SOPHOS

Emotet: Gefährlicher als WannaCry und schwerer abzuwehren

Emotet ist eine extrem gefährliche Bedrohung, die Unternehmen weltweit vor große Probleme stellt. Die Malware ist besonders vielseitig und langlebig und nutzt verschiedene komplexe Techniken zur Kompromittierung Ihrer Systeme. Emotet lässt sich nur mit der besten Verteidigung abwehren.

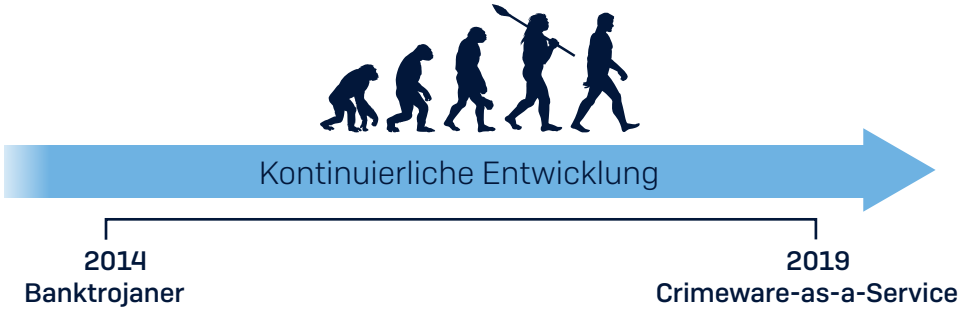
In unserem Whitepaper erfahren Sie, was genau die Malware Emotet ist, wie sie sich verbreitet und warum sie so gefährlich ist. Zudem erklären wir, wie unsere Lösungen Sie an allen Punkten der Angriffskette optimal vor Emotet schützen, und geben Ihnen drei Best Practices an die Hand, mit denen Sie Ihr Risiko verringern, von Emotet getroffen zu werden.

Was ist Emotet?

Bei Emotet handelt es sich um einen besonders raffinierten Wurm. Das US-Ministerium für innere Sicherheit zählt ihn zu den derzeit teuersten und schädlichsten Bedrohungen für US-Unternehmen. Doch Emotet beschränkt sich nicht nur auf die USA – darauf gehen wir in der Folge noch genauer ein.

Emotet ist keine neue Malware und hat im Laufe der Jahre immer mehr an Komplexität und Zerstörungskraft zugenommen. Innerhalb ihrer fünfjährigen Lebenszeit hat sich die Malware von einem Trojaner, der still und heimlich Bankdaten seiner Opfer entwendete, zu einer extrem raffinierten Plattform für die Verbreitung anderer Schadsoftware entwickelt. Die Crimeware-as-a-Service schlechthin.

Das US-Ministerium für innere Sicherheit zählt Emotet zu den derzeit teuersten und schädlichsten Bedrohungen für US-Unternehmen.[1]



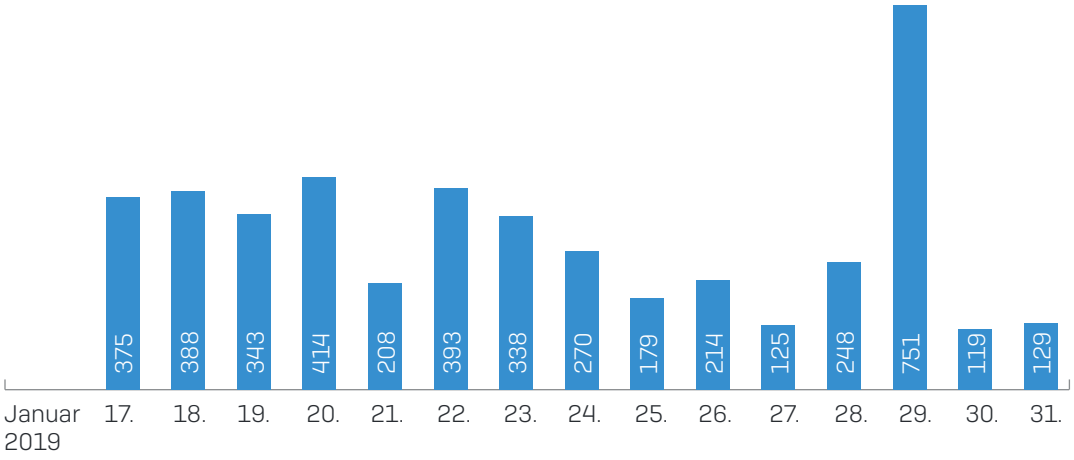
Emotet bietet alles an, wofür Cyberkriminelle zahlen. Im Jahr 2019 wartete Emotet etwa mit den Banktrojanern TrickBot und Qbot auf. Zudem wird die Malware mit BitPaymer in Verbindung gebracht, einer hoch entwickelten Ransomware-Familie, die sechsstellige Summen erpresst.

