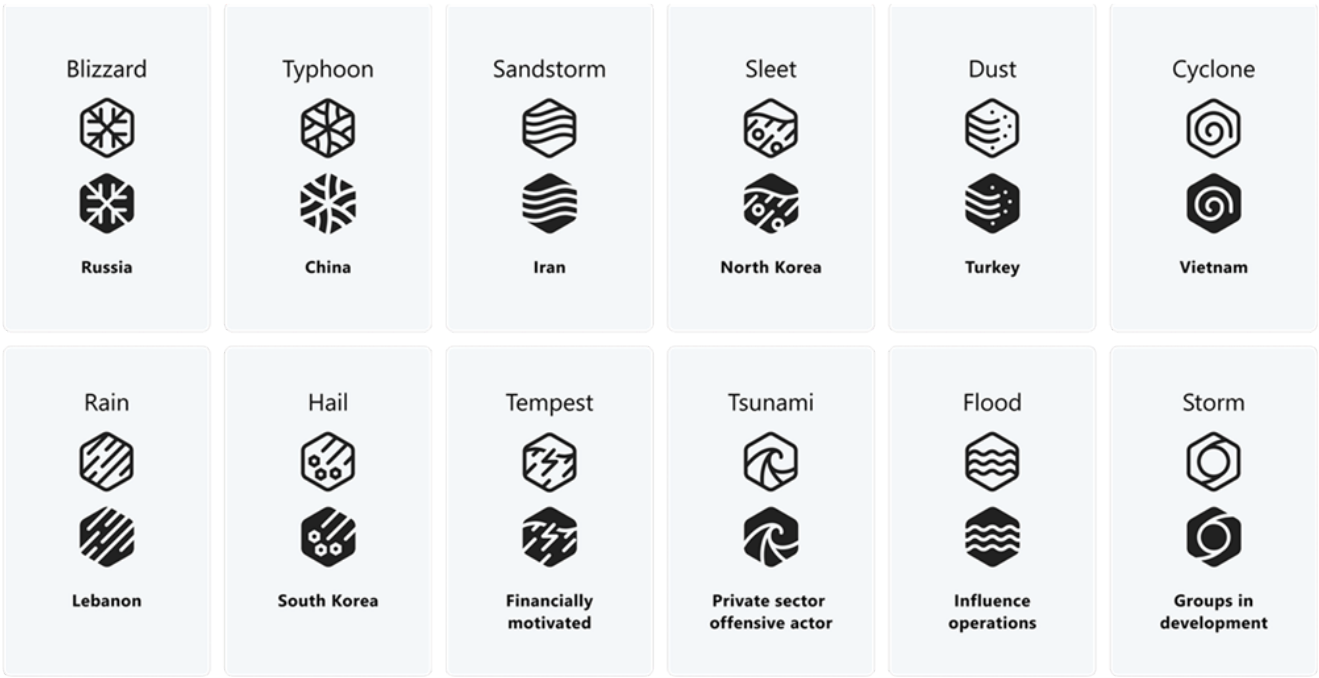
Wie Microsoft Bedrohungsakteure benennt

learn.microsoft.com/de-de/microsoft-365/security/intelligence/microsoft-threat-actor-naming

- Artikel
- 04/21/2023
-

In diesem Artikel

Microsoft hat sich auf eine neue Benennungstaxonomie für Bedrohungsakteure umgestellt, die auf das Thema Wetter ausgerichtet ist. Mit der neuen Taxonomie beabsichtigen wir, Kunden und anderen Sicherheitsforschern, die bereits mit einer überwältigenden Menge an Threat Intelligence-Daten konfrontiert sind, mehr Klarheit zu schaffen und eine besser organisierte, artikulierte und einfachere Möglichkeit zu bieten, auf Bedrohungsakteure zu verweisen, damit Organisationen sich selbst besser priorisieren und schützen können.



Microsoft kategorisiert Bedrohungsakteure in fünf Schlüsselgruppen:

Nationalstaatliche Akteure: Cyber-Operatoren, die im Auftrag oder unter der Leitung eines nationalen/staatsorientierten Programms handeln, unabhängig davon, ob es sich um Spionage, finanzielle Gewinne oder Vergeltung handelt. Microsoft hat festgestellt, dass die meisten nationalen Staatlichen Akteure weiterhin Operationen und Angriffe auf Regierungsbehörden, zwischenstaatliche Organisationen, nichtstaatliche Organisationen und Think Tanks für traditionelle Spionage- oder Überwachungsziele konzentrieren.

