Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Neues Social Engineering bei Spam-Mails mit angeblichen Rechnungen

Word-Dokumente installieren Schadsoftware

CSW-Nr. 2017-182418-1213, Version 1.2, 05.10.2017

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Cyberkriminelle versenden derzeit erneut in großem Umfang Spam-Mails zur Verbreitung von Schadprogrammen. Dabei nutzen sie gezielt den Empfängern bekannte Absender von Mitarbeitern in der jeweiligen Organisation. Das BSI hat bereits zahlreiche Anfragen von Behörden und Unternehmen enthalten, bei denen entsprechende Mails eingegangen sind. In den Mails wird angegeben, dass sich im Anhang eine Rechnung befände. Tatsächlich enthalten die Mails stattdessen einen Link. Beim Aufruf des Links wird eine Word-Datei (.doc) heruntergeladen, welche schädliche Makros enthält. Wird die schädliche Word-Datei geöffnet und die Ausführung von Makros erlaubt, wird über die Makros automatisch Schadsoftware aus dem Internet nachgeladen und auf dem betroffenen System installiert.

Beispiel einer solchen Spam-Mail:

```
Von:     "Mustermann, Heinz /134"
An:      "Mueller, Michael /132"
Betreff: KCR-695 & 3458 Mueller, Michael /132
In der Anlage erhalten Sie Ihre dazugehörige Rechnung als DOC-Dokument.
http://somehost.tld/RCF-93921611.dokument/
Freundliche Grüße
```

* 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.

Mustermann, Heinz /134

Update 1:
Seit dem 26. Juni wird eine neue Welle mit derselben Masche beobachtet. Diese Kampagne lädt verschiedene Downloader und Malware nach, u.a. die Banking-Trojaner Emotet und Dridex.

Update 2:
Das BSI erhält seit Ende September zahlreiche Anfragen aus Behörden und Unternehmen zu neuen Spam-Mails mit Links auf angebliche Rechnungen. Diese werden mit den Empfängern bekannten Absender-Namen bzw. Absender-Adressen (innerhalb der Organisationseinheit oder extern) versendet. Hierbei handelt es sich um den gleichen Modus Operandi wie bereits bei den Spam-Kampagnen im Juni und der vergangenen Wochen. Mit diesem Update möchte das BSI daher erneut auf diesen Sachverhalt hinweisen und weitere Empfehlungen geben.

Bewertung

Die Spam-Mails werden mit gefälschten Absenderangaben über Server im Ausland versendet. Als vermeintlicher Absender wird meist ein existierender Mitarbeiter in derselben Organisation wie der Empfänger eingesetzt. Die Absender- und Empfängerangaben enthalten häufig konkrete Organisationsbezeichnungen. Die Angreifer versuchen dadurch die Authentizität der Mails vorzutäuschen und die Empfänger zum Öffnen der verlinkten Dateien zu verleiten.

Das BSI geht davon aus, dass die Absender- und Empfängerangaben inkl. Organisationsbezeichnungen auf infizierten Systemen von Nutzern ausgespäht wurden, an die in der Vergangenheit E-Mails von betroffenen Empfängern versendet wurden.

Bei der über die Word-Dokumente nachgeladenen Schadsoftware handelt es sich um eine Variante von "Emotet" bzw. "Geodo/Heodo", welche nach der Infektion des System weitere Schadsoftware wie Banking-Trojaner, Information-Stealer oder Spam-Bots nachlädt.

Update 2:
Auch bei den aktuellen Spam-Kampagnen werden die "Anzeigenamen" (Realname, Displayname) und Signaturen der vermeintlichen Absender gefälscht und zeigen üblicherweise eine dem Empfänger bekannte Person (ggf. inkl. Angabe einer Organisationseinheit). Tatsächlich versendet werden die Spam-Mails jedoch wieder über kompromittierte Mailkonten Dritter weltweit.
Die Beziehungen zwischen vermeintlichem Absender und Empfänger wurden zuvor aus Adressbüchern oder E-Mail-Konten auf infizierten Systemen von Nutzern ausgespäht (ggf. bereits vor mehreren Monaten oder Jahren). Hierbei muss nicht unbedingt ein System des vermeintlichen Absenders betroffen gewesen sein. In vielen Fällen wurden die Beziehungen auch E-Mails entnommen, welche an einen größeren Empfängerkreis gesendet wurden. Die Infektion des Systems eines einzelnen Empfängers war dann ausreichend, um Kontaktbeziehungen zwischen allen beteiligten Personen herzustellen und diese in zukünftigen Spam-Kampagnen zur Fälschung der Absenderangaben auszunutzen.

Empfehlung

Information und Sensibilisierung von Nutzern, auch bei vermeintlich bekannten Absendern keine Links in E-Mails anzuklicken und darüber heruntergeladenen Dateien zu öffnen.