Hinter Emotet stehen hochprofessionelle, finanziell motivierte Cyberkriminelle. Durch ständige Updates erhöhen diese unablässig die Leistungsfähigkeit und Zerstörungswirkung ihrer Malware.

Ständig andere Payloads

Ein besonderes Merkmal von Emotet sind die sich ständig verändernden Payloads. Aus unserer Grafik geht die Anzahl neuer, unterschiedlicher ausführbarer Payloads hervor, die die SophosLabs in den letzten beiden Januarwochen dieses Jahres verzeichneten.

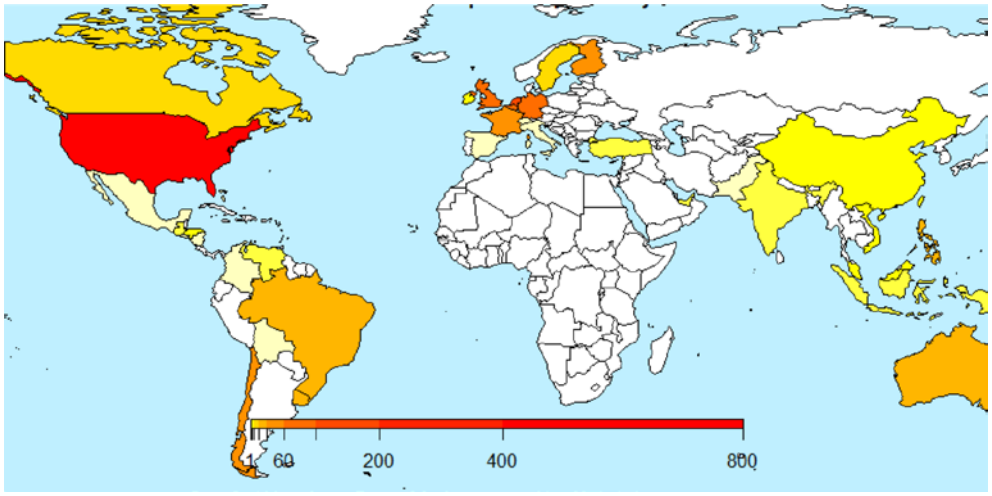
Anzahl unterschiedlicher, von den SophosLabs verzeichneter ausführbarer Emotet-Payloads



Wie Sie sehen, treten täglich Hunderte neue Varianten auf. Im Schnitt beobachten die SophosLabs täglich ca. 300 neue ausführbare Payloads. In den letzten 15 Tagen im Januar allein wurden knapp viereinhalbtausend (4.494) unterschiedliche ausführbare Payloads verzeichnet.

Globale Reichweite

Das US-Ministerium für innere Sicherheit zählt Emotet zu den derzeit teuersten und schädlichsten Bedrohungen. Doch Emotet beschränkt sich nicht auf die USA . Die nachstehende Grafik der SophosLabs zeigt die am meisten von Emotet betroffenen Länder. Rot stellt dabei die höchste Angriffsdichte dar.

