

Cyber Threat Intelligence – Angreifer und Angriffe verstehen

Threat Intelligence identifiziert Cyberbedrohungen, um daraus Sicherheitsmaßnahmen abzuleiten. In meiner Zeit bei der Spionageabwehr habe ich gesehen, wohin ein Mangel an Bedrohungsinformationen führen kann.

Von Sascha Herzog und Jörg Schauff



■ In meiner Zeit in einer Sicherheitsbehörde im Geschäftsbereich des Innenministeriums habe ich dutzende Fälle von Spionage gegen deutsche und internationale Regierungsstellen und die deutsche Wirtschaft untersucht. Ein Beispiel aus dieser Zeit soll zeigen, warum Threat Intelligence (TI), also jegliche Information über Bedrohungen, so wichtig ist. Das deutsche Hightechunternehmen, um das es geht, hatte zu dieser Zeit eine Antivirussoftware mit Hostfirewall von einem der seinerzeit größten AV-Hersteller auf seinen Windows-Systemen (Server und Clients) im Einsatz.

Einige dieser Maschinen wurden von einem – wahrscheinlich chinesischen – staatlichen Angreifer kompromittiert und es wurden Daten gestohlen. Bei der Untersuchung des Einbruchs stellte sich heraus, dass die Schadsoftware über Command-and-Control-Server (C2) gesteuert wurde, die schon über ein Jahr öffentlich als „maliziös“ bekannt waren. Ein Pastebin-User mit dem Pseudonym „RSA Employee #15666“ hatte über 850

C2-Domains mit IP-Adressen auf Pastebin aufgelistet und kontextualisiert. Er hatte also nicht nur beschrieben, dass die Domains und IPs schädlich sind, sondern konnte sie auch China zuordnen (Attribution). Aber offenbar hatte diese Information nicht den AV-Hersteller erreicht.

Hätte das betroffene Unternehmen einen Prozess gehabt, Daten mit Einbruchindikatoren (Indicators of Compromise, IoC-Feeds) als Ergänzung zum AV und zur Erstellung von Filtern auf der Perimeterfirewall oder dem Proxy zu nutzen, wäre der Angriff wahrscheinlich nicht erfolgreich gewesen oder hätte zumindest zu weniger Datenabfluss nach China geführt, da er nicht so lange unentdeckt geblieben wäre. Aktuelle und kontextualisierte IoCs sind eine wertvolle TI-Quelle.

Indicators of Compromise – Spuren eines Vorfalles

Ein IoC ist ein Indikator für einen erfolgreichen Angriff, für eine Kompromittierung

der eigenen Infrastruktur. Damit IoCs sinnvoll genutzt werden können, muss jemand sie erkennen und anderen zugänglich machen, etwa durch Integrieren in ein AV-Produkt. Sie sind also erst nach einem erfolgten Angriff (retrograd) nützlich und wesentlicher Bestandteil der taktischen Cyber Threat Intelligence (CTI).

Bei ihrer Nutzung ist darauf zu achten, dass die enthaltenen Informationen mit Metadaten und Kontext angereichert sind, zum Beispiel: Wann wurde ein Artefakt zuerst und wann zuletzt beobachtet (first seen / last seen), auf welcher Stufe der Kill Chain (siehe Glossar) befindet sich ein IoC, wer steckt dahinter (Attribution)? Welche Branchen (Relevanz) und welche Regionen sind betroffen? Dies ist notwendig, um den Menschen, die die auf der Basis von IoCs erzeugten Alarme auswerten, eine Einordnung des Angriffs zu ermöglichen: Steckt eine Ransomware-Gruppe hinter dem Angriff oder ist es eine nationalstaatliche Spionagegruppe aus Nordkorea oder dem Iran? Welche Tools setzen die Täter ein? Wie sehen typischerweise die Vorgehensweisen dieses Bedrohungsakteurs (Threat Actor) aus? Es geht also um deren Taktiken, Techniken und Vorgehensweisen (Tactics, Techniques and Procedures; siehe auch gleichnamigen Kasten).

Je nach Kontext ergeben sich dann unterschiedliche Risikobewertungen für ein Unternehmen, basierend auf den Bedrohungsakteuren (Threat Agents) und ihren TTPs, was wiederum unterschiedliche Maßnahmen und Abwehrstrategien zur Folge haben sollte.

