Bundesamt für
Verfassungsschutz

Köln, 3. März 2016

BfV Cyber-Brief

Nr. 01/2016

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Referat 4D2/4D3
☎ 0221/792-3322

Mögliche bevorstehende Angriffe der Angriffskampagne Sofacy/APT 28 auf Unternehmen der Energiebranche

Die Angriffskampagne Sofacy/APT 28[1] ist seit spätestens 2007 aktiv und stellt derzeit wohl eine der aktivsten und aggressivsten Kampagnen im virtuellen Raum dar. Führende IT-Sicherheitsunternehmen gehen bei Sofacy/APT 28 von einer Steuerung durch staatliche Stellen in Russland aus.

Seit Ausbruch des Konfliktes in der Ostukraine konnte eine deutliche Intensivierung der Aktivitäten der Angreifergruppierung beobachtet werden. Das Bundesamt für Verfassungsschutz (BfV) stellte in der Vergangenheit wiederholt Angriffe gegen deutsche Stellen durch Sofacy/APT 28 fest.

Sachverhalt

Aktuell gibt es Hinweise auf Vorbereitungshandlungen der Kampagne für Angriffe auf Ziele in der Energiebranche. Es lässt sich jedoch nicht eingrenzen, welche Unternehmen konkret im Fokus von Sofacy/APT 28 stehen könnten.

Dem BfV ist bislang noch kein Fall eines Angriffes auf deutsche Unternehmen der Energiebranche durch Sofacy/APT 28 bekannt. Laut einer Analyse des IT-Sicherheitsunternehmens Trend Micro zur Opferfläche der Kampagne in den USA im Jahr 2015 sind jedoch ca. 3% der Ziele von Sofacy/APT 28 im Energiesektor angesiedelt. Eine Betroffenheit deutscher Energieunternehmen ist daher nicht auszuschließen.

Aus eigenen Quellen wurde ferner bekannt, dass einige deutsche Forschungsinstitutionen und Unternehmen, vor allem aus dem Bereich Lasertechnologie und Optik, ebenfalls von Sofacy/APT 28 betroffen waren. Eine entsprechende Mitteilung und Sensibilisierung der bekannten Opfer erfolgt. Auch hier kann eine weiter reichende Betroffenheit allerdings nicht ausgeschlossen werden.

Handlungsempfehlung

Um festzustellen, ob Ihr Unternehmen von dieser Angriffskampagne betroffen ist, empfehlen wir eine Durchsicht der Netzwerk-Logs nach den in der Anlage aufgeführten Netzwerk-IOC.[2] Zur Angriffskampagne Sofacy/APT 28 existieren zahlreiche öffentliche Reports von IT-Sicherheitsunternehmen. Zudem wurde bereits eine große Anzahl von IOC zu dieser Angriffskampagne veröffentlicht. Das BfV hat sich deshalb bei der Auswahl auf die aktuellsten Indicators zu Sofacy/APT 28 beschränkt.

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr der Infizierung Ihrer Rechner. In diesem Fall können wir Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221-792-3322 oder

E-Mail: sensea@bfv.bund.de

Wir sichern Ihnen absolute Vertraulichkeit zu!

1. APT steht für „Advanced Persistent Threat“ (etwa „fortgeschrittene, andauernde Bedrohung“) und bezeichnet einen komplexen, zielgerichteten und effektiven Angriff auf IT-Strukturen durch einen gut ausgebildeten und ressourcenstarken Angreifer.
   Die Nummerierung der jeweiligen APTs wird von demjenigen IT-Sicherheitsunternehmen vorgenommen, das den Angriff als erstes zuordnet und beschreibt. Im Falle von Sofacy / APT 28 war dies das US-amerikanische Unternehmen FireEye.
   Sofacy / APT 28 ist auch unter den Bezeichnungen Operation Pawn Storm, Sednit, Tsar Team und Fancy Bear bekannt.
2. Indicators of Compromise

Anlage

uzbekistan-mfa.com
luminate-yahoo.com
cc-yahoo-inc.org
opecmember.com
cdncloudflare.com
45645647.com
57567547454.com
ciscohelpcenter.com
intelsupportcenter.com
intelsupportcenter.net
highcomission.org
autoupdater.org
securityupdatereport.com
mozilla-plugins.com
mozillaplagins.com
wincodec.com
securitysls.com
windowsdefenderupdater.com
windowschecker.net
terms-google.com
syslowwindows.com
kenlynton.com
fastcontech.com
mslinux-update.com
web-privacy-guardian.com
smtprelayhost.com
645547657668787.com
android-soft.net
live-settings.com
privatenewstoday.com
servicetransferemail.com
adawareblock.com