ESA AMP(Advanced Malware Protection) 테스트

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)의 AMP(Advanced Malware Protection) 기능을 테스트하고 확인하는 방법에 대해 설명합니다.

ESA에서 AMP 테스트

AMP는 AsyncOS 8.5 for the ESA 릴리스를 통해 첨부 파일에서 악성코드를 탐지하기 위해 파일 평판 검사 및 파일 분석을 수행합니다.

기능 키

AMP를 구현하려면 ESA에서 **파일 평판** 및 **파일 분석** 모두에 대해 유효한 활성 기능 키가 있어야 합니다.기능 키를 확인하려면 **System Administration(시스템 관리) > Feature Keys(**GUI)를 **방문하거나** CLI에서 featurekeys를 사용합니다.

보안 서비스

GUI에서 서비스를 활성화하려면 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)로 이동합니다**.CLI에서 ampconfig를 실행할 수 **있습니다**.컨피그레이션에 변경 사항을 제출하고 커밋합니다.

수신 메일 정책

서비스를 활성화한 후에는 이 서비스가 수신 메일 정책과 연결되어 있어야 합니다.

1. Mail Policies(**메일 정책) > Incoming Mail Policies(수신 메일 정책)로 이동합니다**.
2. 필요에 따라 **기본 정책** 또는 사전 구성된 정책을 선택합니다. [수신 메일 정책] 페이지의 [**Advanced Malware** Protection] 열이 표시됩니다.
3. 열에 **Disabled**(비활성화됨) 링크를 선택하고 옵션 페이지에서 **Enable File Reputation(파일 평판 활성화)** 및 **Enable File Analysis(파일 분석** 활성화)를 선택합니다.
4. 필요에 따라 메시지 검사, 검사할 수 없는 첨부 파일에 대한 작업, 양성으로 식별된 메시지에 대한 작업을 추가로 구성할 수 있습니다.
5. 컨피그레이션에 변경 사항을 제출하고 커밋합니다.

테스트

현재 수신 메일 정책은 악성코드를 검사하고 탐지할 수 있습니다.테스트할 실제 악성코드 샘플이 있어야 합니다.유효한 예제가 필요한 경우 European Institute for Computer Antivirus Research(eicar) 다운로드 페이지를 방문하십시오.

> **주의**: Cisco는 이러한 파일이나 AV 스캐너와 이러한 파일을 함께 사용할 경우 컴퓨터 또는 네트워크 환경에 손상이 발생할 경우 책임을 지지 않습니다.이러한 파일은 사용자 자신의 위험으로 다운로드할 수 있습니다. AV 스캐너, 컴퓨터 설정 및 네트워크 환경을 충분히 안전하게 사용하는 경우에만 다운로드하십시오.이 정보는 테스트 및 복제 목적으로 제공됩니다.

유효한 사전 구성된 이메일 어카운트를 사용하여 ESA 및 일반 처리를 통해 첨부 파일을 전송합니다.ESA의 CLI를 사용하고, **tail mail_logs를** 사용하여 처리 중인 메일을 모니터링할 수 있습니다.메일 로그에 MID(Message ID)가 나열됩니다. 다음과 유사한 출력이 표시됩니다.

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
policy DEFAULT in the inbound table
```

```
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

이전 예에서는 AMP가 악성코드 첨부 파일을 탐지하여 기본 설정에 따라 최종 작업으로 드롭되었음을 보여줍니다.

GUI의 Message Tracking(메시지 추적)에서도 동일한 세부사항이 표시됩니다.

18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 contains attachment 'eicar.com' (SHA256 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f).
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 scanned by Advanced Malware Protection engine. Final verdict: malicious
18 Sep 2014 21:54:30 (GMT -04:00)	Message 1655 attachment 'eicar.com' scanned by Advanced Malware Protection engine. Verdict: Positive
18 Sep 2014 21:54:30 (GMT -04:00)	Message ID 1655 rewritten to new message ID 1656 by AMP.

Incoming Mail Policies(수신 메일 정책)에서 양성으로 식별된 악성코드 또는 AMP 컨피그레이션의 기타 고급 옵션을 전달하도록 선택한 경우 다음 메일 처리 결과가 표시될 수 있습니다.

