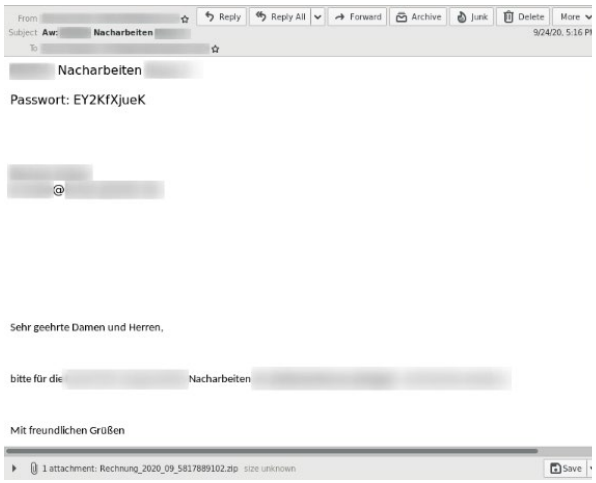
Pressemitteilung

01.10.2020

Emotet in verschlüsselten Anhängen – Eine wachsende Cyberbedrohung

Hannover, den 01.10.2020 *- Die Cyberkriminellen hinter dem Banking-Trojaner Emotet unternehmen viel, um mit verschiedensten Tricks Anti-Viren-Filter zu umgehen und die Malware auf noch mehr Systemen zu verbreiten. Von Email Conversation Thread Hijacking, über Änderungen der Webshells bis hin zum Update des Emotet-Loaders, was zu einem enormen Anstieg an Downloadzahlen der Malware führte. Nun versendet Emotet erneut verschlüsselte Anhänge über seinen Malspam, um sein Botnet-Netzwerk weiter ausbauen.*

Seit September beobachtet das Hornetsecurity Security Lab einen erheblichen Zuwachs an Emotet-Malspam, welcher wieder verschlüsselte Archiv-Dateien versendet. Das Passwort zur Entschlüsselung der Datei ist als Klartext im E-Mail Anschreiben enthalten. Durch die Verschlüsselung des Anhangs ist es herkömmlichen Anti-Viren-Programmen nicht möglich, das versteckte Schadprogramm zu entdecken und zu blockieren. Jedoch kann das Opfer die Datei entschlüsseln, öffnen und ausführen, wodurch die Malware schließlich nachgeladen wird.



Beispiel: Emotet-Malspam (Deutsch) mit verschlüsseltem Anhang (Bild: Hornetsecurity)

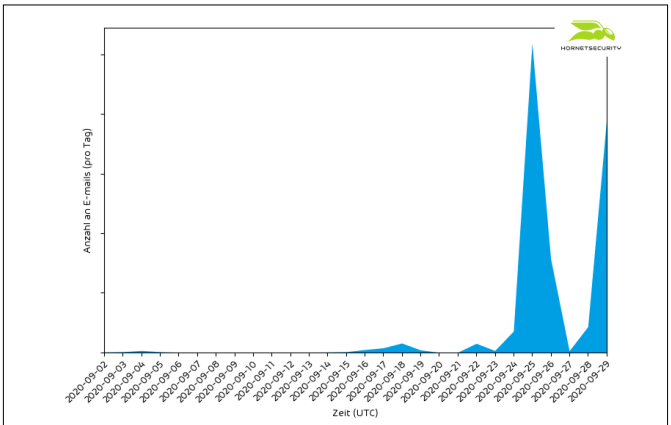
Doch diese Methode ist nicht neu: Bereits im April 2019 entdeckten Security-Analysten erste Wellen des Emotet-Malspams mit verschlüsselten Zip-Dateien. Seitdem treten solche Spamwellen immer mal wieder verteilt über das Jahr auf und halten einige wenige Tage an. Als Operation „Zip Lock" bezeichnet die White-Hat-Group „Cryptolaemus" dieses Vorgehen der Akteure hinter Emotet. Das Team aus über 20 Security Forschern und System Administratoren hat sich als Ziel gesetzt, die Verbreitung der „gefährlichsten Malware der Welt" einzudämmen. Täglich veröffentlicht die Gruppe sämtliche Updates von Emotet auf ihrer Website und dem Twitter-Account. Damit System- und Netzwerkadministratoren die sogenannten Indicators of compromise (IOCs), dazu gehören IP-Adressen für Emotet Befehlsserver, Betreffzeilen und Datei-Hashes von Emotet-infizierten Dateien, in ihren Security-Filtern eintragen und sich so vor möglichen Emotet-Infektionen schützen können.

Screenshot eines geöffneten verschlüsselten Anhangs der Emotet-Kampagne auf Japanisch (Bild: Hornetsecurity)

Die aktuelle Malspam-Welle mit verschlüsselten Archiven sei nun bereits seit mindestens 1. September aktiv und zielte zuerst auf den japanisch-sprachigen Raum. Das Hornetsecurity

Security Lab registrierte schließlich Spam-Wellen auf Spanisch, Englisch und Deutsch ab etwa dem 14. September.

