Emotet bei Heise

Erste Lehren aus einem Emotet-Trojaner-Befall

Emotet hat Heise getroffen. Es gab einen schwerwiegenden Einbruch in das Netz, dessen Auslöser eine Emotet-Infektion war. An der Analyse, Beseitigung und dem geordneten Wiederaufbau einer sauberen Infrastruktur arbeiten aktuell die IT-Abteilungen der Heise Gruppe und eine Reihe hinzugezogener Spezialisten.

Von Jürgen Schmidt

Von dem Vorfall betroffen waren und sind die Heise Gruppe und der Verlag Heinz Heise, also Mutter- und Schwester-Unternehmen der Heise Medien, die unter anderem c't herausgeben. Auf die Netze von Heise Medien gab es nach aktuellem Stand der Untersuchungen keine Übergriffe.

Am Montag, den 13. Mai, um kurz vor 15 Uhr öffnete ein Mitarbeiter eine Mail, die sich auf einen zitierten, echten Geschäftsvorgang bezog. Die Mail stammte scheinbar von einem Geschäftspartner und forderte dazu auf, die Daten im angehängten Word-Dokument zu kontrollieren und bei Bedarf zu ändern. Beim Öffnen des Dokuments erschien eine (gefälschte) Fehlermeldung, die dazu aufforderte, „Enable Editing" anzuklicken. Dieser Aufforderung kam der Mitarbeiter nach – und das Unheil nahm seinen Lauf.

Im Hintergrund infizierte nämlich Emotet sein Windows-System und begann sofort, sein Unwesen im Heise-Netz zu treiben. Dies äußerte sich zunächst in einigen kleineren Infektionen, die auch Alarme der eingesetzten Antiviren-Software (Avira und Windows Defender) auslösten. Die hinzugezogenen Administratoren reinigten diese Systeme oberflächlich und waren zunächst der Überzeugung, das Problem damit im Griff zu haben.

Das änderte sich Mittwochnachmittag, als in den Firewall-Logs reihenweise Verbindungen zu bekannten Emotet-Servern auffielen. Ein schneller Check zeigte, dass bereits eine ganze Reihe von Rechnern über seltsame Verbindungen etwa auf TCP-Port 449 nach draußen kommunizierte. Das bedeutete: „**ROTER ALARM!**"

Einer der Admins entdeckte außerdem, dass es zu diesem Zeitpunkt bereits höchst verdächtige Zugriffe auf den Domain Controller des Active Directory gab – also auf den Verzeichnisdienst, der in Windows-Netzen unter anderem die Zugangsberechtigungen verwaltet. Die Administratoren versuchten zunächst, die Kommunikation mit der Emotet-Kommandoinfrastruktur zu unterbinden. Doch das erwies sich als Hase-und-Igel-Rennen, das nicht zu gewinnen war. Es kamen ständig neue Emotet-Verbindungen hinzu. Letztlich entschieden sich die Admins für einen kompletten Lockdown. Zu diesem Zeitpunkt wurde die Internet-Verbindung für alle betroffenen Netze komplett gekappt.

Parallel dazu entschied die IT, dass man externe Hilfe hinzuziehen musste. Konkret arbeiteten ab Donnerstag mehrere Forensiker und Incident-Response-Spezialisten gemeinsam mit den Heise-ITlern daran, die Vorgänge aufzuklären und wieder einen normalen IT-Betrieb aufzunehmen, ohne dabei eine erneute Infektion zu riskieren. Darüber hinaus wird auch das Sicherheitskonzept auf den Prüfstand gestellt und es werden Konzepte erarbeitet, wie man solch einen IT-GAU zukünftig verhindern kann.

Emotet im Netz

All das ist noch in vollem Gange und wird sich voraussichtlich noch mehrere Wochen hinziehen. Und noch immer gibt es mehr offene Fragen als klare Antworten. Trotzdem haben wir uns entschieden, hier bereits einen Zwischenstand zu dokumentieren, weil wir den Vorfall möglichst transparent aufarbeiten wollen. Nicht zuletzt wollen wir es damit anderen Firmen ermöglichen, aus unseren Fehlern zu lernen.

