swisscom

Der gezielte Angriff
Cyber Security Report 2019

Swisscom (Schweiz) AG
Group Security
Alte Tiefenaustrasse 6
3048 Worblaufen
www.swisscom.ch

Inhalt

Einleitung

Der Cyber Security Report von Swisscom 2019 liegt vor. Abgeleitet aus der Bedrohungslage, die wir auch dieses Jahr wieder aktualisiert haben, betrachten wir ein Thema detailliert, das die Security-Community innerhalb Swisscom, bei unseren Partnern und Kunden, aber auch international aktuell, besonders beschäftigt: APTs.

Advanced Persistent Threats (APTs) zeichnen sich dadurch aus, dass Angreifer mit sehr vielen Ressourcen ein klar definiertes Ziel angreifen, um spezifische Informationen zu erhalten oder nachhaltig Schaden anzurichten. Um die Relevanz dieser Bedrohung besser einordnen zu können, setzen wir sie in den Kontext anderer Bedrohungen, wie Kriminelle, Terroristen und Hacktivisten. Was macht APTs nun so besonders?

Während Kriminelle den Weg des geringsten Widerstands gehen, um möglichst viel Gewinn zu erzielen, zu Terroristen und Hacktivisten, die beide einerseits Angriffe für Publicity nutzen, andererseits über relativ wenig Ressourcen und Know-how verfügen, gehen APTs deutlich subtiler vor. Das Ziel wird über Monate oder Jahre sorgfältig ausgewählt und beobachtet. Schier grenzenlose Ressourcen werden freigegeben, um Know-how aufzubauen und geeignete Werkzeuge zu entwickeln. Während und nach dem Angriff wird auf grösste Geheimhaltung wertgelegt, damit weder Angreifer noch Ziel zu früh bekannt werden.

Der Report beschreibt die Motivation und Mittel der Angreifer. Er zeigt basierend auf von Swisscom gesammelten und ausgewerteten Daten, welche Methoden und Werkzeuge Angreifer am häufigsten verwenden. Und zeigt auch auf, welche Gegenmassnahmen besonders effektiv sind, um einen Angriff bestmöglich erkennen zu können.

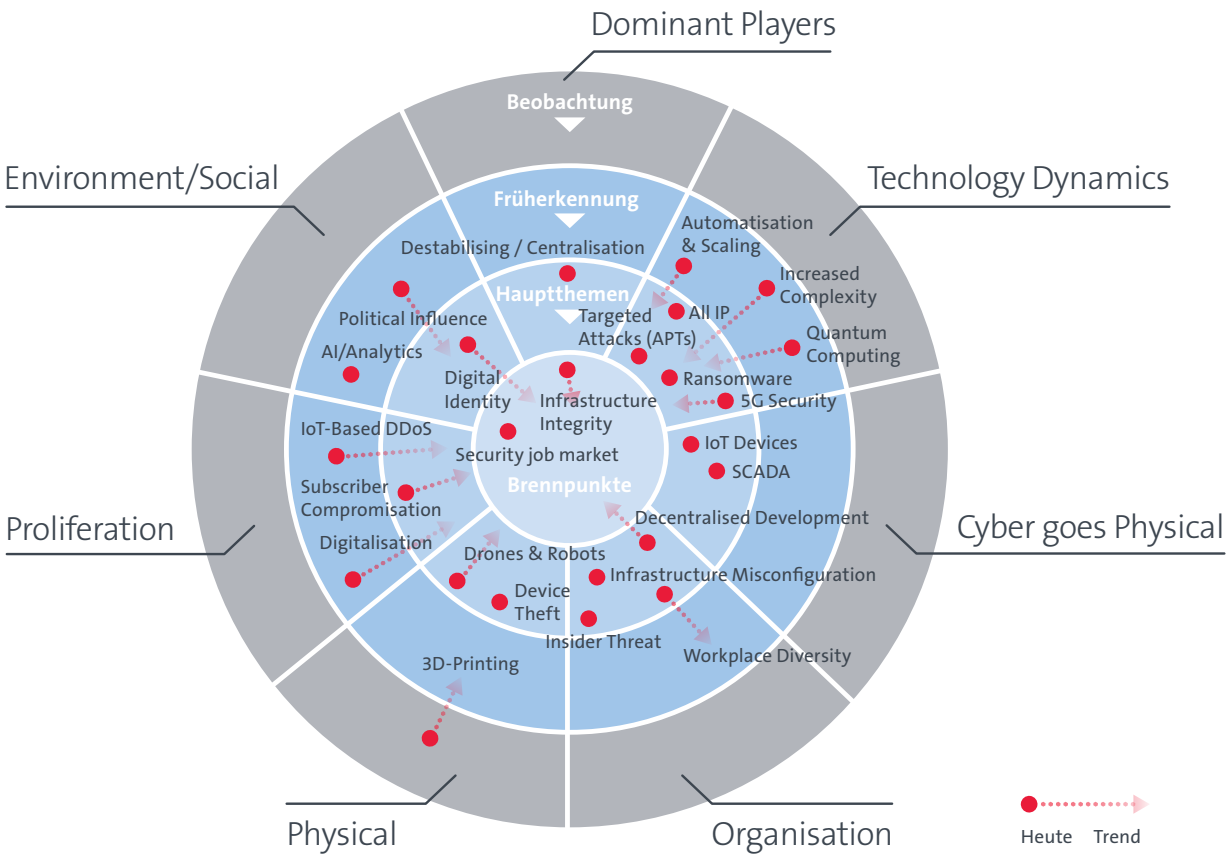
Über den Einstieg in das Thema freuen wir uns besonders. Wir konnten Costin Raiu von Kaspersky GReAT für ein Interview gewinnen. Costin ist ein weltweit anerkannter Experte auf dem Gebiet, der seine Erkenntnisse gerne mit uns teilt.

Dieser Report ist als Gemeinschaftsarbeit mehrerer Abteilungen innerhalb von Swisscom erstellt worden.

Lagebild – Bedrohungsradar

Der Ursprung von Bedrohungen findet sich in der stetigen Entwicklung neuer Technologien, deren Anwendung und Verbreitung in der Gesellschaft.

Potenzielle Bedrohungen müssen frühzeitig erkannt und systematisch erfasst werden. Um die Bedrohungslage und deren Evolution abzubilden, verwenden wir den bekannten Radar, auf den wir auch schon in früheren Publikationen des Cyber Security Reports von Swisscom verwiesen haben.



Bedrohungsradar

Methodik

Der Bedrohungsradar ist in sieben Segmente unterteilt, die die unterschiedlichen Domänen der Bedrohungen voneinander abgrenzen. In jedem Segment können die dazugehörenden Bedrohungen in einem von vier konzentrischen Kreisen zugeordnet werden. Die Kreise zeigen die Aktualität der Bedrohung an und damit auch die Unschärfe, die in der Beurteilung der Bedrohung liegt. Je näher zum Kreismittelpunkt die Bedrohung verortet ist, desto konkreter ist sie und umso wichtiger sind angemessene Gegenmassnahmen.

Die Kreise kennzeichnen wir als

- **Brennpunkte** für Bedrohungen, die bereits real sind und mit relativ grossem Einsatz von Ressourcen bewältigt werden.
- **Hauptthemen** für Bedrohungen, die bereits vereinzelt eingetreten sind und mit normalem Ressourcen-Einsatz bewältigt werden. Oft bestehen geregelte Prozesse, um derartigen Bedrohungen effizient zu begegnen.
- **Früherkennung** für Bedrohungen, die noch nicht eingetreten sind oder aktuell nur sehr wenig Wirkung zeigen. Es wurden Projekte gestartet, um der zukünftig wachsenden Bedeutung dieser Bedrohungen frühzeitig begegnen zu können.
- **Beobachtung** für Bedrohungen, die erst in einigen Jahren eintreten werden. Es gibt keine konkreten Massnahmen für den Umgang mit diesen Bedrohungen.

Weiter weisen die einzelnen, durch benannte Punkte gekennzeichneten Bedrohungen, einen Trend auf. Dieser kann in seiner Kritikalität zunehmend, rückläufig oder stabil sein. Die Länge des Trend-Strahls zeigt die erwartete Schnelligkeit auf, mit der sich die Kritikalität der Bedrohung ändern wird.

Bedrohungen

Im Folgenden werden die sieben Segmente des Bedrohungsradars kurz umschrieben.

Dominant Players

In diesem Segment werden Bedrohungen subsummiert, die von Abhängigkeiten von dominanten Herstellern, Diensten oder Protokollen ausgehen.

Brennpunkte	*Infrastructure Integrity:* In wesentliche Komponenten kritischer Infrastrukturen können fahrlässig oder bewusst Schwachstellen eingebaut worden sein, welche die System-Sicherheit gefährden.
Hauptthemen	*Destabilising Centralisation:* Starke Zentralisierung in der Struktur des Internets führt zu Klumpenrisiken. Der Ausfall eines Services kann weltweit Auswirkungen haben, wie zum Bespiel bei einem Ausfall von Amazon Web Services (AWS).

