Emotet (bei Heise)

Seit die Heise Gruppe von einer Emotet-Infektion betroffen war, erreichen uns immer wieder Rückfragen. Die wollen wir im Folgenden beantworten und außerdem einige bislang offen gebliebene Punkte ergänzen.

Von Sylvester Tremmel

Ausbreitung & Kundendaten

Genau welche Systeme bei Heise konnte Emotet denn infizieren? Waren Daten von Lesern betroffen?

Nein, Daten von Lesern, Abonnenten, Inhabern von heise-online-Accounts und so weiter waren nicht betroffen. Emotet konnte nicht in die Netze des Verlags Heise Medien vordringen, zu dem c't und ihre Schwesterzeitschriften gehören. Die Infektion betraf stattdessen Heise Regio-Concept, ebenfalls eine Tochter der Heise Gruppe, die zwar teilweise im gleichen Gebäude sitzt, aber getrennte Rechnernetze hat.

Erstinfektion

Wie kam Emotet überhaupt in eure Netze?

„Patient Zero", also das erste kompromittierte System, wurde per E-Mail infiziert. Das geschah, wie für Emotet typisch, per Dynamit-Phishing: Ein Mitarbeiter erhielt eine Mail, die scheinbar von einem Hotel stammte, das der Verlag häufig nutzt. Es war also nicht weiter verwunderlich, dass das Hotel darum bat, die Daten eines Word-Dokuments im Anhang zu prüfen und der betroffene Mitarbeiter schöpfte keinen Verdacht. Das Dokument forderte ihn dann auf, „Inhalte" zu aktivieren; er kam dem nach und das Unheil nahm seinen Lauf.

Emotet verbreitete sich zunächst erfolgreich und installierte auf infizierten Systemen die Malware Trickbot. Der nächste Schritt wäre vermutlich das Nachladen einer Ransomware wie Ryuk gewesen. Dem kamen wir zuvor, indem die betroffenen Netze vom Internet getrennt und letztendlich komplett aufgelöst wurden.

Phishing mit Sprengstoff

Was soll denn „Dynamit-Phishing" sein?

Der Begriff lehnt sich an die bekannteren Bezeichnungen „Phishing" und „Spear-Phishing" an. „Phishing" – eine absichtliche Fehlschreibung von „Fishing", also „Fischfang" – ist der Versuch, Malware zu verbreiten (oder Zugangsdaten zu stehlen et cetera), indem eine große Anzahl von Empfängern mit gefälschten Nachrichten, Websites und ähnlichem konfrontiert wird. Die Fälschungen sind notwendigerweise recht generisch und daher leicht zu erkennen. Aber bei einer genügend großen Menge von Empfängern reicht es auch, wenn nur ein kleiner Anteil von ihnen auf die Masche hereinfällt. Es wird sozusagen ein schlechter Köder in fischreichen Gewässern verwendet.

Darauf aufbauend bezeichnet Spear-Phishing (also Fischen mit dem Speer) die Methode, einem ganz gezielt ausgewählten Opfer eine aufwendige Fälschung zu präsentieren, sodass eine hohe Erfolgswahrscheinlichkeit im Einzelfall besteht. Oft ist das mit viel Recherche und Handarbeit verbunden und für das Opfer kaum zu durchschauen. In der Metapher entspricht das dem geduldigen Warten, bis ein einzelner Fisch in Reichweite des Speers kommt.

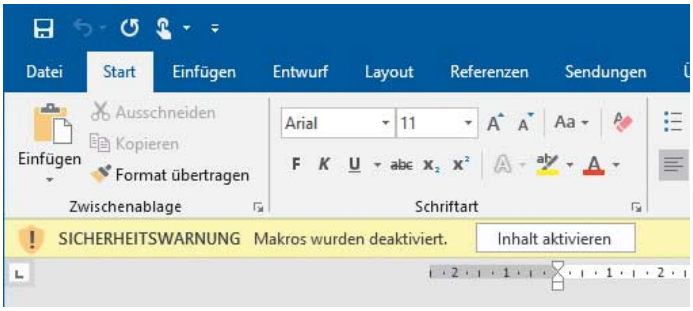
Die Taktik von Emotet verläuft zwischen diesen Extremen: Er verbreitet sich über vergleichsweise gute, aber nicht perfekte Fälschungen, die trotzdem automatisiert erstellt werden; Details erklären wir in ct.de/y4wb. Reichweite und Erfolgswahrscheinlichkeit im Einzelfall befinden sich irgendwo zwischen Phishing und Spear-Phishing, daher das Fischen mit Dynamit als Bild.

Malware-Zoo

Emotet, Trickbot, Ryuk – womit wurde Heise denn nun infiziert?

