Active APT groups in Germany

06.02.2024

Cyber attacks that are not financially motivated but pursue strategic goals are usually not isolated individual events. Instead, there are long-term, persistent threat actors who repeatedly attack specific targets. The threat actors thus shape the threat situation. Since these attacker groups pursue certain strategic goals, the threat situation becomes to a certain extent easier to explain than if it were purely opportunistic random events. Knowing the threat actors and their current targets allows IT security teams to better assess the risk profile of their own company or institution.

On this page, the BSI presents the threat actor groups that have been active against targets in Germany in the last two years, or that have attacked targets in other European countries that could also have been attacked in Germany in a similar manner. The following table lists the threat actors‘ name with aliases, the sectors in which the thret actor is active and, if relevant, special characteristics that can facilitate detection or incident handling.

Institutions that have already implemented basic IT security measures can use this list to prioritize their own threat intelligence research.

The sources for the list are diverse, for example detections in government networks, incidents from BSI incident handling, as well as reports from partners and victims. The list is not necessarily complete, for example if confidentiality agreements exist at the request of victims or sources. In addition, there should be a certain number of unreported cases, the more professional and secretive the threat actors are. Especially in the case of advanced attackers, detection can be made more difficult and attribution to a named threat actor can remain unclear, which means that the corresponding attacks do not appear in the list.

Since the strategic goals and missions of threat actors change over time, the list is not static, but will be updated depending on the BSI's assessment.

Active APT groups that attack targets in Germany:

Threat actor and alias	Sectors, according to German WZ 2008	Characteristics
APT15 Vixen Panda / Mirage / Ke3chang	• Administration of the State and the economic and social policy of the community	The threat actor uses its own relay network of compromised routers and VPN servers.
APT28 Fancy Bear / Sofacy	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community	APT28 uses a variety of attack vectors, e. g. • Outlook-vulnerability CVE-2023-23397 (via email) • WinRAR-vulnerability CVE-2023-38831 (via email-attachment) • Bruteforcing and password-spraying against internet-facing serversOutlook-Schwachstelle CVE-2023-23397 (via E-Mail)
APT29 Cozy Bear / Nobelium	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community	APT29 often uses legitimate cloud services as control servers, in order to blend into legitimate network traffic.
APT43 Velvet Chollima / Kimsuky	• Research and experimental development on social sciences and humanities • Administration of the State and the economic and social policy of the community • Higher education	The threat actor engages in social engineering and initially sends several emails without malicious code until the recipient has built up trust. Only then will malicious code or a phishing link be delivered.

Threat actor and alias	Sectors, according to German WZ 2008	Characteristics
Bitter / Hazy Tiger	• Provision of services to the community as a whole	Attack vector usually are CHM- or RAR-attachments.
Cosmic Wolf / Sea Turtle	• Computer programming, consultancy and related activities	The threat actor may compromise a supply-chain entity first, in order to gather information for follow-up attacks on the intended targets.
Earth Estries	• unknown	
Gamaredon	• Provision of services to the community as a whole	The threat actor continually registers a large number of phishing-domains and sets up new servers.
Ghostwriter / UNC1151	• unspecific	The threat actor targets private email-accounts at commercial webmail-providers via spearphishing.
Labyrinth Chollima Lazarus	• Computer programming, consultancy and related activities	
Mirage Tiger	• Administration of the State and the economic and social policy of the community	
Mustang Panda	• Administration of the State and the economic and social policy of the community	
Outrider Tiger Fishing Elephant	• Administration of the State and the economic and social policy of the community	
Red Dev 61 / UTA0178 / UNC5221	• Administration of the State and the economic and social policy of the community	The attacks are usually targeted against VPN- and other internet-facing systems.

Threat actor and alias	Sectors, according to German WZ 2008	Characteristics
RomCom	• Administration of the State and the economic and social policy of the community	
Salted Earth / Sturgeon Fisher / Yoro Trooper	• unknown	
Sharp Panda	• Administration of the State and the economic and social policy of the community	
Snake / Venomous Bear / Turla	• Administration of the State and the economic and social policy of the community	
Storm-0558	• Research and experimental development on social sciences and humanities	The threat actor uses their own VPN-networks in order to obfuscate their attack traffic.
Viceroy Tiger / Donot	• Provision of services to the community as a whole • Administration of the State and the economic and social policy of the community	
Winter Vivern / TAG-70	• Research and experimental development on social sciences and humanities	
UAC-0050	• Provision of services to the community as a whole	The threat actor sends ZIP-archives as email attachments, containing the publicly available malware Remcos.

Furthermore, BSI observes the following threat actors because of their activity in partner countries:

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