Bundesamt für Verfassungsschutz

Köln, 18. Januar 2021

BfV Cyber-Brief

Nr. 01/2021

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Cyberabwehr
☎ 0221/792-2600

Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung APT31

Dem Bundesamt für Verfassungsschutz liegen Erkenntnisse vor, dass deutsche öffentliche Stellen im Fokus von Cyberangriffen der Gruppierung APT31 stehen könnten. Ziel dieser Warnmeldung ist es, deutsche Stellen zu sensibilisieren und mit den notwendigen technischen Informationen zu versehen, um eine mögliche Infektion detektieren zu können.

Sachverhalt

Cyberangriffe der Gruppierung APT31 richten sich derzeit gegen politische Ziele in westlichen Ländern. Hierunter fallen beispielsweise Ministerien und Behörden, politische Organisationen und Stiftungen.

Entsprechende Ziele werden im Vorfeld der Angriffe durch den Akteur mit technischen Mitteln aufgeklärt. Dem Bundesamt für Verfassungsschutz liegen Erkenntnisse vor, dass auch deutsche Stellen Ziel von Aufklärungsaktivitäten und Angriffsvorbereitungshandlungen sind. Angriffe auf deutsche Ziele sind daher zu befürchten.

Zum Schutz deutscher Stellen werden mit dieser Warnmeldung technische Indikatoren (Indicators of Compromise / IOCs) zur Verfügung gestellt, durch die Angriffsvorbereitungshandlungen und mögliche Infektionen festgestellt werden können.

Vorgehensweise von APT31

Im Mittelpunkt der Aktivitäten von APT31 stehen derzeit vor allem Aufklärungsaktivitäten und Angriffsvorbereitungshandlungen. Zu diesen zählen der Versand von Tracking-E-Mails[1] an mögliche Ziele und Scanning-Aktivitäten gegen Netzwerkinfrastruktur:

- Tracking-E-Mails erwecken einen legitimen Eindruck, indem sie dem Adressaten bekannte Kontakte imitieren und/oder für den Adressat relevante Themen adressieren. Die E-Mails enthalten – wie aus der Werbeindustrie oder für Webseitenoptimierung bekannt – Zähl-Pixel oder –Links, die technische Informationen über das Zielsystem sammeln.

- Scanning-Aktivitäten zielen insbesondere auf die aus dem Internet erreichbaren Dienste und Infrastrukturbestandteile einer Zielorganisation ab. Hierunter zu verstehen ist insbesondere das klassische Port- bzw. Schwachstellen-Scanning. Im Fokus stehen die standardisierten Ports (0 - 1023, auch bekannt als *well known ports*). Neben diversen Standard-Ports für die Webnutzung und Dateiübertragung sind möglicherweise auch Ports von Diensten betroffen, die Fernzugriff ermöglichen.

Im Falle von nachfolgenden Angriffshandlungen wurde in der Vergangenheit unter anderem von Spear-Phishing (Credential-Phishing oder E-Mails mit maliziösen Anhängen) berichtet. Als relevanter erscheint nach derzeitigen Erkenntnissen jedoch die Verwendung von öffentlichen Exploits für aus dem Internet erreichbare Dienste (z.B. Web- und/oder E-Mail-Server) sowie Brute-Force[2]- und Password-Spray-Angriffe[3]. Mitunter kommt es auch zur Nutzung von SQL-Injections[4], XSS[5] und anderen Webtechniken. Möglicherweise werden im weiteren Verlauf der Kompromittierung Webshells eingesetzt.

Aus der Vergangenheit ist bekannt, dass akteur-spezifische Malware (z.B. Dropcat) und frei verfügbare Tools (z.B. Mimikatz) nach Bedarf eingesetzt wurden. Möglicherweise werden auch bekannte Pen-Test-Frameworks eingesetzt.

C2-Verkehr, das Nachladen von Malware sowie eine Datenexfiltration erfolgen möglicherweise über HTTP/HTTPS, GET und POST. Neben dedizierten C2-Servern[6] des Akteurs werden unauffällige Internet-Dienste zur Kommunikation mit installierter Schadsoftware oder zur Ausleitung von Daten genutzt (z.B. GitHub, Pastebin, Dropbox, div. andere Google-Dienste). Es empfiehlt sich, hier insbesondere die Zeiten der Kommunikation und Größenordnungen der übertragenen Daten zu betrachten.

Dedizierte Server für Vorbereitungs- und Angriffsaktivitäten werden in engen zeitlichen Abständen gewechselt. In Kombination mit der breiten Malwarenutzung ist eine Bereitstellung konkreter und tagesaktueller IOCs daher schwierig.

---

1 Tracking-E-Mails enthalten sog. Tracking-Pixel und haben einen grundsätzlich legitimen Einsatzzweck (bspw. im Online-Marketing), um zu verifizieren, ob eine E-Mail-Adresse tatsächlich vergeben ist und ob der Empfänger die Mail öffnet. Cyberangreifergruppierungen können dadurch allerdings auch weitere Informationen abgreifen, beispielsweise welche IP-Adresse der Empfänger nutzt. Durch eine Tracking-E-Mail/-Pixel erfolgt keine Infektion.

2 Bei einem Brute-Force-Angriff wird durch wahlloses und meist automatisiertes Ausprobieren von Zeichenkombinationen versucht, Passwörter oder Schlüssel herauszufinden.