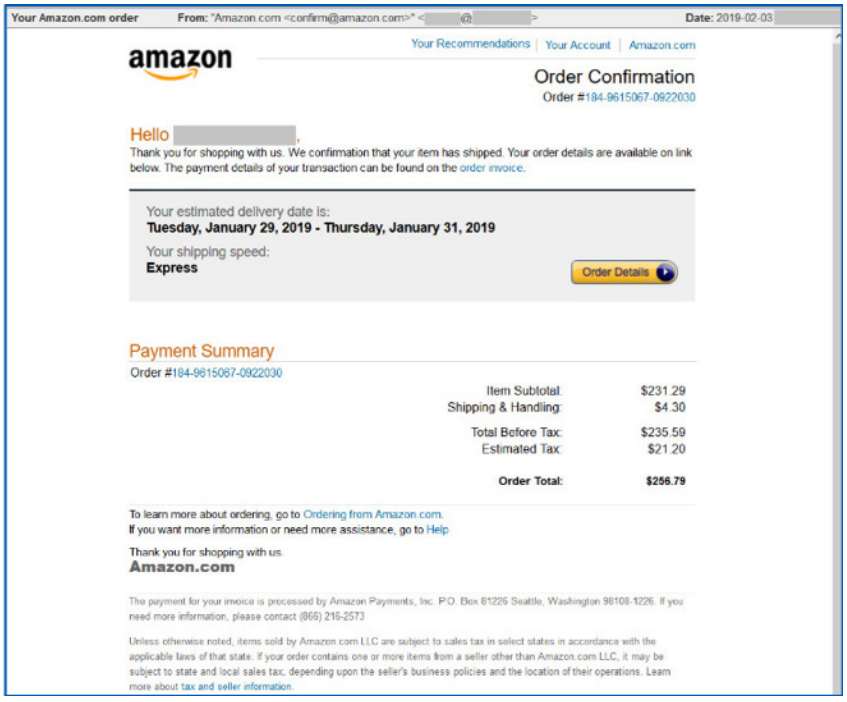


Geographische Ausbreitung von Emotet. Quelle: SophosLabs

Zwar konnten die SophosLabs Emotet in fast allen Regionen feststellen, die Angriffsdichte in Nord- und Südamerika, Nord- und Westeuropa, der Türkei, Australien, Südostasien, China, Indien und Pakistan ist jedoch besonders hoch. Afrika und Osteuropa sind derzeit seltener betroffen, was jedoch nicht heißt, dass sich diese Regionen in Sicherheit wiegen sollten. Die Macher von Emotet nutzen neue Chancen schnell aus und wir wissen nicht, wo sie als nächstes zuschlagen.

Spam ist der Anfang

In der Regel beginnt eine Emotet-Infektion mit einer Spam-Kampagne. Sie werden in E-Mails zum Klick auf eine schädliche Datei aufgefordert. In den Anfängen bestand Emotet-Spam aus E-Mails mit schädlichen Dokumenten im Anhang. Mittlerweile enthalten die Spam-E-Mails Links zu auf Websites gehosteten Schaddokumenten. Häufig nutzt Emotet auch Social Engineering sowie Brand-Spoofing (unter anderem Amazon, PayPal und AT&T).



Your Amazon.com order From: "Amazon.com <confirm@amazon.com>" <[redacted]@[redacted]> Date: 2019-02-03

amazon

Your Recommendations | Your Account | Amazon.com

Order Confirmation

Order #184-9615067-0922030

Hello [redacted],

Thank you for shopping with us. We confirmation that your item has shipped. Your order details are available on link below. The payment details of your transaction can be found on the order invoice.

Your estimated delivery date is:
Tuesday, January 29, 2019 - Thursday, January 31, 2019

Your shipping speed:
Express

Order Details

Payment Summary

Order #184-9615067-0922030

Item Subtotal:	$231.29
Shipping & Handling:	$4.30
Total Before Tax:	$235.59
Estimated Tax:	$21.20
Order Total:	**$256.79**

To learn more about ordering, go to Ordering from Amazon.com.
If you want more information or need more assistance, go to Help.

Thank you for shopping with us.
Amazon.com

The payment for your invoice is processed by Amazon Payments, Inc. P.O. Box 81226 Seattle, Washington 98108-1226. If you need more information, please contact (866) 216-2573

Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about tax and seller information.

Beispiel für Emotet-Spam-E-Mails. Quelle: SophosLabs

Die vielen Ziele von Emotet

Emotet führt mehrere Aktionen auf infizierten Systemen aus. Wenn Emotet Zugriff zu einem Computer erlangt hat, versucht er:

1. **So viele Systeme wie möglich zu infizieren.** Ein Wurm kann sich ja ganz einfach ohne jedes Zutun des Benutzers ausbreiten. Über das Netzwerk bewegt sich die Malware von Computer zu Computer weiter.
2. **Schad-E-Mails zu versenden**, um die Infektion auf andere Unternehmen auszuweiten.
3. **Einen Malware-Payload herunterzuladen.** Bisher handelte es sich bei den Payloads meist um Banktrojaner, allen voran TrickBot. Der Payload injiziert Code in Ihren Browser, um beim nächsten Login automatisch Ihr Bank- und PayPal-Konto zu belasten.
4. Manche Varianten von Emotet **erfassen E-Mail-Adressen und Namen** aus E-Mail-Client-Daten und -archiven, die dann verkauft werden, damit noch mehr schädlicher Spam verbreitet werden kann.
5. Andere Varianten der Malware **inspizieren Ihren Web-Browser, stehlen den Verlauf und gespeicherte Benutzernamen und Passwörter.**
6. Darüber hinaus **dient Emotet auch häufig als Ablenkungsmanöver für gezielte Ransomware-Angriffe**. Während Unternehmen mit der Eindämmung von Emotet-Infektionen beschäftigt sind, nutzt Ransomware wie BitPaymer die Gunst der Stunde, verschlüsselt Unternehmensdaten und gibt diese erst nach Zahlung eines Lösegelds wieder frei.

