Threat Actor Groups Tracked by Palo Alto Networks Unit 42 (Updated Aug. 1, 2025)

By Unit 42

Published: 2025-08-01 · Archived: 2026-04-02 12:38:37 UTC

Nation-State Threat Actor Groups

Unit 42 considers the following groups to have a motivation that is primarily state-backed rather than financial. There can also be some cybercrime motivation for threat groups in this category, but we believe their main motivation is in furthering the interest of their sponsoring nation.

Draco – Pakistan

Draco, the dragon, is the constellation chosen for threat actor groups from Pakistan. These groups have been seen targeting India and other South Asian countries.

Mocking Draco

Also Known As

G1008, sidecopy, unc2269, white dev 55

Summary

Mocking Draco is a Pakistan-based threat actor that has been operating since at least 2019, mainly targeting South Asian countries and more specifically India and Afghanistan. Their malware’s common name, Sidecopy, comes

from its infection chain that tries to mimic the malware SideWinder. This actor has reported similarities with Opaque Draco and is possibly a subdivision of this actor.

Sectors Impacted

Mocking Draco has previously impacted organizations in the following sectors:

- Government

Opaque Draco

Also Known As

APT36, C-Major, Cmajor, COPPER FIELDSTONE, Fast-Cargo, G0134, Green Halvidar, Havildar Team, Lapis, Mythic Leopard, ProjectM, Transparent Tribe

Summary

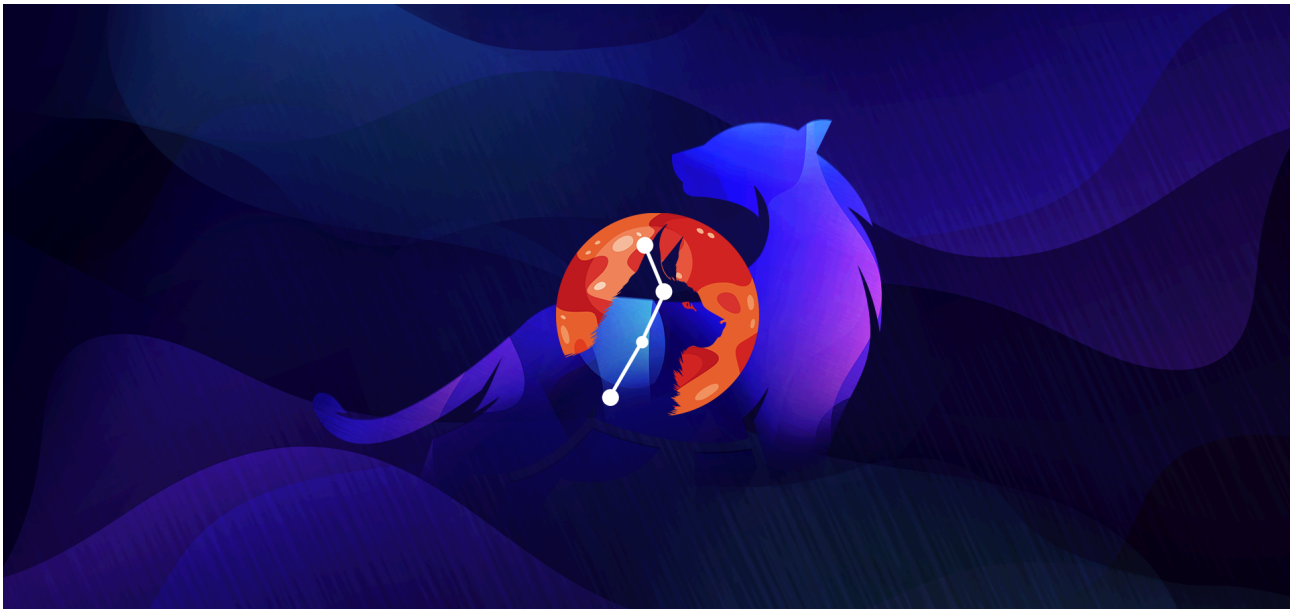
Opaque Draco is a Pakistan-based threat group that has been active since 2013. They primarily target Indian governmental, military and educational sectors.

Sectors Impacted

Opaque Draco has previously impacted organizations in the following sectors:

- Education
- Government
- Military

Lynx – Belarus



Belarusian threat groups are named for the constellation Lynx.

White Lynx

Also Known As

Ghostwriter, Storm-0257, UNC1151

Summary

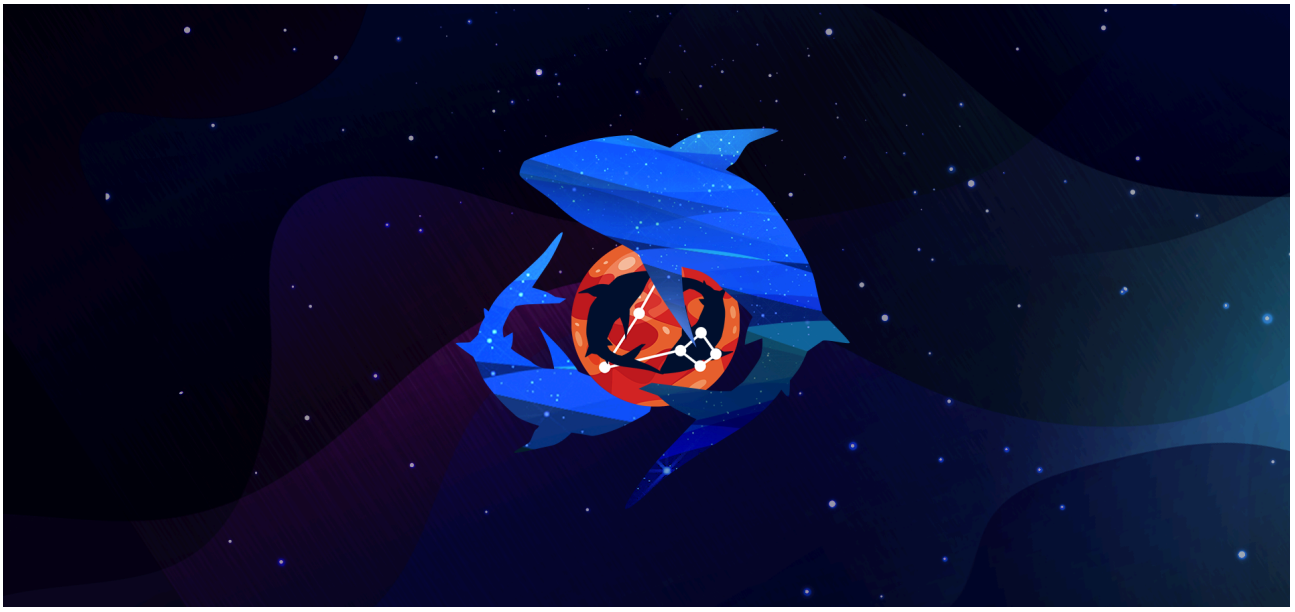
White Lynx is a nation-state threat actor assessed with high confidence to be linked with the Belarusian government. Their main focus is on countries neighboring Belarus, such as Ukraine, Lithuania, Latvia, Poland and Germany. Their targeting also includes Belarusian dissidents, media entities and journalists.

Sectors Impacted

White Lynx has previously impacted organizations in the following sectors:

- Construction
- Education
- Federal Government
- Healthcare
- High Technology
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Wholesale and Retail

Pisces – North Korea



Threat actor groups attributed to North Korea are represented by the constellation Pisces. These groups have impacted many industries with a focus on cyberespionage and financial crime.

Jumpy Pisces

Also Known As

Andariel, Black Artemis, COVELLITE, Onyx Sleet, PLUTONIUM, Silent Chollima, Stonefly, UNC614, Lazarus, Lazarus Group

Summary

Jumpy Pisces is a nation-state threat actor associated with the notorious Lazarus Group and the Democratic People's Republic of Korea (DPRK). Jumpy Pisces is believed to be a subgroup of the Lazarus group that branched out around 2013. The group has demonstrated a high degree of adaptability, complexity and technical expertise in its operations, with a focus on cyber espionage, financial crime and ransomware attacks.

Jumpy Pisces primarily targets South Korean entities with a variety of attack vectors, including spear phishing, watering hole attacks and supply chain attacks. They have been observed exploiting vulnerabilities in various software, including asset management programs and known but unpatched public services, to distribute its malware. The group also abuses legitimate software and proxy and tunneling tools for its malicious activities.

Sectors Impacted

Jumpy Pisces has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Financial Services
- Government
- Healthcare

- IT Services
- Manufacturing
- Pharma and Life Sciences
- Utilities and Energy

Slow Pisces

Also Known As

Dark River, DEV-0954, Jade Sleet, Storm-0954, Trader Traitor, TraderTraitor, UNC4899, Lazarus, Lazarus Group

Summary

Slow Pisces is North Korea's nation state threat group under Reconnaissance General Bureau (RGB) of DPRK. It's believed to be a spin-off from the Lazarus group with focus on financial gathering and crypto industry targeting goals. Their primary task since 2020 is generating revenue for the DPRK regime and they do so by targeting organizations that handle large volumes of cryptocurrency. They have reportedly stolen in excess of $1 billion in 2023 alone.

Secondary to revenue generation, Slow Pisces has also compromised aerospace, defense and industrial organizations, likely with the aim of espionage to advance DPRK’s military capabilities.

Sectors Impacted

Slow Pisces has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Cryptocurrency Industry
- Financial Services
- High Technology

Serpens – Iran

Iranian-attributed groups are named for the constellation Serpens, the snake. Our research on these groups highlights their targets and TTPs as they evolve.

Academic Serpens

Also Known As

COBALT DICKENS, DEV-0118, Mabna Institute, Silent Librarian, Yellow Nabu

Summary

Academic Serpens is a state-sponsored group active since at least 2013 that is attributed to Iran, which has traditionally focused on Middle Eastern targets and Nordic universities in the EU. Members of Academic Serpens are affiliated with the Iran-based Mabna Institute, which has conducted cyber intrusions at the behest of the government of Iran, specifically the Islamic Revolutionary Guard Corps (IRGC). They have targeted research and proprietary data at universities, government agencies and private sector companies worldwide. There has been a notable decrease in activity from this group since the international COVID crisis in 2020.

Sectors Impacted

Academic Serpens has previously impacted organizations in the following sectors:

- Education
- Government

Agent Serpens

Also Known As

Mint Sandstorm (Microsoft), Charming Kitten (Crowdstrike)

APT35, Ballistic Bobcat, Cobalt Illusion, Damselfly, Direfate, G0059, Greycatfish, Group 83, Iridium Group, ITG18, Magic Hound, Newscaster, Phosphorus, Saffron Rose, TA453, White Phosphorous, Yellow Garuda

Summary

Agent Serpens is a suspected nation-state threat actor the threat intelligence community attributes to Iran, with links to the Islamic Revolutionary Guard Corps (IRGC). It has been active since at least 2015.

Agent Serpens is known for sophisticated social engineering (especially spear phishing), malware development and persistent, adaptive tactics. The group uses a diverse and evolving toolkit to facilitate all stages of their attacks, from initial access to command and control (C2). This includes custom-developed backdoors like SnailResin, SlugResin and Sponsor, which the threat actors designed to be used for gaining persistent access and data exfiltration.

The group's arsenal also features credential harvesting kits such as GCollection and DWP, which enable the theft of email user accounts. Agonizing Serpens abuses legitimate tools like PowerShell to deploy tools like AnvilEcho, TAMECAT and CharmPower that enable malicious activities within compromised environments.