Technology Dynamics

Unter diesem Begriff sind Bedrohungen zu verstehen, die von der rasanten technologischen Innovation ausgehen und damit einerseits den Angreifern neue Möglichkeiten bieten, andererseits durch die Entwicklung selber neue Bedrohungen schaffen.

Hauptthemen	*Targeted Attacks:* Gezielte und komplexe Angriffe, um ein konkretes Ziel zu erreichen. Diese Bedrohung wird in weiteren Kapiteln in diesem Report detailliert erläutert. *All IP:* Im Zuge der flächendeckenden All IP-Einführung steigen Risiken im Zusammenhang mit der VoIP-Technologie. *5G Security:* 5G ist eine noch junge Mobilfunk-Technologie, die Einführung wird neben vielen Chancen auch noch unbekannte Bedrohungen mit sich bringen. *Ransomware:* Kritische Daten werden grossflächig verschlüsselt und gegen Lösegeld (möglicherweise) wieder entschlüsselt.
Früherkennung	*Automatisation & Scaling:* Stärkere Automatisierung technischer Betriebsprozesse wird bei erfolgreichen Angriffen oder Fehlkonfigurationen grössere Auswirkungen haben. *Increased Complexity:* Die Komplexität von Systemen, insbesondere über Technologie- und Unternehmensgrenzen hinweg, nimmt laufend zu. Dadurch steigt die Risikoexposition und die Fehlersuche wird erschwert. *Quantum Computing:* Quantencomputer können bestehende kryptographische Verfahren unbrauchbar machen, da sie diese in kürzester Zeit knacken können.

Cyber goes Physical

Unter diesen Begriff fallen Angriffe über die Infrastruktur im Cyberspace, die vermehrt Schaden in der physischen Welt verursachen werden.

Hauptthemen

IoT Devices: Schwach geschützte Geräte können kompromittiert und sabotiert werden. So können sie in der eigenen Funktion, z.B. der Verfügbarkeit oder Datenintegrität, eingeschränkt werden.
SCADA: Es existieren nach wie vor viele schlecht oder gar nicht geschützte Kontrollsysteme für Anlagen der kritischen Infrastruktur.

Organisation

Unter Organisation sind Bedrohungen zu verstehen, die von Veränderungen in Organisationen ausgehen oder Schwächen in Organisationen ausnutzen.

Hauptthemen

Infrastructure Misconfiguration: Ausnutzung fehlkonfigurierter Infrastruktur-Komponenten und/oder von Schwachstellen, die spät identifiziert und behoben werden.
Workplace Diversity: Neben den vielen Chancen, die neue Arbeitsmodelle mit sich bringen, führt der unkontrollierte Einsatz solcher Modelle, wie z.B. «Bring your own Device» (BYOD) oder verstärkter Einsatz von Remote-Arbeitsplätzen, zu einer grösseren Risiko-Exposition.
Insider Threat: Partner oder Mitarbeitende manipulieren, missbrauchen oder verkaufen Informationen fahrlässig oder vorsätzlich.
Decentralised Development: Klassische Entwicklungsabteilungen sterben aus, die Applikations-Entwicklung rückt näher in die Business Units bei gleichzeitig kürzer werdenden Release-Zyklen.

Physical

Bedrohungen, die von der physischen Umgebung ausgehen und in der Regel eher auf physische Ziele ausgerichtet sind.

Hauptthemen

Device Theft: Der Diebstahl insbesondere von Komponenten der kritischen Infrastruktur oder zukünftig vermehrt von IoT-Geräten kann zum Datenverlust führen oder die Verfügbarkeit der Services beeinträchtigen.
Drones and Robots: Aufklärung oder Angriffe über weite Entfernungen werden einfacher und günstiger.

Beobachtung

3D-Printing: Die Herstellung von z.B. Schlüsseln oder anderen physischen Geräten wird mit der besseren Qualität der 3D-Drucker günstiger und einfacher.

Proliferation

Bedrohungen, die von der immer einfacheren und günstigeren Verfügbarkeit von IT-Medien und Know-how profitieren, fallen unter das Segment Proliferation. Einerseits, weil die Verbreitung zu mehr Angriffsflächen führt und andererseits, weil sie die Verfügbarkeit von Angriffswerkzeugen erhöht.

Hauptthemen	*Subscriber Compromisation:* Schadsoftware greift private Daten der Mobile-Nutzer an oder wird für Angriffe auf die Telekommunikations- bzw. IT-Infrastruktur genutzt.
Früherkennung	*IoT-Based DDoS:* Starkes Wachstum bei geringem Schutz von IoT-Geräten führt zu mehr «Übernahme-Kandidaten» für Botnetze. *Digitalisation:* Immer stärkere Vernetzung der realen und virtuellen Welt und von Privat- und Geschäftsleben führt zu mehr Angriffswegen.

Environmental/ Social

Damit sind Bedrohungen gemeint, die von gesellschaftlich-politischen Änderungen ausgehen oder durch solche Änderungen für Angreifer einfacher oder wertvoller werden.

Brennpunkt	*Security job market:* Der Bedarf an Security-Professionals kann nur sehr schwer gedeckt werden, was weniger Know-how im Einsatz gegen immer komplexere und intelligentere Angriffe zur Folge hat.
Hauptthemen	*Digital Identity:* Beglaubigte, persönliche digitale Identitäten können missbraucht oder gestohlen werden, um z.B. unter fremden Namen Verträge abzuschliessen.
Früherkennung	*AI / Analytics:* Mehr Daten und bessere Analysemodelle mittels AI können missbraucht werden, um das Verhalten von Menschen zu beeinflussen. Entscheidungen werden vermehrt autonomen Systemen überlassen. *Political Influence:* Politische Strömungen können Einfluss auf technologische oder wirtschaftliche Entscheide nehmen, z.B. bei der Auswahl von Technologie-Lieferanten. Daraus können neue Risiken entstehen.

Fazit

Die Bedrohungslage bleibt komplex. Angreifer profitieren vom steigenden Wert virtueller Assets, was die Motivation für einen gezielten Angriff erhöht. Weiter schaffen technologische Innovationen und das Zusammenwachsen der physischen und virtuellen Welt neue Angriffsmöglichkeiten. Es zeigt sich aber auch, dass sich nicht eine bestimmte Bedrohung festigt, sondern Schwankungen und Trends unterliegen.

Gegenüber dem Lagebild des letzten Jahres können wir feststellen, dass sich die Bedrohungslage als Ganzes stabil verhält. Auch wenn einzelne Bedrohungen in diesem Jahr rückläufig sind, wie *Infrastructure Misconfiguration* und *Workplace Diversity,* bleiben die meisten bestehen und verändern sich nur minimal.

Bei beiden rückläufigen Bedrohungen sehen wir die «Entlastung» nicht aufgrund gesunkenem Interesse potentieller Angreifer, sondern in der gestiegenen Maturität der betroffenen Infrastrukturen. Die Workplace Diversity z.B. wird von immer mehr Unternehmen aktiv gemanaged, Mobile Device Management (MDM) Tools werden eingesetzt und Vorgaben zur Verwendung von Bring Your Own Devices (BYOD) erarbeitet und durchgesetzt.

Bedrohungen über *SCADA*-Systeme (industrielle Kontrollsysteme) und *IoT-Geräte* (Internet of Things) bleiben weiterhin im Hauptfokus, allerdings sehen wir keine kurzfristigen Veränderungen. Die Durchdringung von IoT ist noch nicht gross genug, um die Bedrohungslage weiter zu verschärfen.

Drohnen hingegen erreichen aktuell eine stärkere Verbreitung mit einhergehenden, auch in den Medien aufgegriffenen, teilweise negativen Folgen. Daher sehen wir hier aktuell einen starken Trend einer sich verschärfenden Bedrohungslage.

Die Bedrohungslage bleibt komplex. Angreifer profitieren vom steigenden Wert virtueller Assets, was die Motivation für einen gezielten Angriff erhöht.

Interview Costin Raiu (Kaspersky GReAT)

Wir hatten die Gelegenheit, Costin Raiu sechs Fragen zu stellen, die sich rund um APTs drehen und uns Einblick in seine Erfahrungen und Beobachtungen als Experte im Thema geben.

1. Costin Raiu, was kennzeichnet einen Advanced Persistent Threat, kurz APT?

Für uns sind Malware oder Angriffe dann fortgeschritten, sofern:

- ein *Zero-Day Exploit* verwendet wird, wie wir es von Sofacy, auch als APT28, Pawn Storm oder FancyBear bekannt, kennen. Dabei handelt es sich wohl um die Nummer Eins in Bezug auf die entdeckten Zero-Days.
- eine *hochkomplexe, modulare Plattform* für die Durchführung verschiedener Funktionen wie Regin und ProjectSauron benutzt wird.
- *ausgefeilte Techniken für Infektion, Persistenz oder Exfiltration* zum Einsatz kommen. So verwendete RedOctober einen sehr cleveren Persistenzmechanismus in Form eines Office- und Adobe Reader-Plugins, der die Fähigkeit hat, in speziell konstruierten Dokumenten versteckten Code auszuführen. Auch verschiedene Bootkit-Techniken gehören dazu.

