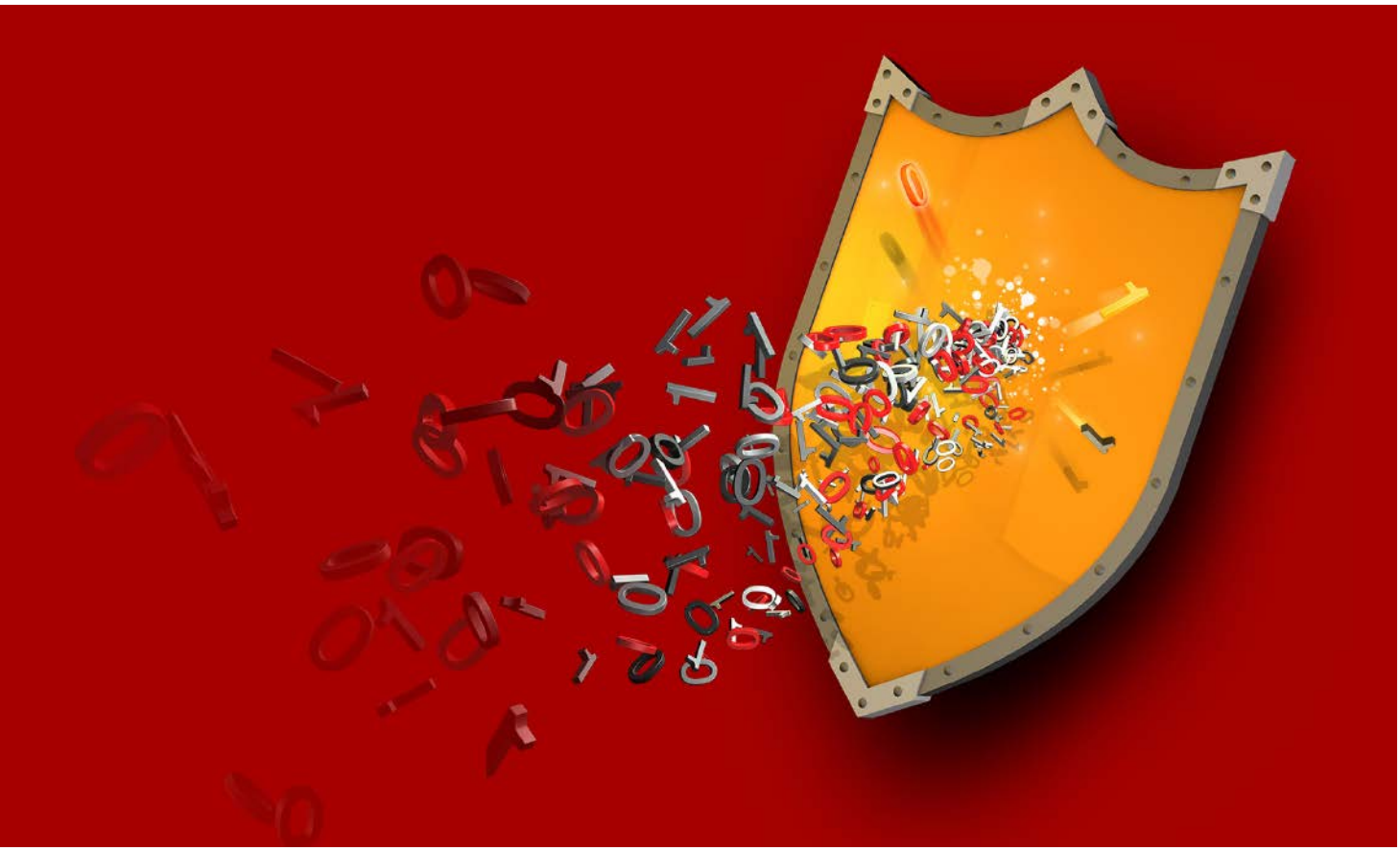


Raus aus dem Maßnahmensumpf:
eine Anleitung zum Emotet-Selbsttest

Gewusst wo

Martin Karl Junghans, Joshua Ziemann

Sicherheitsexperten betreiben viel Aufwand, um Infektionen mit Emotet zu verstehen und daraus Schutzmaßnahmen abzuleiten. Dabei wäre es wichtiger, effektive Maßnahmen schon vor einem Vorfall umzusetzen. Beim gezielten Auffinden der Schwachstellen hilft die Frage: „Wie anfällig sind wir?“ Ein Selbsttest bringt hier Licht ins Dunkel.