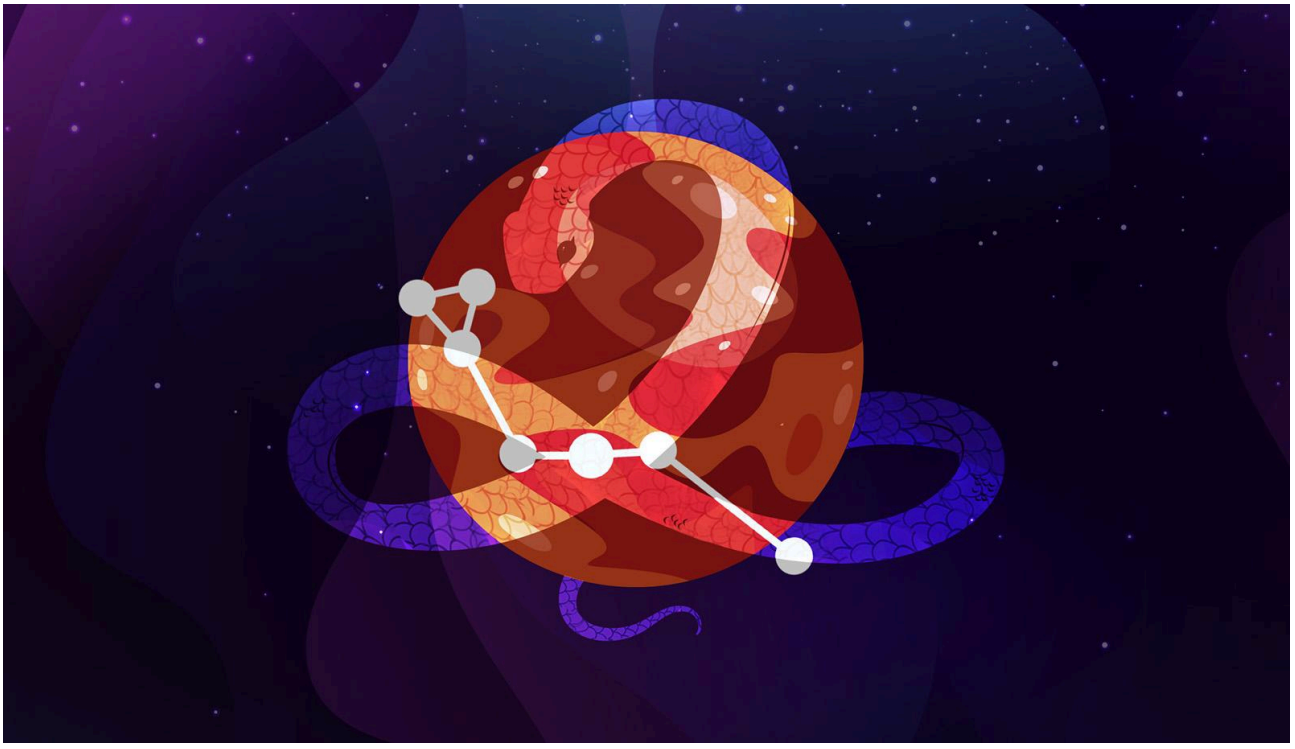
The group's use of Android malware like PINEFLOWER demonstrates an interest in mobile surveillance, likely for monitoring targets and gathering intelligence. Additionally, Agent Serpens incorporates readily available open-source tools like Mimikatz, Chisel and Plink to augment their capabilities and support different phases of their operations.

Sectors Impacted

Agent Serpens has previously impacted organizations in the following sectors:

- Automotive
- Civil Engineering
- Colleges And Universities
- Education
- Federal Government
- Financial Services
- Healthcare
- Higher Education
- High Technology
- Manufacturing
- Media and Entertainment
- Noncommercial
- Research Organizations
- Pharmaceutical and Life Sciences
- Telecommunications

Agonizing Serpens



Also Known As

Pink Sandstrom (Microsoft), Spectral Kitten (CrowdStrike)

Agrius, Americium, Black Shadow, Blackshadow, Cobalt Shadow, Darkrypt, UNC2428, Yellow Dev 21

Summary

Agonizing Serpens is a suspected nation-state threat actor attributed to Iran. This group has primarily disrupted Israeli organizations since 2020, and is linked to attacks throughout the Middle East. The group's modus operandi involves strategically exfiltrating sensitive data before deploying destructive ransomware and wiper malware to disrupt systems and cover their tracks. This group has targeted organizations in the education, technology and financial sectors.

Sectors Impacted

Agonizing Serpens has previously impacted organizations in the following sectors:

- Education
- Financial Services
- Insurance
- IT Services
- Nonclassifiable Establishments
- Professional and Legal Services
- Wholesale and Retail

Boggy Serpens

Also Known As

Mango Sandstorm (Microsoft), Static Kitten (CrowdStrike)

Cobalt Ulster, Earth Vetala, G0069, Mercury, Muddywater, Seedworm, Temp.Zagros, Yellow Nix

Summary

Active since at least 2017, Boggy Serpens is an Iranian, state-sponsored, cyberespionage group that US Cyber Command has attributed to Iran's Ministry of Intelligence and Security (MOIS).

The group's primary objective is cyberespionage aligned with Iranian government interests. This includes intelligence gathering, operational disruption and responding to regional conflicts, particularly those involving Israel.

Sectors Impacted

Boggy Serpens has previously impacted organizations in the following sectors:

- Financial Services
- Healthcare
- Insurance
- Telecommunications
- Transportation and Logistics

Devious Serpens

Also Known As

Cobalt Fireside, Curium, G1012, Imperial Kitten, Tortoiseshell, Yellow Liderc

Summary

Devious Serpens are an Iranian-based threat actor known for using social engineering tactics as well as malware that communicates via IMAP. Their attacks use watering hole attacks as well as their own controlled sites meant to impersonate employment opportunities that might interest their victims.

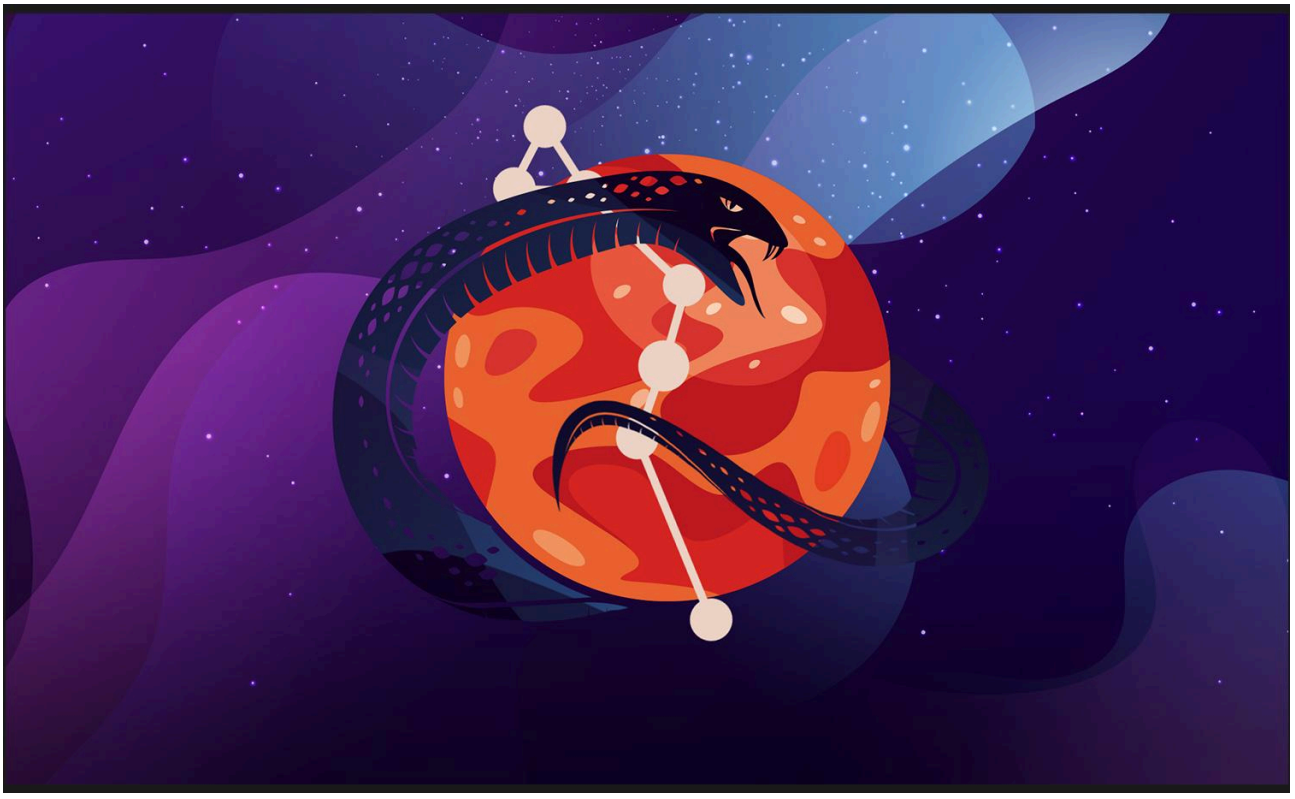
The malware that they have built often uses IMAP with specific email addresses for command and control (C2). With such tools, communication typically occurs via specific folders and message protocols on the C2 email address.

Sectors Impacted

Devious Serpens has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Information Technology Services

Evasive Serpens



Also Known As

Alibaba, APT34, Chrysene, Cobalt Gypsy, Crambus, Europium, G0049, Group 41, Hazel Sandstorm, Helix Kitten, IRN2, OilRig, Powbat, TEMP.Akapav, Twisted Kitten, Yossi

Summary

Evasive Serpens is a threat group Unit 42 discovered in May 2016. They are a nation-state threat group attributed to Iran. This threat group is extremely persistent and relies heavily on spear phishing as their initial attack vector. However, they have also been associated with other more complex attacks such as credential harvesting campaigns and DNS hijacking.

In their spear phishing attacks, Evasive Serpens preferred macro-enabled Microsoft Office (Word and Excel) documents to install their custom payloads that came as portable executables (PE), PowerShell and VBScripts. The group's custom payloads frequently used DNS tunneling as a C2 channel.

Sectors Impacted

Evasive Serpens has previously impacted organizations in the following sectors:

- Chemical Manufacturing
- Financial Services
- Government
- Telecommunications
- Utilities and Energy

Taurus – China

Chinese threat actor groups take their name from the constellation Taurus – the bull. Due to the long history and multiplicity of Chinese APTs, there is a lot to be discovered about these groups in our research archives.

Alloy Taurus

Also Known As

Granite Typhoon (Microsoft), Phantom Panda (CrowdStrike)

G0093, Gallium, Operation Soft Cell, Othorene, Red Dev 4

Summary

Alloy Taurus has been active since at least 2012 and is a suspected nation-state threat actor group attributed to China.

The group is known for its long-term cyberespionage campaigns, primarily targeting telecommunications companies, government entities and financial institutions across Southeast Asia, Europe and Africa. Their operations are characterized by multi-wave intrusions aimed at establishing persistent footholds within compromised networks.

Alloy Taurus gains initial access by exploiting vulnerabilities in internet-facing applications.

Alloy Taurus employs a range of custom and modified malware for multiple operating systems to enhance their espionage capabilities, move laterally and evade detection. This includes backdoors, web shells, credential harvesting tools as well as legitimate applications, such as VPN and remote management tools.

Sectors Impacted

Alloy Taurus has previously impacted organizations in the following sectors:

- Federal Government
- Financial Services
- State and Local Government
- Telecommunications
- Transportation and Logistics

Charging Taurus

Also Known As

Circle Typhoon, DEV-0322, TGR-STA-0027, Tilted Temple

Summary

Charging Taurus is a state-sponsored cyberespionage group attributed to China, active since 2021. The group's goal is to steal intellectual property aligned with China's national interests. The group is capable of exploiting undisclosed zero-day vulnerabilities. The group has a possible tie to Insidious Taurus.