Finanziell motivierte Akteure: Cyberkampagnen/Gruppen, die von einer kriminellen organization/Person mit Beweggründen finanzieller Gewinne geleitet werden und nicht mit großem Vertrauen zu einem bekannten Nicht-Nationalstaat oder einer kommerziellen Entität in Verbindung gebracht wurden. Diese Kategorie umfasst Ransomware-Operatoren, Geschäftliche E-Mail-Kompromittierung, Phishing und andere Gruppen mit rein finanziellen oder erpressten Beweggründen.

Private Sector Offensive Actors (PSOAs): Cyberaktivitäten, die von kommerziellen Akteuren geleitet werden, die bekannte/legitime juristische Personen sind, die Cyber-Geräte erstellen und an Kunden verkaufen, die dann Ziele auswählen und die Cyber-Geräte betreiben. Diese Instrumente bedrohen viele globale Menschenrechtsbemühungen, da sie beobachtet wurden, um Regimekritiker, Menschenrechtsverteidiger, Journalisten, Anwälte der Zivilgesellschaft und andere Privatpersonen zu unterstützen.

Beeinflussen von Vorgängen: Informationskampagnen, die auf manipulative Weise online oder offline kommuniziert werden, um Wahrnehmungen, Verhaltensweisen oder Entscheidungen von Zielgruppen zu verschieben, um die Interessen und Ziele einer Gruppe oder Nation zu fördern.

Gruppen in der Entwicklung: Eine vorübergehende Bezeichnung für eine unbekannte, sich entwickelnde oder sich entwickelnde Bedrohungsaktivität, die es Microsoft ermöglicht, sie als diskreten Satz von Informationen nachzuverfolgen, bis wir ein hohes Maß an Vertrauen in Bezug auf den Ursprung oder die Identität des Akteurs hinter dem Vorgang erreichen können. Sobald die Kriterien erfüllt sind, wird eine Gruppe in der Entwicklung in einen benannten Akteur konvertiert oder in vorhandene Namen zusammengeführt.

In unserer neuen Taxonomie stellt ein Wetterereignis oder *familienname* eine der oben genannten Kategorien dar. Im Falle nationalstaatlicher Akteure haben wir einem Herkunftsland einen Familiennamen zugewiesen, der an die Zuordnung gebunden ist, z. B. Tipphoon gibt Herkunft oder Zuordnung zu China an. Für andere Akteure stellt der Familienname eine Motivation dar. Tempest weist beispielsweise auf finanziell motivierte Akteure hin. Bedrohungsakteure innerhalb derselben Wetterfamilie erhalten ein Adjektiv, um Akteurgruppen mit unterschiedlichen Taktiken, Techniken und Verfahren (TTPs), Infrastruktur, Zielen oder anderen identifizierten Mustern zu unterscheiden. Für Gruppen in der Entwicklung, in denen ein neu entdeckter, unbekannter, sich entwickelnder Cluster mit Bedrohungsaktivitäten vorhanden ist, verwenden wir eine temporäre Bezeichnung storm und eine vierstellige Zahl, sodass wir sie als eindeutigen Satz von Informationen nachverfolgen können, bis wir ein hohes Maß an Vertrauen in den Ursprung oder die Identität des Akteurs hinter dem Vorgang erreichen können.

Die folgende Tabelle zeigt, wie die neuen Familiennamen einer Stichprobe der von uns nachverfolgten Bedrohungsakteure zugeordnet werden.

Actor-Kategorie	Typ	Familienname
Nationalstaat	China Iran Libanon Nordkorea Russland Südkorea Türkei Vietnam	Taifun Sandsturm Regen Graupel Blizzard Hagel Staub Zyklon
Finanziell motiviert	Finanziell motiviert	Tempest
Offensive Akteure des Privatsektors	PSOAs	Tsunami
Beeinflussen von Vorgängen	Beeinflussen von Vorgängen	Flut
Gruppen in der Entwicklung	Gruppen in der Entwicklung	Sturm

Verwenden Sie die folgende Referenztabelle, um zu verstehen, wie sich unsere zuvor veröffentlichten alten Namen von Bedrohungsakteurn in unsere neue Taxonomie übersetzen.

