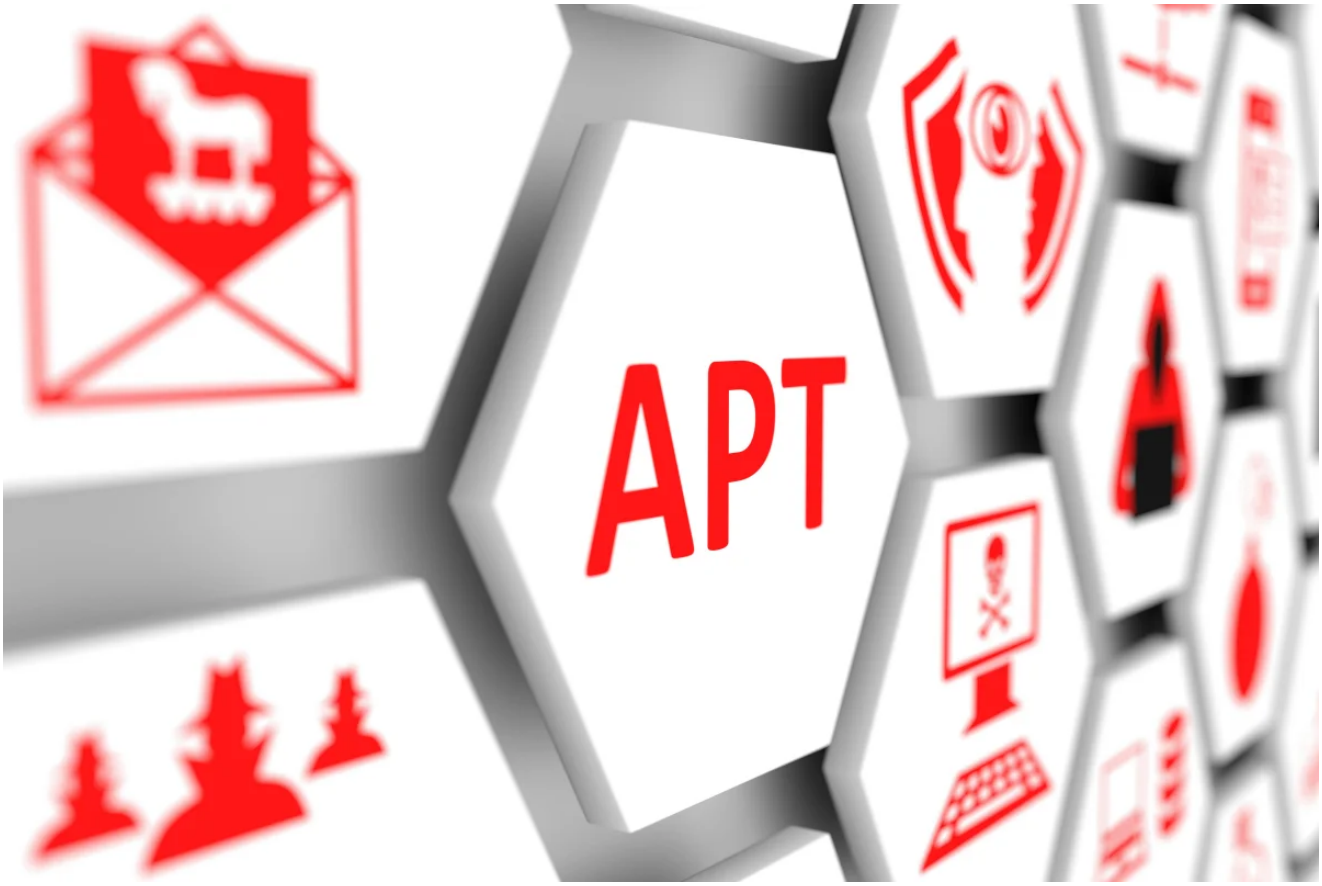
Auf Tätersuche: Herausforderungen bei der Analyse von Cyber-Angriffen

heise.de/hintergrund/Auf-Taetersuche-Herausforderungen-bei-der-Analyse-von-Cyber-Angriffen-5043620.html

Timo Steffens



Das Bedürfnis bei Cyber-Angriffen Täter zu benennen wächst. Doch die verantwortlichen Gruppen spezialisieren sich immer mehr und kooperieren bei Bedarf.