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

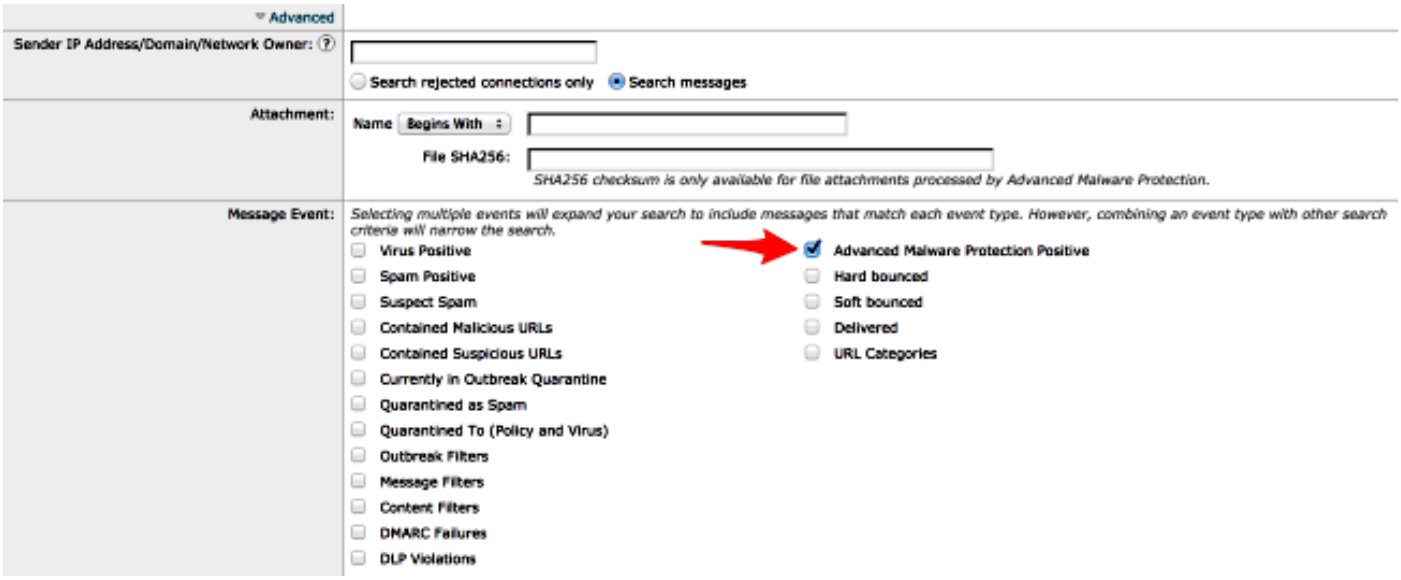
평판 판정은 표시된 대로 **MALWARE**에 대해 여전히 긍정적입니다. 재작성된 조치는 메시지 수정 작업 및 **[경고:탐지된 악성코드**.

처리 시 악성코드로 식별되지 않은 정상 파일 또는 파일은 다음 판정을 메일 로그에 기록합니다.