Emotet – und dann Trickbot. Ryuk oder andere Malware wäre vermutlich der nächste Schritt gewesen. Das Schema ist relativ typisch: Die Kriminellen hinter Emotet infizieren automatisiert so viele Systeme wie möglich und verkaufen diese Zugänge (Malware as a Service). Infizierte Systeme in Deutschland kaufte scheinbar die Gruppe hinter Trickbot ziemlich exklusiv.

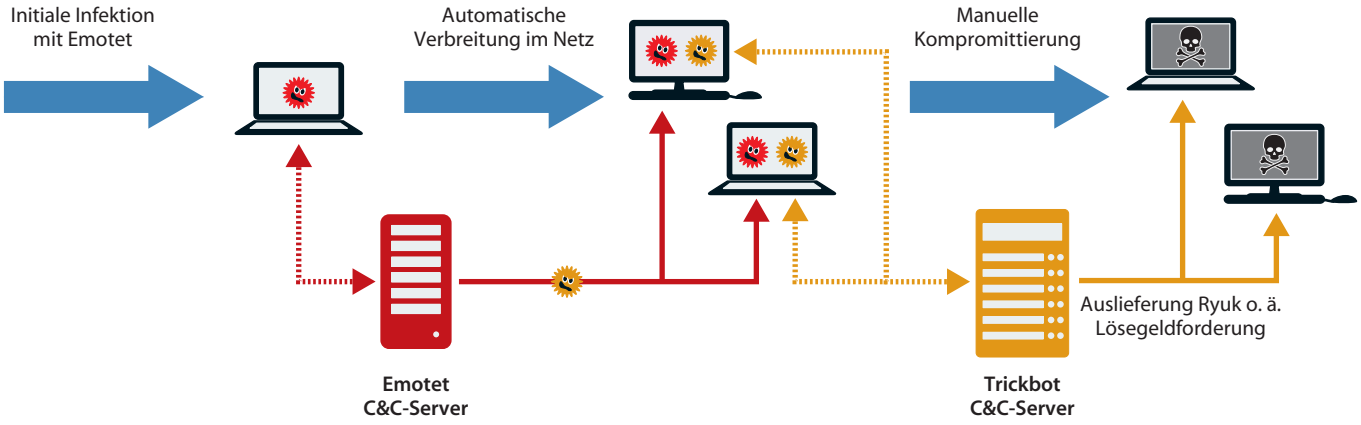
Diese zweite Gruppe nutzt den gekauften Zugang, um ihre Malware Trickbot auf die Systeme zu bringen. Damit sehen sie sich dann bei ihrem Opfer um, was zumindest teilweise Handarbeit ist. Wenn sich das Ziel lohnt, wird über Trickbot wiederum Malware nachgeladen und zielgerecht installiert, um möglichst viel Kasse zu machen. Was genau geschieht, hängt vom Ziel ab, oft werden Verschlüsselungstrojaner wie Ryuk ein-



Das könnte Word deutlich schärfer formulieren. Wer hier auf „Inhalte aktivieren" klickt, hat unter Umständen eine Malware-Infektion am Hals.

Eins, zwei, drei ... Verloren

Der bösartige Dreischritt: Infektion mit Emotet, Sekundärinfektion mit Trickbot und dann die gezielte Kompromittierung relevanter Systeme. Letzterem konnte Heise zum Glück zuvorkommen.



gesetzt, um Daten (und beschreibbare Backups!) zu verschlüsseln und das Opfer zu erpressen.

Die verschiedenen Malware-Typen kommen also nicht nur aus technischer Notwendigkeit zum Einsatz, sondern sind auch ökonomisch bedingt. „Malware“ ist heutzutage ein ganzes Wirtschaftssystem, mit verschiedenen Märkten und florierendem Handel.

Kostproben

Können Sie mir Samples oder zumindest Hash-Werte der gefundenen Schadprogramme zukommen lassen, damit ich bei mir danach suchen kann?

Das ist nicht sinnvoll. Emotet – wie viel andere Malware auch – existiert in vielen verschiedenen Varianten, die alle unterschiedliche Hashes produzieren. Das ist auch der Grund, warum Virenscanner oft ein paar Tage brauchen, bis sie neue Varianten zuverlässig erkennen. Deshalb konnte die E-Mail zur Erstinfektion auch den Mail-Virenscanner von Heise passieren. Die Samples der Heise-Infektion sind also veraltet und ohnehin kein gutes Mittel, um Emotet zu erkennen.

Reaktionszeit

Heise wurde an einem Montag infiziert, bemerkte das volle Ausmaß des Problems aber erst am Mittwoch. Wieso reichen zwei Tage nicht, um Daten abzuziehen oder zu verschlüsseln?

