Bundesamt für Verfassungsschutz

Köln, 8. August 2016

BfV Cyber-Brief

Nr. 03/2016

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Referat 4D2/4D3
☎ 0221/792-2600

Angreifer attackieren deutsche Unternehmen

Das BfV erhielt in den letzten Monaten vermehrt konkrete Hinweise auf Aktivitäten von Angreifern, die verschiedene deutsche Unternehmen und Betriebe attackiert haben sollen. Gemäß den hier vorliegenden Erkenntnissen liegt eine Verbindung zu einer Gruppierung nahe, die durch einen IT-Sicherheitsdienstleister unter den Namen Cadelle und Chafer bearbeitet wird. Dort wird der Gruppierung ein staatlicher iranischer Hintergrund zugeschrieben.[1]

Hintergrund

Die genannten Angreifergruppierungen sollen Einzelpersonen im Iran attackieren.[2] Im Mittleren Osten sollen sowohl Fluglinien wie auch Telekommunikationsanbieter ins Visier geraten sein. Ebenso werden weitere internationale Ziele als identifizierte Betroffene genannt, die z.B. in den Vereinigten Staaten und Pakistan, aber auch in Deutschland und UK zu verorten sind.

Für eine Verbindung zwischen den Angreifern Cadelle und Chafer spricht, dass eine ähnliche Opferauswahl getroffen, ein beinahe gleichzeitiger Aktionszeitraum detektiert sowie dass regelmäßig bei Betroffenen nur die aktive Infektion durch jeweils eine der beiden Angreifergruppen festgestellt wurde.

Die Infektion durch die als Chafer benannte Angreifergruppe soll unter anderem durch die Ausnutzung von Schwachstellen von Webservern erfolgt sein, z.B. durch SQL Injection.[3]

Sachverhalt

Das BfV bearbeitet aktuell und analysierte bereits in der Vergangenheit verschiedene Vorfälle, die mögliche Verbindungen zu den beschriebenen Angreifergruppen aufweisen.

Parallelen liegen hier vor allem in der von den Angreifern verwendeten Infrastruktur, der vorgefundenen Malware sowie der potentiellen Opferauswahl. Ebenso passen die konkret festzustellenden Aktivitäten der Angreifer in die von Symantec beschriebenen Zeitmuster (UTC +4,5), auch unter Einbeziehung des iranischen Wochenendes (Donnerstag und Freitag).

Darüber hinaus erhärtete sich bei einigen vom BfV untersuchten Fällen die Vermutung, dass im Vorfeld zu der genannten Attacke gezielte Spear-Phishing[4] Angriffe erfolgt sind, um z.B. Zugangsdaten zu geschützten Zugängen (z.B. Citrix Gateway) der Opfersysteme zu erlangen. In den folgenden Schritten versuchte der Angreifer Zugriff auf Informationen zu erhalten, die ihm den Zugang zu weiteren zugangsgeschützten Bereichen ermöglichten, wie. z.B. Dateien, in denen Nutzerkonten und Passwörter zentral abgespeichert waren.

1 Vgl. Symantec “Iran-based attackers use back door threats to spy on Middle Eastern targets” auf https://www.symantec.com/connect/blog/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets

2 Neben Zielen, die direkt iranischen Netzbereichen zugeordnet werden können, sollen weitere Ziele Proxys zuzuordnen sein. Proxys können z.B. von Internetnutzern verwendet werden, die einer direkten Identifizierung Ihrer Datenkommunikation entgehen möchten. (z.B. durch die Nutzung des TOR-Netzwerks). Dissidenten und Oppositionelle benutzten häufig solche Hilfsmittel, um Repressionen zu entgehen und sich der staatlichen Kontrolle und Regulierung zu entziehen.

3 Mittels spezieller Benutzereingaben auf Webseiten wird versucht, Zugriff auf den Inhalt von Datenbanken auf dem Webserver zu erlangen. SQL ist die Abkürzung für „Standard Query Language“ und bezeichnet eine standardisierte Abfragesprache für Datenbanken.

4 Spear-Phishing ist eine Spezialform des Phishing-Angriffs, bei dem nicht breitflächig, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträger auf Leitungsebene) attackiert wird. Voraussetzung für einen erfolgreichen Angriff ist eine gute Vorbereitung und die Einbettung des Angriffs in einen für das Opfer glaubwürdigen Kontext.

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. Für eine künftige Sicherung empfehlen wir eine Aufnahme als Regel in die Firewall Ihrer zentralen Netzübergangsstelle zum Internet oder einer vergleichbaren Stelle, die sich für die Überwachung des ein- und ausgehenden Datenverkehres zu Ihrem Netzwerk eignet.

Weiterhin bilden Webserver einen weiteren häufig genutzten Schwachpunkt für die Angreifer. Neben der sorgfältigen Administration von bestehenden Webservern sollten speziell nicht zentrale Webanwendungen, die keine direkte Funktion für Ihr Unternehmen abbilden, im Rahmen Ihrer Risikoabwägung berücksichtigt und ggf. entsprechend aus Ihrem Netz separiert werden.[5]

Sollten Sie 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.: 0221-792-2600 oder

E-Mail: poststelle@bfv.bund.de

Referat 4D3

Wir sichern Ihnen absolute Vertraulichkeit zu!

Anlage[6]

84.241.63.17

87.117.204.143

83.142.230.138

66.69.149.32

5.39.44.16

83.142.230.11

83.142.230.113

5.39.44.17

5.39.119.17

83.142.230.139

5 Gemeint sind hier z.B. Webauftritte von Mitarbeitern, Betriebssportgemeinschaften etc., die aber häufig unabhängig von der Unternehmens-IT im Firmennetzwerk gehosted und verwaltet werden. Dadurch entstehen unter Umständen erhebliche Sicherheitsrisiken, wenn diese nicht effektiv vom Firmennetzwerk getrennt sind und von einem potentiellen Angreifer als Sprungbrett oder Türöffner missbraucht werden können.

6 Die genannten IOC beschränken sich auf Rückmeldeinfrastruktur, die tatsächlich gegen dem BfV bekannte Betroffene eingesetzt worden ist und identifiziert werden konnte. Grundsätzlich sind weiterführende IOC ebenfalls im Symantec Bericht „Backdoor.Cadelspy and Backdoor.Remexi indicators of compromise“ unter https://www.symantec.com/content/en/us/enterprise/media/security_response/docs/Cadelspy-Remixi-IOC.pdf erhältlich.