Threat Agents/Groups Detected

For selected Attack Patterns

Domains (attack-pattern--40f5caa0-4cb7-4117-89fc-d421bb493df3) (T1583.001)
Email Accounts (attack-pattern--65013dd2-bc61-43e3-afb5-a14c4fa7437a) (T1585.002)
Tool (attack-pattern--a2fdce72-04b2-409a-ac10-cc1695f4fce0) (T1588.002)
Malware (attack-pattern--7807d3a4-a885-4639-a786-c1ed41484970) (T1588.001)
Spearphishing Link (attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7) (T1566.002)
Spearphishing Attachment (attack-pattern--2e34237d-8574-43f6-aace-ae2915de8597) (T1566.001)
Match Legitimate Name or Location (attack-pattern--1c4e5d32-1fe9-4116-9d9d-59e3925bd6a2) (T1036.005)
Pass the Hash (attack-pattern--e624264c-033a-424d-9fd7-fc9c3bbdb03e) (T1550.002)
LSASS Memory (attack-pattern--65f2d882-3f41-4d48-8a06-29af77ec9f90) (T1003.001)
Data from Local System (attack-pattern--3c4a2599-71ee-4405-ba1e-0e28414b4bc5) (T1005)
System Service Discovery (attack-pattern--322bad5a-1c49-4d23-ab79-76d641794afa) (T1007)
System Network Configuration Discovery (attack-pattern--707399d6-ab3e-4963-9315-d9d3818cd6a0) (T1016)
Remote Desktop Protocol (attack-pattern--eb062747-2193-45de-8fa2-e62549c37ddf) (T1021.001)
System Network Connections Discovery (attack-pattern--7e150503-88e7-4861-866b-ff1ac82c4475) (T1049)
Process Discovery (attack-pattern--8f4a33ec-8b1f-4b80-a2f6-642b2e479580) (T1057)
Local Account (attack-pattern--25659dd6-ea12-45c4-97e6-381e3e4b593e) (T1087.001)

APT1 (G0006): 92.54%

[APT1](https://attack.mitre.org/groups/G0006) is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

stix id: intrusion-set--6a2e693f-24e5-451a-9f88-b36a108e5662

Aliases: APT1, Comment Crew, Comment Group, Comment Panda

Domains: enterprise-attack

x_mitre_version: 1.4

Kimsuky (G0094): 4.61%

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky](https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group]

(https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups.

stix id: intrusion-set--0ec2f388-bf0f-4b5c-97b1-fc736d26c25f

Aliases: Kimsuky, Black Banshee, Velvet Chollima, Emerald Sleet, THALLIUM

Domains: enterprise-attack

x_mitre_version: 4.0

Lazarus Group (G0032): 0.62%

[Lazarus Group](https://attack.mitre.org/groups/G0032) is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. (Citation: US-CERT HIDDEN COBRA June 2017)(Citation: Treasury North Korean Cyber Groups September 2019) The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by [Lazarus Group](https://attack.mitre.org/groups/G0032) correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.(Citation: Novetta Blockbuster) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group] (https://attack.mitre.org/groups/G0032) instead of tracking clusters or subgroups, such as [Andariel](https://attack.mitre.org/groups/G0138), [APT37] (https://attack.mitre.org/groups/G0067), [APT38](https://attack.mitre.org/groups/G0082), and [Kimsuky](https://attack.mitre.org/groups/G0094).

stix id: intrusion-set--c93fccb1-e8e8-42cf-ae33-2ad1d183913a

Aliases: Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Diamond Sleet

Domains: enterprise-attack, ics-attack

x_mitre_version: 4.0

Magic Hound (G0059): 0.62%

[Magic Hound](https://attack.mitre.org/groups/G0059) is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, likely on behalf of the Islamic Revolutionary Guard Corps. They have targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), via complex social engineering campaigns since at least 2014.(Citation: FireEye APT35 2018)(Citation: ClearSky Kittens Back 3 August 2020) (Citation: Certfa Charming Kitten January 2021)(Citation: Secureworks COBALT ILLUSION Threat Profile)(Citation: Proofpoint TA453 July2021)

stix id: intrusion-set--f9d6633a-55e6-4adc-9263-6ae080421a13

Aliases: Magic Hound, TA453, COBALT ILLUSION, Charming Kitten, ITG18, Phosphorus, Newscaster, APT35, Mint Sandstorm

Domains: enterprise-attack

x_mitre_version: 6.0

Earth Lusca (G1006): 0.23%

[Earth Lusca](https://attack.mitre.org/groups/G1006) is a suspected China-based cyber espionage group that has been active since at least April 2019. [Earth Lusca] (https://attack.mitre.org/groups/G1006) has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency trading platforms; security researchers assess some [Earth Lusca](https://attack.mitre.org/groups/G1006) operations may be financially motivated. (Citation: TrendMicro EarthLusca 2022) [Earth Lusca](https://attack.mitre.org/groups/G1006)

has used malware commonly used by other Chinese threat groups, including [APT41](https://attack.mitre.org/groups/G0096) and the [Winnti Group](https://attack.mitre.org/groups/G0044) cluster, however security researchers assess [Earth Lusca](https://attack.mitre.org/groups/G1006)'s techniques and infrastructure are separate. (Citation: TrendMicro EarthLusca 2022)

stix id: intrusion-set--cc613a49-9bfa-4e22-98d1-15ffbb03f034

Aliases: Earth Lusca, TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Domains: enterprise-attack, mobile-attack

x_mitre_version: 2.0