Zwei Tage würden wohl reichen, die Gruppe hinter Trickbot hat scheinbar bloß zu viel zu tun. Wie erwähnt erfolgt die Infektion mit Emotet und die Folgeinfektion mit Trickbot automatisch. Danach sehen sich die Angreifer auf den Systemen um, und mit dieser Handarbeit kommen sie offenbar nicht hinterher. Deswegen fielen auch in den letzten Wochen relativ konstant neue Trickbot-Infektionen auf, obwohl Emotet in eine Art Sommerpause gegangen war: Die Gang hinter Trickbot scheint ihre von Emotet gut gefüllte „Auftragsliste“ abgearbeitet zu haben. Mittlerweile ist auch Emotet wieder aktiv.

Die Verzögerung durch diesen Rückstau bei Trickbot beträgt typischerweise ein bis zwei Wochen, aber es sind auch Fälle von mehreren Monaten bekannt. Heise jedenfalls hat die Verzögerung nutzen können, um die infizierten Netze vom Internet zu trennen und so das Schlimmste zu verhindern.

Kosten

Welche Kosten sind dem Verlag durch die Infektion entstanden?

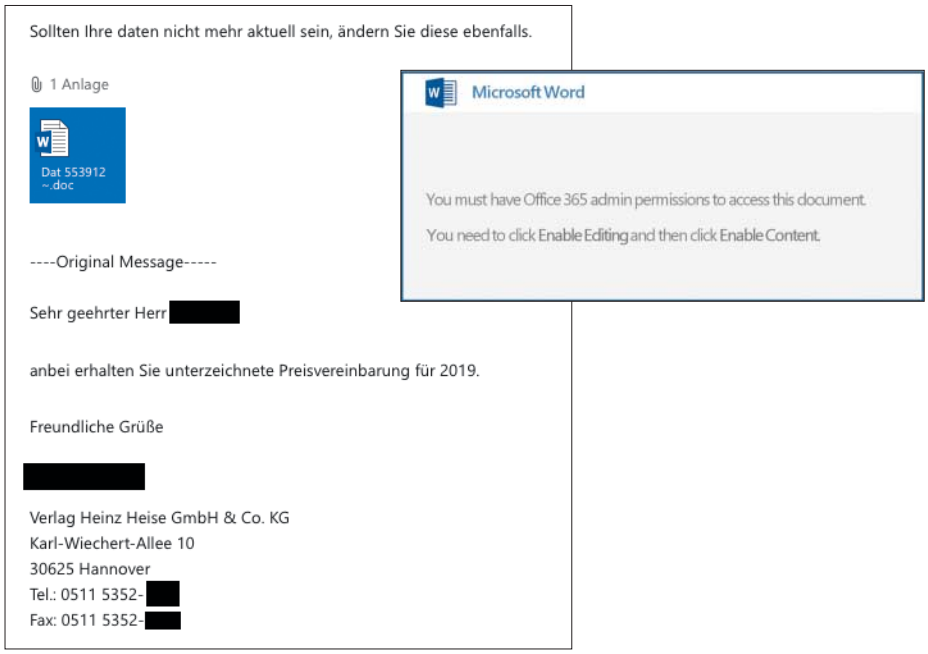
Das kommt darauf an, wie man rechnet. Die direkten Kosten, insbesondere für die hinzugezogenen externen Experten betragen ungefähr 50.000 Euro. Hinzu kommen interne Kosten, wie die Mehrarbeit der hauseigenen IT. Kaum sinnvoll zu beziffern sind mögliche Umsatzeinbußen. Schließlich konnten Mitarbeiter teilweise tagelang nicht oder nur eingeschränkt arbeiten. Entweder weil ihr Computer direkt betroffen war, oder weil ihr Arbeitsplatz an einem kompromittierten Netz hing und deshalb vom Internet getrennt worden war – ohne Internet geht heutzutage nicht viel, auch wenn unsere Kollegen die Faxgeräte wiederentdeckt haben.

Außerdem implementiert der Verlag ein neues Sicherheitskonzept, für das in den nächsten Jahren etwa 500.000 Euro veranschlagt sind – allerdings sind das keine Kosten, die man direkt der Infektion zuordnen kann, IT-Sicherheit muss ohnehin laufend fortentwickelt werden.

Spatzen, Kanonen und die Rosskur

Habt ihr bei euren Gegenmaßnahmen nicht mit Kanonen auf Spatzen geschossen? Die Kosten die entstehen, wenn mangels Internet tagelang niemand vernünftig arbeiten kann, sind ja nicht unerheblich.