Weitere Merkmale sind *langsame Replikation* verbunden mit *Persistenz auf Netzwerkebene* und *Infektion von Pro-Level-Netzwerkhardware* wie Core-Routern und *Supply-Chain-Angriffe.*

Gute Beispiele dafür, wie solche Angriffe verlaufen, sind Duqu2, SYNful Knock oder Shadowpad und CCleaner-Kompromittierung.

Diese Liste ist aber nicht vollständig. Weitere Beispiele sind Angriffe auf Hardware-Funktionen, Infektion des BIOS, destruktive Hardware-Angriffe mit Stuxnet, um nur ein bekanntes Beispiel zu nennen, oder Multiplattform-Malware.

2. Welche hervorstechenden Veränderungen der APT-Aktivitäten beobachten Sie und welche Bereiche sind von diesen Veränderungen besonders betroffen?

Wir verfolgen im Augenblick über 100 APT-Gruppen und ihre Aktivitäten. Mit der regelmässigen Verfolgung von APT-Gruppen begannen wir bereits 2010, denn nach der Stuxnet-Geschichte war klar, dass wir es mit einem Trend zu tun hatten, den wir verfolgen wollten. 2015 kannten wir ca. 100 APT-Gruppen und ihre Aktivitäten. In dieser Zeit starteten wir auch unsere private APT Berichterstattung.

Wir beobachten auch, dass immer mehr APT-Gruppen zu dateilosen Angriffen übergehen. Das macht es noch schwieriger, Infektionen zu erkennen, da im System keine bösartigen Dateien zu finden sind. Ausserdem sehen wir, dass eine zunehmende Zahl von Gruppen öffentliche Tools wie Empire Powershell, Metasploit, Cobalt Strike oder Mimikatz verwendet. Das macht es schwer, sie zu unterscheiden.

3. Was war der interessanteste APT-Angriff, auf den Sie je gestossen sind?

Das war wohl Duqu2. In erster Linie war Duqu2 für uns etwas Spezielles, weil er Kaspersky Lab angriff. Die Vorstellung, dass ein APT ein Sicherheitsunternehmen angreift, ist schon ziemlich kühn, denn die Urheber können ja nicht annehmen, dass der Angriff unbemerkt bleibt. Zweitens war Duqu2 etwas Besonderes, da die Bedrohung ausschliesslich den Speicher betraf. Die Malware wurde also nur im Speicher mehrerer Computersysteme ausgeführt, ohne Artefakte auf Festplatten zu hinterlassen. Das machte die Erkennung viel schwieriger. Ausserdem schien die Nutzung einer Zero-Day-Schwachstelle in Windows zur Umgehung von Kaspersky-Produkten ziemlich interessant und zog mehrere Produktverbesserungen nach sich, damit ein solches Verhalten in Zukunft erkannt werden kann.

4. Welche typischen Fehler begehen Unternehmen in der Vorbereitung auf einen APT Angriff und die Reaktion bei einem Vorfall?

Die meisten Unternehmen konzentrieren sich darauf, einen externen Angreifer daran zu hindern, sich Zugang zu internen Ressourcen zu verschaffen. Aber nur wenige ergreifen Massnahmen zur Erkennung eines Angreifers, der sich bereits Zugang zum internen Netzwerk verschafft hat. Wie ich aus unseren Forschungsarbeiten weiss, wenden die Angreifer den Grossteil ihrer Zeit für die Ausbreitung im Netzwerk und die Exfiltration auf. Deshalb sollten sich Organisationen auf diese Phasen konzentrieren. Ein weiteres Manko ist die fehlende Implementierung von TOP35[1]- mitigierende Massnahmen des australischen DSD gegen APTs.

[1] https://acsc.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

5. Welche typischen Fehler begehen Angreifer während ihrer Attacken? Wo sehen Sie, dass Organisationen gegenüber den Angreifern die Oberhand gewinnen?

Oftmals sehen wir Opsec-Fehler wie beispielsweise VPN-Fehler, vergessene PDB-Pfade in Binärdateien oder Kompilierungszeitstempeln.

6. Über welche Fähigkeiten muss man verfügen, um auf umfangreiche APT-Angriffe vorbereitet zu sein?

Für Unternehmen ist es wichtig, Zugang zu Berichterstattungen von privaten Bedrohungsinformationen zu erhalten. Ebenfalls wichtig sind ein voll betriebsfähiges Security Operation Center, die Implementierung von Netzwerkfiltern und die Erkennung von Ausbreitungs- und Exfiltrationsmechanismen. Ausserdem sollten Unternehmen unbedingt wissen und von Grund auf verstehen, wie Angreifer arbeiten. Zum Beispiel, welche Werkzeuge sie verwenden und wie sie in den Angriffsphasen vorgehen. Die meisten von ihnen verwenden Mimikatz, Powershell und Webshells.

Zur Person

Costin Raiu ist spezialisiert auf die Analyse von Advanced Persistent Threats (APTs) und komplexe Malware-Angriffe. Er leitet das Global Research and Analysis Team (GReAT) bei Kaspersky, das unter anderem die Stuxnet, Duqu, Flame und Equation Group Operationen untersucht hat. Costin verfügt über mehr als 19 Jahre Erfahrung in den Bereichen Antiviren-Technologien und Sicherheitsforschung. Er ist Mitglied des Virus Bulletin Technical Advisory Board, Mitglied der Computer AntiVirus Researchers' Organisation (CARO) und Reporter für die Wildlist Organisation International. Bevor er zu Kaspersky Lab kam, arbeitete Costin für GeCad als Chief Researcher und als Data Security Expert bei der RAV Antivirus-Entwicklergruppe.

Komponenten des gezielten Angriffs

Die Mission, das strategische Ziel, hat je nach Akteur völlig andere Absichten und die Akteure haben unterschiedlichste Fähigkeiten, diese in die Tat umzusetzen.

In den Medien wird oft darüber berichtet, dass Unternehmen mit einer bestimmten Malware befallen sind oder dass eine bestimmte Malware genutzt wurde, um Daten eines Unternehmens zu stehlen. Um gezielte Angriffe zu verstehen, müssen wir uns darüber bewusst werden, dass es nicht die Malware ist, die die Angriffe durchführt, sondern dass die Unternehmen von Menschen angegriffen werden. Diese werden im Cyber-Umfeld häufig als Akteure (Threat Actors / Cyber Operators) bezeichnet und sind die Hauptkomponente hinter dem Angriff. Die Akteure hinter gezielten Angriffen führen diese Angriffe nicht wahllos aus, sondern haben ein strategisches Ziel, unterschiedlichste Motivationen und diversifizierte Vorgehensweisen, die als zusätzliche Bestandteile eines gezielten Angriffs dienen und im weiteren Verlauf aufgezeigt werden.

Threat Actor Landscape

Die Mission, das strategische Ziel, hat je nach Akteur völlig andere Absichten und die Akteure haben unterschiedlichste Fähigkeiten, diese in die Tat umzusetzen. Zur besseren Orientierung und Beurteilung des Potenzials und der Motivation verschiedener Akteure unterteilen wir diese in folgende Gruppen:

Advanced Persistent Threats und der gezielte Angriff

Der Advanced Persistent Threat (APT) zählt zur Königsklasse der Cyber-Akteure. Die gezielten Angriffe eines APTs werden basierend auf einer Mission durchgeführt, die darauf ausgelegt ist, einen strategischen Vorteil zu erhalten um politische Ziele zu erreichen oder Technologieentwicklungen positiv zu beeinflussen. In diesem Zusammenhang geht man bei einem APT von einer Regierung oder von ihr Beauftragte aus. Die Besonderheit des APTs liegt darin, dass die damit in Zusammenhang stehenden Angriffe als «state-sponsored» gelten, was explizit heisst, dass die Akteure staatlich gewollt sind und somit «legale» (oder zumindest staatlich geschützte) Hacker darstellen. Die staatliche Legalität, schwierige Rückverfolgung und relativ risikolose Durchführung haben dazu geführt, dass immer mehr Staaten ihre Cyber-Fähigkeiten und APT Angriffe ausweiten.[2]

[2] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

Neben den «legalen» APTs existiert noch eine weitere Randgruppe, die man als Wegbereiter von Staaten/Regierungen ansehen kann, die bisher selbst keine Fähigkeiten aufgebaut haben, um fortgeschrittene Angriffe wie die eines APT selbst durchführen zu können. Spätestens seit den Hacking Team-Enthüllungen des Hacktivisten Phineas Phisher ist klar, dass diese Randgruppe klare finanzielle, strategische Ziele verfolgt.[3]

Cyber Kriminelle und der gezielte Angriff

Cyber Kriminelle gehen primär opportunistisch vor und verwenden jedes ihrer ihnen zur Verfügung stehenden Angriffsmittel (z.B. einen Exploit gegen Microsoft Office, der veröffentlicht wurde) gegen eine breite Palette von Zielen. Erhalten sie ein neues Angriffsmittel, verwenden sie es, um von möglichst vielen Angriffen zu profitieren. Neben den opportunistischen Angriffen gibt es auch gezielte und gut organisierte, mit dem Ziel, von einem dedizierten Ziel mit einem Angriff viele Daten oder andere Werte zu stehlen, die sich in Geld umwandeln lassen. Dazu benötigen die Angreifer eine lange Zeit («Dwell Time») im System des Zieles. Derart organisierte Kriminelle stehen oftmals in ihren technischen Fähigkeiten vielen APTs in nichts nach. Der entscheidende Unterschied liegt jedoch in den strategischen Zielen dieser Akteure.

