cloud.google.com

IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders

Mandiant

16–21 minutes

Written by: Michael Raggi

Mandiant Intelligence is tracking a growing trend among China-nexus cyber espionage operations where advanced persistent threat (APT) actors utilize proxy networks known as "ORB networks" (operational relay box networks) to gain an advantage when conducting espionage operations. ORB networks are akin to botnets and are made up of virtual private servers (VPS), as well as compromised Internet of Things (IoT) devices, smart devices, and routers that are often end of life or unsupported by their manufacturers. Building networks of compromised devices allows ORB network administrators to easily grow the size of their ORB network with little effort and create a constantly evolving mesh network that can be used to conceal espionage operations.

- By using these mesh networks to conduct espionage operations, actors can disguise external traffic between command and control (C2) infrastructure and victim environments including vulnerable edge devices that are being exploited via zero-day vulnerabilities.
- These networks often use both rented VPS nodes in combination

with malware designed to target routers so they can grow the number of devices capable of relaying traffic within compromised networks.

Mandiant assesses with moderate confidence that this is an effort to raise the cost of defending an enterprise's network and shift the advantage toward espionage operators by evading detection and complicating attribution. Mandiant believes that if network defenders can shift the current enterprise defense paradigm away from treating adversary infrastructure like indicators of compromise (IOCs) and instead toward tracking ORB networks like evolving entities akin to APT groups, enterprises can contend with the rising challenge of ORB networks in the threat landscape.

For even more on ORB networks, listen to our latest The Defender's Advantage podcast.

IOC Extinction and the Rise of ORB Networks

The cybersecurity industry has reported on the APT practice of ORB network usage in the past as well as on the functional implementation of these networks. Less discussed are the implications of broad ORB network usage by a multitude of China-nexus espionage actors, which has become more common over recent years. The following are three key points and paradigm shifting implications about ORB networks that require enterprise network defenders to adapt the way they think about China-nexus espionage actors:

- **ORB networks undermine the idea of "Actor-Controlled Infrastructure":** ORB networks are infrastructure networks administered by independent entities, contractors, or administrators within the People's Republic of China (PRC). They are not controlled by a single APT actor. ORB networks create a

network interface, administer a network of compromised nodes, and contract access to those networks to **multiple APT actors** that will use the ORB networks to carry out their own distinct espionage and reconnaissance. These networks are not controlled by APT actors using them, but rather are temporarily used by these APT actors often to deploy custom tooling more conventionally attributable to known China-nexus adversaries.

- **ORB network infrastructure has a short lifespan and IOC extinction is accelerating:** Based on Mandiant's regular tracking of ORB networks, the lifespan of an IPv4 address associated with an ORB node can be in an ORB network for as few as 31 days. Each ORB network has different practices for cycling infrastructure as part of their ORB networks infrastructure. However, a competitive differentiator among ORB network contractors in China appears to be their ability to cycle significant percentages of their compromised or leased infrastructure on a monthly basis. Therefore, simply blocking infrastructure observed in association with ORB network behavior is not as effective as blocking C2 infrastructure would have been in the period between 2005 and 2016. As a result, IOC extinction is accelerating and the shelf life of network indicators is decreasing.
- **Attributing espionage operations cannot rely on network infrastructure alone:** From a defender's perspective, the egress IP address observed in relation to an APT attack has for years been a key artifact used to research an intrusion's attribution. In the case of China-nexus attacks, attribution is growing both more challenging and more non-specific. Infrastructure or the compromised router device communicating with a victim environment may now be identifiable to a particular ORB network, while the actor using that ORB network to carry out the attack may be unclear and require investigation of the complex

tools and tactics observed as part of an intrusion. These networks allow actors to egress from devices that have a geographic proximity to targeted enterprises, which allows traffic to blend in or otherwise not be anomalous when being reviewed by analysts or operational personnel making risk-based access decisions. One such example would be traffic from a residential ISP that is in the same geographic location as the target that is regularly used by employees and would be less likely to get picked up for manual review. The weaponization phase of the cyber kill chain now appears to be administered by third-party providers, complicating the definitive attribution of cyberattacks using network indicators and increasing the difficulty of detecting anomalous traffic.