Das ist zwar richtig, aber eindeutig das kleinere Übel. Wenn die Angreifer wirklich zum Zug kommen, ist der Schaden in der Regel deutlich größer, oft existenzbedrohend. Die Täter wollen schließlich ihren Gewinn maximieren. An



Perfide Masche: Die „Original Message“ ist eine authentische Mail, was die „Antwort“, mit der Emotet kommt, plausibel macht. Das angehängt Word-Dokument präsentiert dann ein gut gemachtes „Pop-up“, das zum Aktivieren von Inhalten auffordert.

die absolute Schmerzgrenze können Sie mit ihren Forderungen dann gehen, wenn die Alternative der komplette Ruin der Firma ist.

Außerdem ist es brandgefährlich, ein infiziertes Netz wieder mit dem Internet zu verbinden – auch wenn es scheinbar gesäubert ist. Moderne Malware kennt unzählige Tricks um irgendwo zu schlafen und dann Wochen später wieder „auszubrechen“. Wir haben die infizierten Netzwerke deswegen entfernt. Alle beteiligten Maschinen wurden komplett neu aufgesetzt und erst dann mit einem neuen Netz verbunden.

Mailerkennung

Kann man solche Phishing-Mails denn nicht erkennen? Fiel dem Mitarbeiter nicht auf, dass der Absender gefälscht war?

Nein, das lässt sich nicht zuverlässig erkennen und man sollte sich tunlichst nicht auf den eigenen Spürsinn verlassen. Zum einen lassen sich Angaben wie Name oder Mail-Adresse des Absenders fälschen – Emotet macht das. Zum anderen verbreitet sich Emotet unter anderem dadurch, dass auf einem bereits infizierten System E-Mail-Konversationen untersucht werden. Die Malware nimmt dann solche Schriftwechsel wieder auf, baut eine Antwortmail – komplett mit zitiertem originalen Inhalt – und versendet sich an ein neues Opfer.

So ist nicht nur der vorgebliche Ursprung der Mail plausibel, sie referenziert auch eine reale Kommunikation. Hinzu kommt, dass das angehängte Dokument erklärt, man müsse „Inhalte aktivieren“, also Makros ausführen. Gerade wenn Dokumente mit Makros im Alltag genutzt werden, führt das alles schnell zu einem unbedachten Klick.

Ein guter Schutz dagegen ist, Dokumente mit Makros grundsätzlich nicht zuzustellen. Wie ihr E-Mail-System solche und andere Anhänge handhabt, können Sie übrigens mittlerweile mit dem E-Mail-Check von heise Security prüfen, siehe ct.de/y4wb.

Sündenbock gesucht

Gab es Konsequenzen für den Verursacher – also den Mitarbeiter, der die Mail bekommen und Makros in der angehängten Datei aktiviert hat?

Nein, natürlich nicht. Der Verlagsinhaber Ansgar Heise hat in Interviews auch erklärt: „Das hätte mir selbst auch passieren können.“ Individuelle Konsequenzen – welcher Natur auch immer – wären schlicht unfair; Fehler können nun mal jedem passieren. Außerdem führen solche Reaktionen dazu, dass Mitarbeiter aus Angst vor Repressalien Probleme nicht mehr melden, womit niemandem gedient ist.

Stattdessen arbeiten wir daran, die Gefahr solcher Fehler in Zukunft zu verringern, teilweise durch technische Maßnahmen und teilweise durch Schulungen für Mitarbeiter.

Mehr Details

Ich möchte mehr technische Details – insbesondere zu den von Heise jetzt (zusätzlich) getroffenen Schutzmaßnahmen.

Wir haben dazu bereits zwei Webinare veröffentlicht, damit insbesondere andere Firmen und deren Systemadministratoren aus unseren Fehlern lernen können. Darin gehen wir sowohl auf die allgemeine Gefahrenlage und mögliche Schutzmechanismen ein, als auch auf die konkreten Gegenmaßnahmen, die Heise jetzt einführt. Kostenpflichtige Aufzeichnungen dieser Webinare finden Sie unter ct.de/y4wb.

Leidensgenossen

Meine Firma hat auch mit einem Malwarebefall zu kämpfen. An wen kann ich mich denn wenden, um Hilfe zu bekommen?

Von den Polizeien der Bundesländer (und auch vom BKA) gibt es „Zentrale Ansprechstellen Cybercrime“ (ZAC). Dort können Sie nicht nur eine Anzeige zum Vorfall erstatten, sondern Sie bekommen auch praktische Hilfe. Die ZACs können Ihnen außerdem lokale Dienstleister nennen, die Erfahrung mit derartigen Notfällen haben.

Eine Liste aller ZACs samt Mail-Adressen und Telefonnummern finden Sie unter ct.de/y4wb. *(syt@ct.de)*

Weiterführende Links: **ct.de/y4wb**