Stealth Mode: Chinese Cyber Espionage Actors Continue to Evolve Tactics to Avoid Detection

Mandiant Intelligence is tracking several ways in which Chinese cyber espionage activity has increasingly leveraged initial access and post-compromise strategies intended to minimize opportunities for detection. Specifically, this analysis highlights Chinese threat groups' exploitation of zero-days in security, networking, and virtualization software, and targeting of routers and other methods to relay and disguise attacker traffic both outside and inside victim networks. We assess with high confidence that Chinese cyber espionage groups are using these techniques to avoid detection and complicate attribution.

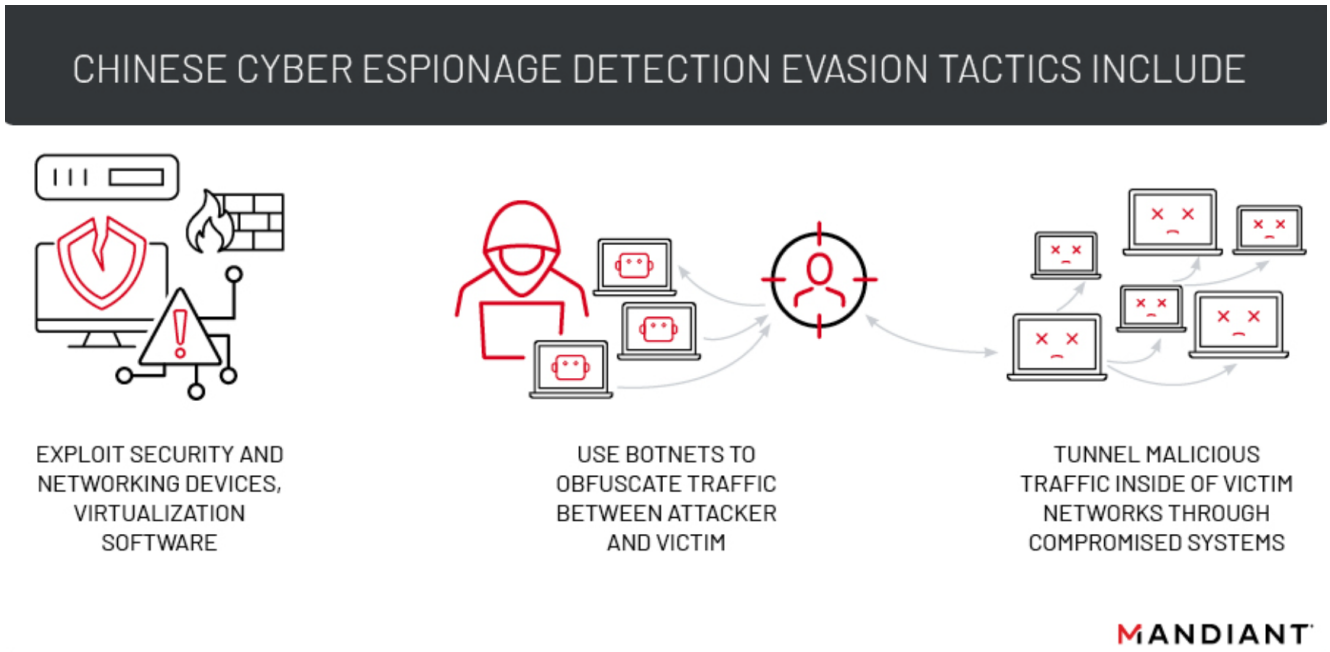

Figure 1: Chinese cyber espionage detection evasion tactics

This post builds upon previous analysis in which Mandiant assessed that Chinese cyber espionage operators' tactics had steadily evolved to become more agile, stealthier, and complex to attribute in the years following the mid 2010s military and intelligence restructuring. The research cites increased use of living-off-the-land (LotL) techniques, software supply chain compromise, and publicly available, fileless, or modular malware as evidence of increased stealth.

China Focuses on Networking, Security, and Virtualization Software

Mandiant Intelligence assesses with high confidence that Chinese cyber espionage zero-day exploitation in 2021 and 2022 has focused on security, networking, and virtualization technologies because targeting these devices affords several tactical advantages in obtaining and retaining surreptitious access to victim networks.