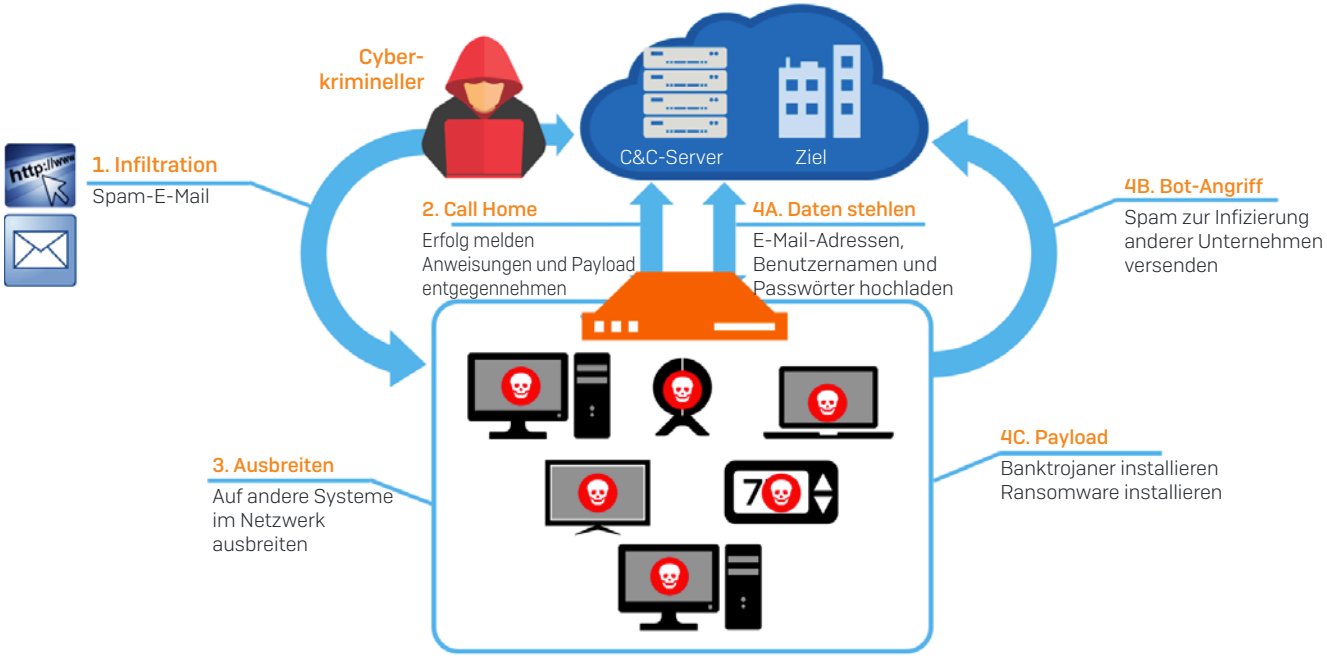
Die Aktivitäten von Emotet richten in betroffenen Unternehmen verheerende Schäden an. Zu den Konsequenzen zählen unter anderem:

- Finanzielle und betriebliche Kosten von Banktrojanern
- Reputationsverlust auf Absenderseite aufgrund der Verbreitung von schädlichem Spam
- Kosten- und Compliance-Folgen einer Datenpanne aufgrund verlorener Kontaktdaten
- Sicherheitsverletzung aufgrund verlorener Benutzernamen und Passwörter
- Potenzielle Kosten aus gezielten Ransomware-Angriffen

Es überrascht daher kaum, dass US-Regierungsbehörden Schäden in Höhe von **$ 1 Million USD pro Vorfall entstanden sind.**[2]