Zu verstehen, aus welchem Grund Maßnahmen notwendig sind, ist elementar, wenn es um die Umsetzung ganzheitlicher IT-Sicherheit geht. Zu wissen, warum die eigene Organisation anfällig für einen Emotet-Befall ist oder eben nicht, macht das Sicherheitsniveau messbarer und fördert das Verständnis und die Akzeptanz für die daraus resultierenden Maßnahmen.

Emotet ist aktuell, relevant und gefährlich. Das zeigt nicht nur die lange Historie, die diese Schadsoftware bereits seit 2014 aufweist, sondern das belegen auch die vielen Fälle in der jüngeren Vergangenheit – das Kammergericht Berlin (September 2019), die Universität Gießen und die Stadtverwaltungen Frankfurt am Main und Bad Homburg (Dezember 2019), diverse Krankenhäuser 2020 – und nicht zuletzt Heise im Mai 2019. Die Ziele sind vielseitig und nicht selten ist ein Komplettausfall der IT-Infrastruktur für Tage oder Wochen die Folge.

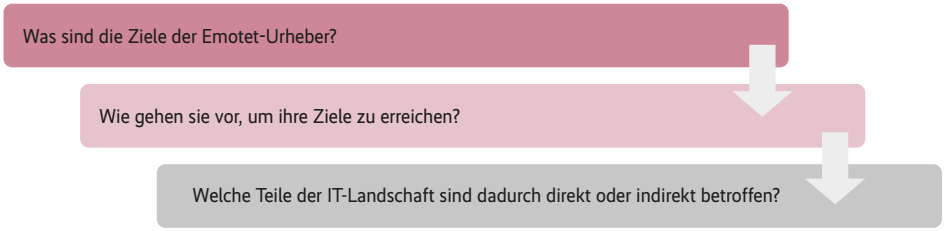
Bei der Risikoanalyse abgeschaut

Wenn entscheidende Warnsignale ignoriert werden, steht schnell alles auf dem Spiel. Daher sollten sich IT-Management, -Sicherheit und -Betrieb gemeinsam die Frage stellen: Wie anfällig ist unsere Organisation für einen Emotet-Befall und welche konkreten Maßnahmen sollten wir ergreifen, um das Schadenspotenzial angemessen einzugrenzen?

Als Grundlage für das Vorgehen nutzen die Autoren, deren Unternehmen den Emotet-Selbsttest bereits erfolg- und erkenntnisreich absolviert hat, ein abgewandeltes Modell der Risikoanalyse. Der Test orientiert sich daher an den in Abbildung 1 dargestellten Schritten.

Der erste Schritt, das Identifizieren des Analysebereichs, bedeutet hier das Erfassen derjenigen Teile der IT-Infrastruktur, die von Emotet direkt angegriffen werden, und solcher, die damit verbunden sind. Das häufigste Einfallstor ist die Phishingmail. Direkt betroffen sind also unter anderem

Die Durchführung eines Emotet-Selbsttests orientiert sich an den einzelnen Schritten der Risikoanalyse (Abb. 1).



Die Beantwortung dieser drei Fragen hilft beim Bestimmen der gefährdeten Bereiche in der IT (Abb. 2).

die E-Mail-Infrastruktur und indirekt der Clientbereich sowie interne Server.

Der Angreifer bestimmt den Analysebereich

Damit der Analysebereich eindeutig abgesteckt werden kann, sollten zunächst die drei Fragen aus Abbildung 2 der Reihe nach beantwortet werden.