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
ACTINIUM	Aqua Blizzard	Russland	UNC530, Primitiver Bär, Gamaredon
AMERICIUM	Rosa Sandsturm	Iran	Agrius, Deadwood, BlackShadow, SharpBoys
BARIUM	Messing-Taifun	China	APT41
BISMUT	Canvas Cyclone	Vietnam	APT32, OceanLotus
BOHRIUM	Rauchsandsturm	Iran	
BROM	Ghost Blizzard	Russland	Energetischer Bär, kauernder Yeti
CER	Ruby Sleet	Nordkorea	
CHIMBORAZO	Spandex Tempest	Finanziell motiviert	TA505
CHROM	Holzkohle-Typhoon	China	ControlX
COPERNICIUM	SaphirLeet	Nordkorea	Genie Spider, BlueNoroff

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
CURIUM	Crimson Sandstorm	Iran	TA456, Schildkröte Shell
DUBNIUM	Zickzack-Hagel	Südkorea	Dark Hotel, Tapaoux
ELBRUS	Sangria Tempest	Finanziell motiviert	Carbon Spider, FIN7
EUROPIUM	Haszel Sandsturm	Iran	Cobalt Gypsy, APT34, OilRig
GADOLINIUM	Gingham Typhoon	China	APT40, Leviathan, TEMP. Periskop, Kryptonit Panda
GALLIUM	Granit-Typhoon	China	
HAFNIUM	Seidentyphoon	China	
HOLMIUM	Pfirsich Sandsturm	Iran	APT33, Raffiniertes Kätzchen
IRIDIUM	Seashell Blizzard	Russland	Sandwurm
KNÜPFERWES	Denim Tsunami	Offensivakteur des Privatsektors	DSIRF
KRYPTON	Geheimer Schneesturm	Russland	Giftbär, Turla, Schlange
LAWRENCIUM	Pearl Sleet	Nordkorea	
MANGAN	Maulbeeren-Typhoon	China	APT5, Keyhole Panda, TABCTENG
QUECKSILBER	Mango Sandsturm	Iran	MuddyWater, SeedWorm, Static Kitten, TEMP. Zagros
NEPTUNIUM	Baumwollsandsturm	Iran	Vice Leaker
NICKEL	Nylon-Typhoon	China	ke3chang, APT15, Vixen Panda
NOBELIUM	Midnight Blizzard	Russland	APT29, Gemütlicher Bär
OSMIUM	Opalleet	Nordkorea	Konni
PARINACOTA	Wein-Tempest	Finanziell motiviert	Wadhrama

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
PHOSPHOR	Mint Sandstorm	Iran	APT35, Charmantes Kätzchen
PLUTONIUM	Onyx Sleet	Nordkorea	Silent Chollima, Andariel, DarkSeoul
POLONIUM	Plaid Rain	Libanon	
RADIUM	Raspberry-Typhoon	China	APT30, LotusBlossom
RUBIDIUM	Zitronensandsturm	Iran	Fox Kitten, UNC757, PioneerKitten
SEABORGIUM	Star Blizzard	Russland	Callisto, Team wiederverwenden
SILICON	Marmorierter Staub	Türkei	Meeresschildkröte
SOURGUM	Karamell-Tsunami	Offensivakteur des Privatsektors	Candiru
SPURR	Tomaten-Tempest	Finanziell motiviert	Vatet
STRONTIUM	Wald-Schneesturm	Russland	APT28, Fancy Bear
TAAL	Camouflage Tempest	Finanziell motiviert	FIN6, Skeleton Spider
THALLIUM	Smaragdleet	Nordkorea	Kimsuky, Samt Chollima
ZINK	Diamantleet	Nordkorea	Labyrinth Chollima, Lazarus
ZIRKONIUM	Violetter Typhoon	China	APT31

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
DEV-0146	Kürbissandsturm	Iran	ZeroCleare
DEV-0193	Periwinkle Tempest	Finanziell motiviert	Wizard Spider, UNC2053
DEV-0196	Carmine Tsunami	Offensivakteur des Privatsektors	QuaDream
DEV-0198 (NEPTUNIUM)	Baumwollsandsturm	Iran	Vice Leaker