Emotet mit Sophos abwehren

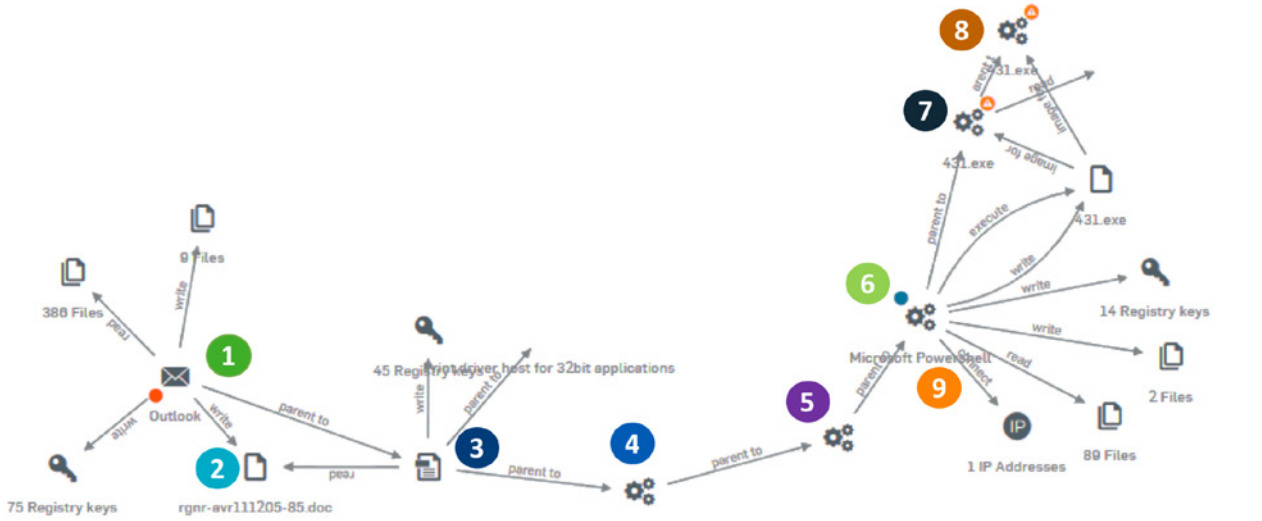
Um sich gegen raffinierte Bedrohungen wie Emotet zu wappnen, benötigen Sie leistungsstarke modernste Schutztechnologien. Hier liegen Sie mit unseren Lösungen genau richtig – und zwar sowohl auf Endpoint- als auch auf Netzwerkebene. Zur Auswahl des richtigen Schutzes ist ein tiefgreifendes Verständnis der Angriffe erforderlich.



Sophos-Lösungen bieten an allen Punkten der Angriffskette mehrschichtigen Schutz. So wird verhindert, dass die Bedrohung überhaupt erst in Ihr Netzwerk gelangt und sich auf andere Netzwerkbereiche ausweiten kann. Dabei werden Call-Home-Versuche, Datendiebstahl und die Installation von Payloads verhindert.

Endpoints vor Emotet-Infektionen schützen

Wie aus der Angriffskette vom Januar 2019 hervorgeht, führt Emotet beim Angriff mehrere Aktionen auf dem Endpoint aus.



1. Benutzer erhält eine schädliche E-Mail (Malspam).	4. Das Makro führt über die Befehlszeile verschleierten Schadcode aus.	7. PowerShell verbindet sich mit einer IP-Adresse und lädt eine Datei „431.exe" herunter
2. Benutzer klickt auf schädlichen Anhang: ein Dokument „rgnr-avr111205-85.doc"	5. Befehlszeile startet eine weitere Befehlszeile.	8. PowerShell führ „431.exe" aus
3. Benutzer aktiviert schädliches Makro in dem Dokument.	6. Die zweite Befehlszeile startet Microsoft PowerShell.	9. Sophos HIPS hat den Verbindungsversuch von PowerShell zu einer verdächtigen IP-Adresse sowie den Download einer ausführbaren Datei mit unbekannter Reputation erkannt und das Verhalten blockiert.

Intercept X Advanced with EDR verfügt über eine Vielzahl an Technologien, die verhindern, dass Emotet seinen Payload abliefern kann. Die Lösung schützt mehrstufig vor schnell mutierenden, raffinierten Bedrohungen wie Emotet.

- **Zustellung.** Unsere Web Protection verhindert die Zustellung schädlicher E-Mails.
- **Exploits.** Anti-Exploit-Schutz (Code/Speicher/APC), Application Lockdown, Schutz vor lokaler Rechteausweitung sowie Application Control verhindern die Ausführung des Exploits.
- **Installation.** Deep Learning und HIPS blockieren die Installation von Malware.
- **Command and Control.** Malicious Traffic Detection (MTD) unterbindet die Kommunikation mit dem C&C-Server, sodass die Bedrohung keine Anweisungen erhalten kann.
- **Zielgerichtete Maßnahme.** Anti-Ransomware und Credential Theft Protection, HIPS in der Laufzeit sowie RCA verhindern, dass Emotet seine Ziele erreicht.