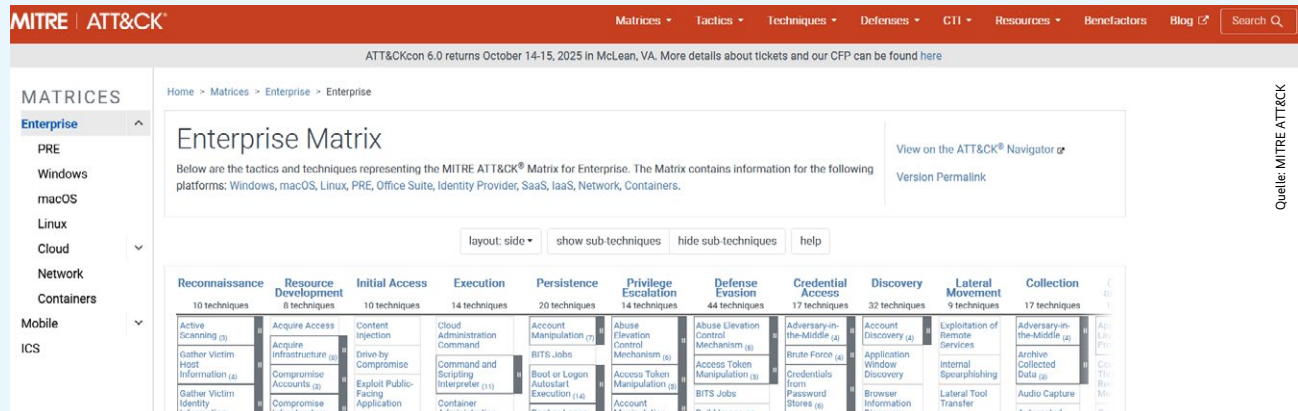
TRACT

- ▶ Threat Intelligence, also Informationen zu Cyberbedrohungen und -angriffen nebst Kontext, kann dabei helfen, Angriffe zu entdecken und einzudämmen.
- ▶ Das Wissen, welche Bedrohungsakteure auf welche Art gegen welche Ziele vorgehen, hilft dabei, sich aktiv auf einen Angriff vorzubereiten und diesen schneller durchzustehen.
- ▶ Manche Informationen, wie kriminell genutzte IP-Adressen oder bekannte Hashwerte, werden automatisiert erfasst und mit Ereignissen auf Systemen und im Netzwerk abgeglichen. Andere müssen erst aufwendig mit Kontext angereichert und bewertet werden. Beide sind für eine Angriffserkennung wertvoll.

Tactics, Techniques and Procedures (TTPs)

TTPs beschreiben das methodische Vorgehen von Angreifern in der Cybersicherheit. **Taktiken** sind die übergeordneten Ziele in einzelnen Angriffsphasen, **Techniken** beschreiben die konkreten Methoden zur Zielerreichung und **Vorgehensweisen (Procedures)** bedeuten die spezifische Umsetzung, die je nach Bedrohungsakteur variieren kann.

Cyber-TTPs helfen bei der Analyse von Angriffsmustern und der Entwicklung effektiver Abwehrstrategien. Bekannt sind die TTPs des MITRE-ATT&CK-Frameworks (siehe [ix.de/znam](https://www.ix.de/znam)), einer Wissensdatenbank zur Klassifizierung und Beschreibung von Cyberbedrohungen (Abbildung 1).



Das MITRE-ATT&CK-Framework klassifiziert bekannte Bedrohungen und hilft dadurch unter anderem bei der Analyse von Angriffen oder der Bewertung von Sicherheitsmaßnahmen (Abb. 1).

Zurück zu IoCs. Diese kann man stark vereinfacht auch als digitale Fingerabdrücke verstehen. Im realen Leben erstellt die Polizei Fingerabdrücke von Tätern, die man schon bei einer Tat erwischt hat, und kann sie mit Fingerabdrücken am Tatort abgleichen. Im Cyberspace entspricht das einem Datei-Hash, einer IP-Adresse oder anderen digitalen Merkmalen, die die Cybersicherheitscommunity als schädlich eingestuft hat.

Hase und Igel

IoCs wie File Hashes, IPs, Domains und Malwaresignaturen können jedoch auch ins Leere laufen, da fähige Angreifer verstärkt Bordmittel der Betriebssysteme, vorinstallierte Admin-Tools und legitime Internetinfrastrukturen für ihre Angriffe nutzen. Diese Techniken heißen „Living off the Land“. Varianten davon sind Living off the VPN und Living off the Foreign Land (Quellen zu diesen Angriffstechniken sind über [ix.de/znam](https://www.ix.de/znam) zu finden). Der Artikel „Living off the Land: Cyberangriffe ohne Malware“ ab Seite 44 geht vertieft auf diese Angriffskategorie ein.