Nach Ansicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind die Ziele der direkten Emotet-Urheber rein finanzieller Natur. Sie werden erreicht, indem „die Entwickler von Emotet ihre Software und ihre Infrastruktur an Dritte untervermieten". In dieser Hinsicht sind also noch keine Erkenntnisse gewonnen. Spannender sind die Ziele der Emotet-Mieter. Das BSI geht hier auch von Cyberkriminalität aus, nicht von Spionage. Das bedeutet, es geht ausschließlich um Geld. Diese Aussage deckt sich auch mit den Beobachtungen bekannter Emotet-Fälle der Vergangenheit.

In der Regel wird Emotet als sogenannter Stager für weitere Malware genutzt – das bedeutet, er prüft, ob es sicher ist, neue Malware nachzuladen, und macht es dann. Am häufigsten hört man von der Emotet-Trickbot-Ryuk-Kombination. Es fallen aber auch Namen wie Ursnif, ZeuS und IcedID. Worum handelt es sich hierbei? Trickbot, Ursnif, ZeuS und IcedID fallen in die Kategorie der Banking-Trojaner. Bei Ryuk handelt es sich um eine klassische Ransomware. Es geht also um Kompromittierung und Missbrauch von Bankkonten und Erpressung.

Erpressung kann, wie man es kennt, nach der Verschlüsselung von Daten erfolgen oder durch Androhung, die auf den kompromittierten Systemen befindlichen Daten zu veröffentlichen. Auch wenn Spionage also kein eigentliches Ziel der Angreifer sein mag, besteht dennoch die Gefahr, dass die Daten in weitere unbefugte Hände gelangen. Zusammenfassend lässt sich sagen: Das Primärziel ist Geld. Daraus resultierende sekundäre Ziele sind das Sammeln von Zugangsdaten, die Übernahme von Onlinebanking-Sitzungen, das Verschlüsseln sowie Sammeln vertraulicher Daten und das Infizieren möglichst vieler weiterer Systeme.

Wie funktioniert die Schadsoftware?

Eine umfassende Aufarbeitung der Funktionsweise von Emotet und Co. würde den Rahmen dieses Artikels sprengen. Es gibt jedoch zahlreiche Quellen und Forschungsarbeiten zu diesem Thema (einige davon sind über ix.de/zefw zu finden). Im Hinblick auf Emotet gilt es allerdings, eine Besonderheit zu berücksichtigen: Die Kernsoftware wird vermietet und kann sehr einfach mit verschiedenen anderen Schadsoftwareprogrammen kombiniert werden.

Die Empfehlung lautet: Zu Beginn des Selbsttests eigene Recherchen anstellen. Emotet ist modular aufgebaut. Da die Software so einfach mit weiterer Malware kombinierbar ist, ist das Sammeln von Informationen zu häufig nachgeladener Schadsoftware unabdingbar. Aktuell betrifft dies vor allem Trickbot und Ryuk. Als wertvolle Quellen haben sich insbesondere Analysen von Malware-Forschern und frei verfügbare Incident-Reports erwiesen.

Letztere sind leider rar gesät, einige, etwa vom Emotet-Befall bei Heise und dem Kammergericht Berlin, sind jedoch öffentlich verfügbar. Mittlerweile ein Standardwerk für Malware und Techniken ist die Mitre-ATT&CK-Matrix (sie ist wie die Reports über ix.de/zefw zu finden). Auch hier finden sich Einträge mit detaillierten Listen von angewandten Techniken zur Infektion eines Systems. Einige davon zeigt Abbildung 3.

Den Analysebereich festlegen

Um nun aus den Rechercheergebnissen auf den Analysebereich zu schließen, eignet sich ein einfaches Mittel: das Emotet-Tool-Set anhand der Schritte der Killchain (siehe Kasten „Die Cyber-Killchain") sortieren und abarbeiten.