Sectors Impacted

Charging Taurus has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Biotechnology
- High Technology
- Semiconductor Industry

Dicing Taurus

Also Known As

Jackpot Panda

Summary

Dicing Taurus is a state-sponsored group attributed to China. They focus on the illegal online gambling sector in Southeast Asia, particularly emphasizing data collection for monitoring and countering related activities in China. The i-Soon leak in February 2024 revealed that i-Soon was likely involved in Dicing Taurus's operations, along with the Ministry of Public Security of China.

The group is also responsible for distributing a trojanized installer for CloudChat, a chat application popular with Chinese-speaking illegal gambling communities in mainland China. The trojanized installer served from CloudChat’s website contained the first stage of a multi-step process.

Sectors Impacted

Dicing Taurus has previously impacted organizations in the following sectors:

- Online Gambling
- Software and Technology

Digging Taurus

Also Known As

BRONZE HIGHLAND, Daggerfly, Evasive Panda, StormBamboo

Summary

Digging Taurus is a suspected nation-state threat group attributed to China, which has been active since at least 2012. The group targets organizations from around the world, including those in Taiwan, Hong Kong, Mainland China, India and Africa. Their activities, including intelligence collection, align with Chinese interests. This group has targeted organizations with advanced malware frameworks like MgBot and CloudScout. They strategically use different initial access vectors, including supply-chain attacks and DNS poisoning.

Sectors Impacted

Digging Taurus has previously impacted organizations in the following sectors:

- Computer Integrated Systems Design
- Executive Offices
- General Government Administration
- Local Government
- Nonprofit
- Telecommunications

Insidious Taurus

Also Known As

BRONZE SILHOUETTE, DEV-0391, UNC3236, Vanguard Panda, Volt Typhoon, Voltzite, G1017

Summary

Insidious Taurus is a Chinese state-sponsored actor typically focusing on espionage and information gathering, active since 2021. Insidious Taurus evades detection by using various living-off-the-land (LotL) techniques, using in-built system tools to perform their objectives and blend in with regular system noise.

The actor leverages compromised small office/home office (SOHO) network devices as intermediate infrastructure to further obscure their activity. Insidious Taurus exploits vulnerabilities in internet-facing devices and systems as an initial access vector.

Sectors Impacted

Insidious Taurus has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Information Technology Services
- Manufacturing
- Telecommunications
- Transportation and Logistics
- Utilities

Jumper Taurus

Also Known As

APT40, BRONZE MOHAWK, Electric Panda, Gadolinium, Gingham Typhoon, IslandDreams, Kryptonite Panda, Ladon, Leviathon, Pickleworm, Red Ladon, TEMP.Jumper, TEMP.Periscope

Summary

Jumper Taurus is a state-sponsored cyberespionage group believed to be linked to the Chinese government. Active since at least 2013, the group has consistently demonstrated advanced tactics, techniques and procedures (TTPs), supporting China's strategic objectives in sensitive research or holding strategic geopolitical relationships.

The group's operations use phishing emails and exploit web server vulnerabilities for initial access. The group has shown a particular interest in maritime-related targets, those associated with China's naval modernization efforts and the Belt and Road Initiative.

Sectors Impacted

Jumper Taurus has previously impacted organizations in the following sectors:

- Education
- Financial Services
- Government
- Healthcare
- Utilities and Energy

Nuclear Taurus

Also Known As

Bronze Vapor, Chimera, G0114, Red Charon, THORIUM, Tumbleweed Typhoon

Summary

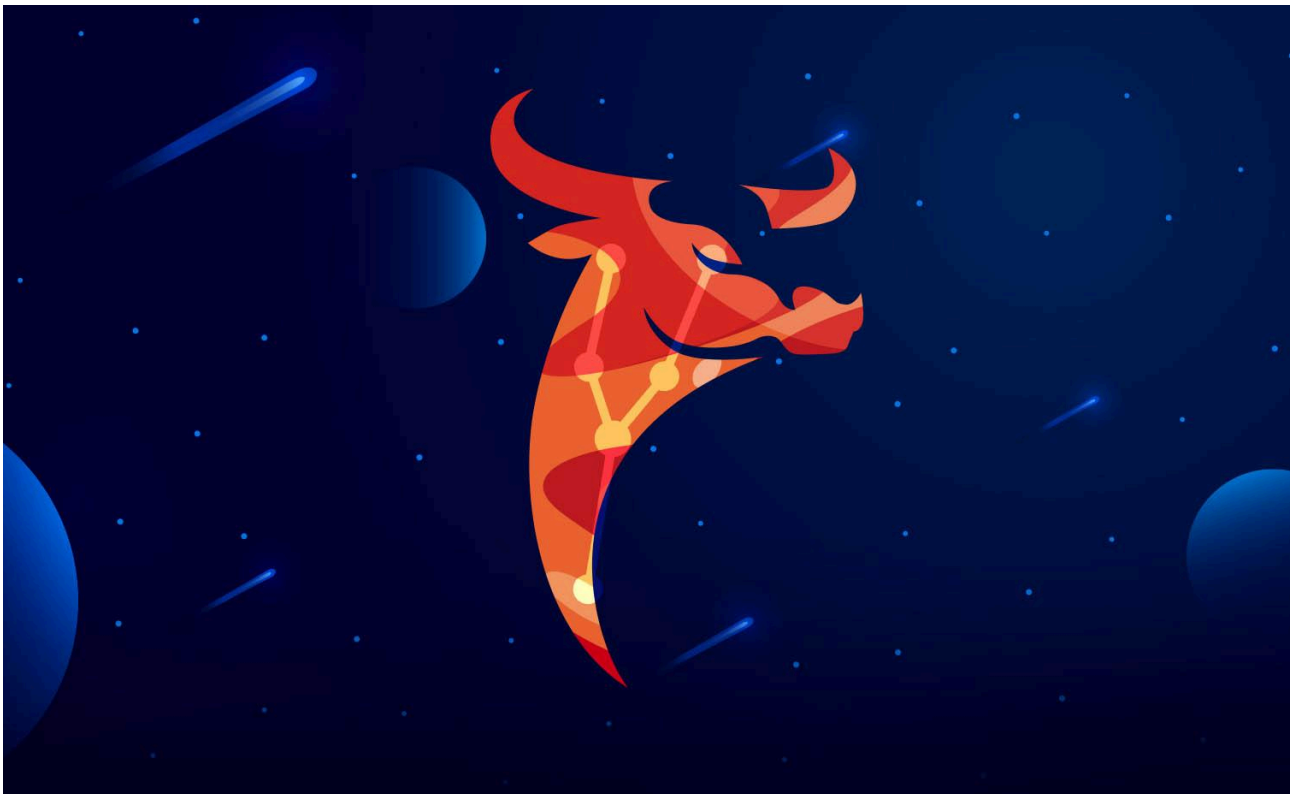
Nuclear Taurus is a suspected nation-state threat actor attributed to China. Active since at least 2017, the group has consistently conducted stealthy, long-term intrusions into organizations, focusing on espionage operations targeting high-technology companies.

Sectors Impacted

Nuclear Taurus has previously impacted organizations in the following sectors:

- Aerospace and Defense
- High Technology
- Semiconductor
- Transportation and Logistics

Playful Taurus



Also Known As

Nylon Typhoon (Microsoft), Vixen Panda (CrowdStrike)

APT15, Backdoor Diplomacy, BRONZE PALACE, Buck09, Bumble Bee, G0004, Gref, Ke3chang, Mirage, Nickel, Playful Dragon, Red Hera, RoyalAPT

Summary

Playful Taurus is a Chinese state-sponsored threat actor with a history of cyber espionage activity dating back to at least 2010. Primarily targeting government entities, diplomatic organizations, and NGOs across Southeast Asia, Europe, and Latin America, Playful Taurus focuses on intelligence gathering and data exfiltration to support Chinese political and economic interests.

Sectors Impacted

Playful Taurus has previously impacted organizations in the following sectors:

- Government
- Nonprofits
- Telecommunications

Sentinel Taurus

Also Known As

Earth Empusa, Evil Eye, EvilBamboo, Poison Carp

Summary

Sentinel Taurus is a state-sponsored threat group that has shown significant interest in Tibetan, Uyghur and Taiwanese targets. The group reportedly used spear phishing and watering hole techniques to deliver iOS and Android mobile malware payloads to their targets.

Sectors Impacted

Sentinel Taurus has previously impacted organizations in the following sectors:

- Education
- State and Local Government

Starchy Taurus

Also Known As

BARIUM, Winnti Group

Summary

Active since at least 2012, Starchy Taurus is a threat group that researchers have assessed as a Chinese state-sponsored espionage group that also conducts financially-motivated operations in over 14 countries.

Sectors Impacted

Starchy Taurus has previously impacted organizations in the following sectors:

- Healthcare
- Technology
- Telecoms
- Video games

Stately Taurus

Also Known As

Twill Typhoon (Microsoft), Mustang Panda (CrowdStrike)

Bronze Fillmore, BRONZE PRESIDENT, DEV-0117, Earth Preta, G0129, HoneyMyte, Luminous Moth, PKPLUG, Red Lich, RedDelta, TA416, Tantalum, TEMP.Hex

Summary

Stately Taurus is a nation-state threat actor attributed to China. The group has been active since at least 2012. Their campaigns are designed to gather sensitive information and exert political influence, aligning with Chinese state interests. This includes monitoring and influencing political developments in regions of strategic importance, such as the South China Sea and areas involved in the global 5G rollout.

Sectors Impacted

Stately Taurus has previously impacted organizations in the following sectors:

- Education
- Federal Government
- Media and Entertainment
- National Security
- Professional and Legal services

Ursa – Russia

Russian threat groups tracked by Unit 42 are named for the Ursa constellation. We report on these groups regularly and have a significant archive of material.

Cloaked Ursa

Also Known As

Midnight Blizzard (Microsoft), Cozy Bear (CrowdStrike)

APT29, Backswimmer, Blue Kitsune, Blue Nova, Cozy, CozyDuke, Dark Halo, DEV-0473, Dukes, Eurostrike, G0016, Group 100, Hagensia, Iron Hemlock, Iron Ritual, Nobelium, Noblebaron, Office Monkeys, Office Space, Solarstorm, TAG-11, The Dukes, UAC-0029, UNC2452, UNC3524, YTTRIUM

Summary

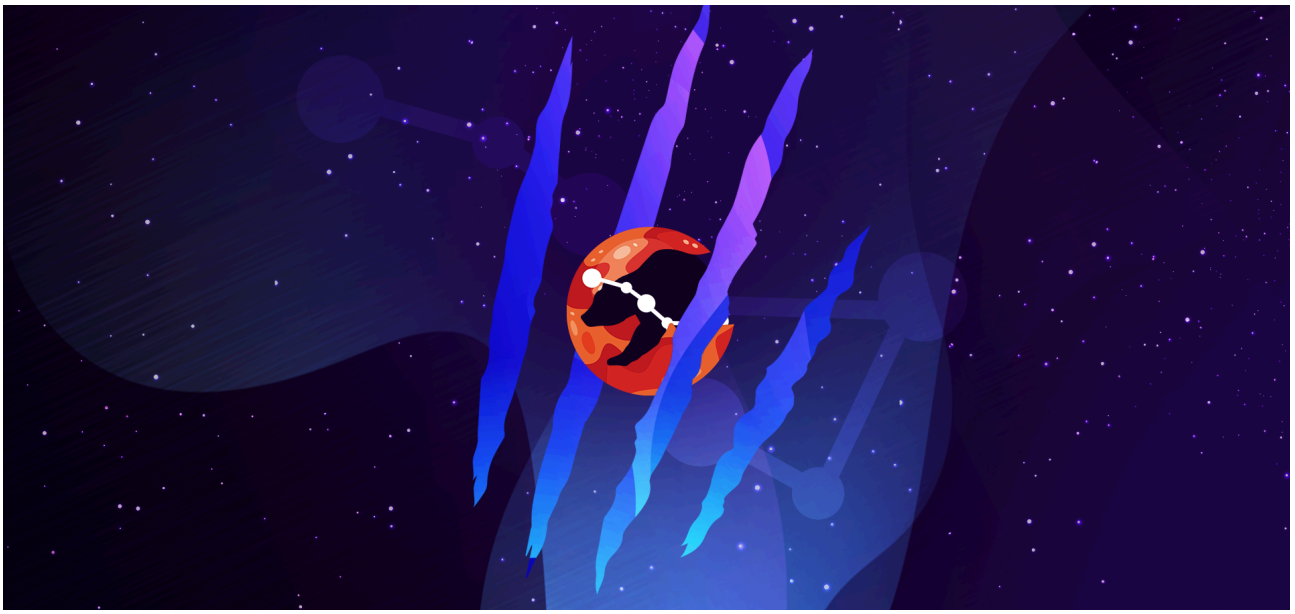
Cloaked Ursa is a nation-state threat actor attributed to Russia's Foreign Intelligence Service (SVR) that has been active since at least 2008. This group targets government, diplomatic, and critical infrastructure entities worldwide across regions such as North America, Europe, and countries opposing Russian geopolitical objectives. Cloaked Ursa's primary focus is intelligence gathering and data exfiltration to support Russian foreign policy goals, gain strategic advantage in geopolitical conflicts, and monitor and disrupt the activities of perceived adversaries.