Verteidiger müssen sich also mehr auf die durch Cyber Threat Intelligence (CTI) erkannten Vorgehensweisen der für sie relevanten Angreifergruppen konzentrieren, um auch LOTL-Angriffe abfangen zu können. Wenn man weiß, dass ein bestimmter Threat Actor mit dem in Windows integrierten Tool certutil.exe arbeitet, kann das verteidigende Blue Team (CSIRT, SOC, IT-Team) entweder dessen Verwendung auf den Windows-Clients sperren – ein normaler Benutzer

muss das Tool ohnehin nie einsetzen – oder eine Zugriffsüberwachung mittels System Access Control List (SACL) und Auditing (zum Beispiel über ein SIEM) einführen, um den Angreifer in eine Falle zu locken (Honeypot). Bei der Benutzung von certutil.exe ist dann sofort ein Alarm aktiv, da man von einem Angriff ausgehen muss, und das Blue Team kann entsprechend reagieren.

Um sich bestmöglich zu verteidigen, muss man regelmäßig mit Purple Teamings trainieren, also Simulationen mit einem angreifenden Red und einem verteidigenden Blue Team. Sie simulieren die einzelnen Kill Chains von Angreiferkampagnen möglichst realistisch und spielen sie durch. Das soll sicherstellen, dass ein solcher Angriff auch entdeckt und entsprechend schnell beendet wird.

Die großen W-Fragen: Wer, wie, was und warum

Nach heutigem Stand gibt es mehrere Tausend aktive kriminelle Hacker und Hackergruppen. Davon ist aber nur ein kleiner Teil für die eigene Organisation relevant – je nachdem, welche Bedrohungsakteure in der Region oder speziell gegen die eigene Branche agieren. Man muss sich zudem auf opportunistische Angriffe einstellen, also solche, die nicht zielgerichtet sind, sondern auf eine breite Masse zielen. Damit sowohl Blue Teams als auch Red Teams in einem Purple-Team-Training sinnvolle und zielführende Übungen durchführen können, müssen sie verstehen, wie welche Angreifer gegen welche Ziele in welchen Regionen und

mit welcher Motivation vorgehen (die W-Fragen). Diese Erkenntnisse erlangen die Spezialisten durch Cyber Threat Intelligence. Im Kasten sind die wichtigsten Kategorien der Bedrohungsakteure dargestellt.

Eine Definition von Cyber Threat Intelligence

Cyber Threat Intelligence bezeichnet das systematische Sammeln, Analysieren und Nutzen von Informationen über aktuelle und potenzielle Bedrohungen im Bereich der Cybersicherheit. Das Ziel von CTI ist, Organisationen ein besseres Verständnis für relevante Bedrohungsakteure, deren Taktiken, Techniken und Verfahren sowie für Schwachstellen und Angriffsmuster zu vermitteln. Welcher Angreifer geht mit welchen Methoden und welchen Werkzeugen gegen seine Ziele vor? CTI hilft dabei, fundierte Entscheidungen zur Verbesserung der Sicherheitslage zu treffen und proaktive Maßnahmen zu ergreifen. Sie trägt zum Lagebewusstsein (Situational Awareness) der Organisation bei.

CTI wird in verschiedenen Bereichen der Cybersicherheit eingesetzt und von unterschiedlichen Stakeholdern genutzt. Intelligence gibt es in verschiedenen Komplexitäts- und Detailstufen, die sich jeweils an unterschiedliche Zielgruppen richten und unterschiedliche Vorteile bieten. Die drei Haupttypen sind taktische, operative und strategische Intelligence. Von taktisch über operativ zur strategischen Aufklärung nimmt die Tiefe der Analyse und des Kontexts zu, wodurch

Die wichtigsten Typen von Bedrohungsakteuren

Nationalstaatliche Akteure wie Geheimdienste, militärische Einheiten et cetera, die im Dienst von Staaten stehen. Prominente Beispiele sind hier

