS(호스트 기반 IDS)와 네트워크 센서가 있는 NIDS(네트워크 기반 IDS)입니다. 둘 다 Nimda 바이러스에 다른 방식으로 응답합니다.자세한 설명과 권장 조치 방법은 Cisco Secure IDS Response to the Nimda Virus(Nimda Virus에 Cisco 보안 IDS가 어떻게 대응하는지)를 참조하십시오.

관련 정보

- 네트워크 기반 애플리케이션 인식 및 액세스 제어 목록을 사용하여 "코드 레드" WORM 차단
- "코드 레드(Code Red)" WORM으로 인한 악성코드 및 높은 CPU 사용률 처리
- DOS 공격 중 CAR 사용
- Cisco 보안 자문 및 통지
- 기술 지원 및 문서 – Cisco Systems