Sectors Impacted

Cloaked Ursa has previously impacted organizations in the following sectors:

- Federal Government
- Government
- High Technology
- Manufacturing
- Utilities and Energy

Fighting Ursa



Also Known As

APT28, Fancy Bear, G0007, Group 74, IRON TWILIGHT, Pawn Storm, PawnStorm, Sednit, SNAKEMACKEREL, Sofacy, STRONTIUM, Swallowtail, TG-4127, Threat Group-4127, Tsar Team, TsarTeam, UAC-0028

Summary

Fighting Ursa is a nation-state threat group attributed to Russia's General Staff Main Intelligence Directorate (GRU), 85th special Service Centre (GTsSS) military intelligence Unit 26165. They are well known for their focus on targets of Russian interest, especially those of military interest. They are known as one of the two Russian groups that compromised the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC) during the 2016 election cycle.

Sectors Impacted

Fighting Ursa has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Education
- Federal Government
- Government
- IT Services
- Media
- Telecommunications
- Transportation
- Transportation and Logistics

- Utilities and Energy

Mythic Ursa

Also Known As

Blue Callisto, Callisto, Callisto Group, COLDRIVER, Dancing Salome, Grey Pro, IRON FRONTIER, Reuse Team, SEABORGIUM, Star Blizzard

Summary

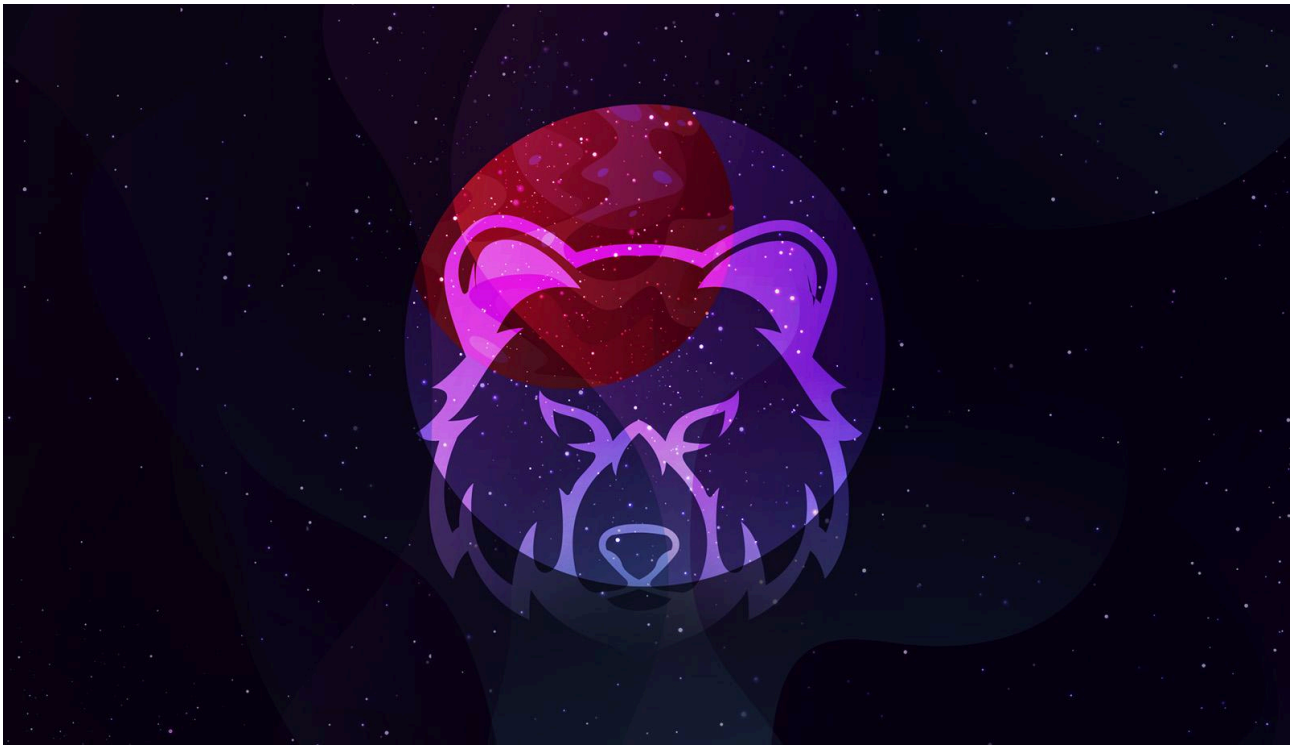
Mythic Ursa is a Russian group linked to Russia's "Centre 18" Federal Security Service (FSB) division, focused on credential harvesting from high-profile individuals. This group often uses fake accounts to establish rapport with their targets and eventually sends a phishing link to gather credentials. This group was last observed using custom malware in November 2022.

Sectors Impacted

Mythic Ursa has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Federal Government
- Higher Education
- International Affairs
- Transportation and Logistics

Pensive Ursa



Also Known As

Turla, Uroburos, Snake, BELUGASTURGEON, Boulder Bear, G0010, Group 88, IRON HUNTER, Iron Pioneer, Krypton, Minime, Popeye, Turla Team, Venomous Bear, Waterbug, White Atlas, WhiteBear, Witchcoven

Summary

Pensive Ursa is a Russian-based threat group operating since at least 2004, which is linked to Russia's "Centre 18" Federal Security Service (FSB).

Sectors Impacted

Pensive Ursa has previously impacted organizations in the following sectors:

- Defense Systems and Equipment
- Education
- Government
- Healthcare
- Nonprofit
- Pharmaceutical Preparations
- Research

Razing Ursa

Also Known As

BlackEnergy, Blue Echidna, Cyclops Blink, ELECTRUM, G0034, Grey Tornado, IRIDIUM, IRON VIKING, OlympicDestroyer, Quedagh, Sandworm, Sandworm Team, Telebots, UAC-0082, Voodoo Bear

Summary

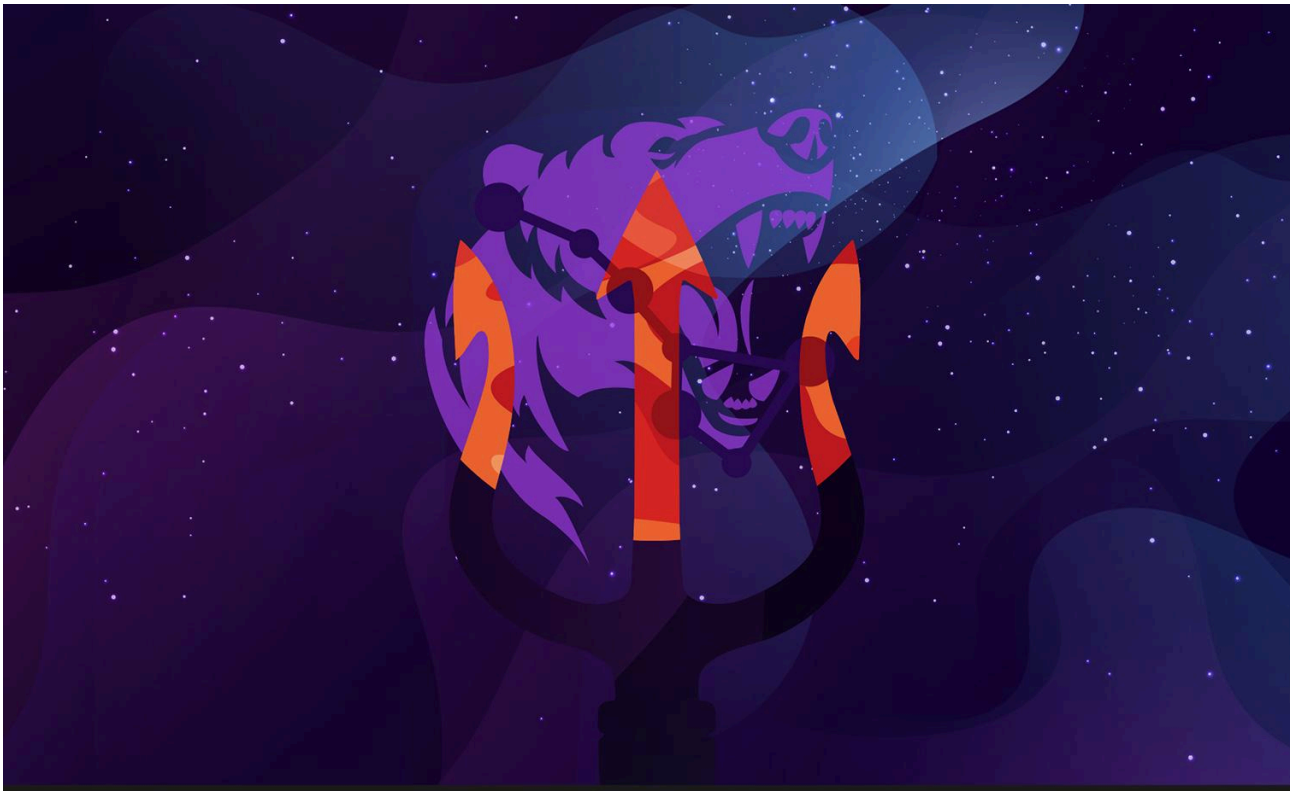
Razing Ursa is a nation-state group attributed to a subgroup of the Russian General Staff Main Intelligence Directorate (GRU). They use spear phishing and vulnerabilities to access systems with the goal of espionage or destruction. This group's activities have targeted industrial control systems or use distributed denial of service (DDoS) attacks to disrupt critical infrastructure.

Sectors Impacted

Razing Ursa has previously impacted organizations in the following sectors:

- Federal Government
- Financial Services
- Media and Entertainment
- Telecommunications
- Transportation and Logistics
- Utilities and Energy

Trident Ursa



Also Known As

Actinium, Armageddon, DEV-0157, G0047, Gamaredon Group, IRON TILDEN, Primitive Bear, Shuckworm, UAC-0010

Summary

Trident Ursa is a nation-state threat group that has been active since at least 2013. This group has targeted individuals likely related to the Ukrainian government and military and is likely the actor behind the 2015 Operation Armageddon that delivered remote access tools, such as UltraVNC and Remote Manipulator System (RMS). The group previously used commodity tools but began using custom-developed tools in 2016.