Zunächst zu den Aktivitäten von Emotet: Der Schädling hat offenbar nach der Erst-Infektion weitere Module nachgeladen – eines davon firmiert unter dem Namen Trickbot. Diese haben dann recht schnell alle Windows-10-Arbeitsplätze im Netz infiziert, an denen die Benutzer lokale Admin-Rechte hatten. Das war eigentlich bereits per Policy untersagt. Allerdings gab es einige Ausnahmen, etwa auf einigen gerade eingerichteten Rechnern für eine interne Schulung, deren Software lokale Adminrechte erforderte. Anschließend infizierte Emotet – also genauer die von Emotet nachgeladenen Schadprogramme – alle im Netz noch aktiven Windows-7-Systeme; die Windows-10-Arbeitsplätze ohne lokale Admins blieben anscheinend verschont. Der Grund dafür ist bisher unklar.

Zumindest ein Teil dieser Infektionen erfolgte über Credentials eines Domänen-Administrators. Über diese richtete Emotet auf dem Zielrechner einen neuen Dienst ein. Wie Emotet an diese Credentials kam, ist noch nicht abschließend geklärt. Die Log-Dateien dokumentieren zwar übermäßig viele fehlgeschlagene Anmeldeversuche durch eine Brute-Force-Attacke auf das Passwort. Angesichts dessen Stärke erscheint es jedoch wahrscheinlicher, dass Emotet die Domain-Admin-Credentials etwa aus dem RAM eines infizierten Systems abgezogen hat. Unter anderem ist nicht auszuschließen, dass sich jemand zur Reinigung eines infizierten Systems als Domain Admin angemeldet hat. Das wäre einer der Kardinalfehler, die man unbedingt vermeiden sollte.

Was alles nicht passiert ist

Nach dem ersten Schreck kehrt jetzt langsam etwas Ruhe ein. Insbesondere auch deshalb, weil sich die Anzeichen verdichten, dass der ganz bittere Kelch gerade nochmal an uns vorbei gegangen ist. Nach der ersten Ausbreitungsphase installieren

Was ist Emotet?

Das US-CERT bezeichnet Emotet als die aktuell wohl zerstörerischste Schad-Software – und das mit gutem Grund. Die Gangs hinter Emotet haben Cybercrime auf ein neues Niveau gehoben. Das Ziel von Emotet sind vor allem Firmen, Behörden und andere Institutionen, bei denen Geld zu holen ist.

Das von Emotet erfundene Dynamit-Phishing knüpft an existierende Kommunikationsbeziehungen an. Dabei erhält das Opfer scheinbar Antworten auf eigene Mails, deren Inhalt Emotet zuvor auf anderen Systemen gestohlen hat. Diese Trojaner-Mails sind so gut gemacht, dass man davon ausgehen muss, dass selbst gut geschulte Mitarbeiter früher oder später darauf reinfallen können.

Emotet lädt verschiedenste Schad-Programme wie Trickbot nach. Die nutzen dann Nachlässigkeiten im Sicherheitskonzept systematisch aus, um sich im lokalen Netz einer betroffenen Firma auszubreiten. Zu den eingesetzten Techniken gehört Passwort-Diebstahl, Pass-the-Hash-Angriffe und der Einsatz der Windows Powershell, unter anderem um Angriffe vor herkömmlicher Schutz-Software wie Antiviren-Programmen zu verbergen.

In der nächsten Eskalationsstufe sehen sich die Angreifer oft sogar manuell im betroffenen Netz um. Ziel ist es unter anderem, weitere Informationen über das Unternehmen zu sammeln und kritische IT-Komponenten und Backups zu lokalisieren. Das CERT-Bund hat auch bereits mehrere Fälle beobachtet, in denen dabei etwa Wartungs-Zugänge eines befallenen IT-Dienstleisters ausgenutzt wurden, um weitere Firmen zu infizieren. Abschließend werden dann häufig Verschlüsselungstrojaner wie Ryuk an strategisch wichtigen Stellen platziert.