Entlang der Übersicht kann man aus dem Wissen über die ersten drei Phasen von Emotet (Reconnaissance, Weaponization und Delivery) auf mögliche Angriffsvektoren innerhalb der eigenen Organisation schließen. Zum Zeitpunkt der Erstellung dieses Artikels war der einzig relevante und genutzte Angriffsvektor von Emotet die Phishingmail mit einem .doc-Dokument im Anhang.

iX-TRACT

- Noch immer gehören Emotet und Co. zu den am weitesten verbreiteten und gefährlichsten Bedrohungen für die IT in Unternehmen und Organisationen – schlimmstenfalls bis zu deren völligem Stillstand. Vorausschau und Selbsthilfe sind gefragt.
- Mithilfe genauer Recherche zu derzeit verbreiteten Schadprogrammen und einer systematischen Analyse der eigenen IT-Landschaft lassen sich die konkreten Gefährdungen herausarbeiten und passende Schutzmaßnahmen ableiten.
- Ein Selbsttest zur rechten Zeit kann helfen, das Unternehmen vor Schaden zu bewahren. Prävention ist wie immer einfacher und billiger, als hinterher die Scherben aufzufegen.

Im Folgenden werden einige Funktionen von Emotet und Co. zur Veranschaulichung genannt. Sie können als Anhaltspunkte für die eigene Recherche genutzt werden, ersetzen diese aber nicht.

Ausgehend von den identifizierten Angriffsvektoren kann man nun entlang der Killchain auf den gesamten Analysebereich schließen. Die Tabelle „Festlegen des Analysebereichs“ veranschaulicht, wie eine solche Übersicht aussehen kann. Wichtig ist vor allem, auch indirekt betroffene Systeme in den Analysebereich aufzunehmen, da Emotet und Co. sehr intensiv Lateral Movement betreiben. Das bedeutet, die Malware bewegt sich im Netzwerk weiter und sucht nach lohnenden Zielen, wenn sie einmal eingedrungen ist.

Teil des Analysebereichs sind demnach – ausgehend vom Clientsystem, auf dem eine Phishingmail vermutlich zuerst eintrifft – alle unterschiedlichen Systeme in diesem Netzwerk, Netzwerkübergänge und zumindest direkt aus diesem Netzwerk erreichbare weitere Netzwerke. Dieses sukzessive Nachvollziehen kann schnell unübersichtlich werden, sodass man Gefahr läuft, den Blick für das Wesentliche zu verlieren. Hinsichtlich der Abbruchbedingung kann man sich fragen: An welcher Stelle hätte der Angreifer einen hinreichenden Hebel, um entweder seine Ziele zu erreichen oder signifikanten Schaden anzurichten? Spätestens mit der Kompromittierung eines Domänencontrollers wäre diese Schwelle dann wohl erreicht.

Eine Zwischenbilanz

Was ist bisher erreicht? Die Antwort ist essenziell für den kommenden Hauptteil des Selbsttests. Klar ist bis jetzt, welche Ziele der Angreifer verfolgt, welche Techniken eingesetzt werden, um die Ziele zu erreichen, und welche Bereiche der IT-Infrastruktur von einer Infektion betroffen sein können. Nun ist es Zeit, den identifizierten Analysebereich mit dem Tool-Set der Angreifer zu vergleichen und potenzielle Schwachstellen beziehungsweise Risiken zu ermitteln.

Zur Veranschaulichung führen wir die Identifikation von Risiken am Beispiel der E-Mail-Infrastruktur durch. Der beschriebene Prozess ist dann übertragbar auf die anderen identifizierten Teile des Analysebereichs.

Zunächst muss der zu betrachtende Bereich aufgeschlüsselt werden. Es gilt zu ermitteln, welche Systeme Teil der E-Mail-Infrastruktur sind. Diese werden dann auf Schwachstellen und Risiken überprüft. Das Stichwort dabei ist Vollständigkeit. Gerade bei den Systemen an vorderer Front sollte man auch auf Sonderfälle wie nicht mehr benutzte Mailserver oder interne Mail-Proxyserver et cetera achten. Wie viele Mailserver sind tatsächlich im Einsatz? Unterscheiden sie sich? Typische Systeme könnten beispielsweise E-Mail-Gateways, E-Mail-spezifische Antivirussysteme, interne und externe E-Mail-Server, Exchange Server oder die lokalen E-Mail-Clients, zum Beispiel Outlook, sein.