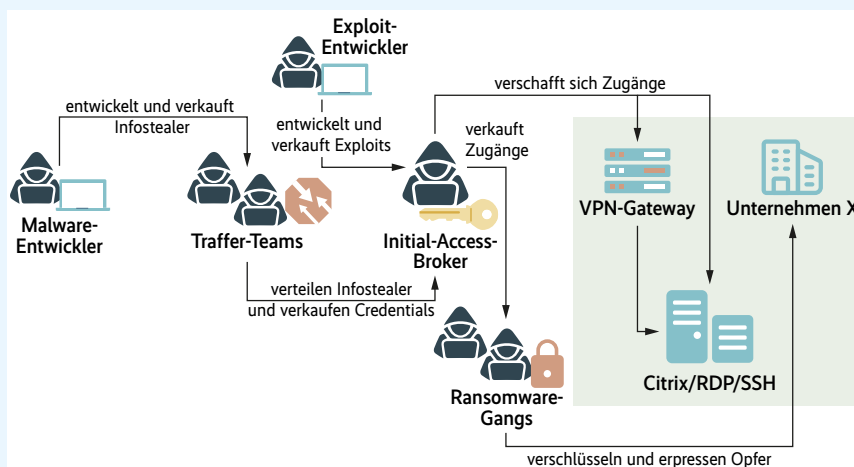
- aus Russland die Gruppe APT29 (Cozy Bear), bekannt für Hackingangriffe auf Microsoft, SolarWinds, die amerikanische Regierung und Dienststellen im deutschen Regierungsnetz;
- aus China Salt Typhoon, bekannt für die Kompromittierung von kritischen Infrastrukturen anderer Nationen, zum Beispiel Telekommunikationsnetzwerke;
- aus Nordkorea die Lazarus-Gruppe, bekannt für massive Angriffe auf Finanzinfrastrukturen und digitalen Bankraub in Milliardenhöhe.

Gruppen des organisierten Verbrechens wie Ransomware-Gangs, Crime-as-a-Service-Akteure, Initial-Access-Broker (IAB) und so weiter (Abbildung 2). Bekannte Beispiele sind

- LockBit, eine Ransomware-Gang aus dem russischsprachigen Raum und wahrscheinlich die bekannteste und erfolgreichste Ransomware-Gruppe mit Hunderten Partnergruppen (Affiliates);
- Scattered Spider, ein sehr kreatives und junges Hackerkollektiv aus Nordamerika, spezialisiert auf Social-Engineering-Angriffe, SMS-Betrug und moderne Cloud-Infrastrukturen;
- Raspberry Robin, Initial-Access-Broker, bekannt für massive und globale Initial-Access-Kampagnen mittels wurmartiger kreativer Techniken und Methoden.

Auftragshacker/Private-Sector Offensive Actors (PSOAs) sind oft für Nationalstaaten oder finanziell sehr starke Interessengruppen aus der Wirtschaft tätig. Einige Beispiele sind

- Intellexa, eine Allianz mehrerer PSOAs, die bekannt ist für die Predator-Spyware für Android- und iOS-Mobiltelefone; zum Konsortium gehören Nexa, WiSpear,



Grober Ablauf des Geschäftsmodells von Initial-Access-Brokern: In der arbeitsteiligen Schattenwelt des organisierten Verbrechens kann man nahezu jede Dienstleistung kaufen, in diesem Fall den initialen Zugang zu einem System. Auch der Initial-Access-Broker greift für seine Arbeit auf fremde Dienste zurück und bezieht beispielsweise Zugangsdaten und funktionierende Exploits von anderen Anbietern. So greift ein Rädchen ins andere, bis am Ende die Ransomware-Gangs Unternehmensdaten stehlen und verschlüsseln und die angegriffenen Unternehmen damit erpressen (Abb. 2).

- Cyrox und Senpai, die jeweils spezielle Fähigkeiten, etwa das Ausspähen von Zielen vor einem Angriff (OSINT), mitbringen;
- die NSO Group, ein PSOA aus Israel, bekannt für seine Pegasus-Spyware-Plattform, die auch zur Verfolgung von Journalisten eingesetzt wurde; die Firma ist weiterhin aktiv trotz Sanktionen aus den USA und der EU;
- Variston, ein PSOA aus Spanien, bekannt für die Entwicklung und den Vertrieb von „waffenfähigen“ Zero-Day-Exploits gegen Google Chrome, Microsoft Defender, Android und iOS. Für das Durchführen von Angriffen mit ihren Exploits kollaboriert Variston mit anderen PSOAs wie Protected AE.

Bei **Haktivisten** handelt es sich um politisch oder ideologisch motivierte Gruppen und Einzelpersonen. Zu den bekanntesten Gruppierungen gehören

- Anonymous, ein ideologisch getriebenes Hackerkollektiv, das nur lose zusammenhängt; bekannt ist es für DDoS-Attacken und Angriffe gegen große Unternehmenskonglomerate wie PayPal oder Regierungen und das Militär, wie bei der #OpRussia; die Ziele finden sich alle auf X (ehemals Twitter);
- NoName057, ein Hackerkollektiv aus Russland, das sich auf DDoS-Angriffe und Defacements spezialisiert hat. Vermutlich arbeitet NoName teilweise auch im Auftrag des russischen Staates.