Bild: Kryptos Logic

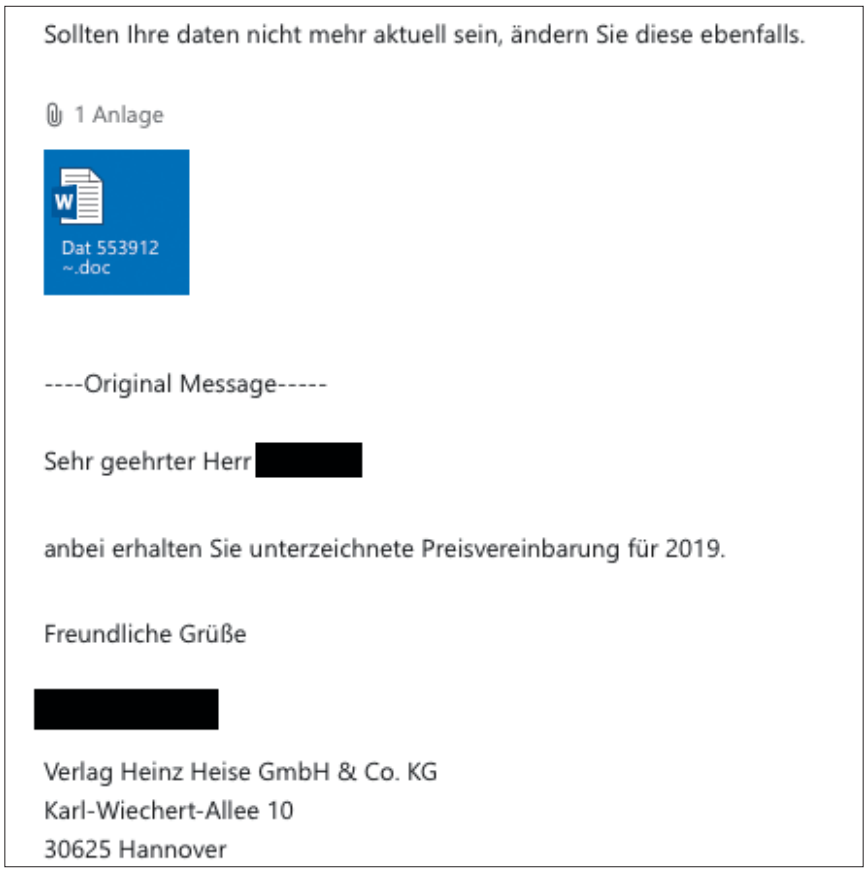
Die Emotet-Gang operiert weltweit mit Schwerpunkten in Asien, Europa und Amerika.

Zum Zeitpunkt X legt Emotet die IT des Opfers komplett lahm und präsentiert eine Lösegeldforderung. Anders als bei Locky & Co handelt es sich dabei nicht um ein paar hundert oder tausend Euro. Die Kriminellen kennen schließlich zu diesem Zeitpunkt ihr Opfer und orientieren ihre Forderungen am geschätzten Umsatz der Firma. Typische Forderungen gehen von 30.000 bis weit über 100.000 Euro. Demgegenüber steht, was das BSI als einen „existenzbedrohenden Datenverlust" für das Opfer bezeichnet. Viele Firmen sehen folglich keinen anderen Ausweg, als zu zahlen.

Alle Zeichen deuten darauf hin, dass Emotet diese Aktivitäten in den nächsten Monaten noch weiter ausweiten wird. Das bedrohliche daran ist, dass das keineswegs nur Großkonzerne oder Banken trifft, sondern alle möglichen Firmen und Branchen: Autohändler und Verlage genauso wie Stadtverwaltungen und Krankenhäuser. Und viele davon sind auf Gefahren dieses Kalibers nur unzureichend vorbereitet.

die Emotet-Gangster sehr häufig Verschlüsselungs-Trojaner; insbesondere wurde in diesem Kontext bereits mehrfach Ryuk in Firmennetzen gefunden. Dabei verlassen sich die Kriminellen dann auch nicht mehr allein auf die automatisierten Fähigkeiten ihrer Tools, sondern besuchen die Netze etwa via RDP persönlich, um dort Backups und zentrale Komponenten der IT-Infrastruktur zu lokalisieren.

Doch selbst eine gezielte Suche lieferte bisher keine Anzeichen für Verschlüsselungs-Trojaner und manuelle Interaktion mit den infizierten Systemen. Es sieht bisher ganz so aus, als hätte der Lockdown der Netze diese Eskalation noch rechtzeitig unterbunden.