Quelle: Mitre ATT&CK

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.003	Account Discovery: Email Account	Emotet has been observed leveraging a module that can scrape email addresses from Outlook.[3][4]
Enterprise	T1560		Archive Collected Data	Emotet has been observed encrypting the data it collects before sending it to the C2 server. [5]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Emotet has been observed adding the downloaded payload to the `HKEY_CURRENT_USER\Software\Microsoft\Windows \CurrentVersion\Run` key to maintain persistence.[6][7][8]
Enterprise	T1110	.001	Brute Force: Password Guessing	Emotet has been observed using a hard coded list of passwords to brute force user accounts. [9][6][7][10][3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Emotet has used Powershell to retrieve the malicious payload and download additional resources like Mimikatz. [6][2][8][11][12]
		.005	Command and Scripting Interpreter: Visual Basic	Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads. [6][13][2][8][12]
		.003	Command and Scripting Interpreter: Windows Command Shell	Emotet has used cmd.exe to run a PowerShell script. [8]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Emotet has been observed creating new services to maintain persistence. [7][10]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Emotet has been observed dropping browser password grabber modules. [2][4]
Enterprise	T1114	.001	Email Collection: Local Email Collection	Emotet has been observed leveraging a module that scrapes email data from Outlook.[3]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	Emotet is known to use RSA keys for encrypting C2 traffic. [2]
Enterprise	T1041		Exfiltration Over C2 Channel	Emotet has been seen exfiltrating system information stored within cookies sent within an HTTP GET request back to its C2 servers. [2]
Enterprise	T1210		Exploitation of Remote Services	Emotet has been seen exploiting SMB via a vulnerability exploit like ETERNALBLUE (MS17-010) to achieve lateral movement and propagation. [6][7][10][11]

Zur Vorbereitung der Schutzmaßnahmen gehört auch die intensive Recherche, etwa der Vorgehensweise der jeweiligen Malware (Abb. 3).

Festlegen des Analysebereichs anhand der Killchain

	Reconnaissance	Weaponization	Delivery
Emotet-Tool-Set	• Bezug zu aktuellen Themen und Gegebenheiten • in der Regel nicht exakt auf das Ziel zugeschnitten	• polymorphe, modulare Schadsoftware, verpackt in harmlos aussehendes Microsoft-Word-Dokument • automatisiertes Generieren von täuschend echten Phishingmails	• Auslieferung von Phishingmails an Organisationsmitarbeiter
Analysebereich	• Mailinfrastruktur (Mitarbeiter-Awareness)		

Die Cyber-Killchain

Die (Cyber-)Killchain ist ein weitverbreiteter und im IT-Sicherheitsumfeld geläufiger Begriff zum Beschreiben des Vorgehens von Angreifern. Sie umfasst sieben allgemeine, aufeinanderfolgende Phasen, zu denen in der Regel für jede Angriffskampagne jedem einzelnen Schritt Aktionen des Angreifers zugeordnet werden können. Die sieben Phasen sind:

1. **Reconnaissance** – Sammeln von Informationen über das Ziel
2. **Weaponization** – Zusammenstellen eines Toolkits, spezifisch für das Ziel
3. **Delivery** – Auslieferung der Malware (z. B. via Phishingmail, Website …)
4. **Exploitation** – Ausführung des Schadcodes, Ausnutzung von Schwachstellen
5. **Installation** – Einnisten der Malware auf dem Zielsystem und Etablierung einer Backdoor zurück zum Angreifer
6. **Command and Control** – Angreifer steuert über die Backdoor das kompromittierte System
7. **Actions on Objectives** – Angreifer initiierte konkrete Aktionen beim Opfer zur Erreichung seiner Ziele, z. B. Datenabfluss, Verschlüsselung

Das Modell der Killchain wird genutzt, um IT-Sicherheitskonzepte ganzheitlich messbar zu machen. Idealerweise sollte ein solches Konzept Sicherheitsmaßnahmen gegen Aktionen in jeder Phase enthalten. Kommt es dann zu einem Angriff, muss der Kriminelle mehrere Verteidigungslinien überwinden – wobei die Verteidigenden in jeder Phase eingreifen und den Angreifer zurückhalten können.