Lesezeit: 14 Min.

In Pocket speichern
vorlesen Druckansicht Kommentare lesen 18 Beiträge

(Bild: Profit_Image/Shutterstock.com)

08.02.2021 15:11 Uhr
Security

Von
Timo Steffens

Inhaltsverzeichnis

Auf einer Seite lesen

Ein Artikel von Timo Steffens

Dr. Timo Steffens im BSI für Threat Intelligence zuständig und beschäftigt sich insbesondere mit der Detektion und Abwehr von gezielten Spionage-Angriffen. Er ist unter anderem Autor des Buchs "Attribution of Advanced Persistent Threats" und twittert privat als

@Timo_Steffens.

Eine der ersten Fragen bei Cyber-Angriffen ist häufig die nach den Tätern. So auch im Fall des SolarWinds-Hacks, bei dem der Update-Mechanismus einer weltweit genutzten Software genutzt wurde, um Hintertüren in bis zu 18.000 Behörden und Unternehmen zu installieren. Die Sicherheitsfirma FireEye, die als erste einen technischen Bericht dazu vorlegte, verwandte erhebliche Mühe darauf herauszufinden, ob der Angriff von einer bereits bekannten Gruppe durchgeführt wurde – bisher ohne eindeutige Ergebnisse. Doch warum ist das überhaupt relevant?

Es geht dabei keineswegs nur darum, Täter vor Gericht zu bringen oder zumindest mit dem Finger auf einen Schuldigen zeigen zu können. Man kann von der Täterschaft einer bestimmten bekannten Gruppe beispielsweise sinnvolle Maßnahmen zum Schutz oder der Schadensminimierung ableiten. Zumindest wenn bereits ausreichend Informationen über deren bisherige Vorgehensweisen und Absichten vorliegen.

Lesen Sie dazu auch bei c't

Hacker-Jagd im Cyberspace

Grundlagen und Grenzen der Suche nach den Tätern

Wenn beispielsweise – wie von den Analysten der Firma Kaspersky vermutet – tatsächlich die Gruppe Snake hinter den SolarWinds-Angriffen steckt, ist die Wahrscheinlichkeit hoch, dass sie die Hintertüren vor allem bei Regierungsbehörden und Rüstungsfirmen einsetzen würden. Wäre es aber die Gruppe APT41, müsste man eher mit Folge-Angriffen auf Chemie- und Hightech-Unternehmen rechnen. Und wenn es sich – rein hypothetisch - gar um die

Gruppe Sandworm handeln sollte, dann weiß man, dass sie laut US-Behörden mit Cyber-Angriffen bereits Stromausfälle in der Ukraine ausgelöst haben. Somit wären sogar Sabotage-Akte über die SolarWinds-Hintertür nicht auszuschließen.

Das Beispiel macht klar, dass die Zuweisung eines Angriffs zu einer bekannten Gruppe Kontext liefert, der für das weitere Vorgehen wichtig ist. Schließlich kann man auch bei der IT-Security nicht alle möglichen Maßnahmen bis ins letzte Detail umsetzen sondern muss Prioritäten setzen. Das gilt umso mehr für die akute Incident Repsonse, die ohne Kontextinformationen viele unnötige Ressourcen binden kann.

Gruppenbildung bei der APT-Analyse

Doch wie werden solche Tätergruppen überhaupt gefunden und definiert? Sicherheitsfirmen und Regierungsbehörden durchlaufen dafür kontinuierlich einen Attributionsprozess. In einem ersten Schritt sammelt man Daten zu möglichst vielen Cyber-Angriffen. Diese werden dann anhand von technischen Ähnlichkeiten zu Clustern zusammengefasst. Ähnlich sind Angriffe, wenn sie zum Beispiel dieselbe Schadsoftware oder dieselben Kontrollserver nutzen, die Täter dieselben Angriffsmethoden verwenden oder Firmen aus derselben Branche betroffen sind. Je mehr Aspekte der Angriffe identisch sind, desto eindeutiger ist der Cluster.