Terroristen und der gezielte Angriff

Während die Befürchtungen in der Gesellschaft gross sind, dass Terroristen Angriffe auf kritische Systeme durchführen, ist bisher kein einziger Fall bekannt geworden, bei denen Terroristen ihre strategischen Ziele durch gezielte Cyber-Angriffe verfolgt und erreicht hätten. Im Gegenteil: Zu den bisherigen Befürchtungen hat das Cambridge Centre for Risk Studies bisher keine nicht-staatlichen, terroristischen Gruppen beobachtet, die die Fähigkeit aufgebaut hätten, fortgeschrittene, gezielte Cyber-Angriffe durchzuführen, die physikalischen Schaden anrichten könnten.[4] Gleichzeitig bewertet das World Wide Threat Assessment of the US Intelligence Community 2018, dass die Nutzung des Cyber-Raumes von Terroristen primär für mediale Zwecke genutzt wird.[5]

Wir gehen weiterhin davon aus, dass eine Gefahr durch Cyber-Terror besteht und in Zukunft eine grössere Rolle spielen wird.

Hacktivisten und der gezielte Angriff

Hacktivisten führen gezielte Angriffe typischerweise aus politischer Motivation durch, um ihren Protest zum Ausdruck zu bringen. Sie finden sich global zusammen in Gruppen von Gleichgesinnten, um Angriffe zu koordinieren und durchzuführen oder führen Angriffe als Einzelgänger durch. Die Skills unter Hacktivisten variieren sehr stark. Es geht darum, das entscheidende strategische Ziel möglichst schnell zu erreichen und grosse Medienaufmerksamkeit zu erhalten. Bisher ist zu beobachten, dass diese Akteure primär Smash and Grab Operationen durchführen, um möglichst schnell ihren Erfolg bekannt zu geben.

[3] https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/
[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf
[5] https://www.wilsoncenter.org/article/world-wide-threat-assessment

Targeting

Die Ziele (Targets) von gezielten Angriffen werden nicht zufällig gewählt, sondern nach einer spezifischen Beziehung, in der das Angriffsziel und der Angreifer zueinander stehen.

Target of Interest

Je mehr das Angriffsziel das Bedürfnis eines Angreifers erfüllt, umso höher steigt der Stellenwert des Angriffsziels und wird zum Target of Interest (TOI) für die Akteure. Die primären Aspekte, die dieses Bedürfnis beschreiben, sind Alleinstellungsmerkmal des Ziels, benötigter Aufwand und die damit verbundenen Kosten, um den Angriff durchzuführen, sowie die Risiken für die Angreifer, die dabei entstehen können.

Target of Opportunity

Einen eher untergeordneten Stellenwert stellt das Target of Opportunity (TOO) dar. Diese Ziele erfüllen ein untergeordnetes Bedürfnis der Akteure und werden kompromittiert, um dann z.B. als Sprungpunkt verwendet zu werden um zum eigentlichen Target of Interest zu gelangen. Es kann aber auch sein, dass das Ziel zu einem bestimmten Zeitpunkt für eine Capability anfällig war und kompromittiert wurde. Dies kann mitunter dazu führen, dass das Target of Opportunity zum Target of Interest wird, wenn die Akteure später feststellen, dass das Opfer einen höheren Wert darstellt als initial erkannt wurde.[6]

Je mehr das Angriffsziel das Bedürfnis eines Angreifers erfüllt, umso höher steigt der Stellenwert des Angriffsziels und wird zum Target of Interest (TOI) für die Akteure.

[6] www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Durchführen des Angriffs

Es gibt viele Methoden, um die Durchführung eines Cyber-Angriffs zu beschreiben. Wir haben uns für das MITRE ATT&CK Framework entschieden, dessen Daten auf Angriffen basieren, die in der realen Welt ausgeführt wurden. ATT&CK ist eine Methode analog der Cyber Killchain[7] zur Beschreibung von Cyber-Angriffen[8]. Während die Cyber Kill Chain eher eine Beschreibung aus Helikoptersicht ist, stellt das ATT&CK Framework detailliert die Aktivitäten von mehr als 80 Threat Actors (Groups) dar. ATT&CK beinhaltet primär die Vorgehensweisen von Advanced Persistent Threats in den unterschiedlichen Angriffsphasen, beschrieben anhand der Tactics, Techniques and Procedures (TTPs)[9] dieser Akteure.

Unsere Auswertung der Daten ist über einen Zeitraum von mehreren Wochen über ATT&CK Enterprise[10] (im Folgenden ATT&CK) durchgeführt worden, mit letztmaligem Zugriff im Januar 2019. ATT&CK wird kontinuierlich erweitert und aktualisiert. Die Daten des Frameworks, zusammen mit den Erfahrungen von Costin Raiu's GReAT Team erlauben jedoch, in qualitativer als auch quantitativer Form sehr genaue Auswertungen.

Im Januar 2019 beinhaltete ATT&CK

Wir haben die nach unserer Ansicht wichtigsten high-level Erkenntnisse aus dem ATT&CK Framework in den folgenden Kapiteln zusammengetragen, mit einem klaren Fokus auf den Advanced Persistent Threat.

[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[8] https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
[9] https://apps.dtic.mil/dtic/tr/fulltext/u2/1004650.pdf
[10] https://attack.mitre.org/matrices/enterprise/

Die Angriffsphasen

Als Tactics versteht ATT&CK die verschiedenen Phasen des Angriffs, die ein Threat Actor durchlaufen muss, um sein strategisches Ziel zu erreichen. In diesem Zusammenhang spricht man auch von taktischen Zielen. ATT&CK definiert die folgenden Tactics:

Initial Access	Die Initial Access Phase bildet die Ausgangslage für alle weiteren Phasen des Angriffs. Sie beinhaltet den Erstkontakt mit dem Angriffsziel und Kompromittierung des Patient Zero.
Persistence	Die Persistenzpunkte innerhalb des Zielnetzwerks gewährleisten weiterhin Zugriff in das Netzwerk. Je bedeutsamer das Ziel (Target of Interest), desto mehr Aufwand wird für die Persistenz während einer Long-Term Intrusion betrieben.
Privilege Escalation	Die Eskalation der Privilegien wird oft benötigt, um Schadsoftware oder Persistenzpunkte installieren zu können. Erhöhte Privilegien sind mitunter auch benötigt, um sich auf weiteren Systemen ausbreiten zu können oder Zugang zu den strategischen Zielen (z.B. Daten) zu erhalten.
Discovery	Die Exploration innerhalb des Zielnetzwerks wird benötigt, um für die Mission relevante Systeme, Benutzer und Daten ausfindig zu machen.
Lateral Movement	Damit ist die Ausbreitung innerhalb des Netzwerks zu den für die Mission relevanten Daten gemeint. Oft sind diese begleitet durch die Execution Phase und Installation von weiteren Persistenzpunkten.
Collection	Die für die Mission relevanten Daten werden gesammelt.
Exfiltration	Dies ist die finale Phase, um die Mission erfolgreich abzuschliessen und beinhaltet das Exfiltrieren der relevanten Daten.

Parallel zu diesen Phasen laufen die folgenden Phasen ab und stehen in Abhängigkeit zur erfolgreichen Zielerreichung der jeweiligen Phasen:

Execution

Die Ausführung von Schadcodes auf einem lokalen oder entfernten System findet primär in den Phasen des Initial Access und Lateral Movement statt. Ohne Ausführung eines Codes, der unter der Kontrolle des Angreifers steht, könnte die nächste Phase nicht erreicht werden. Execution ist somit eine der wichtigsten Voraussetzungen für die weitere Entwicklung des Angriffs und Ausbreitung innerhalb des Zielnetzwerks.

Defense Evasion

Das Umgehen von Verteidigungs- und Erkennungsmechanismen – wie z.B. dem Ausschalten der Firewall auf dem Endpoint oder dem Löschen von Logdaten – ist eines der taktischen Ziele, die der Täter in jeder der anderen Phasen seiner Mission anwendet, um entweder seine Anwesenheit zu verschleiern oder Erkennungsmechanismen zu umgehen.