Sectors Impacted

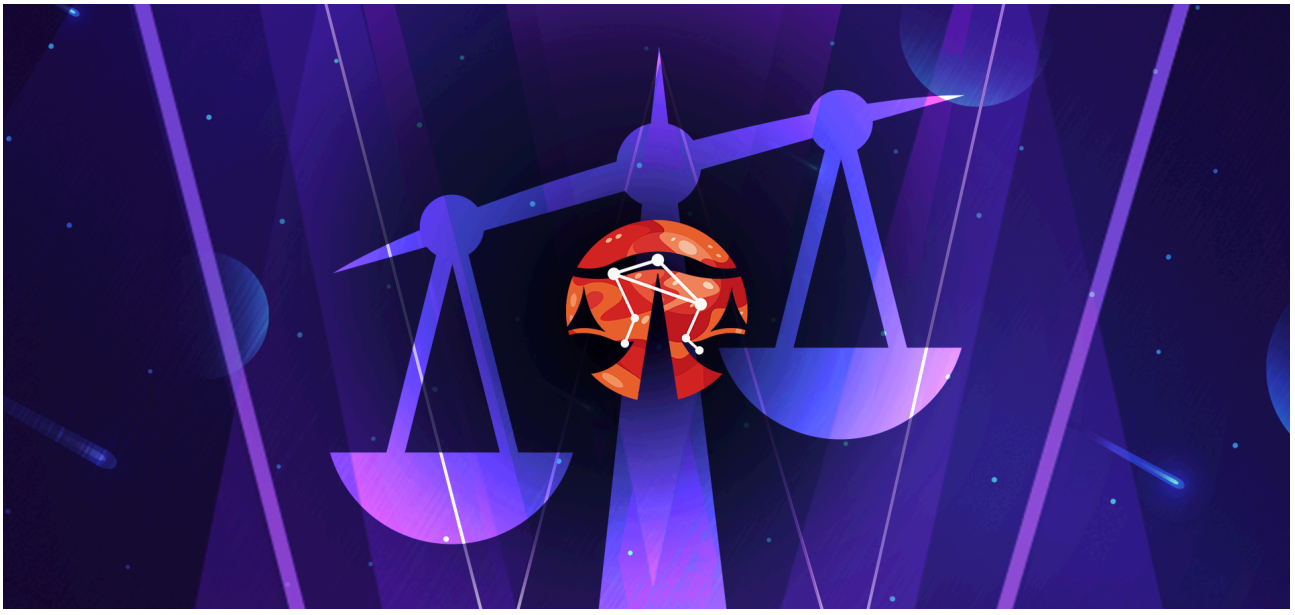
Trident Ursa has previously impacted organizations in the following sectors:

- Finance
- Wholesale and Retail

Cybercrime Threat Actor Groups

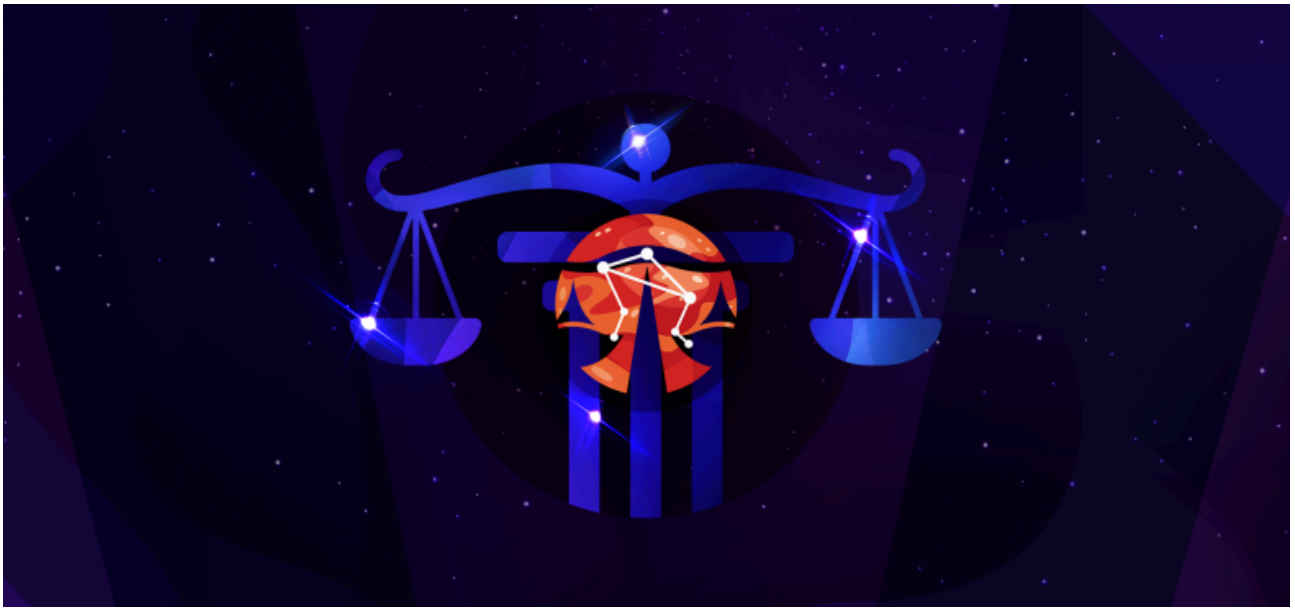
Unit 42 considers the following groups to have a motivation that is primarily financial rather than political. There can be some political motivation for threat groups in this category, but we consider their main motivation to be perpetrating cybercrime. This category is split into two groups: cybercrime in general, and then ransomware.

Libra – Cybercrime



Cybercrime is represented by the constellation Libra – a fitting choice, using the imagery of scales of justice.

Bling Libra



Also Known As

Shiny Hunters, ShinyCorp, ShinyHunters, UNC5537

Summary

Bling Libra is an extortionist group and data broker active since at least 2020. Initially operating on RaidForums, a key member now holds an administrative role on BreachForums.

The group publishes stolen data, particularly after failed extortion attempts, to bolster its reputation. Bling Libra targets industries worldwide, including telecommunications, financial services, entertainment and high technology, across the U.S., Europe, Asia, the Middle East and Latin America.

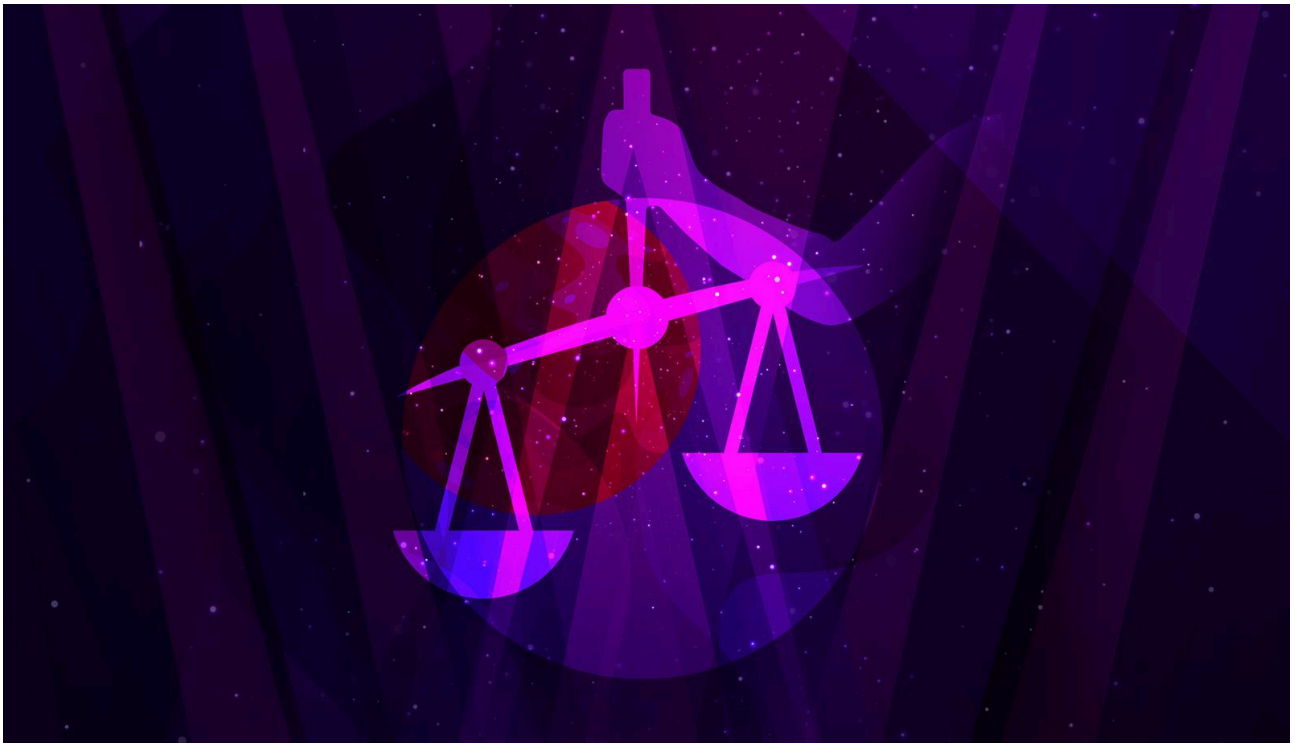
The group gains access through stolen credentials obtained via infostealer malware and phishing campaigns. Its tactics include exploiting unsecured cloud storage, weak security configurations, and using custom tools like FROSTBITE along with publicly available tools.

Sectors Impacted

Bling Libra has previously impacted organizations in the following sectors:

- Financial Services
- High Technology
- Hospitality
- Media and Entertainment
- Real Estate
- Telecommunications
- Wholesale and Retail

Muddled Libra



Also Known As

Octo Tempest (Microsoft), Scattered Spider (CrowdStrike)

G1015, Roasted 0ktapus, Scatter Swine, Star Fraud, UNC3944

Summary

Muddled Libra is a financially motivated cyberthreat group active since at least May 2022.

The group is composed of English-speaking members, some as young as 16. The group initially engaged in SIM swapping and credential harvesting, primarily targeting individuals for cryptocurrency theft. They have since evolved their operations to include data theft and ransomware deployment, aiming to extort large organizations for financial gain. Primarily targeting U.S.-based companies, Muddled Libra has expanded its focus from telecommunications and business process outsourcing (BPO) sectors to a diverse range of industries such as retail, hospitality, gaming, manufacturing and financial services.

Sectors Impacted

Muddled Libra has previously impacted organizations in the following sectors:

- High Technology
- Hospitality
- Media and Entertainment
- Professional and Legal Services
- Telecommunications

Scorpius – Ransomware

Ransomware groups get their naming convention from the constellation Scorpius, and are a frequent target of our research.

Ambitious Scorpius

Also Known As

ALPHV, BlackCat, blackcat_raas

Summary

Ambitious Scorpius is a RaaS group that uses multi-extortion, distributing BlackCat ransomware. The ransomware family was first observed in November 2021. The group is suspected to be of Russian origin and is a possible successor of DarkSide and BlackMatter. The group solicits for affiliates in known cybercrime forums, offering to allow them to keep 80-90% of the ransom payment.

A significant disruption by joint law enforcement in December 2023 appears to have dealt the group a significant blow. Despite actively listing new victims through February 2024, about 40% of the victims were smaller businesses rather than the high value targets usually seen.

Sectors Impacted

Ambitious Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Construction
- Education

- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Bashful Scorpius

Also Known As

Nokoyawa

Summary

Bashful Scorpius ransomware group was first observed in February 2022, distributing Nokoyawa ransomware, which is potentially an evolution of Nemty and Karma ransomware. Bashful Scorpius uses a multi-extortion strategy, in which attackers demand payment both for a decryptor to restore access to encrypted files and for not disclosing stolen data.

This group distributes their ransomware payloads through various means, including third-party frameworks such as Cobalt Strike and phishing emails. The creators of Nokoyawa ransomware have repurposed functions from the leaked Babuk ransomware source code.

