Timeline of the graph

From 5 July 2022 to 7 December 2022: 2 attack-patterns, 2 campaigns, 1 report and 4 intrusion-sets had been published.

On 5 July 2022, 1 report had been published.

report: Test_Hash

On 10 October 2022, 4 intrusion-sets had been published.

intrusion-set: CostaRicto
The aliases used by the group are CostaRicto. The primary motivation of this group is financial gain. CostaRicto was first observed on May 24, 2021, and last observed on October 15, 2021. This intrusion-set is believed to be associated with a hacker-for-hire cyber espionage campaign that has been targeting multiple industries worldwide since at least 2019. The targets of the CostaRicto campaign are scattered across different regions of the world, including Europe, the Americas, Asia, Australia, and Africa, with a particular concentration in South Asia. Financial institutions make up a large portion of the group's targets. The CostaRicto campaign is a significant threat to organizations, and it's essential to remain vigilant to protect against potential attacks.

intrusion-set: Leviathan
The aliases used by this group include Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope, and APT 40. The primary motivation of this group is information theft and espionage. Leviathan was first observed on April 18, 2018, and last observed on April 15, 2022. Leviathan is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company. This group has been active since at least 2009 and has targeted various sectors, including academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation. The group's targets are spread across the US, Canada, Europe, the Middle East, and Southeast Asia. Leviathan's persistent and advanced cyber espionage activities pose a significant threat to national security and global stability. It's crucial for organizations to take proactive measures to defend against such threats and ensure the security of their networks and sensitive data.

intrusion-set: APT29
The intrusion-set known as APT29 has various aliases including IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The

Dukes, Cozy Bear, and CozyDuke. Their main objective is information theft and espionage. The group's activities were first detected on 31 May 2017 and last observed on 14 April 2022. [APT29] has been attributed to Russia's Foreign Intelligence Service (SVR) and has been operational since at least 2008. Their targets include government networks in Europe and NATO member countries, research institutes, and think tanks. The group made headlines in 2015 for compromising the Democratic National Committee, and in April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR. This operation also involved other intrusion-sets such as Cozy Bear, The Dukes, UNC2452, NOBELIUM, StellarParticle, and Dark Halo. The victims of this operation were government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East.

intrusion-set: APT28
The set, known as [APT28], has several aliases including IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127 and TG-4127. The group's primary motivation is information theft and espionage. They have been active since at least 2007, targeting a range of organizations including government, military, and security entities, as well as defense contractors, media outlets, and political organizations.

On 4 November 2022, 2 campaigns had been published.

campaign: Operation Wocao
[Operation Wocao] was a global cyber espionage campaign that targeted a wide range of organizations across multiple industries and countries, including Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. The suspected Chinese-based actors behind the campaign were able to compromise government organizations, managed service providers, and a variety of businesses in sectors such as aviation, construction, energy, finance, healthcare, insurance, offshore engineering, software development, and transportation. Security researchers found that the [Operation Wocao] actors used similar tactics, techniques, and procedures (TTPs) and tools as those used by APT20, which suggests a possible overlap between the two groups. The name of the campaign, [Operation Wocao], was derived from an observed command line entry made by one of the threat actors, possibly indicating frustration at losing webshell access. The first activity related to the campaign was observed on 1 December 2017, and the last known campaign activity occurred on 1 December 2019.

campaign: CostaRicto
The campaign known as CostaRicto was a sophisticated hacker-for-hire cyber espionage operation that targeted various industries worldwide, with a significant focus on financial institutions. This campaign's actors were observed targeting organizations across Europe, the Americas, Asia, Australia, and Africa, with a particular concentration in South Asia, including India, Bangladesh, and Singapore. To achieve their objectives, the CostaRicto

actors utilized a combination of custom malware, open source tools, and a complex network of proxies and SSH tunnels. The first signs of activity related to this campaign were detected on 1 October 2019, and the last campaign's activities were observed on 1 November 2020.

On 7 December 2022, 2 attack-patterns had been published.

attack-pattern: T1573.002 - Asymmetric Cryptography
Adversaries may use a known asymmetric encryption algorithm as a way to hide their command and control traffic. Rather than relying on the inherent protections provided by a communication protocol, adversaries use public key cryptography, also known as asymmetric cryptography. This method uses a keypair per party: one public key that can be freely distributed, and one private key. The sender encrypts data with the receiver's public key, and the receiver decrypts the data with their private key, ensuring that only the intended recipient can read the encrypted data. RSA and ElGamal are common public key encryption algorithms. Although many protocols, including SSL/TLS, use symmetric cryptography for efficiency once a connection is established, they still use asymmetric cryptography to establish or transmit a key. As a result, these protocols are classified as using [Asymmetric Cryptography].

attack-pattern: T1090.003 - Multi-hop Proxy
The attack-pattern involves adversaries chaining multiple proxies together to disguise the source of malicious traffic. This technique poses a challenge for defenders as they may only be able to identify the last proxy before the traffic enters their network. The use of onion routing networks, such as the publicly available TOR network, is a common variant of this technique. In the case of network infrastructure, attackers may leverage multiple compromised devices to create a multi-hop proxy chain within the enterprise's Wide-Area Network (WAN). By exploiting the [Patch System Image] vulnerability, they can add custom code to the compromised network devices to implement onion routing between them. This creates a custom onion routing network that enables adversaries to communicate with any device within the network, while the encrypted command and control (C2) traffic is transported through the compromised devices. To bypass the organization's protected network boundary and enter the WAN, adversaries rely on the [Network Boundary Bridging] method, with protocols such as ICMP serving as a transport.