Aktive APT-Gruppen in Deutschland

Übersicht über APT-Gruppen, die Ziele in Deutschland angreifen
Stand: 28.01.2026

Cyberangriffe, die nicht finanziell motiviert sind, sondern strategische Ziele verfolgen, sind in der Regel keine isolierten Einzelereignisse. Stattdessen stehen langfristig operierende und hartnäckige Angreifergruppen dahinter, die bestimmte Angriffsziele immer wieder angreifen. Die Angreifergruppen prägen so die Bedrohungslage. Da die Angreifergruppen mindestens temporär bestimmte strategische Ziele verfolgen, wird die Bedrohungslage zu einem gewissen Teil besser erklärbar, als wenn es sich um rein opportunistische Zufallsereignisse handeln würde. Die Kenntnis der Angreifergruppen und ihrer aktuellen Ziele ermöglicht es IT-Sicherheitsteams, das Risikoprofil des eigenen Unternehmens oder der eigenen Institution besser zu bewerten.

Das BSI stellt daher auf dieser Seite die Angreifergruppen vor, die in den letzten zwei Jahren gegen Ziele in Deutschland aktiv waren, oder die im europäischen Ausland Ziele angriffen, die so oder auf ähnliche Weise auch in Deutschland hätten angegriffen werden können. Aufgeführt wird der Gruppenname, ggf. mit Alias-Bezeichnungen, die Sektoren, in denen die Gruppe aktiv ist, und ggf. besondere Eigenschaften, die die Detektion oder Vorfallsbereinigung beeinflussen können.

Dadurch soll die Bedrohungslage durch strategisch agierende Angreifergruppen dokumentiert werden. Institutionen, die die Basismaßnahmen der IT-Sicherheit bereits umgesetzt haben, können die Gruppenliste verwenden, um ihre eigenen Threat Intelligence-Recherchen zu priorisieren.

Die Quellen für die Liste sind vielfältig, beispielsweise Detektionen in den Regierungsnetzen, Vorfälle aus der BSI-Vorfallsbearbeitung, sowie Meldungen von Partnern und Betroffenen. Die Liste ist dabei nicht notwendigerweise vollständig, beispielsweise falls Vertraulichkeitsvereinbarungen auf Wunsch der Betroffenen oder Quellen bestehen. Zudem existiert naturgemäß eine gewisse Dunkelziffer, umso mehr, je professioneller und heimlicher die Angreifergruppen vorgehen. Insbesondere bei fortschrittlichen Angreifern kann sowohl die Detektion erschwert werden, als auch eine Zuordnung zu einer benannten Gruppe offen bleiben, was dazu führt, dass die entsprechenden Angriffe in der Liste nicht erscheinen.

Da sich trotz aller Persistenz die strategischen Ziele und Auftragslagen von Angreifergruppen über die Zeit ändern, ist die Liste nicht statisch, sondern wird je nach Einschätzung des BSI zu den Gruppen angepasst.

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
APT15 Vixen Panda /	• Öffentliche Verwaltung	Die Gruppe nutzt eigene Verschleierungsnetzwerke aus

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
Mirage / Ke3chang / Nylon Typhoon		kompromittierten Routern und VPN-Servern.
APT28 Fancy Bear / Sofacy / Forest Blizzard	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung • Erbringung von Dienstleistungen der Informationstechnologie • Erbringung von sonstigen Dienstleistungen für die Luftfahrt • Öffentliche Verwaltung • Politische Parteien und sonstige Vereinigungen	APT28 nutzt diverse Angriffsvektoren, z. B. • Outlook-Schwachstelle CVE-2023-23397 (via E-Mail) • WinRAR-Schwachstelle CVE-2023-38831 (via E-Mail-Anhang) • Bruteforcing und Password-Spraying gegen erreichbare Server
APT29 Cozy Bear / Nobelium / Midnight Blizzard	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung • Erbringung von Dienstleistungen der Informationstechnologie • Öffentliche Verwaltung • Politische Parteien und sonstige Vereinigungen	Um im legitimen Internetverkehr nicht aufzufallen, nutzt APT29 oft legitime Cloud-Dienste als Kontrollserver.