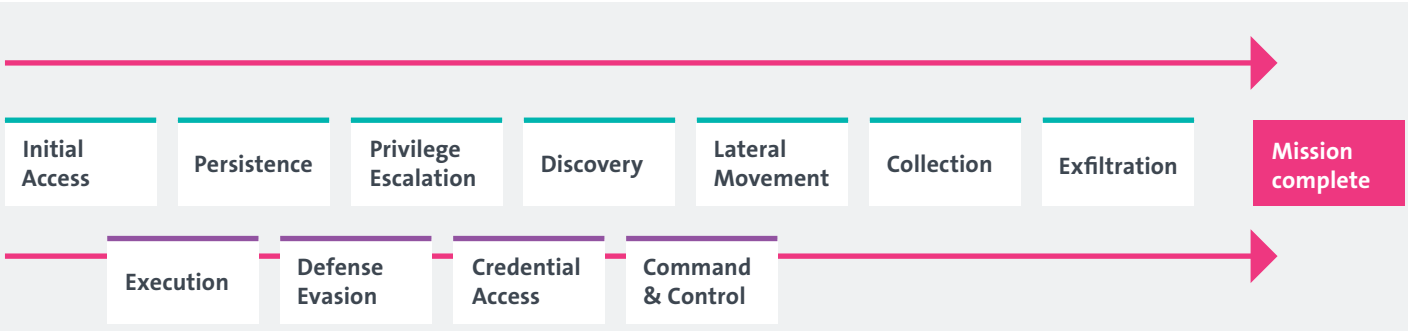
Credential Access

Zugangsdaten spielen eine der Schlüsselfunktionen für Angreifer. Zum einen ermöglichen sie unbemerktes Eindringen und Fortbewegen innerhalb des Zielnetzwerks. Zum anderen gewähren sie den Zugang zu den Daten, die die Angreifer wollen. Weiterhin erlaubt es den Angreifern durch das Wiederverwenden von Zugangsdaten, ressourcenschonend ihren Angriff durchzuführen, da keine Exploits geschrieben, erworben oder anderweitig eingesetzt werden müssen.

Command & Control

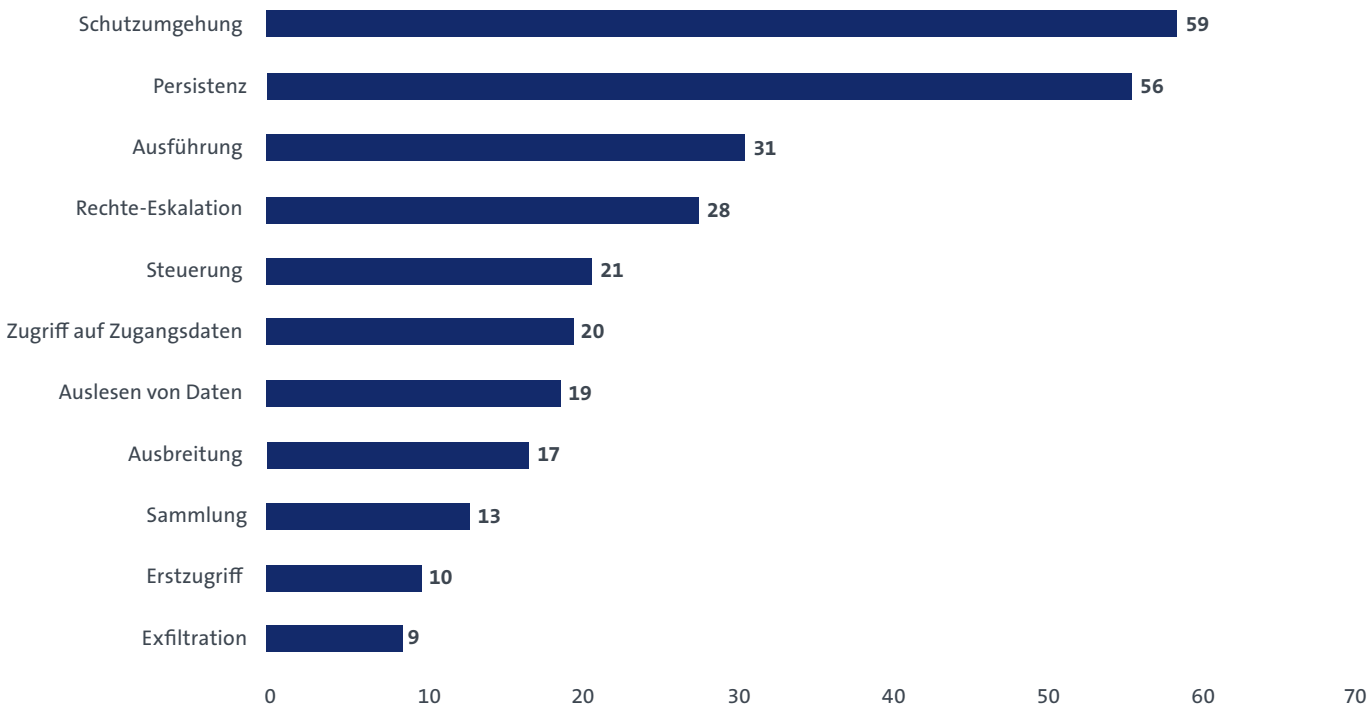
Der Command- & Control-Kanal ist für den Angreifer sein Kommunikationsmittel, um die kompromittierte Zielinfrastruktur unter Kontrolle zu halten. Verliert der Angreifer diesen Kanal, würde der Angriff zunächst aufgehalten. Gezielte Angreifer etablieren häufig mehrere Command & Control Kanäle.

Die folgende Illustration stellt den Zusammenhang dar:



Vorgehensweisen der Akteure

Um eine spezifische Phase zu erreichen oder zu durchlaufen, nutzen die Akteure im ATT&CK Framework[11] verschiedenste Vorgehensweisen, auch Techniques genannt. Jede Phase kann mehrere Vorgehensweisen beinhalten und Vorgehensweisen können in mehreren Phasen vorkommen. ATT&CK beinhaltet 224 dieser Vorgehensweisen, die sich über die verschiedenen Phasen wie folgt aufteilen:



Das Balkendiagram gibt aufschlussreiche Einblicke in den Modus Operandi der Akteure und zeigt deutlich, in welchen Phasen die Akteure die meisten und die wenigsten Fähigkeiten besitzen. Betrachtet man also die Phasen von der Perspektive, in der die meisten Vorgehensweisen vorhanden sind, so lässt sich aus der Analyse entnehmen, dass die Akteure auf ein sehr breites Spektrum zugreifen können, um Verteidigungsmechanismen in den unterschiedlichen Phasen des Angriffs auszuhebeln durch Defense Evasion und ebenso viele Vorgehensweisen zur Verfügung haben, um den Langzeit Zugang sicherzustellen in der Persistence Phase.

Auszug aus dem Interview mit Costin Raiu, die diese Aussage ebenso verdeutlicht:

Über welche Fähigkeiten muss man verfügen, um auf umfangreiche APT-Angriffe vorbereitet zu sein?

Unternehmen sollten wissen und von Grund auf verstehen, wie Angreifer arbeiten. Zum Beispiel, welche Werkzeuge sie verwenden und wie sie in den Angriffsphasen vorgehen. Die meisten von ihnen verwenden Mimikatz, Powershell und Webshells.