Ransomware operators using Nokoyawa ransomware wield a command set that allows them to exercise precise control over the execution and ultimate outcome of the infection. This further increases the threat's effectiveness and potential damage.

Sectors Impacted

Bashful Scorpius has previously impacted organizations in the following sectors:

- Agriculture

- Construction
- Education
- Finance
- Healthcare
- High Technology
- Nonprofits
- Professional and Legal Services
- State and Local Government
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Bitter Scorpius

Also Known As

BianLian, bianlian_group

Summary

Initially discovered in July 2022, Bitter Scorpius is a ransomware group that uses double-extortion (T1486, T1657). The group is known for being highly adaptable and quickly leverages newly disclosed vulnerabilities. They have been among the top ten most active ransomware groups since 2023.

Bitter Scorpius distributes the BianLian ransomware, which is written in the Go programming language. The group gains initial access by exploiting external-facing remote services (T1190, T1133) and using custom remote access malware to maintain persistence.

According to previous research, the threat actors appear technically sophisticated in compromising targeted networks but are likely inexperienced overall based on the following behaviors observed during investigations:

- Mistakenly sends data from one victim to another
- Possesses a relatively stable backdoor toolkit but an encryption tool that remains in active development, including an evolving ransom note
- Maintains unreliable infrastructure, as stated through the group's admission on their Onion site

Sectors Impacted

Bitter Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Construction
- Education
- Financial Services

- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Blustering Scorpius

Also Known As

Stormous

Summary

Blustering Scorpius is an Arabic-speaking cybercrime group that first appeared in 2021. They gained fame by exploiting tensions in the Russia-Ukraine war and targeting Western entities in 2022. They initially sought to specifically target entities in the U.S. but quickly began targeting entities based on global political tensions. While the group has claimed numerous attacks, they have also been accused of posting fake data or claiming attacks perpetrated by other groups.

Blustering Scorpius gains initial access via phishing, vulnerability exploits, remote data protocol (RDP), credential abuse and malvertising. They use X (Twitter) and Telegram to advertise their exploits and to reach their followers and affiliates. The group also uses social engineering to exploit emotions surrounding geopolitical tensions.

Blustering Scorpius began joint operations with GhostSec on July 13, 2023, which they announced via GhostSec's Telegram channel. The two groups have gone on to jointly attack multiple entities in various countries and industries.

Sectors Impacted

Blustering Scorpius has previously impacted organizations in the following sectors:

- Education

- Financial Services
- High Technology
- Manufacturing
- Media and Entertainment
- Telecommunications
- Utilities and Energy
- Wholesale and Retail

Chubby Scorpius

Also Known As

Cl0p, CL0P

Summary

The Chubby Scorpius group, first observed in February 2019, is a financially motivated ransomware group known for its sophisticated operations and large-scale attacks using the Cl0P ransomware. They operate under a ransomware-as-a-service (RaaS) model, meaning they develop and maintain the ransomware while affiliates carry out the attacks.

In June 2021, six suspected members of the Cl0p ransomware gang were arrested in Ukraine during a series of raids conducted in and around Kyiv. Ukrainian law enforcement, working with investigators from South Korea and the United States, searched 21 homes and seized various devices including computers, smartphones and servers. They also confiscated approximately $184,000 USD in what is believed to be ransom payments.

Sectors Impacted

Chubby Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Construction
- Education
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Industrial Automation Industry
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofit

- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Dapper Scorpius

Also Known As

BlackSuit

Summary

Dapper Scorpius is a ransomware group that emerged in early May 2023, distributing BlackSuit ransomware, impacting a broad range of organizations globally. This group is suspected to be the Ignoble Scorpius ransomware group (aka Royal Ransomware) rebranded.

Unlike many ransomware operations that use a RaaS model, Dapper Scorpius operates as a private group without affiliates, most likely composed of ex-Conti and ex-Ignoble Scorpius members. Dapper Scorpius employs a multifaceted distribution strategy that includes phishing campaigns, malicious email attachments, SEO poisoning and using loaders like GootLoader for deploying their ransomware payload.

Sectors Impacted

Dapper Scorpius has previously impacted organizations in the following sectors:

- Construction
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Real Estate
- State and Local Government
- Transportation and Logistics
- Wholesale and Retail

Dark Scorpius

Also Known As

Storm-1811 (Microsoft), Curly Spider (CrowdStrike)

Black Basta, Black_Basta, BlackBasta, Cardina, UNC4393

Summary

Dark Scorpius is a financially motivated ransomware-as-a-service (RaaS) group, with suspected ties to the defunct Conti group. These two groups use similar tactics, techniques, procedures (TTPs) and infrastructure.

Dark Scorpius operations involve double extortion, encrypting data (T1486) and threatening public disclosure of sensitive information to coerce ransom payments (T1657). First observed in April 2022, they target critical infrastructure and high-profile organizations globally, causing significant disruptions and financial losses.

While Dark Scorpius has impacted organizations globally, their reported compromises skewed more toward developed countries such as the U.S., UK, Germany and Canada. While organizations in developed countries are most frequently targeted due to their potential for high-value payouts, this threat actor maintains an opportunistic approach, suggesting they will target any vulnerable organization if the opportunity for profit arises. The group avoids operations within the Commonwealth of Independent States, a common behavior observed in Russia-based groups.

As a RaaS group, Dark Scorpius has affiliates that leverage a wide set of TTPs to achieve their objectives. As such, what we capture in this report may differ from the activities they employ in future attacks.

The group exclusively uses the Black Basta ransomware for data encryption (T1486) after exfiltrating files with tools such as RClone (S1040, T1048, T1567).

Sectors Impacted

Dark Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Construction
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits

- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Fiddling Scorpius

Also Known As

Play, PlayCrypt

Summary

Fiddling Scorpius is a sophisticated cybercriminal organization that emerged in June 2022. This group is notorious for its double-extortion tactics, where they exfiltrate sensitive data before encrypting systems and demanding ransom payments to prevent data leaks.

The tooling employed by Fiddling Scorpius includes a mix of custom and publicly available tools for command and control (C2), lateral movement, credential dumping, and data exfiltration. The primary impact of their attacks is data encryption with a .play extension, causing significant operational disruptions.

Sectors Impacted

Fiddling Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Conglomerates
- Construction
- Federal Government
- Financial Services
- High Technology
- Hospitality
- Industrial Automation Industry
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Professional and Legal Services

- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Fiery Scorpius

Also Known As

Helldown

Top Impacted Industries

- Construction
- High Technology
- Hospitality
- Professional and Legal Services
- Transportation and Logistics
- Wholesale and Retail

Flighty Scorpius

Also Known As

ABCD, LockBit, LockBit 2.0, LockBit 3.0, LockBit Black, Lockbit_RaaS

Summary

Flighty Scorpius is a ransomware as a service (RaaS) group, first observed in September 2019. They were initially known for deploying ABCD ransomware, which was so named due to its characteristic .abcd file extension used during attacks. They later rebranded as LockBit when they became a RaaS operation.

Flighty Scorpius' operational model is distinguished by its affiliate program, which they aggressively marketed on underground forums. The group has innovated in affiliate relations, offering direct ransom payments to affiliates before taking its cut, a practice that contrasts with the norm and incentivizes potential partners.

Over the years, Flighty Scorpius has developed and released multiple LockBit ransomware variants. Each variant signifies an evolution in the group's technical capabilities, from faster encryption speeds to more sophisticated extortion techniques. This evolution is mostly as a result of their acquiring different ransomware source code from competitors.

The group suffered a major disruption with Operation Cronos in February 2024, which led to law enforcement seizing infrastructure and public-facing websites crucial to LockBit's operations. They also exposed Russian nationals as members of the group, including its administrator.

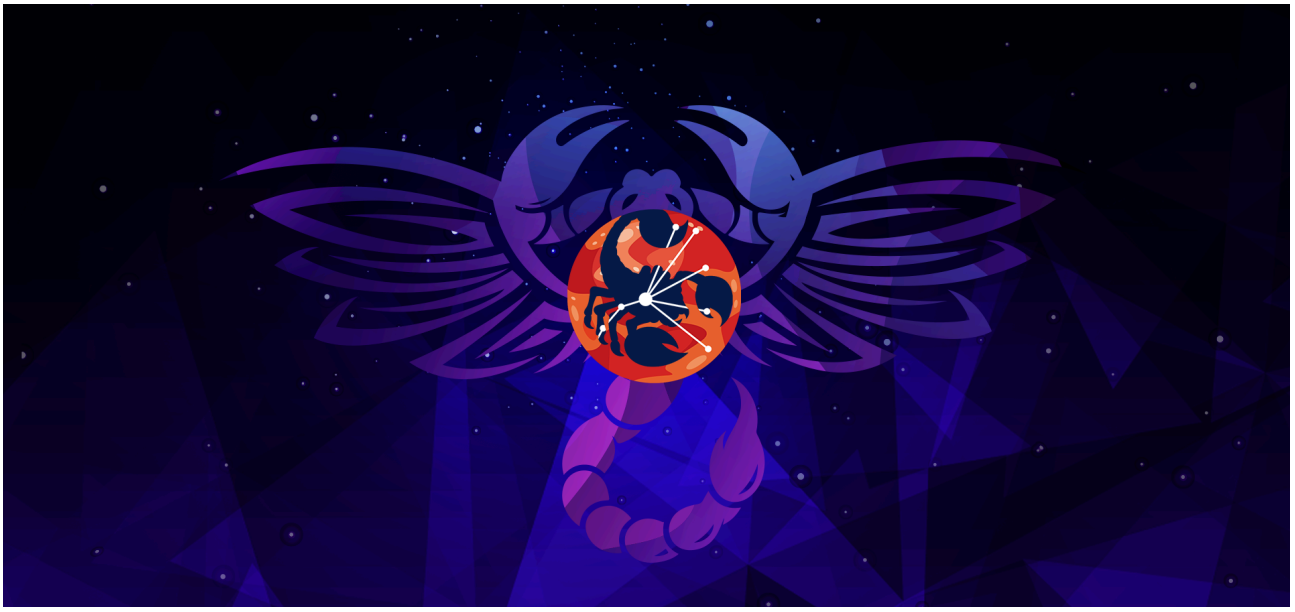
Despite these law enforcement disruptions Flighty Scorpius has resumed operations, including the potential release of a new ransomware variant.

Sectors Impacted

- Aerospace and Defense
- Agriculture

- Construction
- Cryptocurrency Industry
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Fluttering Scorpius



Also Known As

FOG

Summary

Fluttering Scorpius, the group that distributes FOG ransomware, emerged as a significant threat actor in the ransomware landscape when first observed in April 2024. This group is notorious for exploiting vulnerabilities in widely used software to gain unauthorized access to systems.

The group employs various techniques, like using stolen credentials and unpatched vulnerabilities to infiltrate networks. Fluttering Scorpius has shared infrastructure with the Akira ransomware group, which suggests possible collaboration between these groups.

Fluttering Scorpius' operations are marked by rapid encryption attacks and strategically using living-off-the-land binaries (LOLBins) to evade detection.

The group focuses on targeting backup and disaster recovery solutions to maximize the impact of their attacks. The group often uses compromised VPN credentials to get a foothold in the victim's environment. These threat actors accomplish lateral movement using pass-the-hash attacks on administrator accounts to establish RDP connections targeting Hyper-V running on Windows servers. Fluttering Scorpius also uses credential stuffing to take over high-value accounts.

Sectors Impacted

- Agriculture
- Construction
- Education
- Healthcare
- Hospitality
- Manufacturing
- Nonprofits
- Professional and Legal Services
- State and Local Government
- Telecommunications
- Utilities and Energy
- Wholesale and Retail

Howling Scorpius

Also Known As

Storm-1567 (Microsoft), Punk Spider (CrowdStrike)

Akira

Summary

Howling Scorpius is a financially motivated ransomware-as-a-service (RaaS) operation observed since early 2023. It employs double extortion tactics, exfiltrating sensitive data before typically encrypting systems.