For instance, security and networking devices are “edge devices,” meaning they are accessible to the internet. With a successful exploit, an attacker can achieve initial access without human interaction, decreasing chances of detection. As long as the exploit remains undiscovered, the threat actor can reuse it to gain access to additional victims, or reestablish access to targeted systems. Moreover, both edge devices and virtualization software are challenging to monitor and may not support endpoint detection and response (EDR) solutions or methods to detect modifications or collect forensic images, further reducing the likelihood of detection and complicating attribution.

Two recent campaigns exemplify notable strategies Chinese threat actors have used to maximize stealth including, but not limited to, zero-day exploitation.

UNC3886 Burned Two Zero-Days in Complex Ops against Hard Targets

In 2022, Mandiant investigated incidents in which suspected Chinese cyber espionage actor, UNC3886, used multiple attack paths and two zero-day vulnerabilities to establish persistence at targeted organizations and ultimately gain access to virtualized environments. UNC3886 has primarily targeted defense industrial base (DIB), technology, and telecommunication organizations in the U.S. and Asia.

UNC3886 took extraordinary measures to remain undetected in victim environments. The attackers limited their presence on networks to Fortinet security devices and VMware virtualization technologies, devices and platforms that traditionally lack EDR solutions. The group’s custom malware and exploits prioritized circumventing logs and security controls, for example, using non-traditional protocols (VMCI sockets) that are not logged by default and have no security restrictions to interact between hypervisors and guest virtual machines (VMs). UNC3886 also cleared and modified logs and disabled file system verification on startup to avoid getting detected.

- The threat actor used malware families designed to interact with Fortinet devices, including THINCRUST, CASTLETAP, TABLEFLIP, and REPTILE. UNC3886 took advantage of path traversal vulnerability CVE-2022-41328 to overwrite legitimate files in a normally restricted system directory (Figure 2).
- With access to targeted organizations’ Fortinet devices, the threat actor interacted with VMware vCenter servers and leveraged malicious vSphere Installation Bundles (“VIBs”) to install customized backdoors VIRTUALPITA and VIRTUALPIE on ESXi hypervisors. UNC3886 exploited an authentication bypass vulnerability CVE-2023-20867 on ESXi hosts to enable the execution of privileged commands on guest VMs with no additional logs generated on guest VMs.