Skript-Kiddies sind unerfahrenere Hacker, die sich beweisen oder ihren Ruf verbessern möchten.

Bei **böswilligen Insidern** handelt es sich häufig um (ehemalige) Mitarbeiter, Dienstleister oder Partner, oft aus der IT, die Informationen stehlen oder Schaden anrichten wollen.

jeder Typ bei der Erzeugung zunehmend ressourcenintensiver wird.

Taktische CTI bezieht sich auf technische Indikatoren (Indicators of Compromise) und Angriffsmethoden, die vor allem in Sicherheitssysteme integriert werden. Ziel ist es, konkrete technische Gegenmaßnahmen gegen diese IoCs einzusetzen. Beispiele für taktisch-technische CTI sind Hashwerte von Malware, IP-Adressen von Angreifern sowie Signaturen von Exploits. Zielgruppen hier-

für können Incident-Response-Teams, Threat-Intelligence-Analysten im SOC und Threat Hunter sein.

Die **operative CTI** liefert Bedrohungsanalysen, das heißt detaillierte Informationen über Bedrohungsakteure, deren TTPs und spezifische Kampagnen, um Angriffe besser und schneller verstehen zu können und dadurch frühestmöglich zu beenden. Dazu gehören beispielsweise die Zuschreibung (Attribution) zu Tätergruppen und ihre Profile, Analysen von

Angriffstechniken und Exploit-Methoden. Produziert wird diese CTI unter anderem für Incident-Response-Teams, Analysten im SOC und Red Teams.

Die **strategische CTI** dient der langfristigen Planung. Diese Intelligence enthält detaillierte Analysen über langfristige Cyberbedrohungen, deren Auswirkungen auf Organisationen, geopolitische Risiken, Berichte über Cyberkriegsführung, Wirtschaftsspionage und übergeordnete Trends in der Bedrohungslandschaft.

Wer braucht welche Cyber Threat Intelligence?

Art der CTI	Beschreibung	Zielgruppe
strategische CTI	detaillierte langfristige Bedrohungsanalysen, oft mit geopolitischem oder wirtschaftlichem Fokus	<ul style="list-style-type: none"> • Geschäftsführung • CISO • Risikomanagement • Behörden und Regulierer
operative CTI	Informationen über Angriffsvektoren, TTPs von Angreifern, konkrete Details zu Bedrohungsakteuren, Kampagnen und Exploits, oft aus Darknet-Quellen	<ul style="list-style-type: none"> • SOC-Teams • Incident Responder • CTI-Analysten • Forensikteams • Red/Purple Teams
taktisch-technische CTI	IoCs (Indicators of Compromise) wie Hashes, IP-Adressen, Domains, Signaturen	<ul style="list-style-type: none"> • SOC-Analysten • SIEM-Administratoren • Firewall- und IDS/IPS-Teams

CISOs, Vorstände, politische Entscheidungsträger, Regierungsbehörden und IT-Sicherheitsverantwortliche nutzen strategische CTI zur Planung und Priorisierung des Personaleinsatzes und der Umsetzung von Sicherheitsmaßnahmen.

Raw versus Finished Intelligence

Ein zentraler Aspekt der CTI ist der Unterschied zwischen unverarbeiteten (raw) und fertig analysierten (finished) Informationen. Das lässt sich vergleichen mit dem Einkauf von rohen Lebensmitteln und der notwendigen Zubereitung, bevor man sie konsumieren kann. Dieser Unterschied ist entscheidend für das Verständnis, wie CTI funktioniert und wie sie genutzt wird.

Raw Intelligence umfasst rohe, ungefilterte Daten, die direkt aus Quellen wie Netzwerkverkehr, Schadsoftware-Samples, Social-Media-Posts, Dark-Web-Foren oder Datenlecks stammen. Raw Intelligence ist oft schwer zu interpretieren, da sie keinen Kontext und keine Bewertung enthält. Ein Beispiel wäre eine Liste von IP-Adressen, die mit verdächtigen Login-Versuchen in Verbindung stehen, oder ein in der eigenen Infrastruktur gefundenes Fragment einer Schadsoftware, das ohne weitere Analyse wenig aussagt.