The group targets organizations globally, with a focus on North America, the UK, Australia and Europe. It impacts various sectors, including manufacturing, professional services, education, critical infrastructure and retail.

Howling Scorpius targets Windows and Linux/ESXi systems with evolving ransomware variants. It uses various tactics, including exploiting vulnerabilities and credential theft, to exfiltrate data.

Dwell times range from less than 24 hours to a month, likely reflecting varying affiliate capabilities. While Howling Scorpius primarily uses double extortion, threatening to publish stolen data if ransom demands are unmet, it has also engaged in extortion-only attacks. In cases we observed during Fall 2023, the group exfiltrated data for payment extortion without deploying ransomware.

Sectors Impacted

Howling Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Agriculture and Food and Beverage Production Industry
- Automotive Industry
- Civic Leagues and Social Welfare Organizations
- Conglomerates
- Construction
- Consumer Business Industry
- Education
- Engineering and Construction Industry
- Federal Government
- Financial Services
- Health Care Providers and Services Industry
- Health Insurance Providers
- Healthcare
- High Technology
- Hospitality
- Hospitality Industry
- Industrial Products And Services Industry
- Information Technology (IT) or Technology Consulting Industry
- Insurance
- Investment Management Industry
- Law Services and Consulting Industry
- Management and Operations Consulting Industry
- Manufacturing
- Media and Entertainment
- Mining

- Nonprofits
- Oil, Gas and Consumable Fuels Industry
- Operational NGOs
- Pharma and Life Sciences
- Professional and Legal Services
- Public Safety
- Real Estate
- Real Estate Management, Brokerage and Service Provider Industry
- Restaurants and Food Service Industry
- Retail, Wholesale and Distribution Industry
- State and Local Government
- Technology Industry
- Telecommunications
- Telecommunications Industry
- Transportation and Logistics
- Transportation Industry
- Utilities and Energy
- Wholesale and Retail

Ignoble Scorpius

Also Known As

Black Suit, BlackSuit, Dapper Scorpius, Roy, Royal, Royal_Group, Zeon

Summary

Ignoble Scorpius is a cybercriminal organization specializing in ransomware attacks. First emerging in September 2022 as the Royal ransomware group, it rebranded as BlackSuit around May 2023.

This group comprises experienced members possibly linked to the defunct Conti group. It has developed custom ransomware payloads, notably introducing the BlackSuit ransomware as a successor to the earlier Royal ransomware. BlackSuit retained over 90% of Royal's codebase.

The group's ransomware targets Windows and Linux systems, including ESXi servers and employs strong encryption algorithms to render data inaccessible.

Sectors Impacted

Ignoble Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Federal Government

- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Nonclassifiable Establishments
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Invisible Scorpius

Also Known As

Cloak

Summary

Invisible Scorpius is a ransomware group targeting small to medium-sized businesses and using initial access brokers (IABs) for initial access. First seen at the end of 2022, the group is believed to be connected to the Stale Scorpius ransomware group after threat actors posted victim information from Stale Scorpius to Invisible Scorpius' leak site.

Sectors Impacted

Invisible Scorpius has previously impacted organizations in the following sectors:

- Federal Government
- Hospitality
- Professional and Legal Services
- State and Local Government
- Transportation and Logistics

Mushy Scorpius

Also Known As

Karakurt, Karakurt Lair, Karakurt Team

Summary

Mushy Scorpius is the group behind Karakurt ransomware, known for focusing on extortion. It has links to the Conti RaaS group. First emerging in 2021, Mushy Scorpius steals intellectual property and demands ransom from victims without encrypting their data, leveraging threats to auction off the sensitive data or release it to the public.

As part of their extortion efforts, they provide victims with screenshots or copies of stolen file directories as evidence of the data theft. They aggressively contact victims' employees, business partners and clients with harassing emails and phone calls. They also leverage stolen data like social security numbers, payment accounts, private emails and other sensitive business information to exert pressure.

Upon receiving ransom payments, Mushy Scorpius has occasionally provided victims with proof that they deleted the stolen files, along with a brief explanation of how they initially breached the victim's defenses. This underlines the group’s focus on financial gain but also that they seek a level of engagement from their victims toward meeting their demands.

Sectors Impacted

Mushy Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Utilities and Energy
- Wholesale and Retail

Pilfering Scorpius

Also Known As

Robinhood

Summary

Pilfering Scorpius ransomware group gained attention by attacking a number of local and state government entities starting in April 2019. This threat group often gains initial access by phishing, malicious websites and malicious file sharing or downloads.

Once their ransomware has gained access, it obtains persistence by using RDP to spread throughout the victim network. Initial reporting revealed that humans were largely responsible for operating these attacks, as opposed to them being run by automated processes.

Sectors Impacted

Pilfering Scorpius has previously impacted organizations in the following sectors:

- Pharma and Life Sciences
- Utilities and Energy
- Transportation and Logistics
- Education
- Nonprofits
- Insurance
- Healthcare
- Manufacturing
- Federal Government
- State and Local Government
- Real Estate
- Construction
- Financial Services
- Agriculture
- Wholesale and Retail

Powerful Scorpius

Also Known As

BlackByte

Summary

Powerful Scorpius is a RaaS group operating since July 2021, distributing BlackByte ransomware. This group's operational tactics includes exploiting vulnerabilities such as the ProxyShell vulnerability in Microsoft Exchange Servers, using tools like Cobalt Strike, and avoiding detection through obfuscation and anti-debugging techniques.

Their malware checks system languages and exits if it finds Russian or certain Eastern European languages, presumably to avoid impacting systems in those regions. The group uses multi-extortion techniques in their campaigns.

Sectors Impacted

Powerful Scorpius has previously impacted organizations in the following sectors:

- Financial Services
- Food and Agriculture
- Government
- Manufacturing
- Wholesale and Retail

Procedural Scorpius

Also Known As

ThreeAM, 3AM

Summary

Procedural Scorpius is a ransomware group discovered in September 2023, when researchers noticed Procedural Scorpius' malware being deployed in a failed LockBit attack. This group distributes 3 am ransomware, and is thought to be linked to two other notorious ransomware groups, Conti and Ignoble Scorpius (distributor of Royal ransomware).

Procedural Scorpius escalates their extortion tactics by contacting their victim's social media followers, informing them of the data leak. They also use bots that post on highly visible X accounts to advertise the leaks. Procedural Scorpius targets medium to large companies in countries not within the Commonwealth of Independent States (CIS).

Sectors Impacted

Procedural Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Financial Services
- Manufacturing
- Professional and Legal Services
- Wholesale and Retail

Protesting Scorpius

Also Known As

Cactus, Cactus Ransomware Group

Summary

Protesting Scorpius emerged as a ransomware threat actor in March 2023, employing double-extortion tactics. The group distinguishes itself through innovative tactics, often securing initial access to target networks by exploiting vulnerabilities in internet-facing software and services, such as virtual private network (VPN) appliances. This includes the use of zero-day vulnerabilities. The group also gains access through phishing attacks or by acquiring credentials via partnerships with malware distributors.

Protesting Scorpius targets are located primarily in the U.S. The group focuses on infiltrating networks of both public sector organizations and large commercial entities.

The group exfiltrates sensitive data from its victims and engages in extortion using peer-to-peer messaging services. Protesting Scorpius also uploads exfiltrated files to its own leak site to apply additional pressure to victims.

Sectors Impacted

Protesting Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Agriculture
- Construction
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Life Insurance Providers
- Manufacturing
- Media and Entertainment
- Mining
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Repellent Scorpius

Also Known As

Cicada3301, Cicada3301 ransomware-as-a-service

Summary

First observed in June 2024 on multiple predominantly Russian-language cybercrime forums, Repellent Scorpius' is a ransomware-as-a-service (RaaS) affiliate program. While the group's precise origin remains unknown, its presence on these forums and the use of Russian by its members suggest a possible connection to the Russian-speaking cybercriminal underground.

Repellent Scorpius prohibits attacks on Commonwealth of Independent States (CIS) countries (e.g., Russia) and charges affiliates a 20% fee on all ransoms. This relatively high profit share for affiliates likely aims to attract skilled cybercriminals. Prospective affiliates must undergo an interview and vetting process, including providing proof of their activity on cybercrime forums.

The group's ransomware, written in Rust, uses ChaCha20 encryption and operates offline. It supports Windows, Linux, ESXi and NAS platforms.

While no definitive link exists between the groups, some overlaps were observed between Repellent Scorpius and Ambitious Scorpius (aka BlackCat), which disbanded shortly before Repellent Scorpius appeared.

Sectors Impacted

Repellent Scorpius has previously impacted organizations in the following sectors:

- Construction
- Healthcare
- High technology
- Telecommunications

Salty Scorpius

Also Known As

Trigona

Summary

Salty Scorpius claims to be a highly profitable operation, launching global attacks deploying Trigona ransomware with promises of 20%-50% returns from each successful endeavor. First identified in October 2022, their operations partnered with network access brokers, who provided them with compromised credentials via the Russian Anonymous Marketplace (RAMP) forum. This collaboration was crucial for gaining the initial access needed to infiltrate their targets.

Salty Scorpius has ties to the CryLock group, evidenced by their shared methodologies, strategies and the identical ransom note filenames and email addresses they employ. By April 2023, Salty Scorpius shifted their focus toward exploiting compromised Microsoft SQL (MSSQL) servers, leveraging brute-force attacks to penetrate these systems.

This group also performs detailed reconnaissance within the target's network, malware distribution via remote monitoring and management (RMM) software, creation of new user accounts and then finally deployment of ransomware.

They were disrupted by hacktivists in 2023, but posts have appeared on their leak site in 2024.

Sectors Impacted

Salty Scorpius has previously impacted organizations in the following sectors:

- Hospitality
- Wholesale and Retail

Shifty Scorpius

Also Known As

Hunters International

Summary

Shifty Scorpius is a financially motivated ransomware-as-a-service (RaaS) group that emerged in October 2023. Security researchers believe the group to be related to the former Hive ransomware operation, potentially through acquisition or adaptation of Hive's codebase after law enforcement disruptions.

Unlike other ransomware groups, Shifty Scorpius primarily focuses on data exfiltration and extortion, not encryption. This extortion includes leaking pre-operative pictures of patients from breached healthcare

organizations.

The group targets a wide array of industries globally, with particular focus on the healthcare, finance and automotive sectors. It employs a multifaceted approach to infiltrating and exploiting target networks.

Shifty Scorpius has directly contacted the clients and customers of victim organizations, often via email, to solicit payment for not publishing or selling their details on the dark web.

Sectors Impacted

Shifty Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Conglomerates
- Construction
- Education
- Federal Government
- Financial Services
- Health Insurance Providers
- Healthcare
- High Technology
- Hospitality
- Insurance
- Internet of Things (IoT) industry
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Spicy Scorpius

Also Known As

Avos, AvosLocker

Summary

Spicy Scorpius is a RaaS group that first emerged as a significant threat in 2021. This group uses multi-extortion tactics and remote administration tool AnyDesk for manual operation on victim machines. They can operate in safe mode to evade security measures. They also auction stolen data on their site in addition to their ransom demand.

The group's deployment strategies include leveraging vulnerabilities like Log4Shell for initial access. This group has a level of organization resembling that of legitimate tech businesses rather than traditional cybercrime operations.

The threat they use has evolved to specifically target Linux systems and VMware ESXi servers since its debut, where many similar operations primarily focus on Windows systems.

Sectors Impacted

Spicy Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Finance
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Spikey Scorpius

Also Known As

Agenda, Qilin, Qilin Team

Summary

Spikey Scorpius operates as an affiliate program for ransomware as a service and has recently adopted Rust-based ransomware to target its victims. Previously, they used Go as their preferred language.