Das sind die Systeme, die untersucht werden sollten. Auf der anderen Seite steht das Emotet-Tool-Kit für den E-Mail-Weg. Aus bekannten Fällen zeichnet sich bisher ein vielschichtiges, aber in einigen Punkten konsistentes Bild:

1. Der Inhalt der Phishingmail ist täuschend echt und bezieht sich auf aktuelle Ereignisse und Gegebenheiten.
2. Von kompromittierten Systemen werden die E-Mails der letzten 180 Tage kopiert, was den Urhebern der nachgemachten Mails ermöglicht, auf bestehende Konversationen zu antworten und deren Inhalt zu referenzieren. Dabei wird häufig der FROM-Mail-Header verschleiert, wenn die Mails von anderen kompromittierten Accounts versendet werden („Bekannter, Marc kompromittierter.account@example.com“).
3. In verschiedenen Formen ist ein .doc-Dokument mit Makros als Anhang enthalten (direkter Anhang, verpackt in eine Zipdatei, teilweise verschlüsselt, oder ein Download-Link zum Dokument).

Risiken auf die Systeme abbilden

Nun geht es daran, die beiden Seiten zu vergleichen. Um die Arbeit übersichtlich zu gestalten, ist es hilfreich, mit einer zweidimensionalen Matrix zu arbeiten (siehe Tabelle „Dokumentation der festgestellten Risiken“). Die Verantwortlichkeiten IT-Management, IT-Betrieb und IT-Sicherheit bilden die Spalten und die identifizierten Systeme die Zeilen. In jeder Zelle werden dann die ermittelten Risiken für das jeweilige System und der Verantwortungsbereich erfasst. Für ein vollständiges Bild empfiehlt es sich zudem, auch die Stellen festzuhalten, an denen schon wirksame Schutzmaßnahmen im Einsatz sind.

Jeder Verantwortlichkeitsbereich schaut sich für „seine“ Systeme die relevanten Aspekte an und vergleicht sie mit den Emotet-Funktionen. Relevante Aspekte sind für das IT-Management zum Beispiel Richtlinien und Prozesse, für den IT-Betrieb Betriebsdokumentationen und Wissen über die Betriebsrealität und für die IT-Sicherheit isolierte Real-World-Tests der Emotet-Funktionen.

Das Vorgehen sollte sich stets am „What? So What?“-Prinzip orientieren. Das bedeutet zu fragen: Was bringt Emotet für das untersuchte System / den untersuchten Bereich mit, welche Auswirkungen sind denkbar? Was bedeutet das für uns? Also welche Gegenmaßnahmen sind im Einsatz und wo tun sich Lücken auf? Dadurch wird sichergestellt, dass der Fokus und rote Faden erhalten bleibt. Natürlich kann man an diesem Punkt auch die Untersuchungen erweitern und ganz allgemein nach Verbesserungspotenzial Ausschau halten – auf eigene Gefahr.

Am Beispiel der E-Mail-Infrastruktur könnte es wie folgt aussehen: Auf technischer Ebene lassen sich bei Emotet drei Whats identifizieren: Verschleierung der E-Mail-Herkunft, Verschleierung des E-Mail-Inhalts und in irgendeiner Form Ausliefern einer .doc-Datei. Das IT-Management kann sich hier also interne Richtlinien zum Umgang mit E-Mails von Externen anschauen. Müssen Anhänge von einem Antivirusprogramm überprüft werden? Sollen für den normalen Mailverkehr Signaturen verwendet werden, die die Authentizität einer Mail garantieren? Welche Dateiformate sind als Anhang erlaubt?