The Anatomy of an ORB Network

ORB networks are always made up of network infrastructure nodes. These nodes can be compromised routers, leased VPS devices, or often a mixture of both. While earlier commercial incarnations of ORB networks date back to 2016, the modern incarnation of networks like ORB1 / ORBWEAVER can be tracked back to at least 2020. The nodes in any given ORB network are usually distributed globally across the world and are not geographically specific to any one location. ORB network administrators rely on ASN providers in different parts of the world to reduce exposure or dependence on any one nation's internet infrastructure. An example of global distribution of an ORB network can be seen as follows in what Mandiant tracks as ORB3 or SPACEHOP, a very active network leveraged by multiple China-nexus threat actors. The high volume of APT-related traffic through globally distributed nodes indicates that this network is utilized to target a wide array of geographic targets colocated in

the geographies of observed exit nodes. Notably, this network maintains a robust volume of nodes in Europe, the Middle East, and the United States. These geographies have been observed as targets of APT15 and UNC2630 (a cluster of activity with suspected links to APT5) and have previously been observed using this network. This network also diversifies its nodes by registering VPS-based devices with multiple commercially available Autonomous System providers.

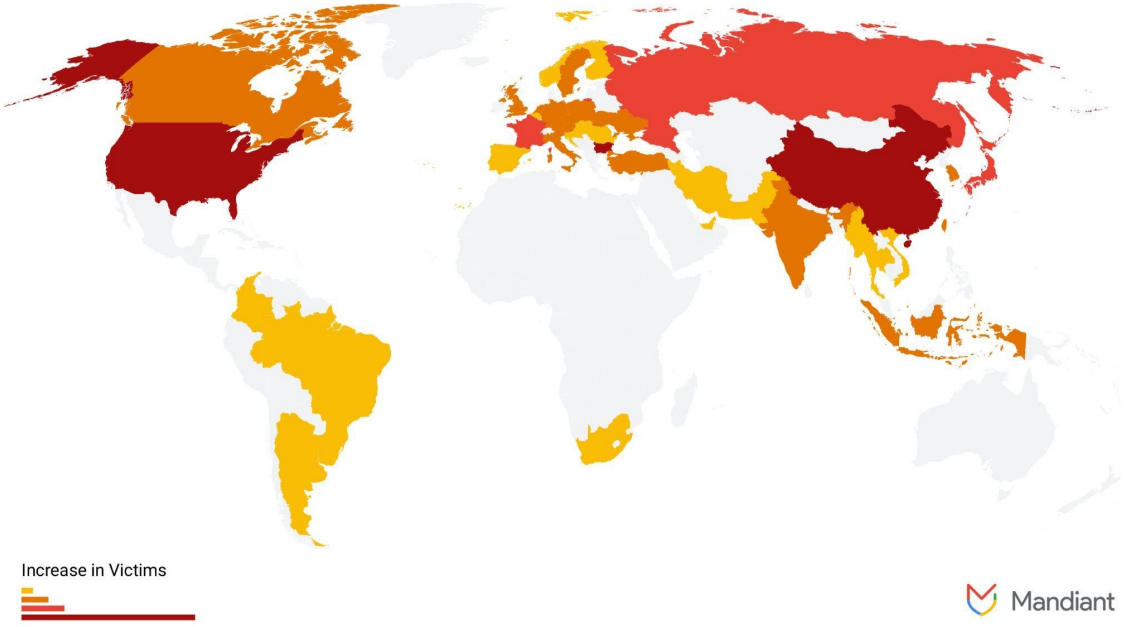


Figure 1: Country heatmap of ORB3 / SPACEHOP nodes 2023

Autonomous System	**Percent of Observed SPACEHOP Nodes**
Shenzhen Tencent Computer Systems Company Limited (CN)	7.73%
Hangzhou Alibaba Advertising Co.,Ltd. (CN)	4.55%
Tencent Building, Kejizhongyi Avenue (CN)	4.24%

OVH SAS (FR)	4.02%
Stark Industries Solutions Ltd (UK)	2.95%
BrainStorm Network, Inc (CA)	2.50%
TWC (US)	2.42%
Green Floid LLC (PL)	2.12%
Kaopu Cloud HK Limited (HK)	2.12%
AS-CHOOPA (US)	1.82%

Table 1: Top 10 Autonomous System providers and percent composition of ORB3 / SPACEHOP network

ORB Network Classifications

Mandiant classifies ORB networks into two fundamental types. Networks can be **provisioned networks**, which are made up of commercially leased VPS space that are managed by ORB network administrators, or they can be **non-provisioned networks**, which are often made up of compromised and end-of-life router and IoT devices. It is also possible for an ORB network to be a hybrid network combining both leased VPS devices and compromised devices. Mandiant notes that it has observed both a wide diversity of China-nexus threat actors using each kind of ORB network. The type of threat actor organization does not appear to limit which type of network threat actors utilize, despite historic indications that military-related entities have preferred procured networks in the past. Alternatively, threat actors with a civilian intelligence background have proven more likely to utilize non-provisioned networks consisting of routers compromised by

custom malware.