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
DEV-0206	Senf Tempest	Finanziell motiviert	Violetter Vallhund
DEV-0215 (LAWRENCIUM)	Pearl Sleet	Nordkorea	
DEV-0227 (AMERICIUM)	Rosa Sandsturm	Iran	Agrius, Deadwood, BlackShadow, SharpBoys
DEV-0228	Kuboider Sandsturm	Iran	
DEV-0234	Lilac Typhoon	China	
DEV-0237	Pistazien-Tempest	Finanziell motiviert	FIN12
DEV-0243	Manatee Tempest	Finanziell motiviert	EvilCorp, UNC2165, Indrik Spider
DEV-0257	Storm-0257	Gruppe in Entwicklung	UNC1151
DEV-0322	Kreistyphoon	China	
DEV-0336	Nacht-Tsunami	Offensivakteur des Privatsektors	NSO-Gruppe
DEV-0343	Grauer Sandsturm	Iran	
DEV-0401	Zimt-Sturm	Finanziell motiviert	Kaiser-Libelle, Bronze Starlight
DEV-0500	Ringelblume Sandsturm	Iran	Moses Staff
DEV-0504	Samt-Tempest	Finanziell motiviert	
DEV-0530	Storm-0530	Nordkorea	H0lyGh0st
DEV-0537	Erdbeer-Sturm	Finanziell motiviert	LAPSUS$
DEV-0586	Cadet Blizzard	Russland	
DEV-0605	Wisteria Tsunami	Offensivakteur des Privatsektors	CyberRoot
DEV-0665	Sunglow Blizzard	Russland	

Vorheriger Name	Neuer Name	Ursprung/Bedrohung	Andere Namen
DEV-0796	Phlox Tempest	Finanziell motiviert	ClickPirate, Chrome-Ladeprogramm, Choziosi-Ladeprogramm
DEV-0832	Vanilla Tempest	Finanziell motiviert	
DEV-0950	Spitze Tempest	Finanziell motiviert	FIN11, TA505

Weitere Informationen finden Sie in unserer Ankündigung zur neuen Taxonomie: https://aka.ms/threatactorsblog

Intelligenz in die Hände von Sicherheitsexperten geben

Intel-Profile in Microsoft Defender Threat Intelligence wichtige Erkenntnisse von Bedrohungsakteur direkt in die Hände der Verteidiger bringen, damit sie den Kontext abrufen können, den sie benötigen, wenn sie sich auf Bedrohungen vorbereiten und darauf reagieren.

Um die Threat Intelligence, die Sie von Microsoft erhalten, weiter zu operationalisieren, bietet die Microsoft Defender Threat Intelligence Intel Profiles-API die aktuellste Sichtbarkeit der Infrastruktur für Bedrohungsakteur in der Branche, sodass Teams von Threat Intelligence und Sicherheitsvorgängen (SecOps) ihre erweiterten Workflows zur Bedrohungssuche und -analyse optimieren können. Weitere Informationen zu dieser API finden Sie in der Dokumentation: Verwenden der Threat Intelligence-APIs in Microsoft Graph (Vorschauversion).

Ressourcen

Verwenden Sie die folgende Abfrage für Microsoft 365 Defender und andere Microsoft-Sicherheitsprodukte, die die Kusto-Abfragesprache (KQL) unterstützen, um Informationen zu einem Bedrohungsakteur mithilfe des alten Namens, des neuen Namens oder des Branchennamens abzurufen:

```
let TANames = externaldata(PreviousName: string, NewName: string, Origin: string,
OtherNames: dynamic)
[@"https://raw.githubusercontent.com/microsoft/mstic/master/PublicFeeds/ThreatActorNa
ming/MicrosoftMapping.json"] with(format="multijson",
ingestionMapping='[{"Column":"PreviousName","Properties":{"Path":"$.Previous name"}},
{"Column":"NewName","Properties":{"Path":"$.New name"}},
{"Column":"Origin","Properties":{"Path":"$.Origin/Threat"}},
{"Column":"OtherNames","Properties":{"Path":"$.Other names"}}]');
let GetThreatActorAlias = (Name: string) {
TANames
| where Name =~ NewName or Name =~ PreviousName or OtherNames has Name
};
GetThreatActorAlias("ZINC")
```

Die folgenden Dateien, die die umfassende Zuordnung alter Bedrohungsakteurnamen mit ihren neuen Namen enthalten, sind ebenfalls verfügbar:

- JSON-Format
- Herunterladbares Excel