Geteilte Aufgabenbereiche – spezifische Fragen

Eine Abstraktionsebene tiefer kann sich der IT-Betrieb fragen: Sind Sicherheitsmaßnahmen aktiviert, die bei der Validierung der Absenderauthentizität helfen, etwa SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) oder DMARC (Domain-based Message Authentication, Reporting and Conformance)? Gibt es ein zentrales E-Mail-Gateway, das E-Mails überprüft und klassifiziert? Ist der Exchange Server so konfiguriert,

	Exploitation	Installation	Command and Control	Actions on Objectives
	• Makrocodeausführung • PowerShell-Code-Ausführung	• Nachladen weiterer Malware • verschiedene Persistence-Funktionen	• Trickbot-Post-Exploitation-Framework PowerTrick • Nachladen von Ryuk-Ransomware	• Sammeln von Zugangsdaten • Hijacking von Onlinebanking-Sessions • Datenverschlüsselung und -diebstahl • Lateral Movement
	• Sicherheit der Clientsysteme unter den relevanten Aspekten		• Sicherheit der Clientsysteme unter diesem Aspekt • Firewall-Infrastruktur • Absicherung von Remote-Access-Möglichkeiten	• Sicherheit der Clientsysteme unter diesem Aspekt • Sicherheit von Serversystemen wie Fileserver und Server für interne Applikationen • Netzwerksegmentierung • Backup-Konzepte und Wiederanlaufprozesse

Dokumentation der festgestellten Risiken basierend auf den Systemen und Ebenen				
Verantwortung		**IT Management (High-Level-Emotet-Funktionen mit IT-Richtlinien vergleichen)**	**IT-Betrieb (Low-Level-Emotet-Funktionen mit IT-Betriebsdokumentation vergleichen)**	**IT-Sicherheit (einzelne Low-Level-Funktionen auf dedizierten Testsystemen auf Erfolg überprüfen)**
System	**Mail-Gateways**	Eine Filterung bestimmter Dateiformate im Anhang einer E-Mail ist nicht vorgesehen.	übergreifendes Risiko auf Managementebene	übergreifendes Risiko auf Managementebene
	Mailserver	kein Risiko festgestellt	Es sind keine Maßnahmen zur Authentizitätsfeststellung von Mailservern im Einsatz.	Risiko ...
	Antivirus	kein Risiko festgestellt	kein Risiko festgestellt	Ein Test mit dem EICAR-Virus ergab, dass das eingesetzte Antivirus-Produkt nicht einsatzfähig konfiguriert ist.
	Exchange	Risiko ...	Risiko ...	Risiko ...
	Mail-Clients	Risiko ...	Risiko ...	Risiko ...

dass er dem Endnutzer eine Warnung bei verschlüsselten Zipdateien im Anhang anzeigt?

Die IT-Sicherheit schließlich kann sich nun die ganz konkreten Aspekte auswählen und testen, wie die bestehende IT-Infrastruktur damit umgeht. Wie sieht eine E-Mail mit verschleiertem FROM-Header im Outlook aus? Werden E-Mails mit .doc-Dokumenten im Anhang zugestellt? Mithilfe des EICAR-Test-Virus kann man das grundsätzliche Funktionieren einer Antivirus-Engine überprüfen. Ein nützliches Tool hierfür ist der Heise Emailcheck (siehe ix.de/zefw). Darüber können verschiedene E-Mails angefordert werden, die gängige Techniken von Phishing umsetzen, ohne dass man das Risiko einer Infektion eingeht.

Alle Auffälligkeiten, positive wie negative, sollten in der Matrix dokumentiert werden. An dieser Stelle können es auch noch allgemeine Bemerkungen sein, zum Beispiel wenn jemand den Eindruck hat, dass an einer Stelle keine hinreichenden Schutzmaßnahmen installiert sind, ohne diese konkret benennen zu können. Letztendlich sollte das Ergebnis dieser Phase aber eine Übersicht bereits wirkungsvoller Schutzmechanismen und kritischer Stellen sein, die noch einmal auf Best Practices untersucht werden sollten.

Bewertung der ermittelten Risiken

Bewertung bedeutet Einschätzung. Es geht also darum, die identifizierten Risiken einschätzen zu können. Die Frage, welche Bedeutung ein Risiko hat, liegt in diesem Fall eigentlich schon auf der Hand: Emotet verfügt über Funktion X, die an Stelle Y zum Einsatz kommt, und wir verfügen über keine wirkungsvolle Gegenmaßnahme. Die Schwere des Risikos hängt dann nur noch von der entsprechenden Funktion und der angegriffenen Stelle ab.