Provisioned Networks	Non-Provisioned Networks
Leased VPS devices via commercial services	Compromised routers and IoT devices
Actor administration of nodes	Actor augmentation of network through custom router-based payloads
Provisioned networks require actors to manage virtual images or operating systems on leased devices.	Many non-provisioned networks will use leased VPS devices as adversary-controlled operations servers ("ACOS nodes")

Table 2: Characteristics of provisioned and non-provisioned ORB networks

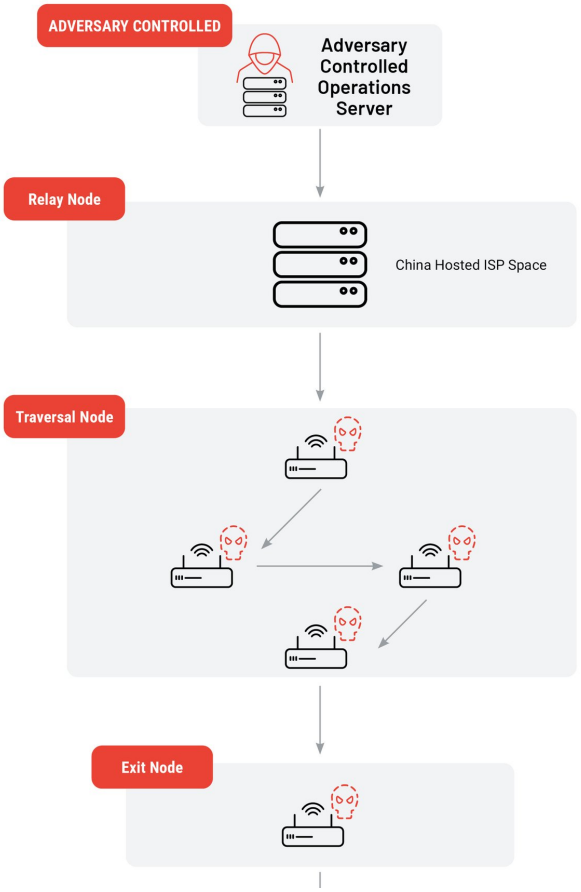
ORB Network Universal Anatomy

After continuous analysis of numerous ORB networks spanning years, Mandiant has designed a universal anatomy for analyzing and labeling ORB network components. This anatomy is intended to serve as a guide for enterprise defenders when identifying malicious ORB network node infrastructure. All networks that are identified will have a universal set of identifiable components. While the configuration of these components may differ between networks and the traversal path through an ORB network may appear different on a case by case basis, the following components are essential for an ORB network to function:

- **Adversary Controlled Operations Server ("ACOS")**: This is an adversary-controlled server used to administer nodes within an

ORB network.

- **Relay Node:** This is most commonly a leased VPS node at a major China or Hong Kong-based cloud provider. This node allows users of an ORB network to authenticate to the network and relay traffic through the larger traversal pool on ORB nodes.
- **Traversal Nodes:** These are the primary volume of nodes that make up an ORB network. These can be either provisioned or non-provisioned nodes and are used to relay traffic across an ORB network obfuscating the origin of network traffic. Some networks may utilize multiple types of traversal nodes or include multiple traversal layers.
- **Exit/Staging Nodes:** These are actor-controlled nodes often exhibiting the same characteristics as traversal nodes that are used to egress from an ORB network into a victim environment.
- **Victim Server:** The targeted victim's infrastructure communicating with the ORB network node.



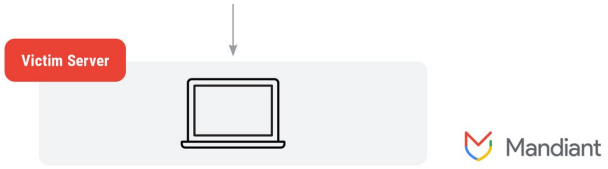


Figure 2: Diagram of the Universal Anatomy of an ORB network

Mandiant notes that the ACOS servers and relay nodes are most commonly hosted in PRC-affiliated and Hong Kong-based IP space. Analysts believe that by placing these critical servers behind the Great Firewall, ORB network administrators may limit their exposure to both legal and disruptive actions of targeted entities.