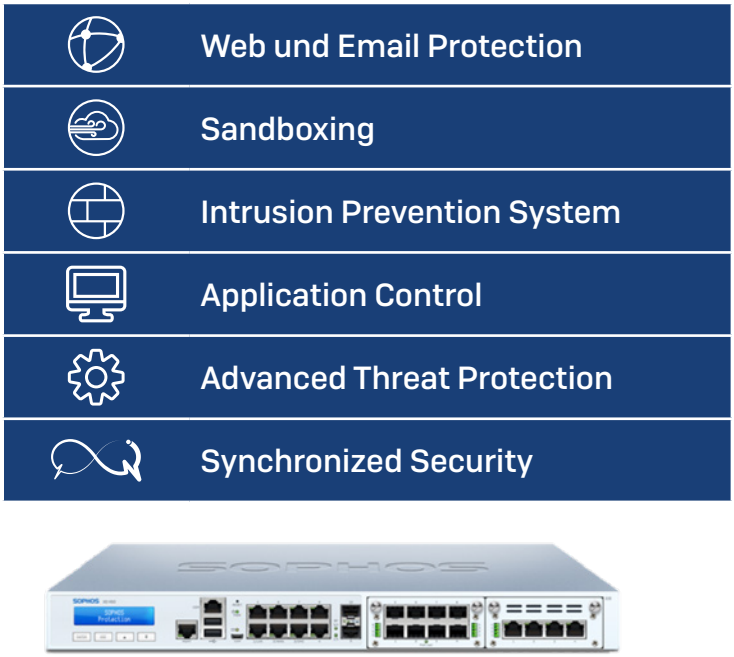
Bei sich rasant entwickelnden Bedrohungen wie Emotet muss Sicherheitssoftware neue Entwicklungen prognostizieren und bisher unbekannte Varianten blockieren können. Hier kommt die Deep-Learning-Technologie von Intercept X ins Spiel, die neue Bedrohungen vorhersagen kann. Auch wenn wir nicht wissen, wie Emotet in einer Woche oder einem Monat aussehen wird, blockieren prädiktive Technologien bisher unbekannte Bedrohungen und bieten so den bestmöglichen zukunftssicheren Schutz.

Endpoint Detection and Response (EDR)-Technologie ist ein wichtiger Bestandteil einer effektiven Emotet-Abwehr. Wie wir bereits gesehen haben, handelt es sich bei Emotet um eine äußerst komplexe und widerstandsfähige Bedrohung. Die EDR-Funktionen in Intercept X bieten Antworten auf die schwierigen Fragen:

- Was war passiert?
- Welche Bereiche sind betroffen?
- Kam es zu Datenverlusten?
- Wurden verborgene Bedrohungen eingeschleust?

Netzwerkübergriffe durch Emotet verhindern

Es gibt keine Wunderwaffe, mit der sich verhindern lässt, dass Emotet in Ihr Netzwerk gelangt. Unsere XG Firewall umfasst jedoch eine breite Palette an Schutztechnologien, die bei der Abwehr von Emotet eine entscheidende Rolle spielen und Ihnen die bestmögliche Verteidigung bieten. Da sich alle Optionen über einen Bildschirm in einer Firewall-Regel verwalten lassen, können Sie ganz einfach sehen, welche Sicherheitsmaßnahme Sie auf eine bestimmte Verbindung bzw. Art von Netzwerkverkehr angewandt haben.



Email Protection erkennt dank der Bedrohungsdaten unserer SophosLabs schädliche E-Mails und blockiert eingehenden und ausgehenden Emotet-Spam.

Sophos Sandstorm Sandboxing stellt den besten Schutz vor Zero-Day- und neuen dateibasierten Bedrohungen bereit. Emotet-Dropper sind das beste Beispiel für Bedrohungen, zu deren Erkennung Sandstorm konzipiert wurde. Sandstorm umfasst leistungsstarke Technologien, von Intercept X in der virtuellen Sandbox in der Cloud bis hin zu Exploit-Erkennung, Anti-Ransomware und Deep Learning.

Im Falle von Emotet erkennt Sandstorm:

- Emotets Speichersignaturen
- Schädliches Verhalten in zu Emotet gehörigen Office-Dokumenten
- Missbräuchliche Nutzung von PowerShell
- Verbindungsversuche zu Hochrisiko-URLs
- Und, natürlich, offenkundiges schädliches Verhalten

Einer der Hauptvorteile von Sandstorm besteht darin, dass die Technologie aggressiver als herkömmliche Endpoint-Analysen agieren kann, die Benutzer-Performance keine Rolle spielt. Zudem zeichnet sie sich durch ein hohes Maß an Effektivität aus.

Intrusion Prevention (IPS) sollte einen weiteren essenziellen Bestandteil Ihrer Netzwerkverteidigung darstellen. IPS ist das Pendant zur Exploit-Erkennung auf Netzwerkebene. Die Technologie sucht den Netzwerkverkehr auf Anzeichen von Exploits und Pakete mit Code ab, die Bestandteile eines Angriffs sind.

Sophos IPS erkennt Exploits von Sicherheitslücken in Betriebssystemen, Netzwerk-Stacks, Servern, Endpoints, Browsern, Anwendungen und mehr. So nutzt etwa TrickBot, ein gängiger Payload von Emotet, die gleiche SMB-Schwachstelle aus wie WannaCry, um sich in Netzwerken ausbreiten zu können – und wird von IPS ganz einfach erkannt und blockiert.

