INFOPAPER:
EMOTET - DIE GEFÄHRLICHSTE SCHADSOFTWARE DER WELT

Inhalt

Einleitung

++++ Emotet-Schadsoftware knackt WLANs ++++

++++ Emotet: IT-Totalschaden beim Kammergericht Berlin ++++

++++ Emotet hat Deutschland weiterhin im Griff ++++

Immer wieder taucht der Name „Emotet" in den Nachrichten im Zusammenhang mit besonders schweren Hacker-angriffen auf Unternehmen, Verwaltungen, Krankenhäuser und Universitäten auf. Im Jahr 2019 betitelte das BSI die Malware als **gefährlichste Schadsoftware der Welt,** denn das Schadprogramm richtet Schäden in Millionenhöhe an. Was Emotet so bedrohlich macht und wie man sich dagegen schützen kann, wird im Folgenden beschrieben.

Was ist Emotet?

Das erste Mal tauchte Emotet als **Banking-Trojaner** im Jahr 2014 auf. Die Attacke zielte darauf ab, Online-Zugangsdaten von deutschen und österreichischen Bankkunden abzufangen. Mittlerweile kann Emotet jedoch eine Vielzahl **weiterer Module mit anderen Schadfunktionen nachladen und ausführen.**

Emotet schlägt vor allem **mittels Spam-E-Mail zu und trifft sowohl private Anwender als auch Unternehmen,** Krankenhäuser, staatliche Einrichtungen und Kritische Infrastrukturen. Dabei werden Methoden hochprofessioneller Advanced Persistent Threat-Angriffe adaptiert und automatisiert. Cyberkriminelle gehen sehr zielgerichtet und mit großem Aufwand vor, um möglichst lange im befallenen System handlungsfähig zu bleiben.

Ein Aspekt macht Emotet besonders gefährlich: Seit Ende 2018 ist die Malware in der Lage mittels sogenanntem **Outlook-Harvesting** die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme auszulesen, um auf dieser Basis weitere Angriffe zu starten. Die Verbreitung erfolgt dadurch besonders schnell. Weitere Empfänger erhalten dann ebenso authentisch wirkende E-Mails von Personen, mit denen sie erst kürzlich im Kontakt standen. Schadhafte Dateianhänge oder in der Nachricht enthaltende URLs werden unbedacht geöffnet.

Neben diesem Spam-Modul **kann Emotet auch ein Wurm-Modul laden,** mit dem es sich selbstständig im Firmennetzwerk verbreitet. So kann es sich auf weiteren Rechnern einnisten, ohne dass Nutzer einen Anhang anklicken und aktivieren müssen.

In diesem Rahmen unternimmt Emotet **auch Brute-Force-Angriffe mit dem Ziel Passwörter zu knacken.** Dies kann schwerwiegende Konsequenzen haben. Ist der Computer erst infiziert, lädt Emotet je nach Ziel weitere Schadsoftware über Command-and-Control-Server nach. Es drohen Datendiebstahl, Kontrollverlust über Systeme, der Ausfall der kompletten IT-Infrastruktur und Einschränkungen von kritischen Geschäftsprozessen. In Extremfällen müssen ganze Unternehmensnetzwerke nach einer Infektion neu aufgebaut werden. **Die Schäden liegen oft in Millionenhöhe.**

Meister der Tarnung: Warum Emotet so schwierig zu bekämpfen ist

Emotet ist nicht einfach zu identifizieren und abzufangen, da es herkömmliche Antivirenprodukte täuscht: Als **polymorpher Virus verändert sich der Code bei jedem neuen Abruf leicht,** um der Erkennung durch signaturbasierte Virenscanner zu entgehen.

Darüber hinaus **erkennt der Virus, wenn er in einer virtuellen Maschine ausgeführt wird.** Sobald eine Sandbox registriert wird, fällt das Programm in eine Art Stand-By-Modus und führt in diesem Moment keine schadhaften Aktionen aus.

Eine gefährliche Allianz: Emotet, TrickBot und die Ransomware Ryuk

Wie bereits erwähnt, lädt Emotet nach einer erfolgreichen Infektion weitere Schadprogramme nach. Eine besonders gefährliche Allianz entsteht im Zusammenspiel mit TrickBot und Ryuk: Getarnt in einem Word-Dokument dringt Emotet beim Ausführen der Datei in ein Unternehmensnetzwerk ein und kundschaftet dieses aus. **Als „Türöffner" lädt er den Banking-Trojaner TrickBot** nach, der unter anderem Kontozugangsdaten

Eine gefährliche Allianz: Emotet, TrickBot und die Ransomware Ryuk

kopiert. Diese **Information gibt er an die Ransomware Ryuk weiter,** die schließlich als letztes nachgeladen wird. Ryuk verschlüsselt nun alle im System befindlichen Dateien, die TrickBot und Emotet zuvor als sensibel bzw. wichtig eingestuft haben.