Raw Intelligence erfordert Fachkenntnisse, um sie nutzbar zu machen, und wird häufig als Ausgangspunkt für tiefer gehende Analysen verwendet. Ihr Wert liegt in ihrer Aktualität und Authentizität, aber sie ist für Entscheidungsträger oft schwer verständlich.

Ein Beispiel für Raw Intelligence ist die Data-Breach-Datenbank unseres Unternehmens NSIDE (Auszug siehe Abbildung 3). Die Daten stammen aus verschiedenen Darknet-Quellen wie Information-Stealer-Logs, die in Untergrundforen und speziellen Telegram-Kanälen getauscht und verkauft werden, und aus veröffentlichten oder geleakten Data-Breach-Vorfällen. Wir sammeln diese Daten, normalisieren sie aufwendig und indizieren sie in unserem leistungsstarken Elasticsearch-Cluster, um sie in Sekundenschnelle durchsuchbar zu machen.

Angreifer haben diese Daten auch und wir als Red-Team-Unternehmen, das Angreifer simuliert, nutzen diese Zugangsdaten, um uns Zugänge zu Computersystemen und Onlineplattformen unserer Kunden in deren Auftrag zu verschaffen. So können wir die Vorgehensweisen realer Bedrohungsakteure möglichst realistisch nachempfinden.

Daten aufwendig aufbereiten

Im Gegensatz dazu ist Finished Intelligence das Endergebnis eines Analyseprozesses, bei dem Raw Intelligence verarbeitet, kontextualisiert und in verständliche, handlungsrelevante Informationen

umgewandelt wird. Im Fall unserer Datenbank, wenn wir die Daten verifiziert und die Kritikalität für einen bestimmten Kunden bestimmt haben. Finished Intelligence enthält nicht nur Fakten, sondern auch Einschätzungen, Prognosen und Empfehlungen. Auch hier spielen einige „Ws“ eine wichtige Rolle: What (was ist passiert)? So what (warum berichtet der Analyst dazu, Relevant für den Stakeholder)? Und what's next (was ist die Handlungsempfehlung für den Stakeholder)?

Ein Beispiel zur Finished Intelligence wäre eine Threat-Intelligence- oder Bedrohungsanalyse, die beschreibt, dass eine bestimmte russische Tätergruppe, bekannt als TURLA, den europäischen Finanzsektor mit einer neuen Variante von Schadsoftware angreift. Sie enthält außerdem die verwendeten Techniken, mögliche Eintrittspunkte und empfohlene Gegenmaßnahmen wie proaktives Threat Hunting (siehe Glossar) basierend auf den IoCs und den TTPs aus der Analyse, Red-Team-Simulationen und Purple-Team-Trainings und schließlich die Priorisierung von System-Patches und Mitarbeiterschulungen. Die Finished Intelligence ist also für Führungskräfte, IT-Sicherheitsmanager und andere Stakeholder