Examples of Active ORB Networks in the Wild

ORB3 / SPACEHOP - Provisioned Network

A primary example of a provisioned ORB network leveraged in the wild by numerous APTs is a network tracked by Mandiant as ORB3 / SPACEHOP. This network consists of servers provisioned by a single entity operating in China. The network has facilitated network reconnaissance scanning and vulnerability exploitation conducted by China-nexus threat actors, including APT5 and APT15.

The infrastructure present in the ORB3 network represents a threat to entities that have historically been targeted by APT15 and APT5, including entities in North America, Europe, and the Middle East. Active since at least 2019, UNC2630 (with suspected links to APT5), used a known SPACEHOP node to exploit CVE-2022-27518 in late December 2022. The National Security Agency (NSA) linked exploitation of CVE-2022-27518 within the same time frame to APT5.

This ORB network's topography is rather flat when compared to

more complex ORB networks. It leverages a relay server hosted in either Hong Kong or China by cloud providers and installs a C2 framework available on GitHub for the administration of downstream relay nodes. The relay nodes are often cloned Linux-based images, which are used to proxy malicious network traffic through the network to an exit node that communicates with targeted victim environments.

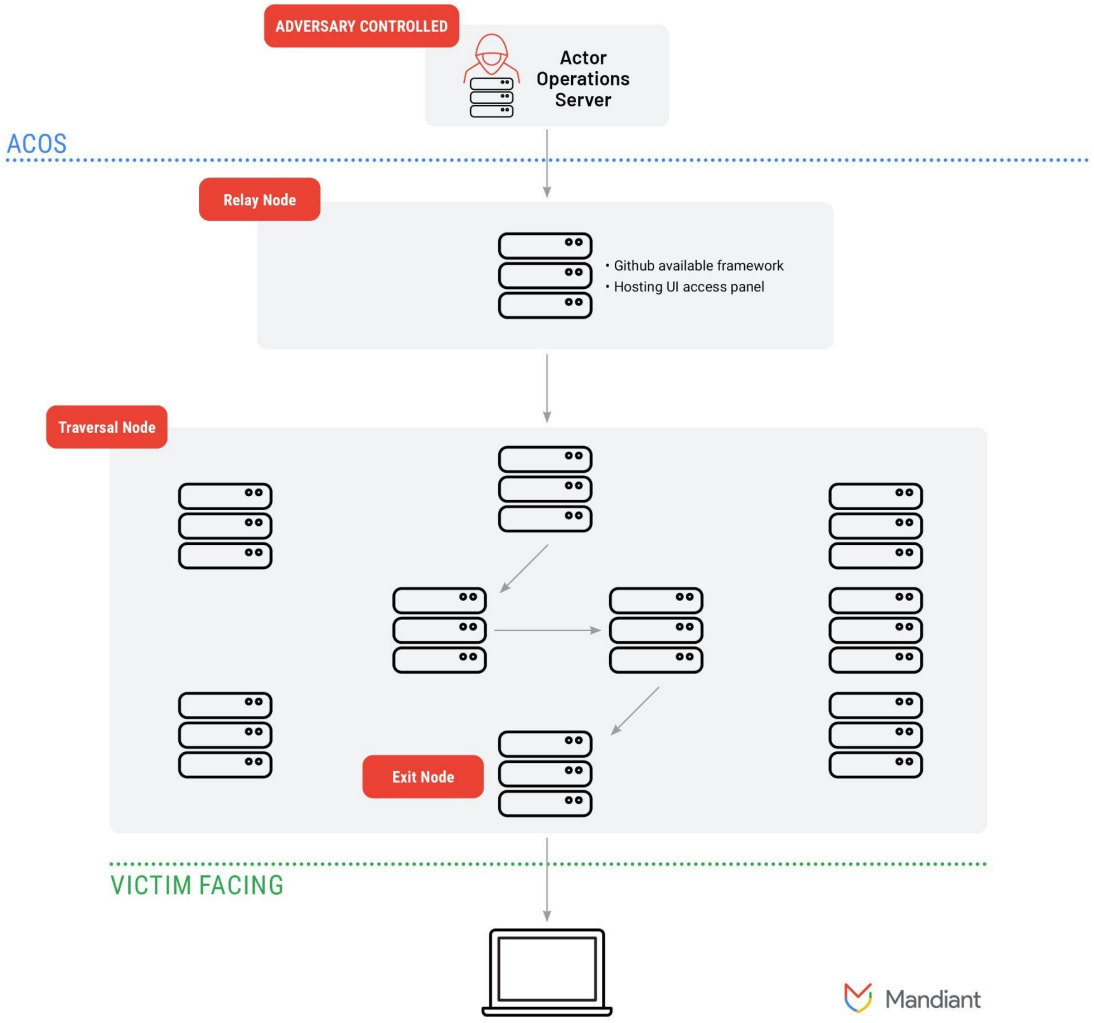


Figure 3: ORB3 / SPACEHOP network diagram

ORB2 FLORAHOX - Non-Provisioned Network

FLORAHOX is an example of both a non-provisioned and a hybrid ORB network. It is composed of an ACOS node, compromised network router and IOT devices, and leased VPS servers that interface with a customized TOR relay network layer. The network