Das besonders Hinterlistige an Ryuk ist allerdings, dass es neben der Verschlüsselung wichtiger Daten im gleichen Zuge alle hiervon **existierenden Sicherheitskopien löscht** und somit die Wiederherstellung erheblich erschwert. Den Experten von Hornetsecurity zufolge kristallisiert sich mit dieser Löschfunktion ein neuer Trend in der Entwicklung von Erpressungssoftware heraus. Die geforderte Summe richtet sich zudem nach dem Wert, den TrickBot als derzeitigen finanziellen Verfügbarkeitsrahmen des Unternehmens ausmachen konnte. Dabei ist die **Attacke sehr zielgerichtet und betrifft vor allem Unternehmen,** die in der Lage sind, eine hohe Summe zu zahlen, um wieder Zugriff auf ihre Daten zu erlangen.

Ryuk tauchte erstmalig im August 2018 auf und erwirtschaftete seitdem mehrere Millionen Euro. Welche Hackergruppe dahinter steckt ist bislang noch unklar.

Wie kann man sich schützen?

Um sich effektiv vor Emotet zu schützen, muss man sich vor allem auf das **Haupteinfallstor des Schadprogramms konzentrieren: Der E-Mail-Kommunikation.** Hornetsecurity Advanced Threat Protection erkennt in E-Mails Emotet und Ryuk mühelos und stellt beide Malware-Programme unter Quarantäne. Bereits in der ersten Analyse-Instanz wird der Emotet-Trojaner identifiziert. Die nachgelagerten Trojaner Ryuk und TrickBot können mithilfe der **dynamischen Verhaltensanalyse in der ATP Sandbox entlarvt werden.** E-Mails, die die perfiden Schadprogramme enthalten, werden den Empfängern nicht zugestellt.

Diese grundlegenden Verhaltensweisen sollten beachtet werden

Da sich Emotet **häufig in Microsoft Office-Dateien versteckt** und Makros benötigt, um Schadprogramme installieren zu können, ist es sinnvoll diese nicht zuzulassen. Im privaten sowie in den meisten geschäftlichen Bereichen werden diese auch nicht benötigt. Sollte dennoch nicht darauf verzichtet werden können, ist es möglich nur signierte Makros zu erlauben.

Regelmäßige Daten-Backups sind empfehlenswert.

Sicherheitsupdates müssen umgehend für Betriebssysteme, Antiviren-Programme, Web-Browser, E-Mail-Clients und Office-Programme installiert werden.

Wachsamkeit ist das oberste Gebot: Auch bei vermeintlich bekannten Absendern sollte man bei Dateianhängen von E-Mails, insbesondere bei Office-Dokumenten und enthaltenen Links, vorsichtig sein.

Im Zweifelsfalle ist es ratsam bei einer verdächtigen E-Mail den direkten Kontakt zum Absender zu suchen und die Glaubhaftigkeit des Inhaltes zu überprüfen.

Zugriffe im **unternehmenseigenen Netzwerk sollten kontinuierlich überwacht** werden, denn so kann rechtzeitig festgestellt werden, ob eine Emotet-Infektion stattgefunden hat.

Checkliste: Was muss bei einer Emotet-Infektion geschehen?

Sollten die getroffenen Sicherheitsmaßnahmen versagen und es trotz alledem zu einer Infektion kommt, müssen umgehend folgende Schritte eingeleitet werden:

Um eine Weiterverbreitung zu unterbinden, muss schnellstens die **Unternehmens-IT und das Umfeld über die Infektion informiert werden.** Mailkontakte sind besonders gefährdet sich ebenfalls zu infizieren.

Emotet C&C IPs müssen umgehend blockiert werden. Dadurch bekommt das Schadprogramm keine neuen Befehle mehr und kann keine weiteren Module herunterladen.

Die Malware nimmt tiefgreifende sicherheitsrelevante Änderungen am infizierten System vor und lässt sich nicht so leicht von Rechnern entfernen. Daher ist es unumgänglich betroffene IT-Komponenten neu aufzusetzen.

Sämtliche zuvor genutzte Passwörter sollten ausgetauscht werden, da Angreifer diese vermutlich abgegriffen haben und sich damit Zugang zu weiteren sensiblen Bereichen verschaffen können.

Es gilt bestehende Sicherheitskonzepte zu hinterfragen und Einfallstore zu identifizieren, um sich vor neuen Angriffen besser schützen zu können.

- ☑ **Unternehmens-IT und Umfeld schnellstens informieren**
- ☑ **Emotet C&C IPs blockieren**
- ☑ **Betroffene IT-Komponenten neu aufsetzen**
- ☑ **Sämtliche zuvor genutzte Passwörter austauschen**
- ☑ **Bestehende Sicherheitskonzepte hinterfragen**
- ☑ **Einfallstore identifizieren**