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 set's aliases are CostaRicto. The primary motivation of the group is financial gain. The group was observed for the first time on 24 May 2021 and for the last time on 15 October 2021. The intrusion-set's description is: [CostaRicto] is a suspected hacker-for-hire cyber espionage campaign that has targeted multiple industries worldwide since at least 2019. [CostaRicto]'s targets, a large portion of which are financial institutions, are scattered across Europe, the Americas, Asia, Australia, and Africa, with a large concentration in South Asia.

intrusion-set: Leviathan
The set's aliases are Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope and APT 40. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 18 April 2018 and for the last time on 15 April 2022. The intrusion-set's description is: [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. Active since at least 2009, [Leviathan] has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia..

intrusion-set: APT29
The set's aliases are APT29, IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear and CozyDuke. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 31 May 2017 and for the last time on 14 April 2022. The intrusion-set's description is: [APT29] is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and

think tanks. [APT29] reportedly compromised the Democratic National Committee starting in the summer of 2015.

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to [APT29], Cozy Bear, and The Dukes. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.

intrusion-set: APT28
The set's aliases are APT28, IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127 and TG-4127. The primary motivation of the group is information theft and espionage. The group was observed for the first time on 31 May 2017 and for the last time on 16 March 2022. The intrusion-set's description is: esempio di modifica.

On 4 November 2022, 2 campaigns had been published.

campaign: Operation Wocao
The campaign's aliases are Operation Wocao. Its description is: [Operation Wocao] was a cyber espionage campaign that targeted organizations around the world, including in Brazil, China, France, Germany, Italy, Mexico, Portugal, Spain, the United Kingdom, and the United States. The suspected China-based actors compromised government organizations and managed service providers, as well as aviation, construction, energy, finance, health care, insurance, offshore engineering, software development, and transportation companies.

Security researchers assessed the [Operation Wocao] actors used similar TTPs and tools as APT20, suggesting a possible overlap. [Operation Wocao] was named after an observed command line entry by one of the threat actors, possibly out of frustration from losing webshell access. First activity related to the campaign dates back to 1 December 2017, last campaign's activities were seen on 1 December 2019.

campaign: CostaRicto
The campaign's aliases are CostaRicto. Its description is: [CostaRicto] was a suspected hacker-for-hire cyber espionage campaign that targeted multiple industries worldwide, with a large number being financial institutions. [CostaRicto] actors targeted organizations in Europe, the Americas, Asia, Australia, and Africa, with a large concentration in South Asia (especially India, Bangladesh, and Singapore), using custom malware, open source tools, and a complex network of proxies and SSH tunnels. First activity related to the campaign dates back to 1 October 2019, last campaign's activities were seen on 1 November 2020.

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

attack-pattern: T1573.002 - Asymmetric Cryptography
The attack-pattern's description is: Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver's public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography]..

attack-pattern: T1090.003 - Multi-hop Proxy
The attack-pattern's description is: To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source. A particular variant of this behavior is to use onion routing networks, such as the publicly available TOR network.

In the case of network infrastructure, particularly routers, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain within the Wide-Area Network (WAN) of the enterprise. By leveraging [Patch System Image], adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This custom onion routing network will transport the encrypted C2 traffic through the compromised population, allowing adversaries to communicate with any device within the onion routing network. This method is dependent upon the [Network Boundary Bridging] method in order to allow the adversaries to cross the protected network boundary of the Internet perimeter and into the organization's WAN. Protocols such as ICMP may be used as a transport.