Emotet kommt häufig wie hier, als scheinbare Antwort auf eine Mail, die man tatsächlich selbst verfasst hat. Bei einem Emotet-Angriff auf Ihre Firma steht dann dort Ihr Firmenname anstelle von Heise.

Aufräumarbeiten

Die infizierten Rechner wurden alle komplett außer Betrieb genommen. Auch die scheinbar sauberen Windows-10-Rechner kamen nicht mehr mit anderen Netzen oder gar dem Internet in Verbindung. Und das wird auch so bleiben. Weil es sich als aussichtslos erwiesen hat, alle Emotet-Aktivitäten lückenlos zu dokumentieren und man kein Risiko einer erneuten Infektion etwa durch eine übersehene Backdoor eingehen will, werden die betroffenen Komponenten alle stillgelegt beziehungsweise neu aufgesetzt.

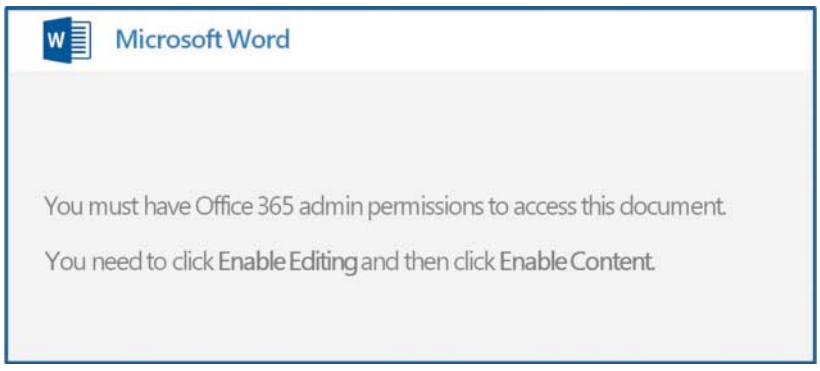
Die Admins haben sich entschieden, ein komplett neues Netz mit neu aufgesetzten Rechnern und einem neuen Active Directory hochzuziehen. Dabei werden auch gleich neue, verschärfte Sicherheitsmaßnahmen umgesetzt, die eine vergleichbare Eskalation zukünftig unterbinden oder doch deutlich erschweren sollen. Existierende Daten, Werkzeuge und Ähnliches werden unter größter Vorsicht Schritt für Schritt in dieses neue Netz übertragen. Zwar ist mittlerweile die Arbeitsfähigkeit weitgehend wiederhergestellt, doch es wird sicher noch einige Wochen dauern, bis dieser Umzug vollständig abgeschlossen ist.

Welche Daten die Kriminellen bereits abziehen konnten, ist noch nicht ausreichend geklärt. Die Verantwortlichen haben den Vorfall jedenfalls bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet, wie es die DSGVO fordert. Darüber hinaus wurde der Vorfall bei der Polizei zur Anzeige gebracht. Auch Geschäftspartner wurden über das gesteigerte Risiko von Trojaner-Mails informiert.

Die Infrastruktur von Heise Medien und insbesondere der Redaktionen von c't und heise online ist weitgehend unabhängig von der IT der Heise Gruppe. Es gibt dort keine Anzeichen für eine Kompromittierung durch Emotet. Insbesondere gibt es keinerlei Hinweise, dass Daten von Abonnenten und anderen Geschäftspartnern der Heise Medien in Gefahr waren.

Dieser Vorfall ist noch lange nicht abschließend geklärt. Doch wir werden ihn auch weiterhin so transparent wie möglich handhaben und sicher weitere Artikel dazu veröffentlichen. Ganz oben auf der Liste steht dabei „Wie schützt man sich besser vor Emotet“. Das Wichtigste dazu bereits kurz vorab: Gehen Sie davon aus, dass es auch Ihre Firma treffen wird. Bereiten Sie sich am besten jetzt darauf vor.

(ju@ct.de) c't



Wer einer Aufforderung wie dieser nachkommt, aktiviert das Ausführen von Makros und Emotet kann heimlich im Hintergrund den PC infizieren.