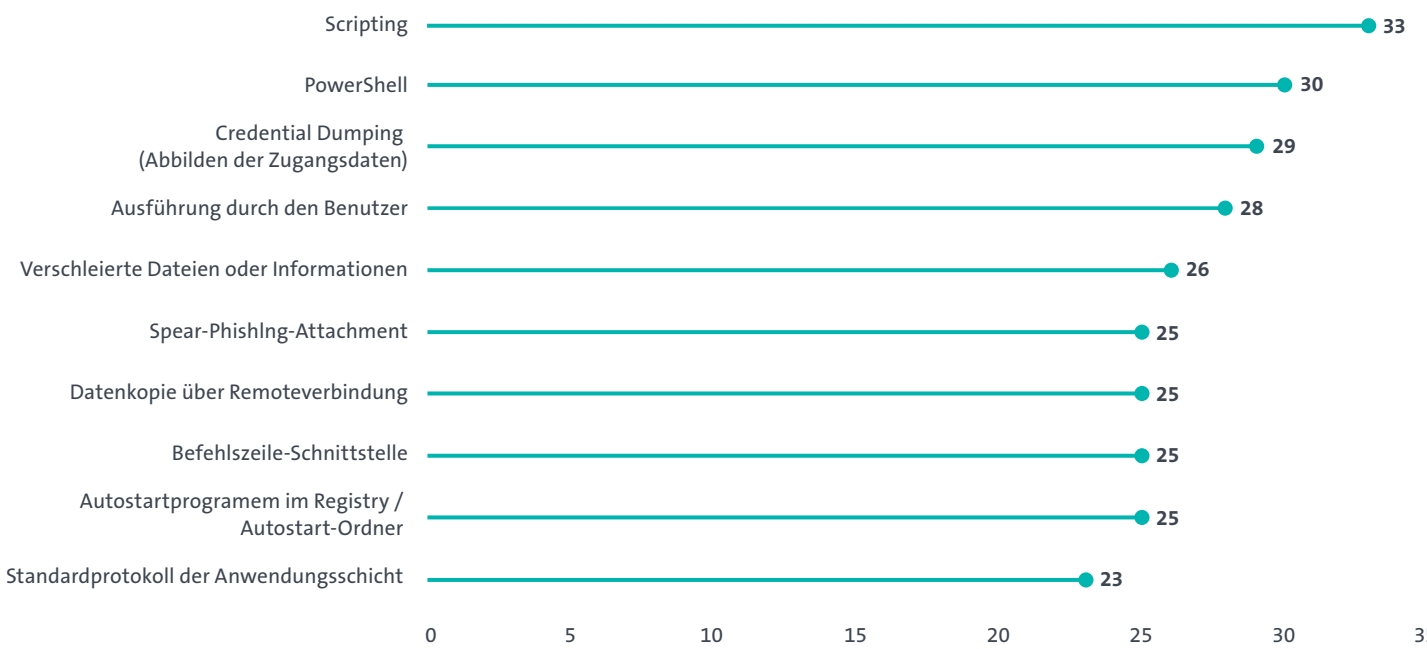
[11] https://attack.mitre.org/

Meistgenutzte Vorgehensweisen nach Akteuren
Eine Auswertung über die APT Gruppen und deren Vorgehensweisen zeigt einen klaren Trend zu fileless Attacks, der auch von Costin Raiu so bestätigt wird.

Die folgende Illustration zeigt die Top 10 der meist-genutzten Vorgehensweisen über die 80 Akteure innerhalb von ATT&CK.

Welche hervorstechenden Veränderungen der APT-Aktivitäten beobachten Sie und welche Bereiche sind von diesen Veränderungen besonders betroffen?

Wir beobachten auch, dass immer mehr APT-Gruppen zu dateilosen Angriffen übergehen. Das macht es noch schwieriger, Infektionen zu erkennen, da im System keine bösartigen Dateien zu finden sind.



Die Top 10 der Vorgehensweisen lassen sich unter den zwei Themen «Living off the Land» und «Bewährte Methoden» zusammenfassen.

Living off the Land

Immer mehr APT Gruppen greifen auf Scripts zurück, die mittlerweile standardmässig in Windows Betriebssysteme integrierte sind wie Powershell und Command-Line Interfaces, um ihren Schadcode auszuführen. Dies unerkannt von Application Whitelisting-Lösungen und ohne signifikante Spuren auf dem System zu hinterlassen.

Als Persistenzmechanismus bleiben Registry Run Keys und Einträge im Windows Startup Folder die beliebtesten Vorgehensweisen unter den Akteuren.

Bewährte Methoden führen zum Ziel

Nicht alle Akteure haben die Ressourcen, Zero Day Exploits zu entwickeln. Ein Grossteil der Akteure setzt weiterhin auf Spear Phishing Attachments und User Execution für die Ausführung des Schadcodes durch den Benutzer.

APT Akteure nutzen einfache Wege, um ihr Ziel zu erreichen. Durch Credential Dumping werden valide Zugangsdaten erlangt und dann genutzt, um sich innerhalb der Infrastruktur bewegen zu können und den Zugang sicherzustellen.

Für Data Exfiltration, dem zusätzlichen Laden und Abspeichern von Codes, der unter der Kontrolle des Angreifers steht, bleiben weiterhin das simple Kopieren von Dateien (Remote File Copy) über legitime Protokolle (Standard Application Layer Protocol) und dem Anwenden von Kodierungen und Verschlüsselungen (Obfuscated Files or Information) die beliebtesten Vorgehensweisen.

Software der Akteure

Die eingesetzte Software der Akteure implementiert benötigte Vorgehensweisen für eine Angriffsphase. Hierbei greifen die Akteure auf unterschiedlichste Kategorien von Software zurück, die innerhalb von ATT&CK entweder ein Tool, Utility oder Malware repräsentieren.[12]

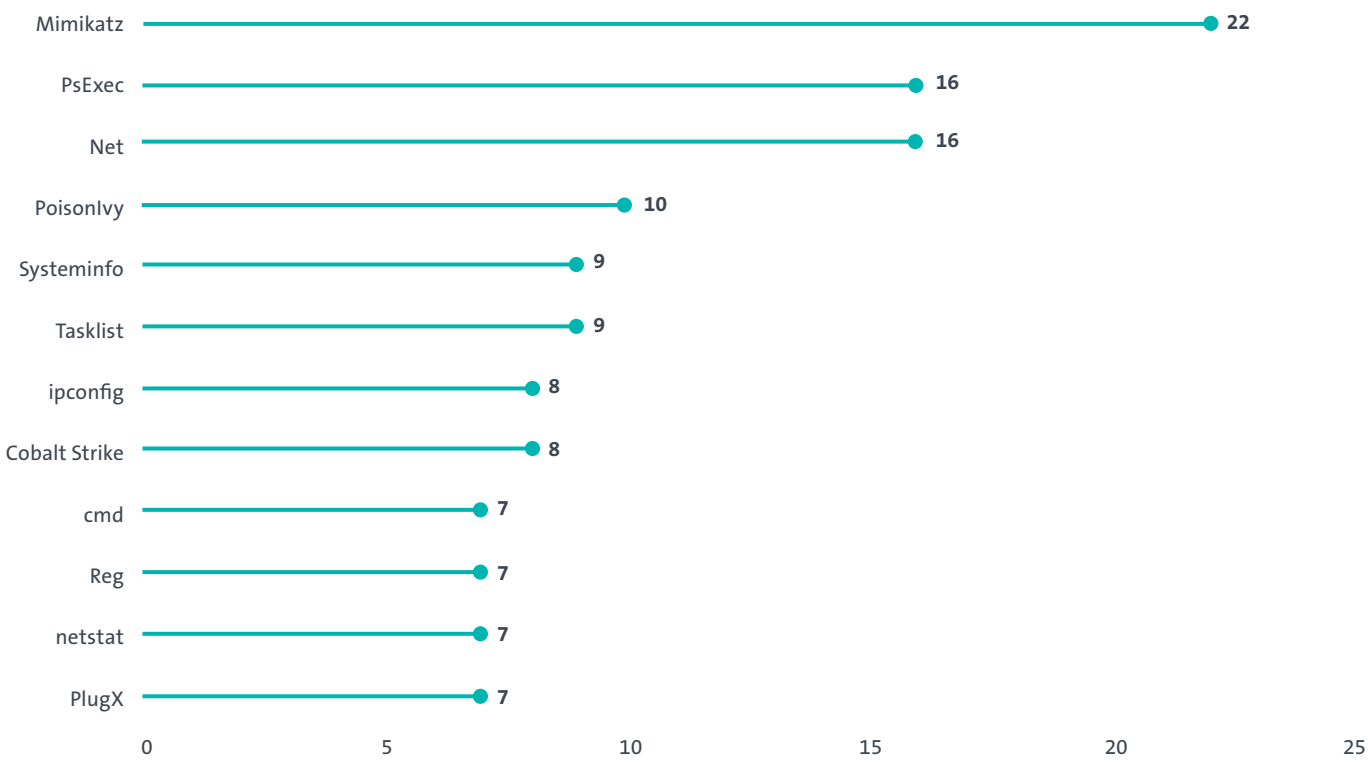
[12] https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Meistgenutzte Software nach Akteuren
Eine Auswertung über die APT Gruppen und deren eingesetzte Software zeigt auf, dass Off-the-Shelf Tools und Software, die das Betriebssystem bereits mitbringt, am häufigsten zum Einsatz kommen. Diese Beobachtung geht einher mit den Erfahrungen von Costin Raiu.

Die folgende Illustration zeigt die Top 10, der meistgenutzten Software der 80 Akteure innerhalb von ATT&CK.

Welche hervorstechenden Veränderungen der APT-Aktivitäten beobachten Sie und welche Bereiche sind von diesen Veränderungen besonders betroffen?

Wir sehen, dass eine zunehmende Zahl von Gruppen öffentliche Tools wie Empire Powershell, Metasploit, Cobalt Strike oder Mimikatz verwendet. Das macht es schwer, sie zu unterscheiden.



Gegenmassnahmen und Wirkung

Gegenmassnahmen gegen gezielte Angriffe bauen auf einem Grundschutz auf, basierend auf Präventivmassnahmen, wie dem Anwenden von aktuellen Patches, Implementierung von 2-Faktor Authentifizierung, Internet Verbindungen nur durch Proxies, etc. Diese Massnahmen reichen mitunter dazu aus, um das Interesse von nicht-staatlichen Akteuren auf andere Ziele zu lenken.