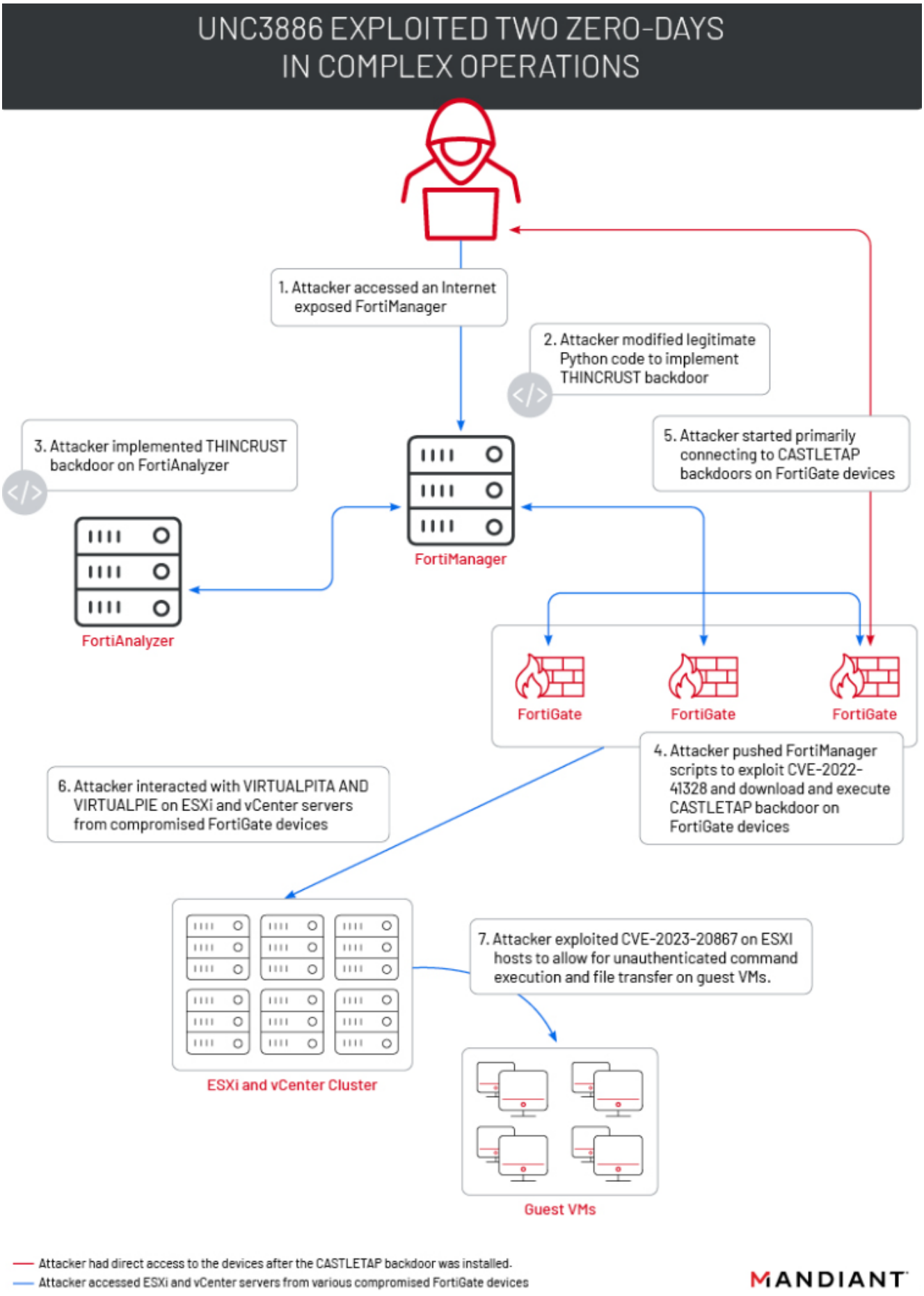

Figure 2: UNC3886 exploits two zero-days in complex operations

Mandiant recommends organizations using ESXi and the VMware infrastructure suite follow the hardening steps outlined in [this blog post to minimize the attack surface of ESXi hosts](), and refer to this

additional guide laying out detection, containment, and hardening opportunities to counter observed UNC3886 operations.

UNC4841 Exploitation of Barracuda ESG Began Stealthy, Turned Aggressive

Beginning in at least October 2022, suspected Chinese cyber espionage actor UNC4841 exploited a zero-day vulnerability, CVE-2023-2868, in Barracuda Email Security Gateway (ESG) appliances in a campaign targeting public and private organizations worldwide. In several cases we observed evidence of the actor searching for email data of interest before staging it for exfiltration. The actor showed specific interest in information of political or strategic interest to China. This included the global targeting of governments and organizations associated with verticals of high priority to China. Further, in the set of entities selected for focused data exfiltration, shell scripts were uncovered that targeted email domains and users from Ministries of Foreign Affairs (MFAs) of ASEAN member nations as well as individuals within foreign trade offices and academic research organizations in Taiwan and Hong Kong.

UNC4841 sought to disguise elements of its activity in a number of ways. In addition to continuing the pattern of targeting a security appliance, UNC4841 sent emails with specially crafted TAR file attachments that exploited CVE-2023-2868 and allowed the attackers to execute arbitrary system commands with the elevated privileges of the ESG product (Figure 3). We assess that the subject line and body of the emails UNC4841 sent as part of this campaign were likely crafted to be caught in spam filters and discourage further investigation. Mandiant has observed advanced groups exploiting zero-days use this tactic in the past. UNC4841 also developed custom malware utilizing naming conventions consistent with legitimate ESG files (including SALTWATER, SEASIDE, SEASPY) as well as inserted custom backdoor code into legitimate Barracuda modules (including SEASPRAY and SKIPJACK). In some cases, UNC4841 used legitimate self-signed SSL temporary certificates that are shipped on ESG appliances for setup purposes as well as certificates stolen from victim environments to masquerade the command and control (C2) traffic.

