CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

June 24, 2024

Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation

RedJuliett targeted government, university, technology, and diplomacy sectors in Taiwan and likely compromised entities in Hong Kong, South Korea, Laos, the United States, Rwanda, Kenya, and Djibouti.

Internet-facing devices such as firewalls, load balancers, and enterprise VPNs were targeted for initial access. SQL injection and directory traversal was attempted against web and SQL applications.

RedJuliett likely operates from Fuzhou, Fujian province, China. The group used SoftEther VPN to administer operational infrastructure from suspected source range infrastructure geolocating to Fuzhou.

Note: The analysis cut-off date for this report was April 26, 2024

Executive Summary

Between November 2023 and April 2024, Insikt Group identified cyber-espionage activity predominantly targeting government, education, technology, and diplomatic organizations in Taiwan, conducted by a likely Chinese state-sponsored threat activity group we track as RedJuliett.[1] While this focus on Taiwan aligns with the group's past activity, we also observed wider targeting against entities in Hong Kong, Malaysia, Laos, the Philippines, South Korea, Kenya, Rwanda, Djibouti, and the United States.

Insikt Group identified 24 suspected victim organizations communicating with RedJuliett servers via a SoftEther bridge, including government organizations in Taiwan, Laos, Kenya, and Rwanda. RedJuliett also conducted network reconnaissance or attempted exploitation against over 70 Taiwanese organizations in the academic, government, think tank, and technology sectors, as well as multiple de facto embassies. The group targets internet-facing appliances such as firewalls, load balancers, and enterprise virtual private network (VPN) products for initial access, as well as attempting structured query language (SQL) injection and directory traversal exploits against web and SQL applications. In some cases, we identified RedJuliett conducting post-exploitation activity using open-source web shells and exploiting a known elevation of privilege vulnerability in the Linux operating system. Additionally, RedJuliett used SoftEther to administer operational infrastructure consisting of both threat actor-controlled servers leased from virtual private server (VPS) providers and compromised infrastructure belonging to three Taiwanese universities.

Insikt Group assesses that RedJuliett likely operates out of Fuzhou, Fujian province, China, given that multiple RedJuliett SoftEther nodes have been consistently administered from IP addresses that geolocate to Fuzhou. This operating location aligns with the group's persistent targeting of Taiwan. Given the close geographical proximity between Fuzhou and Taiwan, Chinese intelligence services operating in Fuzhou are likely tasked with intelligence collection against Taiwanese targets.

RedJuliett is likely targeting Taiwan to collect intelligence and support Beijing's policy-making on cross-strait relations. RedJuliett displayed an interest in targeting critical technology companies, which aligns with previous public reporting. Targeting patterns also suggest that RedJuliett is likely interested in collecting intelligence on Taiwan's economic policy and trade and diplomatic relations with other countries. RedJuliett, like many other Chinese threat actors, is likely targeting vulnerabilities in internet-facing devices because these devices have limited visibility and security solutions available, and targeting them has proven to be an effective way to scale initial access.

Due to a focus on exploiting known vulnerabilities in public-facing devices and applications, organizations likely to be targeted by RedJuliett should complement routine vulnerability patching with

[1] RedJuliett closely overlaps with public reporting under the aliases Flax Typhoon (Microsoft) and Ethereal Panda (CrowdStrike).

additional defense-in-depth strategies. These strategies should emphasize detecting post-exploitation persistence, discovery, and lateral movement activities. Organizations should also regularly audit internet-facing and perimeter appliances and reduce attack surfaces by disabling interfaces or portals where not required. Many public-facing appliances have limited visibility, logging capabilities, and support for traditional security solutions; organizations should consider these factors when initially procuring network appliances to better detect and respond to threats.

Unless the security of internet-facing devices is improved or organizations take steps to move away from vulnerable edges, Chinese state-sponsored threat actors will almost certainly continue to exploit these devices. As Taiwan faces ongoing sovereignty threats from the People's Republic of China (PRC) while simultaneously serving as a critical global technology and manufacturing hub, RedJuliett will almost certainly continue to conduct high-tempo cyber-espionage operations with a focus on Taiwanese technology, government, educational, and think tank organizations.

Key Findings

- RedJuliett has likely compromised organizations in Taiwan, Hong Kong, South Korea, Laos, the United States, Rwanda, Kenya, and Djibouti.
- Additionally, RedJuliett has conducted vulnerability scanning or attempted exploitation against de facto embassies, Taiwanese universities, government entities, think tanks focused on Taiwanese economic policy, aerospace companies, electronics manufacturers, computing industry associations, and more.
- RedJuliett was observed administering multiple SoftEther nodes from suspected source-range infrastructure geolocating to Fuzhou, Fujian province, China.
- Insikt Group anticipates that Chinese state-sponsored groups will continue to target Taiwanese government agencies, universities, and critical technology companies. We also anticipate that RedJuliett will continue to focus on exploiting public-facing devices, as these have limited visibility, logging capabilities, and support for traditional security solutions.

Background

As first reported by Microsoft in August 2023, Flax Typhoon (RedJuliett) has been observed primarily targeting organizations in Taiwan using living-off-the-land (LotL) techniques and the open-source VPN software SoftEther. The group has been active since mid-2021 and has targeted government agencies, education, critical manufacturing, and IT organizations in Taiwan. To gain initial access to Taiwanese networks, Flax Typhoon exploited vulnerabilities in public-facing services, such as VPN, web, and SQL applications. The group then used the China Chopper web shell on compromised servers to establish persistence and remotely execute code. Following initial access, the group relied on open-source tools, such as JuicyPotato and BadPotato, and LotL techniques. CrowdStrike reporting on Ethereal Panda notes very similar tactics, techniques, and procedures (TTPs) and the group's use of the open-source web shell Godzilla.

