ESA FAQ:Outbreak Filter/VOF(Virus Outbreak Filter) FAQ

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 Outbreak Filter 또는 VOF(Virus Outbreak Filter)와 관련하여 자주 묻는 몇 가지 질문에 대해 설명하고 이에 대한 답변을 제공합니다.

Outbreak Filter란?

> **참고**: 현재 실행 중인 AsyncOS for Email Security 버전에 대한 사용 설명서를 검토하십시오. 예: AsyncOS 13.0 for Cisco Email Security Appliances 사용 설명서, 장:신종 바이러스 필터

Outbreak Filter는 대규모 바이러스 침투 및 피싱 스캠, 악성코드 배포 등 비바이러스성(non-viral) 공격이 발생하는 경우 네트워크를 보호합니다.데이터가 수집되고 소프트웨어 업데이트가 게시될 때까지 새로운 보안 침해를 탐지할 수 없는 대부분의 악성코드 차단 보안 소프트웨어와 달리, Cisco는 전파 시 보안 침해 데이터를 수집하고 업데이트된 정보를 실시간으로 ESA에 전송하여 이러한 메시지가 사용자에게 도달하는 것을 방지합니다.

Cisco는 글로벌 트래픽 패턴을 사용하여 수신 메시지가 안전한지 아니면 전파 확산의 일부인지를 결정하는 규칙을 개발합니다.Cisco의 업데이트된 Outbreak 정보를 기반으로 안전하다고 판단될 때까지 Outbreak의 일부인 메시지가 격리되거나 Sophos 및 McAfee에서 새로운 안티바이러스 정의를 게시합니다.

소규모의 비 바이러스성 공격에 사용되는 메시지는 합법적인 디자인, 수신자의 정보, 사용자 지정 URL을 사용하여 짧은 시간 동안만 온라인 상태이고 웹 보안 서비스에 알려지지 않은 피싱 및 악성코드 웹 사이트를 가리킵니다.Outbreak Filter는 메시지 내용을 분석하고 URL 링크를 검색하여 이러한 유형의 비 바이러스성 공격을 탐지합니다.Outbreak Filter는 웹 보안 프록시를 통해 잠재적으로 유해한 웹 사이트로 트래픽을 리디렉션하도록 URL을 재작성할 수 있습니다. 이 경우 액세스하려는 웹 사이트가 악의적일 수 있음을 사용자에게 경고하거나 웹 사이트를 완전히 차단합니다.

ESA에서 Sophos 또는 McAfee Anti-Virus를 실행하고 있지 않더라도 Outbreak Filter를 사용할 수 있습니까?

바이러스 첨부 파일에 대한 방어를 강화하기 위해 Outbreak Filter 외에도 Sophos 또는 McAfee Anti-Virus를 활성화하는 것이 좋습니다.그러나 Outbreak Filter는 Sophos 또는 McAfee Anti-Virus를 활성화하지 않고도 독립적으로 작동할 수 있습니다.

Outbreak Filter는 언제 메시지를 격리합니까?

메시지가 현재 Outbreak Rules 및 메일 관리자가 설정한 임계값을 충족하거나 초과하는 파일 첨부 파일이 포함된 경우 격리됩니다.Cisco는 유효한 기능 키가 있는 각 ESA에 현재 Outbreak Rules를 게시합니다. Cisco의 업데이트된 Outbreak 정보를 기반으로 보안 상태가 될 때까지 또는 Sophos 및 McAfee에서 새 안티바이러스 정의를 게시할 때까지 Outbreak의 일부인 메시지가 격리됩니다.

Outbreak Filter 규칙은 어떻게 작성됩니까?

Outbreak 규칙은 Cisco SIO(Security Intelligence Operations)가 게시합니다. 이 보안 에코시스템은 글로벌 위협 정보, 평판 기반 서비스, Cisco 보안 어플라이언스의 정교한 분석을 연결하여 더 빠른 응답 시간으로 더 강력한 보호를 제공합니다. 기본적으로 어플라이언스는 서비스 업데이트의 일부로 5분마다 새 Outbreak 규칙을 확인하고 다운로드합니다.

SIO는 세 가지 구성 요소로 구성됩니다.

- SenderBase, 세계 최대 규모의 위협 모니터링 네트워크 및 취약성 데이터베이스
- Cisco의 글로벌 보안 분석가 및 자동화된 시스템으로 구성된 Talos입니다.
- 동적 업데이트, 전파 확산이 발생할 때 어플라이언스에 자동으로 실시간 업데이트 제공

Outbreak Filter를 구성하는 모범 사례가 있습니까?

네. 서비스 레벨에 대한 권장 사항은 다음과 같습니다.

- 적응형 *규칙 활성화*
- 최대 *메시지 크기를 스캔으로* 2M으로 설정
- *웹 상호 작용 추적 사용*

수신 메일 정책 레벨의 컨피그레이션은 고객별, 정책별로 결정되어야 합니다.

잘못된 Outbreak Filter 규칙을 보고하려면 어떻게 해야 합니까?

다음 두 가지 방법 중 하나로 오탐 또는 오탐을 보고할 수 있습니다.

1. Cisco 지원 사례 열기: https://mycase.cloudapps.cisco.com/case
2. Talos로 평판 티켓 열기:https://talosintelligence.com/reputation_center/support

다음은 Outbreak Filtering 규칙을 구체화할 수 있는 조건입니다.