is used to proxy traffic from a source and relay it through a TOR network and several compromised router nodes to obfuscate the source of the traffic. It is believed to be used in cyber espionage campaigns by a diverse set of China-nexus threat actors.

The network appears to contain several subnetworks composed of compromised devices recruited by the router implant FLOWERWATER as well as other router-based payloads. Subnetworks are capable of being used in an overlapping manner to relay malicious traffic through the network segments. FLORAHOX appears to be multi-tenanted with several distinct router compromise payloads being used for the augmentation of the network and several APT threat actors leveraging the network. While it appears several actors may utilize the FLORAHOX network, China-nexus threat actors including clusters of activity publicly tracked as APT31 and Zirconium have been reported by multiple trusted third-party sources to utilize the network.

An additional tool that was determined to be a MIPS router tunneler payload (PETALTOWER) and related controller Bash scripts, which provide command-line inputs to the PETALTOWER payload (SHIMMERPICK), were identified in January 2023. The purpose of these tools appears to be providing a configuration for the traversal of the network and traversing the network of pre-existing FLORAHOX nodes based on command-line inputs.

ORB2 represents a more complicated design including the relay of traffic through TOR nodes, provisioned VPS servers, and different types of compromised routers including CISCO, ASUS, and Draytek end-of-life devices. The network embodies years of continual augmentation and several generations of distinct router-based payloads used simultaneously to recruit vulnerable devices into the FLORAHOX traversal node pool.