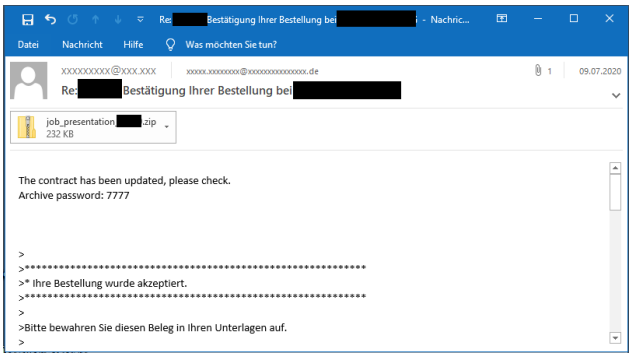
Um die Chance noch weiter zu erhöhen, dass ihr Opfer die Schad-Mail beim Eintreffen im Postfach auch tatsächlich öffnet und den Anhang aktiviert, bedienen sich die Cyberkriminellen zusätzlich der „Email Conversation Thread Hijacking" Technik. Dabei werden bereits bestehende E-Mail-Konversations-Threads des Opfers verwendet, um „authentischer" zu wirken. Die Angreifer antworten dann auf bestehende Unterhaltungen, die ihr Angriffsziel in der Mailbox noch gespeichert hat.



Aufzeichnung der Emotet-Malspam Kampagne (Bild: Hornetsecurity)

Ein beliebter Cybercrime-Trend

Generell ist die E-Mail Angriffsmethode mit verschlüsselten Anhängen recht beliebt unter cyberkriminellen Gruppen. So entdeckten die Security-Analysten von Hornetsecurity auch in Malware-Kampagnen von GandCrab verschlüsselte Office-Dokumente und die Malware Ursnif verbreitet sich ebenfalls durch verschlüsselte Zip-Anhänge.



Beispiel: GandCrab Schad-E-Mail mit verschlüsseltem Anhang (Bild: Hornetsecurity)

Wie kann ich mich davor schützen?

Die verschlüsselten Emotet-Dateien werden bis heute nicht von herkömmlichen Antivirenprogrammen entdeckt, dass beweist der Malwarescanner Dienst VirusTotal.

Auch die Technik des Email Conversation Thread Hijacking trägt zum „Erfolg" der Cyberkriminellen bei, denn für die Empfänger ist es kaum möglich, einen solchen Angriff zu erkennen, da die Schad-E-Mails von einem legitimen, aber kompromittierten Konto versendet werden.

Tiefergehende Filter und intelligente Security-Mechanismen sind jedoch in der Lage, beide dieser Angriffstechniken zu entdecken und diese vom Postfach des Empfängers fernzuhalten. Das Vorgehen der Cyberkriminellen hinter Emotet verdeutlicht, dass es auch für Unternehmen an der Zeit ist, den nächsten Schritt im Bereich der Cybersecurity zu gehen. Denn erfolgreiche Attacken treiben die Ambitionen der Hacker weiter an und bringen auch weitere Cyberkriminelle auf den Plan.

Weitere Informationen unter: https://www.hornetsecurity.com/de/wissensdatenbank/emotet/.

Zeichenzahl: 4.091 (inkl. Leerzeichen)

Über die Hornetsecurity Group

Hornetsecurity ist der in Europa führende deutsche Cloud Security Provider für E-Mail und schützt die IT-Infrastruktur, digitale Kommunikation sowie Daten von Unternehmen und Organisationen jeglicher Größenordnung. Seine Dienste erbringt der Sicherheitsspezialist aus Hannover über weltweit 9 redundant gesicherte Rechenzentren. Das Produktportfolio umfasst alle wichtigen Bereiche der E-Mail-Security, von Spam- und Virenfilter über rechtssichere Archivierung und Verschlüsselung, bis hin zur Abwehr von CEO Fraud und Ransomware. Hornetsecurity ist mit rund 200 Mitarbeitern global an 11 Standorten vertreten und operiert mit seinem internationalen Händlernetzwerk in mehr als 30 Ländern. Zu den über 40.000 Kunden zählen unter anderem Swisscom, Telefonica, KONICA MINOLTA, LVM Versicherung, DEKRA und Claas.

Unternehmenskontakt:

Hornetsecurity GmbH

Micha Beyersdorf
Kommunikationsmanagement
Am Listholze 78
30177 Hannover
Tel.: +49 (511) 515 464 -917
E-Mail: presse@hornetsecurity.com

Pressekontakt

trendlux pr GmbH

Petra Spielmann
Presskontakt
Oeverseestr. 10-12
22769 Hamburg
Tel.: +49 (40) 800 80 99-00
E-Mail: ps@trendlux.de