- 파일 확장명
- File Signature(Magic)(파일의 'true' 유형을 나타내는 이진 서명)

- URL
- 파일 이름
- 파일 크기

Outbreak 격리가 가득 차면 어떻게 됩니까?

격리가 할당된 최대 공간을 초과하거나 메시지가 최대 시간 설정을 초과하면 메시지가 격리에서 자동으로 정리되어 제한 내에서 유지됩니다.메시지는 FIFO(First-In, First-Out) 기준으로 제거됩니다.즉, 가장 오래된 메시지가 먼저 삭제됩니다.격리를 해제(즉, 전달)하거나 격리에서 삭제해야 하는 메시지를 삭제하도록 구성할 수 있습니다.메시지를 릴리스하도록 선택한 경우 메시지가 쿼런틴에서 제외되었음을 수신자에게 알릴 지정된 텍스트와 함께 제목 줄에 태그를 지정할 수 있습니다.

Outbreak 격리에서 릴리스된 메시지는 안티바이러스 모듈에서 다시 검사되며 안티바이러스 정책에 따라 조치가 수행됩니다.이 정책에 따라, 바이러스 첨부 파일이 제거된 메시지를 전달, 삭제 또는 전달할 수 있습니다.Outbreak 격리에서 릴리스된 후 재스캔하는 동안 바이러스가 자주 발견됩니다.ESA mail_logs 또는 메시지 추적을 참조하여 격리에 표시된 개별 메시지가 바이러스인지 여부, 전달되었는지 여부 및 방법을 확인할 수 있습니다.

시스템 격리가 채워지기 전에 격리가 75% 찼을 때 알림이 전송되고, 95% 찼을 때 또 다른 알림이 전송됩니다.Outbreak Quarantine에는 특정 바이러스 위협 레벨(VTL)과 일치하는 모든 메시지를 삭제하거나 릴리스할 수 있는 추가 관리 기능이 있습니다. 이를 통해 특정 바이러스 위협을 해결하는 안티바이러스 업데이트를 받은 후 격리를 쉽게 정리할 수 있습니다.

Outbreak Rule에 대한 위협 레벨의 의미는 무엇입니까?

Outbreak Filter는 0~5 사이의 위협 레벨 아래에서 작동합니다. 위협 레벨은 바이러스 전파 확산 가능성을 낮춥니다.바이러스 전파 확산의 위험에 따라 위협 레벨이 의심스러운 파일의 격리에 영향을 미칩니다.위협 레벨은 네트워크 트래픽, 의심스러운 파일 활동, 안티바이러스 벤더의 입력, Cisco SIO의 분석 등 다양한 요소를 기반으로 합니다. 또한 Outbreak Filter를 사용하면 메일 관리자가 네트워크에 대한 위협 수준의 영향을 늘리거나 줄일 수 있습니다.

레벨	위험	의미
0	없음	메시지가 위협.
1	낮음	메시지가 위협 낮습니다.
2	낮음/보통	메시지가 위협 낮음에서 중간 값까지입니다."의심" 위협.
3	중간	메시지가 확인된 보안 침해의 일부이거나 콘텐츠가 보안 침해로 인해 위협.
4	높음	메시지가 대규모 보안 침해의 일부로 확인되었거나 콘텐츠가 매우 위험합니다.
5	익스트림	메시지 내용은 매우 큰 규모 또는 큰 규모이며 매우 위험한 전파 확산의 일부로 확인됩니다

신종 바이러스 발생 시 알림을 받으려면 어떻게 해야 합니까?

Outbreak Filter에서 새로운/업데이트 규칙을 수신하여 특정 유형의 메시지 프로필에 대한 격리 위협 레벨을 높이는 경우 구성된 알림 이메일 주소로 전송되는 이메일 메시지를 통해 알림을 받을 수 있습니다.위협 레벨이 구성된 임계값 아래로 떨어지면 다른 알림이 전송됩니다.따라서 바이러스 첨부 파일의 진행 상태를 모니터링할 수 있습니다. 이러한 이메일은 "Info" 이메일로 전송됩니다.

> **참고:**이러한 이메일 알림을 수신하려면 alertconfig 명령 또는 GUI를 사용하여 CLI에서 알림이 전송되는 이메일 주소를 확인합니다.**System Administration(시스템 관리) > Alerts(경고)**.

구성을 구성하거나 검토하려면

- GUI:Security Services(보안 서비스) > Outbreak Filters를 선택하고 Edit Global Settings(전역 설정 편집...) 아래의 컨피그레이션을 검토합니다.
- CLI: outbreakconfig > 설정

예:

```
> outbreakconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine esa2.hc3033-47.iphmx.com).

What would you like to do?
1. Switch modes to edit at mode "Cluster Hosted_Cluster".
2. Start a new, empty configuration at the current mode (Machine esa2.hc3033-47.iphmx.com).
3. Copy settings from another cluster mode to the current mode (Machine esa2.hc3033-
47.iphmx.com).
[1]>

Outbreak Filters: Enabled

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back down
below), meaning that new messages of certain types could be quarantined or will no longer be
quarantined, respectively.


Would you like to receive Outbreak Filter alerts? [Y]> y

What is the largest size message Outbreak Filters should scan?
[2097152]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently enabled.

Do you wish to disable logging of URL's? [N]>

Web Interaction Tracking is currently enabled.

Do you wish to disable Web Interaction Tracking? [N]>

The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable Outbreak
Filters for the desired Incoming and Outgoing Mail Policies.
```

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- 기술 지원 및 문서 – Cisco Systems