Comeback von Emotet

HORNETSECURITY

Nach der Abschaltung des Emotet Botnet im Januar 2021 durch eine gemeinsame Aktion internationaler Strafverfolgungs- und Justizbehörden, stellten die Threat Researcher von Hornetsecurity nun wieder erste Aktivitäten fest. Das Security Lab beobachtete bereits neue Emotet-Malspam-Kampagnen im Umlauf.

Hintergrund

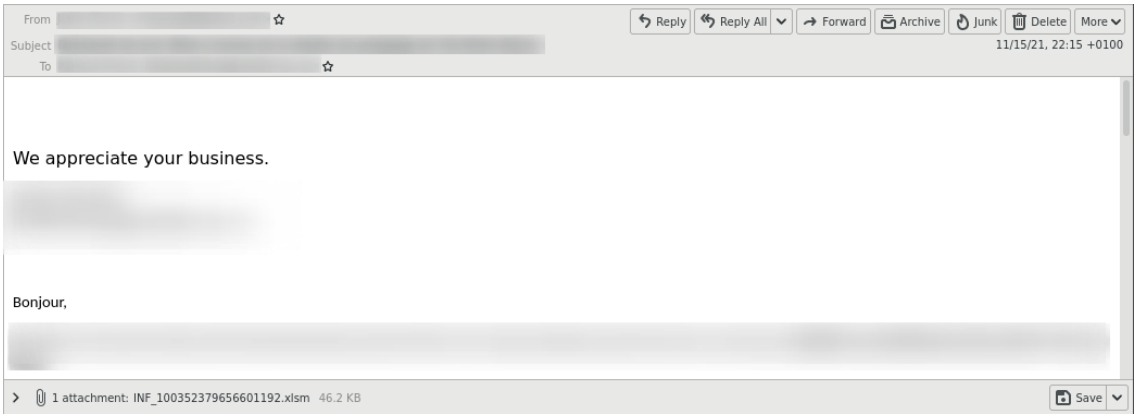
Emotet (auch bekannt als Heodo) wurde erstmals 2014 beobachtet. Es handelte sich um einen Banking-Trojaner, der Bankdaten und Anmeldedaten seiner Opfer stahl. Er wandelte sich jedoch zu einem Malware-as-a-Service (MaaS)-Betrieb, der anderen Cyberkriminellen Malware-Verbreitungsdienste bereitstellte. Bis Januar 2021 war Emotet die am weitesten verbreitete Malware-Operation. Zu diesem Zweck stahl es die E-Mails seiner Opfer und antwortete auf frühere Konversationen der Betroffenen. Diese Vorgehensweise wird auch als E-Mail-Konversations-Thread-Hijacking bezeichnet.5 Hornetsecurity veröffentlichte zahlreiche Blogposts über Emotet.[2,3,4,5,6,7]

Am 27.01.2021 gab Europol bekannt, dass eine internationale, weltweit koordinierte Aktion der Strafverfolgungs- und Justizbehörden das Emotet-Botnet aushebeln und die Ermittler die Kontrolle über die Infrastruktur der Schadsoftware übernehmen konnten. Das Emotet-Botnet wurde daraufhin von den Strafverfolgungsbehörden abgeschaltet.[8]

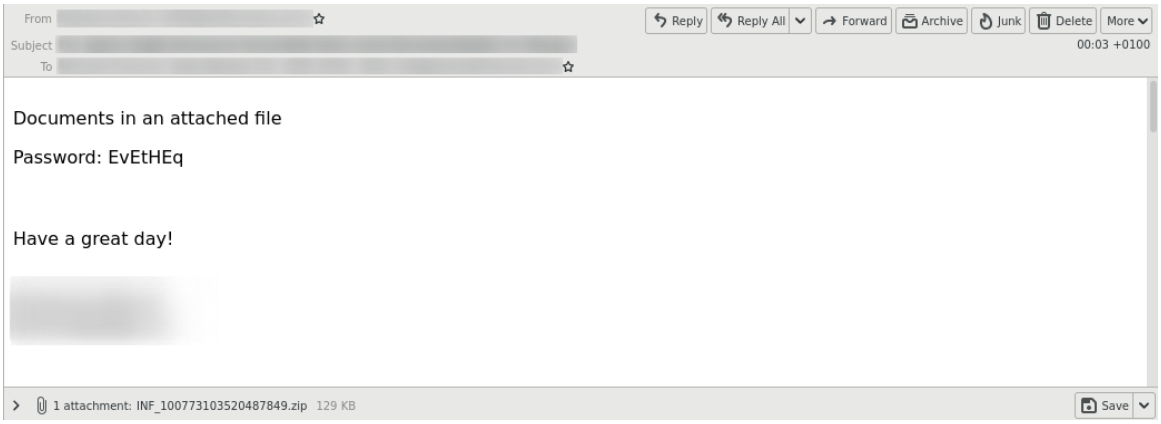
Das Comeback

Am 15.11.2021 wurde die TrickBot-Malware über Malspam verbreitet, heruntergeladen und installierte schließlich die Emotet-Malware. Anschließend wurde das Emotet-Botnet neu aufgebaut und begann erneut, Malspam aus seinem Botnet zu versenden.