3 Password-Spraying ist ein Angriff, bei dem versucht wird, mit häufig verwendeten oder Standardpasswörtern auf eine große Anzahl von unterschiedlichen Konten (bspw. E-Mail) zugreifen zu können.

4 SQL-Injection beschreibt das Einschleusen von Datenbankbefehlen durch eine Nutzereingabe bspw. auf einer Webseite. Durch SQL-Injection können sensible Daten verändert oder ausgespäht und ggf. die Webseite kompromittiert werden.

5 XSS, auch Cross-Site-Scripting beschreibt eine Methode zur Einschleusung von schädlichem Code in eine Webanwendung. Durch XSS können sensible Daten ausgespäht und ggf. Benutzerkonten übernommen werden.

6 Ein C2 (auch Command & Control) ist ein vom Angreifer kontrollierter Server zur Steuerung von Befehlen an ein mit Malware infiziertes System. Er dient außerdem zum Empfang von Daten und Kommunikation aus dem infizierten Opfersystem.

Handlungsempfehlung

Grundsätzliche Risikoabwägung und Prävention

Zwecks Erreichung eines angemessenen IT-Sicherheitsniveaus wird grundsätzlich eine Orientierung an öffentlich verfügbaren Standards empfohlen, etwa den Richtlinien des BSI-Grundschutzes oder den praxisbewährten CIS Controls des Centers for Internet Security.

Detektion

Es wird empfohlen, die eigenen Systeme mit den zur Verfügung gestellten IOCs zu prüfen. Insbesondere sollte in Logdateien und aktiven Netzwerkverbindungen nach Verbindungen zu den im Bereich IOCs genannten externen Systemen gesucht werden. Da die bereitgestellten IOCs durch den Akteur in engen zeitlichen Abständen gewechselt werden, sollten außerdem historische Netzwerk-Logs (zumindest die der letzten 9 Monate) geprüft werden, um bereits in der Vergangenheit erfolgte Infektionen feststellen zu können. IOCs, die sich zu anderen als den genannten Zeitpunkten maliziöser Nutzung (siehe Spalte Monat in nachfolgender Tabelle) in Logs wiederfinden, können für eine legitime Nutzung sprechen, die zugehörigen Verbindungen sollten aber dennoch eingehend geprüft werden.

Reaktion

Bei Hinweisen auf eine Infektion bzw. verdächtiges Systemverhalten sollten die erprobten Pläne für Incident Response ausgeführt werden, um das Ausmaß einer etwaigen Kompromittierung zu erfassen, einzudämmen und effektiv begegnen zu können.

Darüber hinaus bieten wir Ihnen zusätzliche Hintergrundinformationen an. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221-792-2600 oder

E-Mail: poststelle@bfv.bund.de

Cyberabwehr BfV

Indicators of Compromise

Indikator	Verwendung im Monat
31.214.157.113	10.2020
185.158.248.160	10.2020
185.189.149.208	10.2020
185.189.149.219	10.2020
45.156.23.115	10.2020
45.156.23.129	10.2020
185.189.149.141	09.2020
45.156.24.29	09.2020
23.111.204.33	08.2020
23.111.204.172	07.2020
138.197.206.214	07.2020
139.162.96.8	07.2020
23.81.225.79	07.2020
104.156.253.199	07.2020
104.207.150.231	07.2020
153.122.102.229	07.2020
141.164.62.103	07.2020
161.35.232.33	07.2020
23.81.225.78	07.2020
3.113.5.175	07.2020
64.225.33.133	07.2020
170.130.55.138	07.2020
41.251.84.81	07.2020
45.11.180.122	07.2020
2.124.196.235	06.2020
41.141.191.244	06.2020
41.250.135.152	06.2020
88.107.233.211	06.2020
160.178.109.226	06.2020
160.178.113.149	06.2020
196.206.181.146	06.2020
196.217.199.166	06.2020
105.154.12.165	06.2020
105.157.234.0	06.2020
105.159.122.85	06.2020
106.71.42.57	06.2020
110.175.224.15	06.2020
160.178.122.34	06.2020
160.179.31.245	06.2020
176.24.161.84	06.2020
196.64.185.13	06.2020
203.40.118.87	06.2020
209.93.143.115	06.2020
220.233.172.57	06.2020

41.141.68.24	06.2020
41.251.47.226	06.2020
41.251.49.41	06.2020
45.11.180.118	06.2020
45.11.180.119	06.2020
49.188.79.238	06.2020
79.72.8.33	06.2020
80.7.131.64	06.2020
82.32.111.169	06.2020
90.240.80.66	06.2020
90.254.98.120	06.2020
92.11.152.71	06.2020
92.13.77.81	06.2020
92.15.52.33	06.2020
185.158.250.231	06.2020
185.158.250.236	06.2020
41.251.68.5	06.2020
185.219.226.42	06.2020
194.76.226.100	06.2020
185.120.144.167	05.2020
185.158.248.167	05.2020
185.158.248.169	05.2020
108.61.126.255	05.2020
176.10.118.162	05.2020
173.232.146.144	05.2020
173.232.146.155	05.2020
173.21.181.37	05.2020
194.76.224.133	05.2020
47.39.69.128	05.2020
50.91.182.189	05.2020
73.53.7.208	05.2020
75.64.125.253	05.2020
75.74.38.242	05.2020
54.64.124.36	04.2020
60.249.95.79	04.2020