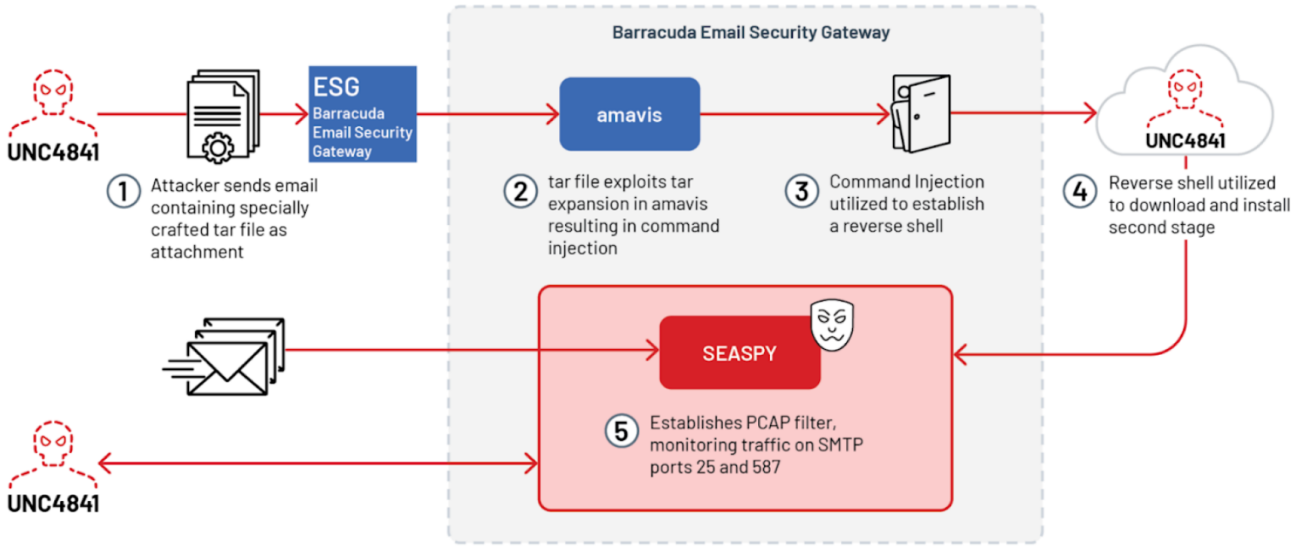

Figure 3: SEASPY attack path

Another remarkable element of this campaign was the threat actor's aggressive response to remediation efforts and the activity going public. Following Barracuda's vulnerability disclosure and initial remediation actions, UNC4841 countered by moving rapidly to alter its malware, employ additional persistence mechanisms, and move laterally in an attempt to maintain access to compromised environments. Barracuda currently recommends replacing compromised appliances. Mandiant also released a hardening, remediation, and hunting guide for Barracuda ESG devices earlier this year.

Additional Examples

The previous case studies represent just two among a growing list of notable Chinese cyber espionage incidents and campaigns exploiting zero-days in security and networking products.

- Mandiant described exploitation of CVE-2022-42475, a vulnerability in Fortinet's FortiOS SSL-VPN, with the earliest evidence dating to October 2022.
- In December 2022, Citrix reported in-the-wild exploitation of CVE-2022-27518 in its Application Delivery Controller (ADC), which the U.S. National Security Agency (NSA) attributed to APT5.
- In March 2022, Sophos reported in-the-wild exploitation of CVE-2022-1040 in its Firewall product, which Volexity linked to Chinese cyber espionage actors.
- Mandiant investigated multiple intrusions that occurred between August 2020 and March 2021 and involved exploitation of CVE-2021-22893 in Pulse Secure VPNs.
- In March 2021, Mandiant identified three zero-day vulnerabilities that were exploited in SonicWall's Email Security (ES) product (CVE-2021-20021, CVE-2021-20022, CVE-2021-20023).

Chinese Actors Disguise External and Internal Traffic with Botnets and Tunnels

More frequently in the last three years, Mandiant has identified examples of Chinese cyber espionage operations using botnets of compromised internet of things (IoT) devices, smart devices, and routers to disguise external traffic between C2 infrastructure and victim environments, as well as numerous malware families that include functionalities to covertly relay attacker traffic within compromised networks. We judge that the operators are using these tactics to evade detection and to complicate attribution.

Botnet-as-Smokescreen

We identified a number of examples of Chinese cyber espionage groups using botnets to obfuscate traffic between attackers and victim networks, including APT41, APT31, APT15, TEMP.Hex, and Volt Typhoon.