Eine entscheidende Annahme ist dabei, dass hinter ähnlichen Angriffen dieselben Täter stecken. Selbst professionelle Angreifer nutzen nämlich gern immer wieder dieselben Ressourcen und Methoden. Deswegen hat es sich eingebürgert, die Cluster von ähnlichen Angriffen als APT-Gruppen zu bezeichnen. APT steht für Advanced Persistent Threat und beschreibt die insbesondere von Geheimdiensten praktizierte Vorgehensweise systematischer, gezielter Angriffe. Je nach Sicherheitsfirma werden diese Gruppen dann durchnummeriert (von APT1 bis APT42) oder es werden fantasievolle Namen vergeben, wie eben Snake oder Sandworm.

Gerade im Regierungsumfeld wechselt übrigens nach diesem Analyseschritt typischerweise die Zuständigkeit. In Deutschland übernehmen Ermittlungs- und Sicherheitsbehörden wie der Verfassungsschutz vom BSI und führen die Analysen weiter. Denn der Verfassungsschutz hat das Mandat, konkrete Täter wie Regierungen und Personen zu benennen; das BSI nicht. Bei Sicherheitsunternehmen gibt es in der Regel keine unterschiedlichen Zuständigkeiten für die einzelnen Prozessschritte.

Auch chinesische Analysten betreiben Attribution und kommen zu ähnlichen Herkunftsangaben wie ihre Kollegen.

(Bild: Qi-Anxin)

Für eine Attribution nimmt man die nach einem Angriff vorgefundenen Spuren und sucht nach Übereinstimmungen mit den Daten der bekannten Cluster. Unter anderem werden Schadprogramme, Kontrollserver und das Cui Bono untersucht. Eine der typischen Untersuchungsmethoden ist beispielsweise das Suchen nach Spracheinstellungen in Schadprogrammen. Wenn Schadprogramme kompiliert werden, erzeugt der Compiler automatisch Platzhalter für grafische Elemente wie Buttons und Fenster – selbst wenn das Schadprogramm gar keine grafische Oberfläche hat. Diese Platzhalter spezifizieren auch eine Codepage, also eine Angabe darüber, welche Sprache die GUI-Elemente benutzen. Per Default wird dabei die Codepage gesetzt, die der eingestellten Sprache des Betriebssystems entspricht.

In Schadprogrammen der Gruppe Snake wurde beispielsweise die Codepage für kyrillische Zeichen gefunden. Erhalten die Analysten Zugriff auf einen Kontrollserver, finden sich dort mit etwas Glück Quellcodes, Anleitungen oder sogar Opferlisten, die die Täter dort abgelegt haben. Das sind Indizien, denen typischerweise mehr Gewicht beigemessen wird, da sie direkt aus dem virtuellen Schaltzentrale der Angreifer stammen, wo sie vermutlich weniger auf der Hut sind als bei einem Streifzug durchs Feindesland. Auf Kontrollservern der Gruppe APT1 fanden sich etwa grafische Benutzeroberflächen mit chinesischen Schriftzeichen.

Das Cui Bono ist die Frage, wer Interesse an den identifizierten Opfern hat. Das Bundesamt für Verfassungsschutz weist beispielsweise in seinen Jahresberichten darauf hin, dass chinesische APT-Gruppen regelmäßig religiöse und ethnische Minderheiten in China

angreifen.

Dies sind nur Beispiele für die Analyse-Methoden. Inzwischen verfügen Analysten über einen ganzen Katalog an Spuren, auf die man prüfen kann, um Rückschlüsse auf die Täter und deren Ursprungsland zu ziehen. Je mehr Spuren gefunden werden, und je konsistenter sie sind, desto stärker wird die Attributionshypothese. Dies führt dann zu einer standardisierten Klassifizierung wie "eher wahrscheinlich" oder "sehr wahrscheinlich", die die Belastbarkeit der Ergebnisse quantifiziert. Ein Ergebnis des Attributionsprozesses kann durchaus auch sein, dass man keine belastbaren Hinweise auf die Täter finden konnte.