Malwarebytes

Emotet-Notfall-Kit

Was ist Emotet?

Emotet ist für Unternehmen derzeit eine der häufigsten und weit verbreiteten Bedrohungen. Dieser Downloader, der sich aus einem Trojaner heraus entwickelt hat, hält sich seit fast einem Jahr an der Spitze der Erkennungen von Malwarebytes. Emotet wird auf Unternehmen rund um die Welt losgelassen, verleitet Benutzer dazu, Endpunkte über Phishing-E-Mails zu infizieren und verbreitet sich anschließend lateral in Netzwerken, indem es gestohlene NSA-Exploits ausnutzt. Aufgrund seiner modularen, polymorphischen Form und seiner Fähigkeit, mehrere, sich verändernde Payloads einzuschleusen, ist Emotet sowohl Cybersicherheitsforschern als auch IT-Teams ein Dorn im Auge.

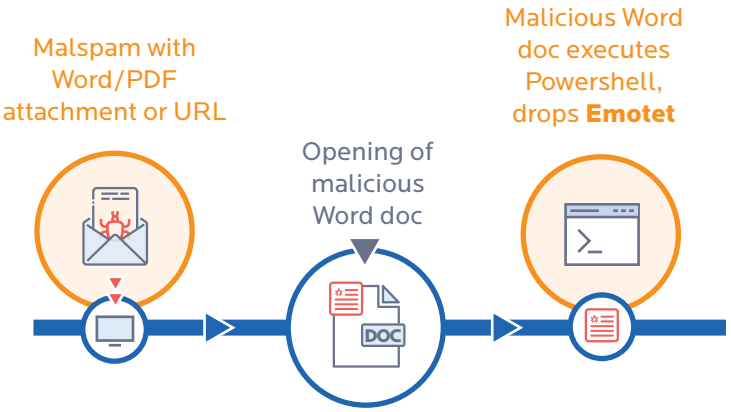
Warum ist Emotet für Ihr Unternehmen gefährlich?

Emotet trat zunächst als ein Banking-Trojaner auf, doch dank seiner effektiven Kombination von Persistenz und Netzwerkverbreitung hat es sich in einen beliebten Infektionsmechanismus für andere Formen von Schadsoftware entwickelt, wie zum Beispiel TrickBot und Ryuk-Ransomware. Außerdem ist Emotet dafür bekannt, dass es eine der am schwierigsten zu beseitigenden Infektionen ist, nachdem es das Netzwerk einer Organisation infiltriert hat.

Was seine Beseitigung so schwierig macht, ist die bereits erwähnte laterale Bewegung über NSA-Exploits, insbesondere EternalBlue, mit dem der Ausbruch der WannaCry-Ransomware 2017 verbreitet wurde. EternalBlue erfordert, dass Administratoren eine strenge Richtlinie zur Isolation infizierter Endpunkte vom Netzwerk, zum Patchen, zum Deaktivieren administrativer Freigaben und schließlich zum Entfernen des Trojaners einhalten, bevor die Verbindung mit dem Netzwerk wiederhergestellt wird – andernfalls lässt sich mit Sicherheit davon ausgehen, dass die bereinigten Endpunkte immer wieder durch andere infizierte Endpunkte infiziert werden.

Wenn man zudem noch bedenkt, dass ständig neue Funktionen entwickelt werden, wie zum Beispiel VM-Fähigkeit, Vermeidung von Spamfiltern oder Deinstallation von Sicherheitsprogrammen, dann liegt es auf der Hand, warum Emotet sich zum Albtraum von Netzwerkadministratoren entwickelt hat.

Emotet Infektionsvektor



BRAUCHEN SIE HILFE BEI EINER INFIZIERUNG?

Kontaktieren Sie uns unter emeasales@malwarebytes.com, damit sich einer unserer Sicherheitsexperten mit Ihnen in Verbindung setzt.

malwarebytes.com/business emeasales@malwarebytes.com

Malwarebytes ist ein Unternehmen für Cybersicherheit, dem Millionen Menschen weltweit vertrauen. Malwarebytes schützt Endanwender und Unternehmen proaktiv vor bösartigen Bedrohungen, einschließlich Ransomware, die herkömmlichen Antivirusprogrammen entgehen. Das führende Produkt des Unternehmens verwendet signaturfreie Technologien, um einen Cyberangriff zu erkennen und zu stoppen, bevor er Schaden anrichtet. Erfahren Sie mehr dazu unter www.malwarebytes.com.

Malwarebytes

Tipps für **die Beseitigung**

Remediation tips

Malwarebytes kann Emotet in Unternehmensendpunkten erkennen und beseitigen, ohne dass eine Benutzerinteraktion dazu erforderlich ist. Um auf vernetzten Rechnern wirkungsvoll zu sein, sind jedoch weitere Schritte notwendig.