Quelle: NSIDE Data-Breach-Datenbank

```
{
  "email": ["ge***@****.com"], "password": ["210***2147"]
},
{
  "email": ["ge***@****.com"], "password": ["hrt4***tt4"]
},
{
  "email": ["lg***@zjawn****.com"], "password": ["dIW***m8492"]
},
{
  "email": ["gw***@****.com"], "password": ["Surf***g1"]
},
{
  "email": ["ji***@****.com"], "password": ["196***626"]
},
{
  "email": ["jo***@****.com"], "password": ["123***03740"]
},
{
  "email": ["na***@****.com"], "password": ["MSL***0409"]
},
{
  "username": ["ck****"], "password": ["sone***81"], "url": ["https://my.***.com/webmail/"]
},
{
  "username": ["se***@****.com"], "password": ["20***engul"], "url": ["https://shop.***.com/my-account/login-or-register"]
},
{
  "username": ["pu***@****.com"], "password": ["P.a***ha29"], "url": ["https://account.acronis.com"]
},
{
  "username": ["na***@****.com"], "password": ["28***ncl"], "url": ["https://login***partner.com/"]
},
{
  "username": ["pa***@****.com"], "password": ["pas****"], "url": ["http://localhost:4200/home"]
},
{
  "username": ["aI***@****.com"], "password": ["Pau***virus"], "url": ["https://idmsa.apple.com/appleauth/auth/authorize/signin"]
},
{
  "username": ["DE****"], "password": ["Xpo***234"], "url": ["http://sap***.corp.***.com:50000/trj/portal"]
},
{
  "username": ["na***@****.com"], "password": ["283***cfl"], "url": ["https://login.*****.com/ndp/tdff/sso"]
},
{
  "username": ["8082****"], "password": ["Zl***3#"], "url": ["http://m***.corp.***.com"]
},
{
  "username": ["b***@****.com"], "password": ["Dm12****"], "url": ["https://suppl***.***.com/trj/portal"]
},
{
  "username": ["se****"], "password": ["fis***468"], "url": ["https://portal.*****.com/portal(bd***ZjPTA2MA=)/loginframe.htm"]
},
{
  "username": ["ck****"], "password": ["bek***452"], "url": ["http://my.*****.com/webmail/"]
},
{
  "email": ["ju***@****.com"], "password": ["Enil***501"]
},
{
  "email": ["sa***@****.com"], "password": ["1m***pace"]
},
{
  "email": ["fr***@****.com"], "password": ["CHA***922"]
},
{
  "email": ["na***@****.com"], "password": ["suh***uru"]
},
{
  "email": ["ys***@****.com"], "password": ["zan***oba"]
},
{
  "email": ["ya***@****.com"], "password": ["qu***qaka"]
},
{
  "email": ["ca***@****.com"], "password": ["nar***iec"]
},
{
  "email": ["je***@****.com"], "password": ["Some***3"]
},
{
  "email": ["ed***@****.com"], "password": ["eda9***078"]
},
{
  "email": ["ka***@****.com"], "password": ["rino***opi"]
},
{
  "email": ["ro***@****.com"], "password": ["ml***ey-1"]
},
{
  "email": ["na***@****.com"], "password": ["R9***708"]
},
{
  "email": ["so***@****.com"], "password": ["chi***ie"]
},
{
  "email": ["ja***@****.com"], "password": ["Bar***ra1"]
}

[*] Found 7.892 results
[*] Wrote results to ./****.com/****.out
[*] Searching took 10.24 seconds
[*] 21.126.767.502 documents were searched
```

Mit den (hier anonymisierten) gestohlenen Zugangsdaten eines Unternehmens aus unserer Darknet-Datenbank können wir Angriffe simulieren, wie sie wirklich stattfinden, und daraus Schutzmaßnahmen ableiten (Abb. 3).

direkt nutzbar und bildet die Grundlage für strategische und operative Entscheidungen.

TURLA – ein Beispiel aus der Praxis

TURLA ist unter anderem bekannt für Spionage gegen Außenministerien. Als Verantwortlicher für die IT-Sicherheit im diplomatischen Umfeld muss man sich nun mit den IoCs, den TTPs und den bekannten Zielen von TURLA auseinandersetzen. Hier stellt sich als erste Frage, wie und wo TURLA ihre Angriffe beginnt. Die CTI kann das beantworten: unter anderem mit Watering-Hole-Attacks (siehe Glossar) durch für Diplomaten relevante Webseiten, zum Beispiel die Presse-Webseiten in Hauptstädten und in den Städten, in denen sich Konsulate im Gastland befinden. Hier müssen Analysten über die eigentlichen Fakten hinausdenken, um gezielt nach erfolgten und unentdeckten Angriffen und möglichen Angriffsvektoren zu suchen.

Die nächste Frage, die man an die CTI stellen kann, ist die nach potenziellen Zielpersonen, die für Cyberangriffe aus TURLA-Sicht von Wert sind. Hier lautet die Antwort: Mitarbeiter in der IT einer Botschaft, eines Konsulats und in Bildungseinrichtungen, die von Diplomatenkindern besucht werden. Daraus folgt, dass der IT-Sicherheitsverantwortliche die entsprechenden Webseiten nach Kompromittierungen durch TURLA untersuchen muss. TURLA-Watering-Holes wurden beispielsweise in den Webseiten privater Schulen in Berlin und Control-Panels einer deutschen Schule im Ausland beobachtet. So helfen aufbereitete Informationen dabei, die Risiken im Zusammenhang mit einer bestimmten Angreifergruppe einzudämmen.

Wie entstehen IoC-Feeds?

Viele Anbieter verkaufen Threat Intelligence in Form von IoC-Feeds. Wie werden diese kommerziellen Feeds erzeugt? Zum weitaus größten Teil automatisch. Nur ein geringer Teil wird manuell durch Recherchen oder Schadsoftwareanalyse erzeugt. Somit kann nur das, was ein Hersteller in seinen Daten beobachtet hat, auch in seinen Feeds landen. Oft ist es so, dass Angreifer, insbesondere nationalstaatliche Gruppen aus Russland und China, zwar unterschiedliche Schadsoftware in unterschiedlichen Kampagnen verwenden, aber die vielen zugehörigen Command-and-Control-Domains auf relativ wenige IP-Adressen verteilen. Wenn man

Glossar

Attribution (Zuschreibung): Der Prozess, durch den die Identität oder die Herkunft eines Cyberangriffs ermittelt wird, um den Verantwortlichen zu identifizieren.