- In May 2023, Microsoft reported Chinese cyber espionage activity dubbed "Volt Typhoon" targeting critical infrastructure organizations in the United States. In conjunction with other techniques, likely intended to limit detection opportunities, the threat actor reportedly used a botnet of compromised SOHO devices to route network traffic.
    - Mandiant believes the activity described in Microsoft's report overlaps substantially with an activity cluster we have seen targeting government and transportation organizations, as well as exploiting a recently disclosed vulnerability in Zoho ADSelfService Plus.

- In 2023, CheckPoint described a suspected Chinese cyber espionage group it describes as “Camaro Dragon” using a custom backdoor dubbed “Horse Shell” in activity targeting European foreign affairs organizations. Horse Shell is a malicious implant that was discovered within a modified TP-Link router firmware image. It enables the attacker to establish an SSH encrypted SOCKS proxy and transfer files. CheckPoint assesses that the threat actor infected residential routers to obfuscate traffic between command and control servers and compromised victims. Mandiant has not independently verified this activity, but the reported network infrastructure has limited overlaps to public reporting we track as TEMP.Hex.
- In 2022 PricewaterhouseCoopers (PwC) reported on BPFDOOR malware, which allegedly received commands from virtual private servers (VPS) that were controlled by a network of Taiwan-based compromised routers.
    - Mandiant has observed evidence that an activity cluster potentially related to APT41 used BPFDOOR to target South Asian government organizations and a Chinese multinational corporation.
- PwC also reported that it observed Chinese cyber espionage actor Red Vulture using a shared proxy network dubbed RedRelay in 2021 and 2022. Red Vulture is described as corresponding to APT15, APT25, and Ke3chang.
- French and U.S. authorities issued public reports highlighting Chinese state sponsored actors’ exploitation of network devices such as small office/home office (SOHO) routers to route traffic between C2 infrastructure and victim networks (see Figure 4). The 2022 U.S. advisory also mentions exploitation of Network Attached Storage (NAS) devices. The 2021 French advisory describes a specific campaign they attribute to APT31.
- ESET reportedly observed a Linux backdoor they track as SideWalk used to compromise a Hong Kong university in February 2021. ESET believes SideWalk to be exclusively used by the SparklingGoblin APT. While they were unable to confidently identify the initial infection vector for this operation, they hypothesized that it could have been exploitation of a router vulnerability because of significant overlaps between SideWalk and a botnet malware, dubbed Specter, that Netlab 360 described in September 2020. Specter reportedly propagates by exploiting vulnerabilities in AVTECH IP camera, NVR, and DVR devices.
    - Mandiant attributes most of the activity ESET described to APT41. We track the SideWalk malware family as MOPSLED and its loader as DUSTPAN. We have seen both APT41 and UNC3886 use MOPSLED. We consider MOPSLED to be an evolution of CROSSWALK, which can act as a network proxy.