IPS ist besonders effektiv, wenn ein unverwalteter, infizierter Endpoint ans Netzwerk angeschlossen wird. IPS identifiziert und blockiert Versuche, andere Systeme im Netzwerk zu infizieren.

Unsere IPS Engine zählt zu den branchenweit besten und schaffte es in aktuellen Tests der NSS Labs im Bereich effektive Sicherheit und Performance unter die ersten Drei.

Kommunikation und Datendiebstahl durch Emotet verhindern

Technologien in der XG Firewall verhindern, dass Bedrohungen wie Emotet Daten stehlen oder nach außen kommunizieren. Advanced Threat Protection (ATP) überwacht den gesamten von der Firewall ausgehenden Datenverkehr auf Anzeichen für Kommunikation mit Malware-Servern, Command-and-Control- Servern oder Hackersystemen und erkennt betroffene Systeme sowie die Bedrohung sofort.

Die SophosLabs pflegen und aktualisieren unsere umfassende Datenbank bekannter Hacker- und C&C-Server regemäßig über Live Cloud. So wird sichergestellt, dass wir Call-Home-Versuche von aktuellen Bedrohungsvarianten wie dieser erkennen. Dies spart nicht nur viel Zeit bei der Bedrohungslokalisierung, sondern ermöglicht zudem eine schnelle Bereinigung.

Mehr Schutz vor Emotet dank Synchronized Security

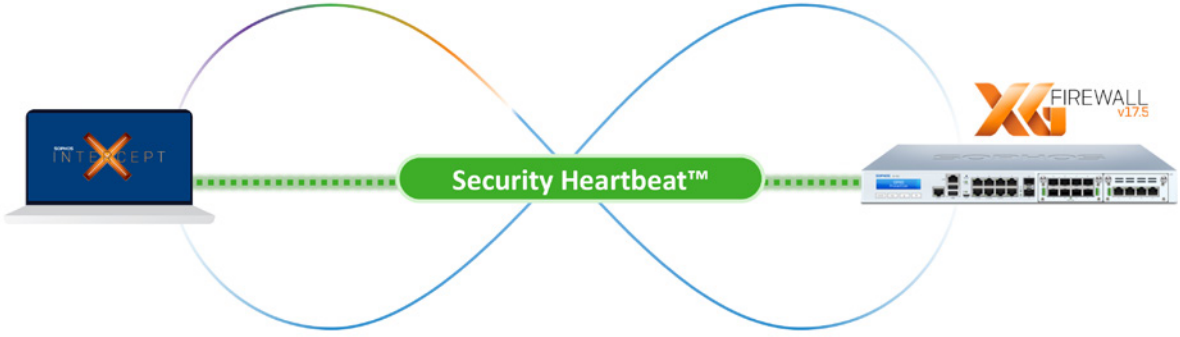
Intercept X schützt Ihre Endpoints vor Emotet, und die XG Firewall sichert Sie auf Netzwerkebene ab. In Kombination liefern die beiden Lösungen branchenweit unerreichten Schutz. Wir nennen diese leistungsstarke Kombination Synchronized Security. Dabei arbeiten unsere Produkte zusammen, um Bedrohungen wie Emotet zu erkennen und einzudämmen. Und das alle ganz automatisch, ohne Benutzerinteraktion, in Sekundenschnelle. Intercept X und die XG Firewall tauschen über unseren Security-Heartbeat™ in Echtzeit Sicherheitsinformationen aus und reagieren ganz automatisch, dank dynamischer Richtlinien in der Firewall.

Zero-Touch-Reaktion auf Emotet

1 **Malware-Erkennung**
Intercept X erkennt, dass Emotet ausgeführt wird

2 **Netzwerkweite Kommunikation**
Intercept X teilt der XG Firewall mit, auf welchen Systemen Emotet erkannt wurde

3 **Geräte-Isolation**
Die XG Firewall isoliert mit Emotet infizierte Systeme sofort.
- Von der Außenwelt isoliert
- Von anderen Endpoints isoliert



5 **Zugriff wiederhergestellt**
XG stellt den Netzwerkzugriff wieder her. Geführte Analysen bieten detaillierte Einblicke in den Vorfall

4 **Bereinigung**
Intercept X bereinigt die Infektion automatisch. Intercept X informiert die XG Firewall über die Entfernung von Emotet

Erkennt Intercept X Emotet, wird die XG Firewall darüber informiert und das betroffene System wird unmittelbar von der Außenwelt und anderen Endpoints isoliert, auch wenn sich diese im gleichen Netzwerksegment bzw. auf dem gleichen Switch befinden. So werden laterale Bewegungen unterbunden.