Blue Team (BT): Eine Gruppe von Sicherheitsexperten, die für den Schutz und die Verteidigung eines Netzwerks oder Systems gegen Cyberangriffe verantwortlich ist.

Command and Control (C2): Ein Kommunikationskanal, über den Angreifer Malware steuern und Daten von infizierten Systemen abrufen können.

(Cyber) Kill Chain: Ein Modell, das die Phasen eines Cyberangriffs beschreibt, von der Aufklärung bis zur Ausführung. Es bildet die Basis dafür, Sicherheitsmaßnahmen zu entwickeln.

Data Breach: Ein Vorfall, bei dem unbefugter Zugriff auf sensible Daten erfolgt, was zu deren Offenlegung oder Verlust führt.

Endpoint Detection and Response (EDR) System: Eine Sicherheitslösung, die Endgeräte überwacht, Bedrohungen erkennt und darauf reagiert, um Angriffe zu verhindern.

Initial-Access-Broker (IAB): Ein Akteur, der an Cyberkriminelle den Zugang zu kompromittierten Netzwerken verkauft oder vermietet.

Information Stealer (Infostealer): Malware, die darauf abzielt, sensible Informationen wie Passwörter oder Kreditkartendaten von einem infizierten System zu stehlen.

Purple Team: Kombination aus Red Team und Blue Team, die zusammenarbeitet, um Sicherheitslücken zu identifizieren und zu schließen.

Red Team (RT): Eine Gruppe von Sicherheitsexperten, die simulierte Angriffe auf ein System oder Netzwerk durchführt, um Schwachstellen zu identifizieren.

Security Operation Center (SOC): Eine zentrale Einheit, die Sicherheitsereignisse überwacht, analysiert und darauf reagiert, um die IT-Sicherheit zu gewährleisten.

Security Incident and Event Management (SIEM) System: sammelt und analysiert Sicherheitsereignisse in Echtzeit, um Bedrohungen zu erkennen und darauf zu reagieren.

Threat Hunting: Der proaktive Prozess, bei dem Sicherheitsexperten nach Anzeichen von Bedrohungen in einem Netzwerk suchen, um potenzielle Angriffe frühzeitig zu erkennen.

Watering-Hole-Angriffe: Eine Angriffstechnik, bei der Angreifer eine Website kompromittieren, die häufig von einer bestimmten Zielgruppe besucht wird, um Malware zu verbreiten.

nun Domains von Angreifern aus Blogs, Reports und behördlichen Warnungen (von BKA, BSI oder BfV) mit historischen und aktuellen DNS-Einträgen abgleicht, kann man händisch IoCs finden, die den kommerziellen Anbietern aufgrund ihrer Arbeitsweise entgangen sind, und diese zur Eigensicherung und zum Teilen in Sharing-Communitys verwenden.

Jeder Hersteller hat unterschiedliche Marktanteile in bestimmten Regionen und Branchen, beispielsweise im Automobilbau in Deutschland oder im öffentlichen Dienst in Skandinavien. Man braucht einen Antivirus- beziehungsweise EDR-Anbieter (Endpoint Detection and Response), der in dem für die Organisation relevanten Sektor und der Region einen ausreichend großen Marktanteil hat. Idealerweise verfügt er noch über ein eigenes CTI-Team, das neben den Informationen dieses einen Herstellers weitere Informationen aus anderen Quellen bezieht und auswertet.

Der Übergang von Raw Intelligence zu Finished Intelligence erfordert mehrere Schritte, darunter Datenkorrelation, Bedrohungsbewertung, Trendanalyse sowie die Integration von Kontextinformationen wie geopolitischen Entwicklungen oder Branchentrends. Dieser Prozess

macht CTI zu einem dynamischen und wertvollen Werkzeug in der Cybersicherheit. (ur@ix.de)

Quellen

Das MITRE-ATT&CK-Framework und Informationen zu einigen Angriffen sind über [ix.de/znam](https://www.ix.de/znam) zu finden.

SASCHA HERZOG



ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.

JÖRG SCHAUFF



ist Head of Threat Intelligence bei NSIDE. Seine Erfahrungen mit Threat Intelligence sammelte er unter anderem beim deutschen Bundesamt für Verfassungsschutz in der Abteilung Spionageabwehr.