Über das Botnet werden verschiedene schädliche Dokumente (XLSM und DOCM) versendet.



In einigen Fällen wurden die schädlichen Dokumente auch in verschlüsselten ZIP-Archiven platziert. Die Passwörter waren in den E-Mails im Klartext zu sehen.



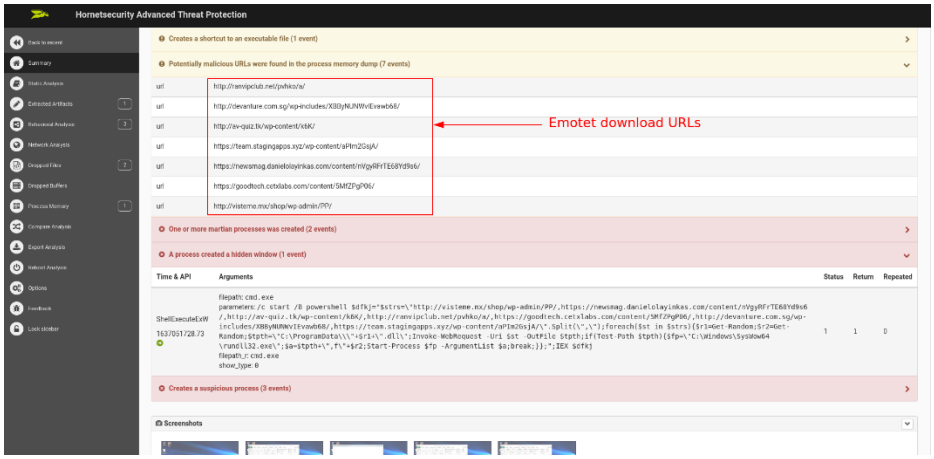
Wie bereits erwähnt, nutzt Emotet die Methode des E-Mail-Konversations-Thread-Hijacking[5], d. h. es stiehlt die E-Mails seiner Opfer und antwortet dann (oft sogar vom Konto des Opfers aus) auf abgeschlossene E-Mail-Konversationen, wobei es die vorherige Konversation in der E-Mail zitiert. Auf diese Weise wird der Betrug nicht direkt bzw. schwer ersichtlich.

Gegenmaßnahmen

Die technischen Schutzmechanismen von Hornetsecurity lassen sich nicht durch Social-Engineering-Techniken wie das Email Conversation Threat Hijacking täuschen.

Hornetsecuritys Advanced Threat Protection bietet die folgenden Features zur Abwehr der Emotet-Bedrohung:

- Malicious Document Decryption kann das in der E-Mail angegebene Kennwort verwenden, um die verschlüsselten ZIP-Archive zu entschlüsseln.
- Hornetsecuritys ATP-Sandbox erfasst die schädlichen Dokumente (auch wenn sie zuvor unbekannt waren).



Mit den oben genannten Informationen empfehlen wir unbedingt unseren Advanced Threat Protection Service für einen ausreichenden Schutz gegen anspruchsvolle Angreifer wie Emotet, die ihre Angriffsmuster jederzeit ändern können. Signaturen für bekannte schädliche Emotet-Dokumente werden Hornetsecuritys Spam- and Malware Protection hinzugefügt, um auch Kunden zu schützen, die kein ATP Service gebucht haben.

Referenzen

- [1] https://www.hornetsecurity.com/de/security-informationen/email-conversation-thread-hijacking/
- [2] https://www.hornetsecurity.com/de/security-informationen/emotets-rueckkehr-steht-bevor/
- [3] https://www.hornetsecurity.com/de/security-informationen/emotet-ist-zurueck/
- [4] https://www.hornetsecurity.com/de/security-informationen/webshells-hinter-emotet/
- [5] https://www.hornetsecurity.com/de/security-informationen/emotet-update-steigert-downloads/
- [6] https://www.hornetsecurity.com/de/security-informationen/trickbot-malspam-nutzt-black-lives-matter-aus/
- [7] https://www.hornetsecurity.com/de/security-informationen/der-malspam-qakbot-verbreitet-prolock/
- [8] https://www.hornetsecurity.com/de/threat-research/emotet-botnet-takedown/

Indicators of Compromise (IOCs)

URLs

- http[:]//ranvipclub[.]net/pvhko/a/
- http[:]//devanture[.]com[.]sg/wp-includes/XBByNUNWvIEvawb68/
- http[:]//av-quiz[.]tk/wp-content/k6K/
- https[:]//team.stagingapps[.]xyz/wp-content/aPIm2GsjA/
- https[:]//newsmag.danielolayinkas[.]com/content/nVgyRFrTE68Yd9s6/
- https[:]//goodtech.cetxlabs[.]com/content/5MfZPgP06/
- http[:]//visteme[.]mx/shop/wp-admin/PP/