Die nachgeladenen Schadprogramme werden häufig (in den ersten Stunden nach Verbreitung) nicht von AV-Software erkannt. Die Schadprogramme nehmen teilweise tiefgreifende Änderungen am infizierten System vor, die nicht einfach rückgängig gemacht werden können. Das BSI empfiehlt daher grundsätzlich, infizierte Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.

Auf betroffenen Systemen gespeicherte bzw. nach der Infektion eingegebene Zugangsdaten sollten als kompromittiert betrachtet und die Passwörter geändert werden.

Weiterhin empfiehlt das BSI die Umsetzung der in Kapitel 4 des Dokuments "Ransomware: Bedrohungslage, Prävention & Reaktion" [1] beschriebenen Präventionsmaßnahmen.

Update 1:
Für diese konkrete Kampagne stellt das BSI die folgenden technischen Signaturen zur Verfügung. Wie üblich werden diese auch über den MISP-Server des BSI für eine automatische Verarbeitung bereitgestellt. Es wird kein Anspruch auf Vollständigkeit erhoben.

Links in Emails (zum Schutz vor versehentlichem Anklicken durch hxxp geschützt):

[... veraltete Informationen entfernt ...]

Kontrollserver nachgeladener Emotet-Schadprogramme z.B.:

```
hxxp://192.210.199.181:8080/
hxxp://209.126.98.150:8080/
```

Update 2:
Für die erfolgreiche Infektion eines Systems muss der Empfänger zunächst das angebliche (Rechnungs-)Dokument herunterladen, dieses öffnen und anschließend die Ausführung von Makros bestätigen. Berichte der letzten Wochen zeigen, dass sich viele Nutzer jedoch offenbar von den gefälschten vermeintlich bekannten Absenderangaben zu diesem aufwändigen "Infektionsverfahren" verleiten lassen.

Das BSI empfiehlt IT-Sicherheitsbeauftragten daher erneute und regelmäßige Sensibilisierungsmaßnahmen für Nutzer in Behörden und Unternehmen.

Bei dieser Spam-Kampagne wird nur der "Anzeigename" (Realname, Displayname) des vermeintlichen Absenders gefälscht. Die eigentliche Absenderadresse zeigt jedoch das für den Spam-Versand jeweils missbrauchte E-Mail-Konto. Nutzer sollten sensibilisiert werden, insbesondere bei verdächtig erscheinenden E-Mails die Absenderadresse zu überprüfen. In der Übersicht des Posteingangs zeigen viele E-Mail-Clients nur den Anzeigenamen der Absender an. In der Detailansicht wird jedoch häufig auch die Absenderadresse angezeigt. Einige E-Mail-Clients zeigen den vollständigen Absender (Anzeigename und Adresse) auch beim Überfahren des Absenders in der Übersicht als Pop-Up an.

Beispiele in aktuellen Spam-Mails enthaltener Download-Links:

hxxp://tourdebali.com/Rechnungsnummer-66001/
hxxp://syntios.com/xxx_questprofile_20170920/Lastschrift/
hxxp://snowlightdesign.co.nz/Rechnung/
hxxp://rockyhill.com.au/Rechnung-Bestellung-47988341/
hxxp://procomservices.co.uk/gescanntes-Dokument/
hxxp://mediaattitude.com.au/Dokumente/
hxxp://detektor.com.pl/allegro/112302573-41600-Neuer-RV/
hxxp://capecourtesy.com/Ihre-Online-Rechnung-103287-vom-04.10.2017/
hxxp://audre.com/Rechnungs-Details/
hxxp://monkeybong.com.au/Rechnung-42403367673/
hxxp://longridgeclayshooting.co.uk/Rechnung-01717537996/
hxxp://kmdsales.com/Rechnung-41605926505/

Eine abschließende Auflistung ist nicht möglich, da eine sehr große Anzahl derartiger Download-Links existiert.

Kontrollserver für die in den letzten Spam-Kampagnen nachgeladenen Emotet-Schadprogramme:

5.9.167.178
5.45.108.249
51.255.58.18
74.50.52.130
74.208.155.175
108.59.253.38

Links

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html

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 Point of Contacts (SPOCs) welche das Dokument direkt vom BSI-Lagezentrum erhalten haben, können sich direkt an die bekannten Kontaktdaten des BSI-Lagezentrums 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 : Unbegrenzt**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP-GREEN: Organisationsübergreifende Verteilung**
     Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
   - **TLP-AMBER: Organisationsinterne Verteilung**
     Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig“. Der Informationsersteller muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
   - **TLP-RED: Persönlich, nur für benannte Empfänger**
     TLP-RED-Informationen sind auf den Kreis der Anwesenden in einer Besprechung, einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen 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.