



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Erneuter Versand von Emotet-Spam

CSW-Nr. 2021-269890-1032, Version 1.0, 16.11.2021

IT-Bedrohungslage*: **2 / Gelb**

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Nach übereinstimmenden Berichten mehrerer Quellen wurde gestern die Verteilung einer neuen Variante der Schadsoftware Emotet auf bereits mit TrickBot infizierte Systeme beobachtet [CYB2021] [TWI2021b]. Diese Beobachtung markiert die beginnende Rückkehr der Schadsoftware, deren alte Infrastruktur im Januar 2021 durch einen koordinierten Takedown erfolgreich zerschlagen wurde. Ebenfalls nach übereinstimmenden Berichten wurde bereits der Versand von Spam-Mails zur weiteren Verbreitung der Schadsoftware über ein neues Emotet-Botnetz bestätigt [TWI2021a] [TWI2021c] [SAN2021]. Derzeit werden mit den Spam-Mails schädliche .doc(m)- und .xls(m)-Dateien versendet bzw. passwortgeschützte ZIP-Archive, welche diese Dateien enthalten. Es ist davon auszugehen, dass anstelle von Dateianhängen mit den Spam-Mails zukünftig auch wieder Links versendet werden, welche zu schädlichen Office-Dateien führen.

Emotet war insbesondere für E-Mail-Thread-Hijacking bekannt. Dabei werden nicht nur Absenderadressen von E-Mails gefälscht, sondern vermeintliche Antworten auf zuvor ausgespähete E-Mails an die Kommunikationspartner versendet. Die bekannten Betreffzeilen und zitierten E-Mail-Inhalte tatsächlicher vorausgegangener Kommunikation lassen die Spam-Mails für die Empfänger authentisch erscheinen und verleiten sie dazu, die angehängten schädlichen „Köder“-Dokumente zu öffnen und die Ausführung aktiver Inhalte freizugeben. Dies führt zu einer erhöhten Durchschlagsquote dieser Angriffe. Das Vorgehen hat das BSI etwa unter [BSIa] beschrieben.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Bewertung

Es muss davon ausgegangen werden, dass es in Kürze erneut zu umfangreichen Emotet-Spam-Wellen kommen wird, wie sie 2019 und 2020 häufig beobachtet werden konnten. Durch von Emotet nachgeladene weitere Schadsoftware könnte es wieder zu zahlreichen Kompromittierungen von Netzwerken von Behörden und Unternehmen kommen, bei denen von den Tätern nachfolgend Ransomware zur Verschlüsselung von Daten ausgerollt wird.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann in ähnlicher Art auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

Empfehlung an IT-Sicherheitsverantwortliche

Das BSI empfiehlt zu prüfen, ob die Schutzmaßnahmen vor Emotet [BSIb] (weiterhin oder erneut) umgesetzt werden können. Wie bereits unter [BSI2021] beschrieben wird entsprechender authentisch wirkender Spam nicht nur von Emotet versendet.

Derzeit dürfte insbesondere die Einschränkung von unsignierten Makros vor Emotet schützen.

Links

[BSIa] Informationen zur Schadsoftware Emotet

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Sonderfall-Emotet/sonderfall-emotet_node.html

[BSIb] Maßnahmen zum Schutz vor Emotet und gefährlichen E-Mails im Allgemeinen

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/Malware/Emotet/emotet_node.html

[BSI2021] Kompromittierte Exchange-Server - Zunahme von Angriffen per Mail

<https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-269486-1032.pdf>

[CYB2021] <https://cyber.wtf/2021/11/15/guess-whos-back/>

[SAN2021] Emotet Returns

<https://isc.sans.edu/diary/28044>

[TWI2021a] <https://twitter.com/Cryptolaemus1/status/1460403592658145283>

[TWI2021b] https://twitter.com/VK_Intel/status/1460308855129313281

[TWI2021c] <https://twitter.com/wesdrone/status/1460420794207682562>

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

- 1) Was ist das Traffic Light Protokoll?
Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
- 2) Welche Einstufungen existieren?
 - **TLP:WHITE: Unbegrenzte Weitergabe**
Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
 - **TLP:GREEN: Organisationsübergreifende Weitergabe**
Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
 - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
 - **TLP:RED: Persönlich, nur für benannte Empfänger**
Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
- 3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
- 4) Was passiert, wenn ich die Einstufung nicht beachte?
Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.