- [ ] **1.** Identifizieren Sie die infizierten Rechner. Wenn ungeschützte Endpunkte/Rechner vorhanden sind, können Sie das Farbar Recovery Scan Tool (FRST) ausführen, um mögliche Bedrohungsindikatoren (IOC) aufzuspüren. Abgesehen von der Bestätigung einer Infizierung kann FRST zur Bestätigung einer Beseitigung verwendet werden, bevor ein Endpunkt/Rechner erneut mit dem Netzwerk verbunden wird. In der Anleitung für das Farbar Recovery Scan Tool finden Sie Einzelheiten zur Installation und Ausführung eines FRST-Scans.
- [ ] **2.** Suchen Sie in der Datei FRST.txt nach den folgenden IOC:
  - HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\1A345B7
  - HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\12C4567D
  - (Gornyk) C:\Windows\SysWOW64\servicedcom.exe
  - C:\WINDOWS\12345678.EXE
  - C:\WINDOWS\SYSWOW64\SERVERNV.EXE
  - C:\WINDOWS\SYSWOW64\NUMB3R2ANDL3373RS.EXE
  - C:\WINDOWS\TEMP\1A2B.TMP
- [ ] **3.** Trennen Sie die infizierten Rechner vom Netzwerk.
- [ ] **4.** Wenden Sie den Patch für EternalBlue an.
- [ ] **5.** Deaktivieren Sie die administrativen Freigaben. Windows Server gibt durch standardmäßige Installation verborgene Freigabeordner frei, die speziell für den Administratorzugriff auf andere Rechner vorgesehen sind. Die Admin$-Freigaben werden von Emotet verwendet, nachdem es das lokale Adminkennwort über die Brute-Force-Methode in seine Gewalt gebracht hat. Ein Dateifreigabe-Server hat eine IPC$-Freigabe, die von Emotet abgefragt wird, um eine Liste aller Endpunkte zu erhalten, die damit verbunden sind. Diese AdminIP-Freigaben sind in der Regel durch die UAC-Sicherheitsfunktion geschützt, doch Windows lässt den lokalen Administrator ohne eine Aufforderung durch.

  Die allerneuesten Emotet-Varianten verwenden C$ mit den Admin-Anmeldeinformationen, um sich frei zu bewegen und all die anderen Endpunkte erneut zu infizieren.

  Es empfiehlt sich, diese Admin$-Freigaben über die Registry zu deaktivieren. Wenn Sie diesen Registry-Schlüssel nicht finden, können Sie ihn manuell hinzufügen und so einrichten, dass er deaktiviert ist.
- [ ] **6.** Entfernen Sie den Emotet-Trojaner.
- [ ] **7.** Ändern Sie die Konto-Anmeldeinformationen, einschließlich lokale und Domain-Administratorkennwörter. Wiederholte Infizierungen sind ein Anzeichen dafür, dass der Wurm Erfolg damit hatte, das Administratorkennwort zu erraten oder zu erzwingen.

Tipps für den Schutz

Um Emotet von Endpunkten fernzuhalten, empfehlen sich die folgenden Best Practices – für Sie wie auch für Ihre Mitarbeiter.

- [ ] **1.** Scannen Sie E-Mails, die einen Anhang enthalten, damit MalSpam den Endbenutzer gar nicht erst erreicht.
- [ ] **2.** Schulen Sie Ihre Mitarbeiter, vor allem diejenigen, die schon einmal reingelegt wurden, damit sie Phishing-Versuche (die Methode, mit der sich Emotet verbreitet) erkennen und sie an die zuständigen Stellen in Ihrem Unternehmen melden.
- [ ] **3.** Schulen Sie die Fähigkeit des Emotet-Reaktionsteams, damit es eine Emotet-Kampagne erkennt, potenziell infizierte Hosts identifiziert, Aktionen auf den manipulierten Rechnern feststellt und bestätigt, ob Datenklau stattgefunden hat.
- [ ] **4.** Wenden Sie auf sämtliche Software, Systeme oder Browser bei Bedarf Patches an.
- [ ] **5.** Beschränken Sie administrative Freigaben auf das absolute Minimum, um den Emotet-Schaden in Grenzen zu halten.
- [ ] **6.** Verwenden Sie starke Kennwörter mit Multi-Faktor-Authentifizierung oder erwägen Sie die Einführung eines Einzelkennwort-Managers in der gesamten Organisation.
- [ ] **7.** Investieren Sie in Anti-Exploit-Technologie, um zu verhindern, dass sich laterale Infektionen wie Emotet im Netzwerk verbreiten.

BRAUCHEN SIE HILFE BEI EINER INFIZIERUNG?

Kontaktieren Sie uns unter emeasales@malwarebytes.com, damit sich einer unserer Sicherheitsexperten mit Ihnen in Verbindung setzt.

malwarebytes.com/business emeasales@malwarebytes.com