In den vorangegangenen Kapiteln haben wir die grundlegenden Aspekte der Threat Actors betrachtet, die sich in Intent (strategische Ziele), Opportunity (Angriffsfläche) und Capability (Vorgehensweisen) wiederfinden. Genau diese Aspekte müssen miteinbezogen werden, um entsprechende Gegenmassnahmen zu entwickeln, die die effektivste Wirkung haben. Die wohl effektivste Verteidigung wäre das strategische Ziel (Intent) zu eliminieren. Regierungen oder Unternehmen, die keine Daten speichern, werden nicht zum Ziel eines staatlichen Akteurs, der Spionage durchführt und sich durch gestohlene Daten einen Vorteil verschaffen möchte. Diese Verteidigung ist allerdings in den wenigsten Fällen umsetzbar. Betrachten wir die zur Verfügung stehende Angriffsfläche, so ist diese in den letzten Jahren eher vergrössert als verkleinert worden. Die zunehmende Digitalisierung, das Speichern von Daten in der Cloud und everything connected, always-on und IoT Devices leisten ihren Beitrag zu einer exorbitant gross gewordenen Angriffsfläche für Unternehmen, Gesellschaft und Einzelpersonen.

Wir müssen also unsere zur Verfügung stehenden Gegenmassnahmen auf den Aspekt der Fähigkeiten und den Vorgehensweisen der Threat Actors abstützen, was oftmals in einem Kopf-an-Kopf Rennen endet und in Anbetracht der Vielzahl an Vorgehensweisen zunächst äusserst komplex erscheint.

Beim genauen Hinschauen jedoch zeichnet sich ab, dass die meisten Vorgehensweisen und die genutzte Software durch Erkennungsmethoden aufgedeckt werden können, die System Aktivitäten verfolgen.

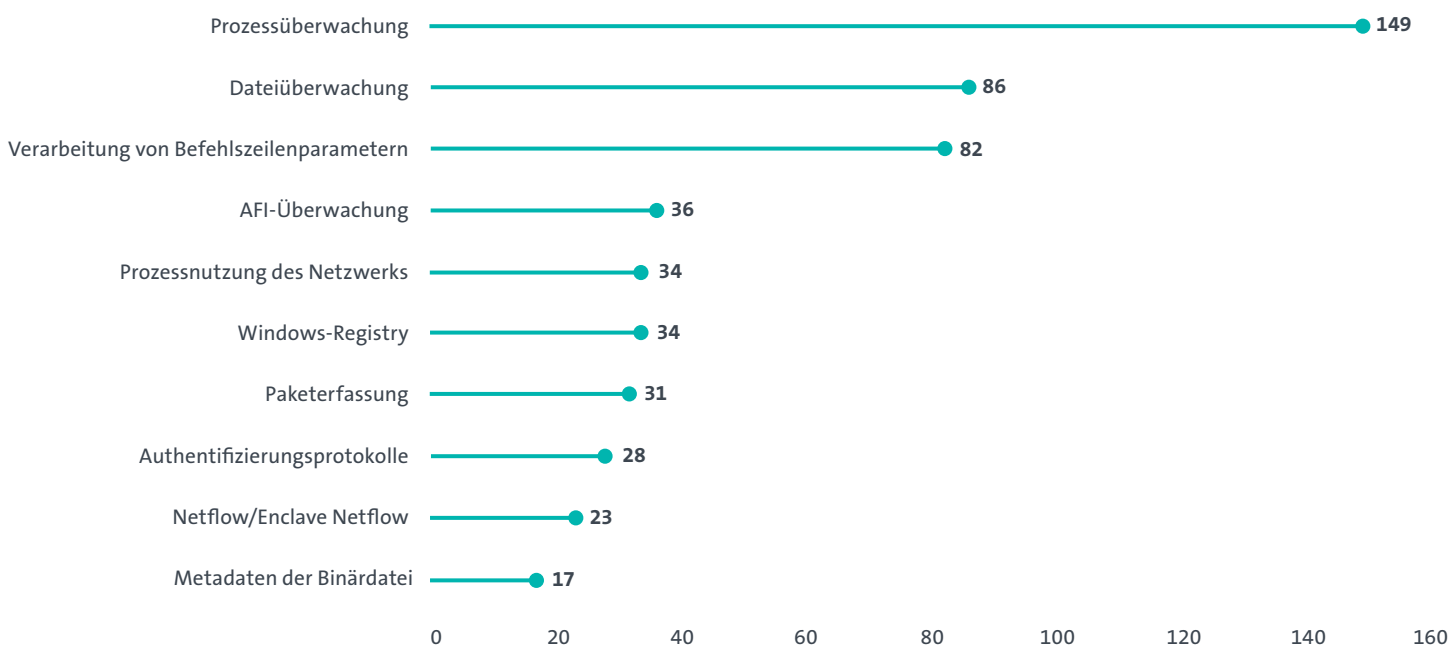
Erkennungsmethoden mit der grössten Abdeckung

Unsere Analyse zeigt, dass von den Vorgehensweisen der Akteure ein Grossteil durch das Monitoring von Prozess- und Dateioperationen erkannt werden kann. Diese Erkenntnis muss so verstanden werden, als dass diese Erkennungsmethoden am vielversprechendsten sind, um die Aktivitäten eines Angreifers nach dem Initial Access weiter mitverfolgen zu können.

Die folgende Illustration der Top 10 Erkennungsmethoden macht dies noch einmal deutlich:

Welche typischen Fehler begehen Angreifer während ihrer Attacken? Wo sehen Sie, dass Organisationen gegenüber den Angreifern die Oberhand gewinnen?

Die meisten Unternehmen konzentrieren sich darauf, einen externen Angreifer daran zu hindern, sich Zugang zu internen Ressourcen zu verschaffen. Aber nur wenige ergreifen Massnahmen zur Erkennung eines Angreifers, der sich bereits Zugang zum internen Netzwerk verschafft hat.



Erkennungsmethoden für Prozess-Aktivitäten erkennen einen Grossteil der vorhandenen Vorgehensweisen der Akteure. Benutzer- und Netzwerkaktivitäten geben zusätzlichen Kontext.

System Aktivitäten

Die Ausführung von Code, der unter der Kontrolle der Akteure steht, ist eine Grundvoraussetzung, um das strategische Ziel der Akteure zu erreichen. Um dem Angriffsmuster der Akteure zu folgen, sind das Überwachen von Prozessen, Dateien und Veränderungen in der Windows Registry die effektivsten Erkennungsmethoden für die Vorgehensweisen der Akteure. Auch wenn diese Form der Erkennung den grössten Mehrwert bringt, so ist mit sehr hohem Datenvolumen und Tuning zu rechnen. Prozesse, Netzwerkverbindungen, Datei- und Registry Operationen müssen vollumfänglich verstanden werden.

Benutzer- und Netzwerkaktivitäten

Neben dem Monitoring von Systemaktivitäten geben Netzwerkdaten und Logs von Benutzerauthentifizierungen Visibilität in einen Grossteil der Vorgehensweisen der Akteure.

Was macht Swisscom

Gezielte Angriffe werden immer wahrscheinlicher und die derzeit verfügbaren technologischen Mittel sind oft nicht ausreichend, um mit den Fähigkeiten professioneller Cyber-Akteuren mithalten zu können. Swisscom setzt aus diesen Gründen auf ein risikobasiertes Sicherheitsmodell, das eine hohe Sicherheitskultur im Unternehmen durch Mitarbeiterschulung fördert, die Community in die Sicherheitskultur miteinbezieht, z.B. durch das Bug Bounty Programm[13] und fundamentale präventive Sicherheitsvorkehrungen wie z.B. dem Whitelisting und Patching von Applikationen, dem Einschränken von Netzwerkverkehr und Email Attachments voraussetzt. Die Prävention ist nur ein Teilbereich, der schlussendlich gegen hochmotivierte Akteure versagen wird. Es ist deshalb nötig, proaktiv zu werden und die Tactics, Techniques and Procedures der Akteure zu verstehen und die daraus erkannten Erkenntnisse in die Detektion miteinfliessen zu lassen. Wir nennen diesen Ansatz Threat Intelligence als Basis der Detektion, indem wir beispielsweise die Simulation eines gezielten Angriffs durch Red Teaming durchführen, das Suchen nach bisher unentdeckten Gefahren im eigenen Netzwerk durch Threat Hunting abbilden und uns regelmässig mit anderen Unternehmen in derselben Branche, in Sharing Groups, austauschen.