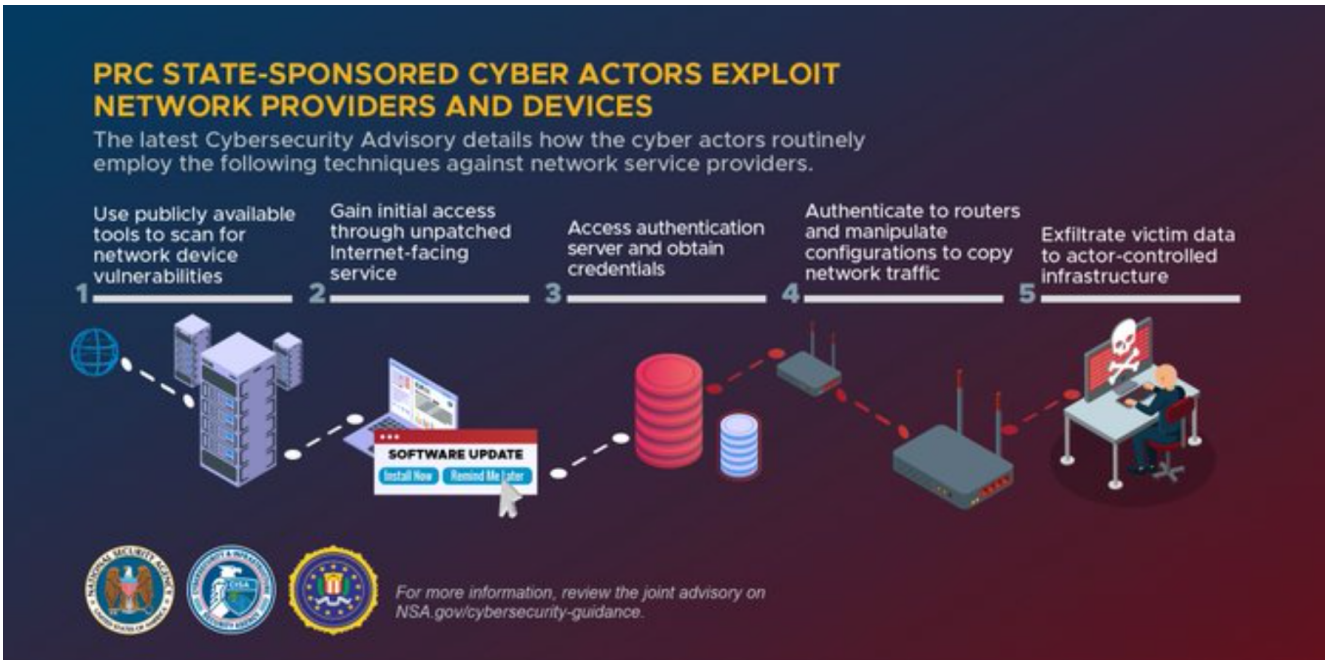

Figure 4: Chinese cyber espionage tactics exploiting network devices (Source: NSA)

Your Router is My Router

Mandiant also noted evidence of suspected Chinese cyber espionage operators deploying custom malware to relay and disguise traffic within victim networks, for example, using DNS, HTTP, and TCP/IP hijacking.

Table 1: Malware families used to proxy malicious traffic within compromised networks

Malware	Description
ZuoRAT	In June 2023, Lumen's Black Lotus Labs described a multi-stage remote access Trojan (RAT) dubbed "ZuoRAT" that it observed exploiting known vulnerabilities affecting Asus, Cisco, DrayTek, and Netgear SOHO routers throughout North America and Europe. According to the researchers, "ZuoRAT is a MIPS file compiled for SOHO routers that can enumerate a host and internal LAN, capture packets being transmitted over the infected device, and perform adversary-in-the-middle attacks (DNS and HTTPS hijacking based on predefined rules)." The researchers also claim to have identified infected routers acting as proxy C2 nodes. Mandiant has not independently verified this activity.
DELIMEAT	In early 2022, Symantec described malware dubbed Daxin that can hijack legitimate TCP/IP encrypted channels and relay its communications across infected machines within a targeted network. Notably, Symantec reports that the earliest sample of this malware they identified dates from 2013. Mandiant tracks elements of Daxin as DELIMEAT.
EYEWELL	EYEWELL, malware we have seen TEMP.Overboard deploy primarily against Taiwanese government and technology targets, contains a passive proxy capability that can be used to relay traffic from other systems infected with EYEWELL within a victim environment. Notably, Mandiant reported that a TEMP.Overboard malware identified in 2019 that shared similarities with EYEWELL also included functionality customized to disable part of the process listing and network functionality of an endpoint security product.

HYPERBRO and FOCUSFJORD	In an analysis of UNC215 intrusions against Middle Eastern and Central Asian targets in 2019 and 2020, Mandiant noted evidence that UNC215 made technical modifications to HYPERBRO and FOCUSFJORD to incorporate the ability to act as proxies and relay communications to their C2 servers, likely to minimize the risk of detection and blend in with normal network traffic.
LOOTALLEY	In 2019, Mandiant identified samples of the LOOTALLEY backdoor that contained a module potentially supporting the capability to conduct HTTP hijacking or other adversary-in-the-middle (AiTM) functionality. We observed LOOTALLEY in suspected Chinese cyber espionage operations likely targeting foreign companies operating in China and other domestic targets of interest.

Conclusion

Use of botnets, proxying traffic in a compromised network, and targeting edge devices are not new tactics, nor are they unique to Chinese cyber espionage actors. However, during the last decade, we have tracked Chinese cyber espionage actors' use of these and other tactics as part of a broader evolution toward more purposeful, stealthy, and effective operations. We suggest that the military and intelligence restructure, evidence of shared development and logistics infrastructure, and legal and institutional structures directing vulnerability research through government authorities point to long term investments in equipping Chinese cyber operators with more sophisticated tactics, tools, and exploits to achieve higher success rates in gaining and maintaining access to high value networks. The examples highlighted here indicate that these investments are bearing fruit.