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
APT43 Velvet Chollima / Kimsuky / Emerald Sleet	• Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunstwissenschaften • Herstellung von Waffen und Munition • Luft- und Raumfahrzeugbau • Öffentliche Verwaltung • Rechtsberatung • Tertiärer und post-sekundärer, nicht tertiärer Unterricht	Die Gruppe betreibt Social Engineering und versendet zunächst mehrere Emails ohne Schadcode, bis der Empfänger schließlich Vertrauen aufgebaut hat. Erst dann wird Schadcode oder ein Phishing-Link übermittelt.
APT 44 / Sandworm / Seashell Blizzard / Voodoo Bear		
Bitter / Hazy Tiger	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung	Der Angriffsvektor sind meistens CHM- oder RAR-Mailanhänge.
Charming Kitten / APT42 / Mint Sandstorm	• Öffentliche Verwaltung	
Contagious Interview / Beaver Tail / Invisible Ferret / Famous Chollima	• Mit Finanzdienstleistungen verbundene Tätigkeiten	Die Angreifer geben sich als Job-Bewerber oder Programmier-Freelancer aus, um Zugang zum Zielnetzwerk zu erhalten.

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
Cosmic Wolf / Sea Turtle / Marbled Dust	• Erbringung von Dienstleistungen der Informationstechnologie	Die Täter kompromittieren mitunter zunächst Zwischenziele, um Informationen für Folge-Angriffe auf die eigentlichen Ziele zu erlangen.
Cruel Jackal / MoleRats / WIRTE	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung	Die Täter versenden u. a. maliziöse LNK-Dateien, die in Archivdateien (wie RAR) enthalten sind.
Dark Hotel	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung	
Labyrinth Chollima / Lazarus / Diamond Sleet	• Erbringung von Dienstleistungen der Informationstechnologie	Als Angriffsvektor dienen oft Emails mit maliziösen Dokumenten zu vermeintlichen Jobangeboten.
Mirage Tiger	• Öffentliche Verwaltung	
Muddy Water / Static Kitten / Mango Sandstorm	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung • Öffentliche Verwaltung	
Mustang Panda	• Öffentliche Verwaltung	
Outrider Tiger Fishing Elephant	• Öffentliche Verwaltung	
Red Dev 61 / UTA0178 / UNC5221	• Öffentliche Verwaltung	Die Angriffe richten sich typischerweise gegen VPN-Systeme und andere Perimeter-Systeme.

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
	• Wirtschaftsförderung, -ordnung und -aufsicht	
Rezet / Rare Wolf / Librarian Ghouls	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung • Güterbeförderung in der See- und Küstenschifffahrt	Angriffsvektor besteht im Versand von passwortgeschützten RAR-Datei, die ausführbare Dateien mit doppelter Dateiendung enthalten.
RomCom / Storm-0978	• Öffentliche Verwaltung	
Salted Earth / Sturgeon Fisher / Yoro Trooper	• unbekannt	
Salt Typhoon	• diverse	Die Gruppe kompromittiert u. a. schlecht gewartete Perimeter-Systeme. Die Motivation und Zielauswahl für Deutschland ist bislang unklar.
Sidewinder / Razor Tiger	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung	
Snake / Venomous Bear / Turla / Secret Blizzard	• Öffentliche Verwaltung	
Viceroy Tiger / Donot	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung • Öffentliche Verwaltung	

Gruppenname und Aliase	**Wirtschaftszweig in Deutschland nach WZ 2008**	**Besondere Eigenschaften**
Winter Vivern / TAG-70	• Forschung und Entwicklung im Bereich Rechts-, Wirtschafts- und Sozialwissenschaften sowie im Bereich Sprach-, Kultur- und Kunstwissenschaften	
UAC-0050	• Auswärtige Angelegenheiten, Verteidigung, Rechtspflege, öffentliche Sicherheit und Ordnung	Die Täter versenden ZIP-Archive als Mail-Anhänge, in der die öffentlich verfügbare Malware Remcos enthalten ist.

Zusätzlich stehen beim BSI aufgrund von Vorfällen im benachbarten EU-Ausland unter Beobachtung:

- APT30 / Naikon / Raspberry Typhoon
- APT31 / Judgment Panda / Violet Typhoon
- Gallium / Softcell / Phantom Panda / Alloy Taurus / Granite Typhoon

---