Red Teaming

Angreifer sind immer einen Schritt voraus, also werden wir selber zum Angreifer. Swisscom hat 2015 entschieden, neue Wege zu gehen und gründete als erstes Schweizer Unternehmen ein offizielles Red Team. Das Red Team besteht aus einer kleinen Gruppe von Mitarbeitenden der Swisscom, welche möglichst reale Angriffe gegen Swisscom-Infrastruktur und -Dienste durchführt. Es sind Ethical Hackers, also Hacker mit guten Absichten, die gezielte Angriffe gegen Swisscom, NICHT aber gegen Endkunden-Anwendungen und -Daten durchführen.

Was sind ihre Ziele?

- Schwachstellen finden und deren Auswirkungen aufzeigen, bevor es andere tun
- Das Blue Team zu testen und damit dem Unternehmen helfen, Gegenmassnahmen zu entwicklen und Abläufe zu verbessern
- Aus Vorfällen anderer Firmen lernen und testen, ob das Swisscom auch hätte passieren können

Gezielte Angriffe werden immer wahrscheinlicher und die derzeit verfügbaren technologischen Mittel sind oft nicht ausreichend, um mit den Fähigkeiten professioneller Cyber-Akteuren mithalten zu können.

[13] https://www.swisscom.ch/en/about/company/portrait/network/security/bug-bounty.html

Threat Hunting

Threat Hunting hat das Ziel, bisher unerkannte Bedrohungen zu erkennen. Es ist kein Ersatz für ein funktionierendes Security Operations Centre (SOC), sondern verwendet teils automatisierte, aber auch manuelle Methoden für das Erkennen von Angriffsverhalten und Mustern, die durch existierende Schutzmechanismen nicht erkannt werden konnten. Dieser Vorgehensweise liefert zum Beispiel neue Erkennungsmethoden. Das Swisscom CSIRT führt regelmässig Threat Hunting Sessions durch, um Gefahren innerhalb des Swisscom Netzes zu erkennen. Das ATT&CK Framework dient hierbei oftmals als Referenz, um die Tactics und Techniques der einzelenen Akteure zu verstehen. In diesem Zusammenhang veröffentlicht das CSIRT regelmässig neue Erkennungsmethoden für SIGMA[14] und YARA[15] und macht diese für die Community zugänglich. SIGMA ist ein generisches und offenes Signaturformat, mit dem relevante Log-Daten als Erkennung einmal beschrieben werden und es für eine Vielzahl von SIEM und Log-Systeme verwendbar wird. SIGMA ist eines der wenigen Tools, die Angriffe mit ATT&CK Tactics und Techniques beschreiben können und die Erkennung direkt für andere nutzbar macht. Mit YARA ist es möglich, eigene Signaturen und Erkennungen zu erstellen, die sowohl für Dateien als auch Memory Scans genutzt werden können. Das Swisscom CSIRT erstellt regelmässig YARA Regeln für Angreifer Toolsets und teilt diese mit Public Communities, wie beispielsweise der signature-base von Florian Roth[16] oder anderen geschlossenen Communities.

Wie in vorangehenden Kapiteln ausgeführt, müssen wir verstehen, dass Angriffe nicht von Systemen, sondern von Menschen durchgeführt werden und es entsprechend auch Menschen benötigt, um auf diese zu reagieren. Deshalb hat Swisscom mehrere Security Operations Centre (SOC) im Einsatz, um möglichen Aktivitäten von Angreifern systematisch nachgehen zu können. Die Analysten des Swisscom CSIRT werden aktiv, sobald Aktivität erkannt wurde, die auf gezieltere Angriffe auf die IT-Infrastruktur von Swisscom hinweist.

Sharing Groups und Community

Neben dem Teilen von Erkennungen basierend auf SIGMA und YARA ist das Swisscom CSIRT und deren Mitarbeitende als aktives Mitglied in vielen Trust Groups für die operative Zusammenarbeit im Alltag von CSIRTs, SOCs und Threat Intelligence Teams. Ziel dieser Trust Groups ist es, Personen mit denselben Problemen im Alltag zusammen zu bringen und den Austausch zu vereinfachen. Swisscom teilt regelmässig Informationen zu aktuellen Beobachtungen, Gefahren sowie Indikatoren zu Schadsoftware und Angriffen innerhalb dieser Sharing Groups und Communities aus.

Umfassender Unternehmensschutz dank Früherkennung und professionellem Agieren bei Cyber-Security-Attacken – als Dienstleistung zu beziehen

Heute sind gigantische Mengen an Unternehmens- und Personeninformationen auf unterschiedlichen Datenquellen (Netzwerke, Applikationen, Endgeräte, Social Media, Cloud, Darknet uvm.) verfügbar. Mit der stetig wachsenden Vernetzung und Digitalisierung wächst die Vielschichtigkeit der Bedrohungen. Eine zeitnahe Erkennung sicherheitsrelevanter Vorfälle ist essentiell.

Professionelles Threat Detection & Response erfordert spezifische Prozesse, Tools, langjährige Erfahrung sowie hochspezialisierte Mitarbeitende. Als einzelnes Unternehmen ist es kaum mehr möglich, die sich ständig ändernden Cyber-Security-Attacken zu verstehen und

[14] https://github.com/Neo23x0/sigma/

[15] https://yara.readthedocs.org

[16] https://github.com/Neo23x0/signature-base

entsprechend zu reagieren. Ein erfahrener Partner soll Unterstützung bieten. Swisscom schützt Netzinfrastruktur, Kunden- und Produktdaten sowie sich selbst seit Jahren erfolgreich gegen Cyber-Bedrohungen. Diese Erfahrungen nutzt sie, um gemeinsam mit Kunden Cyber-Risiken zu minimieren. Eine gute Visualisierung der Daten unterstützt die frühzeitige Erkennung potentieller Sicherheitsvorfälle. Die zeitnahe Analyse und die richtige Reaktion bei einem Security Incident verbessert das Sicherheitsniveau und die Ressourcenaufwendungen im Unternehmen.

Mit der Dienstleistung Threat Detection & Response können Unternehmenskunden zwischen vier Service-Ausprägungen wählen, je nachdem, wie weit Swisscom sie bezüglich Cyber Security unterstützen soll.
Hier eine kurze Übersicht:

Security Analytics as a Service: Kunden erhalten einen Überblick via Dashboard über potentielle Sicherheitsvorfälle aus definierten Log-Daten der Unternehmung.

Security Operation Center (SOC) as a Service: Zusätzlich zu Security Analytics erhalten Kunden Analysen mit konkreten Handlungsempfehlungen und einen direkten Zugriff auf die Spezialisten im SOC von Swisscom. Seit mehr als 10 Jahren erbringen wir SOC Dienstleistungen für Schweizer Unternehmen im In- und Ausland. Unsere SOC Analysten können Security Events & Incidents kompetent und schnell interpretieren.

Computer Security Incindent Response Team (CSIRT as a Service): Zur Analyse und Bewältigung von kritischen Sicherheitsvorfällen können Experten von Swisscom beigezogen werden, welche den Security Incident Management Prozess leiten. Diese erfahrenen Experten unterstützen Kunden bei der Beweissicherung sowie der Kommunikation zu Kunden und Partnern.

Threat Intelligence as a Service: Kunden werden proaktiv informiert über das Vorkommen von sensitiven Business- und Personeninformationen ihrer Unternehmung in öffentlichen und geschlossenen Netzen (z.B. Darknet).[17]

Fazit

Gezielte Angriffe, besonders von APTs mit staatlichen, strategischen Zielen, werden in den meisten Fällen nicht verhindert werden können. Die immer stärker digitalisierte Welt zieht zunehmend Akteure in den Cyber-Raum. Deshalb müssen wir immer mehr damit rechnen, zu einem bestimmten Zeitpunkt zum Target of Interest oder zumindest zum Target of Opportunity zu werden. Die Akteure haben eine Vielzahl an Vorgehensweisen in den unterschiedlichen Phasen des Angriffs zur Verfügung, für die sie immer mehr auf Off-the-Shelf Tools und Living-off-the Land Methoden zurückgreifen. APTs gehören zur Königsklasse der Cyber-Akteure, dennoch entwickeln sie nicht für jede Operation Zero Day Exploits, sondern greifen auf bewährte Methoden zurück, bei denen der Mensch weiterhin ein attraktives Ziel bleibt, um Sicherheitsmechanismen zu umgehen und Schadcode zur Ausführung zu bringen.

Es wird oft behauptet, dass Angreifer nur einmal Erfolg haben müssen um reinzukommen. Wie unsere Analyse gezeigt hat, können wir gegenargumentieren und sagen, dass wenn wir unsere Erkennungsmassnahmen so ausbauen, dass die Vorgehensweisen der Akteure erkannt werden, dann muss der Angreifer nur einen Fehler machen, um erkannt zu werden. Ein Fokus auf das Erkennen der Ausführung, die Execution Phase, ist hier ein vielversprechender Ansatz. Insbesondere aber bei APTs sollte der gesamte Intrusion Pattern verstanden sein bevor der Angriff gestoppt wird.

[17] Weitere Informationen und Kontaktinformationen dazu: www.swisscom.ch/detection