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

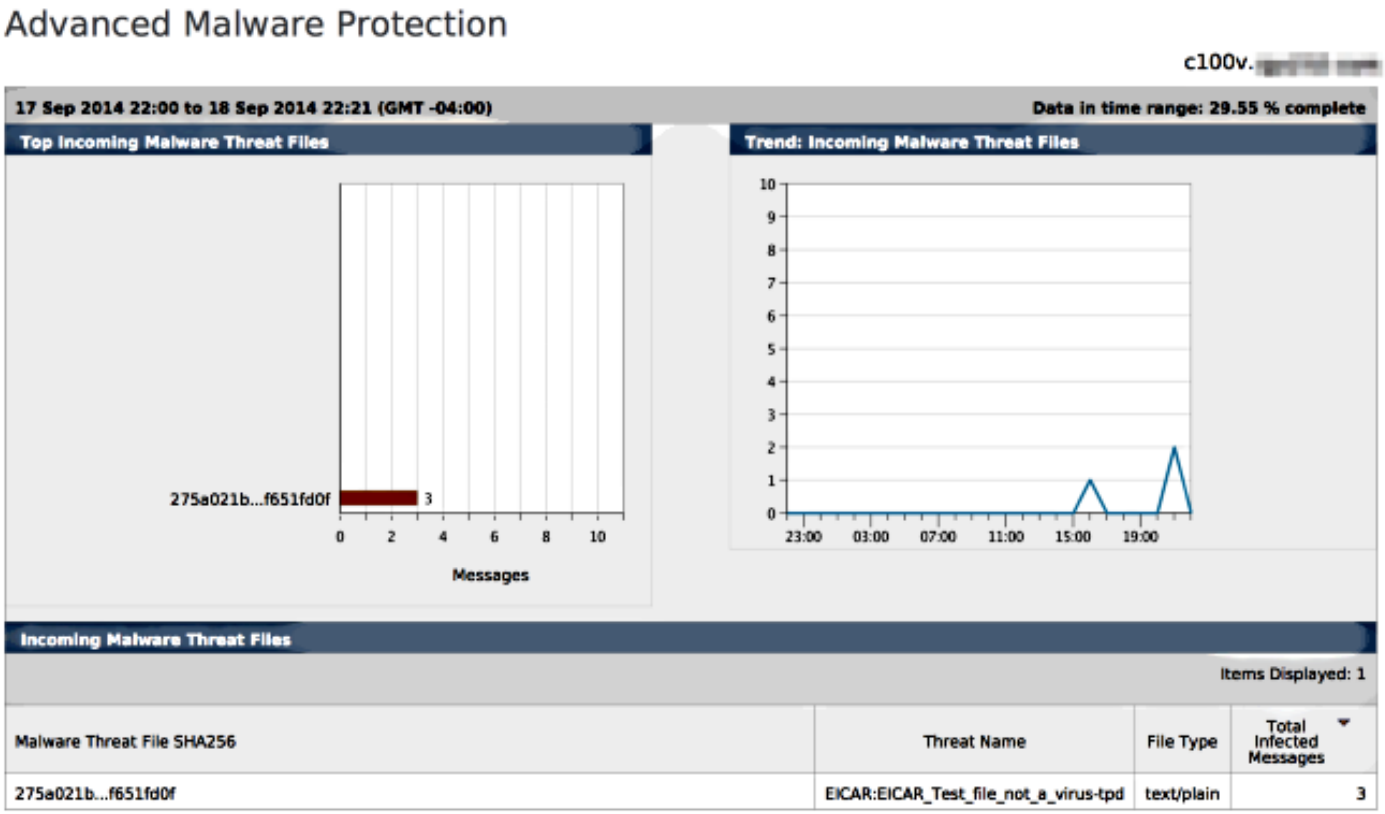
AMP+ 메시지에 대한 고급 메시지 추적

또한 GUI에서 Message Tracking(메시지 추적) 및 Advanced(고급) 드롭다운 메뉴를 사용할 때 Advanced Malware Protection Positive(지능형 악성코드 차단) 메시지를 직접 검색하도록 선택할 수 있습니다.



AMP 보고서

ESA GUI에서 AMP를 통해 양성으로 식별된 메시지에 대한 보고서 추적도 볼 수 있습니다 .Monitor(**모니터링) > Advanced Malware Protection(Advanced Malware Protection)**으로 이동하고 필요에 따라 시간 범위를 수정합니다.입력에 대한 이전 예와 함께 비슷한 것을 볼 수 있습니다.



문제 해결

AMP에서 긍정적으로 스캔하는 알려진 실제 악성코드 파일이 표시되지 않으면 메일 로그를 검토하여 AMP에서 메시지를 검사하기 전에 다른 서비스가 메시지 및/또는 첨부 파일에 대해 조치를 취하지 않았는지 확인합니다.

사용된 이전 예에서 Sophos Anti-virus가 활성화된 경우 실제로 첨부 파일을 찾아 조치를 취합니다.

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
```

```
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

수신 메일 정책의 Sophos Anti-virus 구성 설정은 바이러스 감염 메시지에 대해 **삭제하도록** 설정되어 있습니다. 이 경우 AMP에 도달하지 않아 첨부 파일을 스캔하거나 조치를 취할 수 없습니다.

항상 그런 것은 아니다.다른 서비스 또는 콘텐츠/메시지 필터가 MID에 대해 조치를 취하지 않고 AMP 처리 및 조치에 도달하기 전에 조치를 취하지 않았는지 확인하기 위해 메일 로그 및 MID(Message ID)를 검토해야 할 수 있습니다.

관련 정보

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