Emotet versendet aufwendig erstellte Phishingmails, die auch für geschulte Augen schwer von normalen E-Mails zu unterscheiden sind. Ein zentrales Mail-Gateway, das E-Mails nach technischen Indikatoren klassifiziert und vielleicht auch noch eine Antivirus-Engine mitbringt, um Anhänge auf verschiedenen Ebenen zu untersuchen, bietet hier das notwendige Tool-Set, das Emotet-Phishingmails vielleicht schon in erster Instanz abwehren kann. Ohne einen solchen Spamfilter im Einsatz würden Emotet-Phishingmails ungehindert in den Posteingängen der normalen Benutzer landen und es ergäbe sich zumindest ein mittelschweres Risiko. Es bedarf also einer letzten Wissenskomponente, um die gefundenen Risiken bewerten zu können: Best Practices zum Schutz vor Emotet.

Geklärt ist jetzt: Wo besteht Verbesserungsbedarf und wo könnte Emotet Erfolg haben? Um das Ausmaß der identifizierten Schwachstellen abschätzen zu können, muss man noch wissen, was notwendig wäre, um die betreffenden Emotet-Funktionen einschränken zu können. Jetzt geht es also in den Maßnahmensumpf hinein, um die relevanten Maßnahmen zu identifizieren. Das Zurechtfinden sollte nun allerdings einfach sein. Es ist ja nach der Analysevorarbeit bekannt, wo und an welcher Stelle es hakt. Also gilt es zu sondieren: Welche Maßnahmen sind für unsere Organisation relevant? An welchen Stellen setzen sie an? Nun müssen sie noch zugeordnet werden.

Eine Auswahl anerkannter Empfehlungen kann der Linksammlung (zu finden über ix.de/zefw) entnommen werden. Damit liegt nun alles für die Bewertung der Risiken samt spezifischen Gegenmaßnahmen vor und kann strukturiert festgehalten werden.

Ergebnisinterpretation und Fazit

Zur Interpretation der Ergebnisse sollten alle Beteiligten des Selbsttests, IT-Management, IT-Betrieb und IT-Sicherheit, wieder zusammenkommen. Jetzt geht es darum, die Ergebnisse und Erkenntnisse zu teilen, zu diskutieren und letztendlich etwas daraus zu machen. Das bedeutet Umsetzungsplanung. Maßnahmen müssen nach Aufwand und Nutzen priorisiert werden, dann sollte ein Plan erstellt werden, in welcher Reihenfolge die Umsetzung erfolgen soll. Alle waren beteiligt, alle wissen, welche Maßnahmen zu ergreifen sind. Und: Alle wissen warum.

Sicherlich ist ein Emotet-Selbsttest nichts, was innerhalb von zwei Meetings abgehakt werden kann oder sollte. Aber er bietet Organisationen jeden Sicherheitsniveaus am Ende einen Mehrwert. Solche, die vielleicht noch am Anfang der IT-Sicherheitsumsetzung stehen, haben die Chance, eine wirkungsvolle Schutzstrategie anhand eines praktischen Anwendungsszenarios zu erarbeiten, und bekommen ein Gefühl für die sonst nur als diffus wahrgenommene Gefahr. IT-Sicherheits-erfahrene Unternehmen können Detailschwächen in ihren Konzepten in Bezug auf Emotet entlarven und eine Wissensbasis aufbauen. So sind sie für den Ernstfall gut gerüstet. Denn eins lässt sich auch nach sechs Jahren Emotet-Historie noch sagen: Die Urheber sind aktiv und die Wahrscheinlichkeit, Opfer der Malware zu werden, steigt eher, als dass sie sinkt. (ur@ix.de)

Quellen

Die zitierten Forensikberichte und Malware-Analysen sowie Best Practices und allgemeine Sicherheitsempfehlungen sind über ix.de/zefw zu finden.

Martin Karl Junghans

ist Principal bei der HiSolutions AG in Berlin mit den Schwerpunkten kritische Infrastrukturen und ISO 27001.

Joshua Ziemann

ist Werkstudent bei der HiSolutions AG in Berlin mit den Schwerpunkten IT-Forensik und Protokollierung.