Gleiches gilt auch im Umkehrschluss, wenn die XG Firewall Emotet oder einen seiner Payloads, wie TrickBot, über IPS oder ATP erkennt: Der Endpoint wird benachrichtigt, und das infizierte System wird sofort isoliert. In beiden Fällen werden Ihnen im Control Center der XG Firewall sofort, ohne Ihr Zutun, betroffene Systeme, Benutzer, Prozesse und Bedrohung angezeigt.

Best Practices zur Abwehr von Emotet

Unsere Best Pratices gehen Hand in Hand mit Ihren Schutztechnologien, um Sie vor Emotet zu schützen. Wir empfehlen, dass alle Unternehmen die drei folgenden Maßnahmen umsetzen:

1. ALLE Geräte schützen

Emotet kann sich auf unbekannten, ungeschützten Geräten verstecken und sich anpassen. Zwar beschränkt sich der Wurm möglicherweise dank Ihrer Security-Software auf den anderen Systemen momentan noch auf das ungeschützte System, doch er wird unablässig versuchen, sich im Netzwerk auszubreiten. Aufgrund seiner beständigen Updates stellt Emotet die IT immer wieder vor neue Herausforderungen.
Je länger Emotet auf unbekannten Geräten ausgeführt wird, umso größer ist das Risiko, dass er aufgrund eines Updates oder eines neuen Payloads eine Lücke in Ihrer Verteidigung findet und sich im Netzwerk ausbreitet.

Suchen Sie mit einem Netzwerk-Scanner (wie etwa Advanced IP Scanner) nach ungeschützten Computern im Netzwerk. In vielen Unternehmen wurde Emotet auf unbekannten und somit auch ungeschützten Systemen entdeckt.

2. Installieren Sie Patches zeitig und regelmäßig

Gewiss nicht die neueste Erkenntnis und dennoch sollten Sie Patches auf keinen Fall vernachlässigen. Emotet öffnet anderer Malware die Tür. Wenn Sie einen Emotet-Ausbruch stoppen, stoppen Sie deshalb auch alles, was der Wurm mit sich bringt.
Und da man nie weiß, worum es sich dabei handeln kann, sollten Sie alle möglichen Vorsichtsmaßnahmen treffen und Patches für bekannte Sicherheitslücken installieren.

EternalBlue ist ein Exploit, der 2017 durch WannaCry und NotPetya bekannt wurde. Trotz des Medieninteresses nutzt TrickBot, einer der häufigsten Payloads von Emotet, auch zwei Jahre nach Veröffentlichung entsprechender Patches von Microsoft den Exploit weiterhin aus.

3. PowerShell standardmäßig blockieren

Wie man in der Angriffskette vorhin sehen konnte, nutzen Emotet -Angriffe in der Regel PowerShell. Gehen Sie bei der Konfiguration von der Annahme aus, dass keine Benutzer (inklusive Administratoren) auf PowerShell zugreifen müssen und lassen Sie die Funktion im Anschluss gezielt für alle Mitarbeiter zu, die wirklich damit arbeiten müssen. Wir empfehlen dabei, dass PowerShell blockiert und nicht nur per Richtlinie deaktiviert wird. Richtlinien lassen sich umgehen. Nehmen Sie PowerShell daher also in Ihre Blacklist auf. (Die entsprechende Sophos-Anwendung hierzu ist Application Control).

Fazit

Emotet ist ein agiler Gegner, der verheerende Schäden in Unternehmen anrichtet. Nur modernste IT-Sicherheit in der gesamten Infrastruktur schafft hier Abhilfe. Unsere Lösungen bieten den bestmöglichen Schutz vor Emotet:

- Nachweislich leistungsstarker Schutz auf Endpoint- und Firewall-Ebene
- Einzigartige Zero-Touch-Bedrohungsisolation und automatisierte Bereinigung mit Synchronized Security
- Deep-Learning-Technologien zur Minimierung der Risiken durch künftige Emotet-Varianten

Wenn Sie die leistungsstarken Schutztechnologien von Sophos mit unseren empfohlenen Best Practices kombinieren, erhalten Sie den bestmöglichen Schutz vor Emotet.

Weitere Informationen zu unseren Lösungen sowie Testversionen finden Sie unter www.sophos.de

1 U.S. Computer Emergency Readiness Team
2 https://www.us-cert.gov/ncas/alerts/TA18-201A

Jetzt testen unter

www.sophos.de/freetrials

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

07.02.2019 WP-DE (NP)

SOPHOS