Spikey Scorpius often tailors ransomware attacks to each victim for maximum impact. To achieve this, threat actors employ strategies like altering file extensions of encrypted files and terminating specific processes and services.

The group advertises their ransomware Qilin on the dark web. This ransomware features a proprietary data leak site (DLS) containing unique company IDs and leaked account information.

Spikey Scorpius' operators employ a double extortion approach, which involves encrypting a victim's sensitive data and exfiltrating it. They then demand payment for a decryption key and threaten to release the stolen data even after receiving the ransom.

The malware offers various encryption modes, all under the operator's control. Additionally, they may attempt to reboot systems in normal mode and halt server-specific processes to complicate the victim's data recovery efforts.

Sectors Impacted

Spikey Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Industrial Automation Industry
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life Sciences
- Professional & Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Spoiled Scorpius

Also Known As

Cyclops, Knight, RansomHub

Summary

Spoiled Scorpius is a prominent ransomware-as-a-service (RaaS) operation that emerged in February 2024. This cybercriminal group has rapidly become one of the most active ransomware threats, leveraging a double-extortion model to maximize financial gains. Analysis of code indicates significant overlap with Knight ransomware, suggesting that Spoiled Scorpius could have evolved or built upon this earlier threat.

While the group's primary focus has been on organizations within the U.S., it has also expanded operations to European targets This indicates a strategic shift toward a more global victim base. Its victims cover a diverse range of industries.

Sectors Impacted

Spoiled Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Chemical Manufacturing
- Conglomerates
- Construction
- Cryptocurrency Industry
- Education
- Federal Government
- Financial Services
- Health Insurance Providers
- Healthcare
- High Technology
- Holding Companies
- Hospitality
- Industrial Automation Industry
- Insurance
- Internet of Things (IoT) Industry
- Manufacturing
- Media and Entertainment
- Manufacturing Chemical Preparations
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications

- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Squalid Scorpius

Also Known As

8Base

Summary

Squalid Scorpius ransomware group first emerged in March 2022, using a multi-extortion tactic. The group initially remained under the radar with relatively few attacks, but in June 2023, their activity spiked dramatically, showcasing a more aggressive approach.

They leverage encryption techniques alongside name-and-shame strategies to pressure victims into paying ransoms. Squalid Scorpius has used a number of ransomware variants, including a customized version of the Phobos ransomware. This indicates their technical adaptability, as well as their focus on evading detection and maximizing impact. This adaptability is evident in their use of advanced encryption techniques and strategies to bypass User Account Control (UAC) mechanisms on Windows systems, enabling them to execute their malicious payloads without immediate detection.

Sectors Impacted

Squalid Scorpius has previously impacted organizations in the following sectors:

- Utilities and Energy
- Wholesale and Retail

Squeaking Scorpius

Also Known As

Rhysida

Summary

Squeaking Scorpius is a RaaS group first observed in May 2023. They are believed to go after targets of opportunity rather than specific industries or organizations. They employ a double extortion model, demanding a ransom to decrypt victim data and threatening to publish sensitive data unless a ransom is paid.

Squeaking Scorpius operates as a ransomware-as-a-service, where tools and infrastructure are leased out to affiliates. Any ransom paid is split between the group and the affiliated. They have been known to engage in ransom negotiations and disclose compromised victim data.

Their primary means of initial access is through phishing emails, malvertising, or using stolen credentials to authenticate to remote services, such as through VPNs, especially in organizations not using multi-factor authentication.

Once in a victim's environment, they use Living off the Land (LotL) techniques including PowerShell for enumerating the environments and RDP connections for lateral movement. They have also used Cobalt Strike in victim environments as well as a script that terminates anti-malware programs. The group distributes Rhysida ransomware, which encrypts data using a 4096-bit RSA encryption key.

Some researchers have suggested links between this group and the actors behind Vice Society ransomware, suggesting a rebrand.

Sectors Impacted

Squeaking Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Utilities and Energy
- Wholesale and Retail

Stale Scorpius

Also Known As

Good Day

Summary

Stale Scorpius is a ransomware group initially observed in May of 2023. Their infrastructure as well as purported victims are closely linked with Invisible Scorpius, leading researchers to believe the groups are connected. Contact information such as threat actor channels and email addresses that were observed in Invisible Scorpius attacks have also been seen in Stale Scorpius attacks.

Sectors Impacted

Stale Scorpius has previously impacted organizations in the following sectors:

- Construction
- Education
- Federal Government
- Healthcare
- High Technology
- Insurance
- Manufacturing
- Media and Entertainment
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Wholesale and Retail

Stumped Scorpius

Also Known As

NoEscape, No Escape

Summary

Stumped Scorpius is a RaaS group that first emerged in May 2023 and quickly established themselves as a successor to the Avaddon ransomware group, which ceased operations in 2021. Stumped Scorpius uses aggressive multi-extortion tactics, targeting a broad range of industries including healthcare.

They encrypt files on Windows, Linux and VMware ESXi servers, demanding ransoms ranging from hundreds of thousands of dollars to over $10 million. Their developers claim to have built the malware and infrastructure from scratch, differentiating the threat from other ransomware families that often repurpose existing code.

Stumped Scorpius employs techniques like reflective DLL injection to target VMware ESXi servers. They have a robust RaaS platform that allows affiliates to customize attacks, including encryption strategies and ransom demands.

Their ransomware can bypass UAC on Windows, executing commands to delete shadow copies and system backups to prevent file recovery. It also uses the Microsoft Enhanced RSA and AES Cryptographic Provider for file encryption.

Sectors Impacted

Stumped Scorpius has previously impacted organizations in the following sectors:

- Education
- Federal Government
- Media and Entertainment

Tarnished Scorpius

Also Known As

Gold Ionic, Inc, Inc Group, Inc Ransom, Inc.

Summary

Tarnished Scorpius is a cybercriminal group that emerged in mid-2023. It specializes in ransomware attacks focusing on financial gain through double and triple extortion tactics. Originally targeting a wide variety of industries in the U.S., Tarnished Scorpius has notably shifted focus by launching attacks on healthcare institutions in the UK.

Tarnished Scorpius gains initial access to target networks through the exploitation of known vulnerabilities in public-facing applications. The group uses a wide range of tools and platforms to carry out operations.

Sectors Impacted

- Aerospace and Defense
- Agriculture
- Construction
- Cryptocurrency Industry
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Transforming Scorpius

Also Known As

Medusa (Note: Medusa should not be confused with a similarly named RaaS, MedusaLocker, which has been available since 2019)

Summary

Transforming Scorpius, which appeared in late 2022, operates under a ransomware-as-a-service (RaaS) model. They use encryption techniques to lock the victim's data and demand a ransom for the decryption keys. The ransomware avoids encrypting extensions like .dll, .exe and .lnk and excludes specific folders from encryption to ensure the system's operability remains intact.

Transforming Scorpius has introduced multiple variants, differentiated mainly by their ransom notes, which have transitioned from text to HTML formats in newer versions. The ransomware also features a dedicated data leak site, launched in early 2023, to publish victim data as part of a multi-extortion strategy. Based on their unwillingness to comply with ransom demands, victims are offered options like data deletion or download for a fee.

Sectors Impacted

Transforming Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Construction
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Hospitality
- Industrial Automation Industry
- Insurance
- Manufacturing
- Media and Entertainment
- Mining
- Nonprofits
- Pharma and Life Sciences
- Professional and Legal Services
- Real Estate
- State and Local Government
- Telecommunications
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Tropical Scorpius

Also Known As

Storm-0671 (Microsoft), Storm-0978 (Microsoft)

Cuba, DEB-0978, Romcom, UAT-5647, UNC2596, Void Rabisu

Summary

Tropical Scorpius is a cybercriminal group active since 2021. Initially deploying the Cuba ransomware family in financially motivated attacks, the group has since expanded its ransomware operations to include the Industrial Spy, Underground and Trigona families.

They maintain a variety of custom implants written in different programming languages, relying on the malware RomCom in particular. They have used zero and n-day exploits for initial access.

Following the start of the Russia-Ukraine conflict in 2022, Tropical Scorpius also began conducting cyberespionage campaigns against Ukraine and its allies, supporting Russian geopolitical interests. While Microsoft researchers have placed the group's operations in Russia, the exact relationship between Tropical Scorpius and the Russian government remains unknown. It could be direct state-sponsorship, a contractual relationship or independent action aligned with Russian interests.

Sectors Impacted

- Agriculture
- Construction
- Education
- Federal Government
- Financial Services
- Healthcare
- High Technology
- Insurance
- Manufacturing
- Media and Entertainment
- Professional and Legal Services
- Real Estate
- State and Local Government
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Twinkling Scorpius

Also Known As

HelloKitty, Gookie, HelloGookie

Summary

Twinkling Scorpius is a ransomware group distributing HelloKitty ransomware that was identified in November 2020, targeting Windows systems and using unpatched vulnerabilities like those in SonicWall devices to gain initial access to victim networks. In July 2021, Unit 42 observed the group using a Linux variant of HelloKitty targeting VMware's ESXi hypervisor.

The group uses both email and Tor chats for communications. In late 2023, the ransomware developer and operator, also known as Gookee/kapuchin0 and Guki, leaked the source code and shut the operation down.

In March 2024, the group rebranded, and now calls themselves Gookie or HelloGookie. To mark the occasion of the rebrand, the malware author released the data stolen in the CD Projekt Red breach and 2022 Cisco attack.

Sectors Impacted

Twinkling Scorpius has previously impacted organizations in the following sectors:

- Aerospace and Defense
- Information Technology Services

Weary Scorpius

Also Known As

Backmydata, Devos, Eight, Eking, Elbie, Faust, Phobos

Summary

Weary Scorpius is a financially motivated cybercriminal group active since late 2018. The group has used Phobos ransomware and its variants (e.g. Eking, Eight, Elbie, Devos, Faust and BackMyData) to operate under a ransomware-as-a-service (RaaS) model.

This group has targeted a diverse range of industries, including critical infrastructure and essential services. It has primarily focused on the U.S., Western Europe and the Asia-Pacific region. In early 2024, the group intensified its focus on the technology sector and adopted double extortion tactics.

As a RaaS group, Weary Scorpius exhibits a wide range of tactics, techniques and procedures (TTPs) during the pre-encryption attack stage. It gains initial access by exploiting exposed Remote Desktop Protocol (RDP) services through brute-force attacks, conducting phishing campaigns with malicious macros and employing loader malware to distribute ransomware variants.

The group performs the following activities:

- Accessing credentials using public tools then using those credentials for lateral movement within the network
- Performing network discovery with network scanning tools to identify valuable targets
- Exfiltrating data before encryption, leveraging double extortion tactics by threatening to leak stolen data if victims have not paid the ransom

Sectors Impacted

Weary Scorpius has previously impacted organizations in the following sectors:

- Agriculture
- Aviation and Aeronautical Engineering
- Education
- Financial Services
- Healthcare
- High Technology
- Manufacturing
- Nonprofits
- Professional and Legal Services
- State and Local Government
- Transportation and Logistics
- Utilities and Energy
- Wholesale and Retail

Updated Aug. 7, 2024, at 12:05 p.m. PT to clarify headings.

Updated Sept. 3, 2024, at 9:56 a.m. PT to remove StellarParticle from Cloaked Ursa akas.

Updated Sept. 11, 2024, at 11:25 a.m. PT for clarifying language.

Updated Jan. 29, 2025, at 7:55 a.m. PT.

Updated June 19, 2025, at 9:55 a.m. PT to add Nuclear Taurus and Starchy Taurus.

Updated Aug. 1, 2025, at 11:05 am P.T. to update many entries and add Bling Libra, Fiery Scorpius, Flighty Scorpius, Repellent Scorpius, Tarnished Scorpius and Tropical Scorpius.