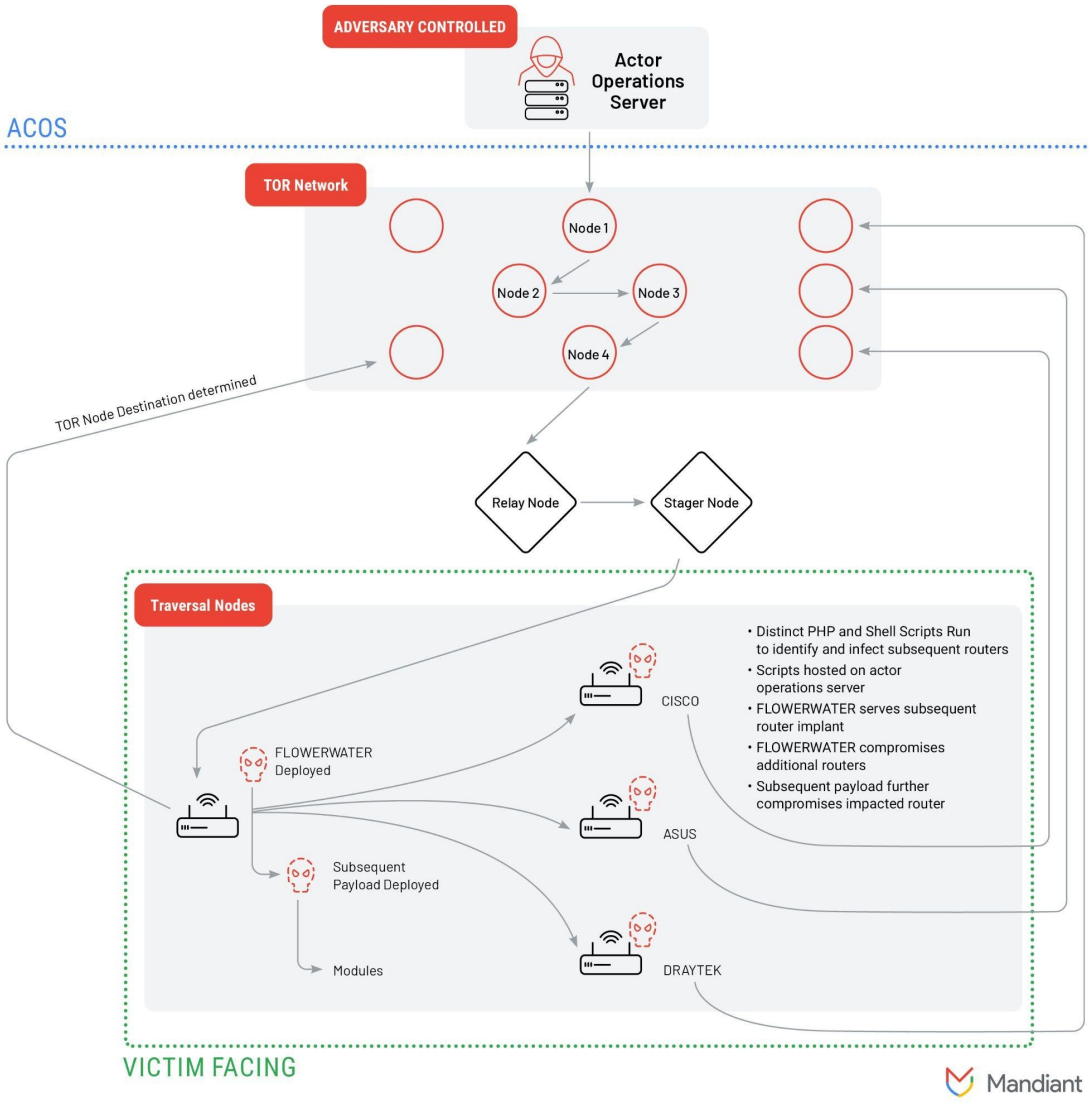


Figure 4: ORB2 / FLORAHOX network diagram

The Defender's Dilemma

The widespread adoption of ORB networks by China-nexus espionage actors introduces a new layer of complexity to defending enterprise environments from malicious infrastructure. Rather than earlier practices allowing for the outright blocking of adversary infrastructure, defenders must now consider:

- **Temporality:** What Infrastructure is part of the ORB network right now?
- **Multiplicity of Adversaries:** Which adversaries are using this ORB network and am I seeing one of them targeting my network?

- **Ephemerality:** How long is this infrastructure part of the ORB network being defended against and are changing characteristics of infrastructure indicative of new tactics?

  Mandiant asserts that the best way to rise to the challenge posed by ORB networks is to stop tracking espionage C2 infrastructure as an inert indicator of compromise and start tracking it as an entity with distinct TTPs. We no longer operate in the world of "block and move on" where IPs are part of APT's weaponization and C2 kill chain phase. Instead, infrastructure is a living artifact of an ORB network that is a distinct and evolving entity where the characteristics of IP infrastructure itself, including ports, services, and registration/hosting data, can be tracked as evolving behavior by the adversary administrator responsible for that ORB network.

  By shifting awareness and our enterprise defender paradigm toward treating ORB networks like APTs instead of IOCs, defenders can begin to turn their dilemma into a defender's advantage.

Conclusion

Use of ORB networks to proxy traffic in a compromised network is not a new tactic, nor is it unique to China-nexus cyber espionage actors. However, its ubiquity that has evolved over the past four years now requires defenders to meet this challenge head on to keep pace with adversaries in the cyber espionage landscape. We have tracked China-nexus cyber espionage using these tactics as part of a broader evolution toward more purposeful, stealthy, and effective operations. In addition to wanting to be stealthy, actors want to increase the cost and analytical burden on defenders of enterprise environments. The rise of the ORB network industry in China points to long-term investments in equipping China-nexus

cyber operators with more sophisticated tactics and tools that facilitate enterprise exploitation to achieve higher success rates in gaining and maintaining access to high-value networks. Whether defenders will rise to this challenge depends on enterprises applying the same deep tactical focus to tracking ORB networks as has been done for APTs over the last 15 years. Mandiant is equipped to provide enterprise defenders with the capability to meet this challenge and scale to overcome it.

Posted in

- Threat Intelligence