Threat and Technical Analysis

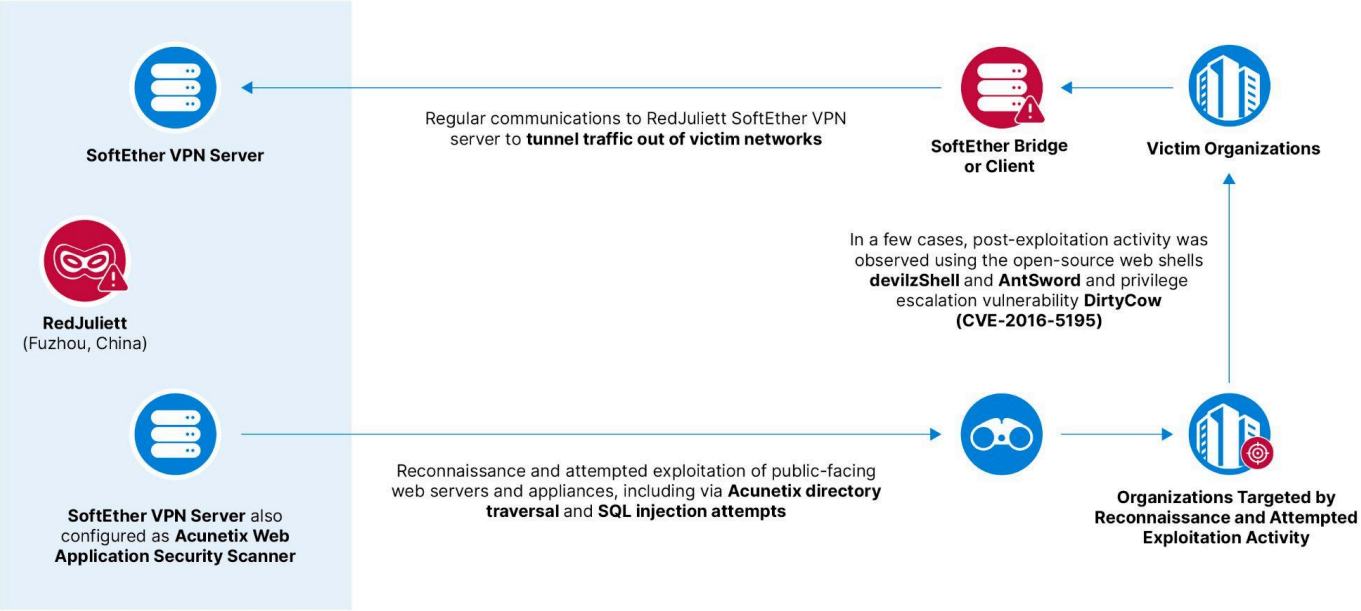

Figure 1: *Overview of RedJuliett operations (Source: Recorded Future)*

RedJuliett SoftEther Infrastructure

In August 2023, Microsoft highlighted multiple self-signed transport layer security (TLS) certificates used in Flax Typhoon (RedJuliett) activity targeting Taiwan, which were all generated through the open-source client and server VPN software SoftEther (see **Table 1**). Insikt Group has observed RedJuliett continuing to reuse these certificates, allowing us to identify multiple new RedJuliett servers, including three likely compromised Taiwanese universities that served the TLS certificates.

SHA-1 TLS certificate fingerprint	Common name (CN)
7992c0a816246b287d991c4ecf68f2d32e4bca18	vpn437972693.sedns[.]cn[2]
5437d0195c31bf7cedc9d90b8cb0074272bc55df	asljkdqhkhasdq.softether[.]net
cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1	vpn472462384.softether[.]net
2c95b971aa47dc4d94a3c52db74a3de11d9ba658	softether

Table 1: *Known RedJuliett SoftEther VPN self-signed TLS certificates (Source: Microsoft)*

[2] If SoftEther VPN Servers run within mainland China, the softether[.]net dynamic DNS domain is replaced with sedns[.]cn. The sedns[.]cn domain is owned and operated by the Chinese SoftEther subsidiary Beijing Daiyuu SoftEther Technology Co., Ltd (北京大游索易科技有限公).

Through the identification of shared administration infrastructure, Insikt Group also discovered two additional unreported self-signed certificates being used across RedJuliett SoftEther servers (**Table 2**).

SHA-1 TLS certificate fingerprint	Common name (CN)
`0cc0ba859981e0c8142a4877f3af99d98dc0b707`	cloud
`9f01fc7cad8cdd8d934e2d2f033d7199a5e96e4a (likely stolen certificate)`	eec2.test[.]thinkyes[.]tw

Table 2: *Newly observed RedJuliett SoftEther VPN self-signed TLS certificate (Source: Recorded Future)*

Insikt Group also previously observed known RedJuliett SoftEther TLS certificates on servers associated with three Taiwanese universities. We have not observed evidence to confirm whether these entities were end targets of RedJuliett activity or were being used to facilitate further targeting of entities within Taiwan. However, observed scanning of additional Taiwanese universities and historical industry reporting further supports the group's interest in Taiwanese organizations within the education sector.

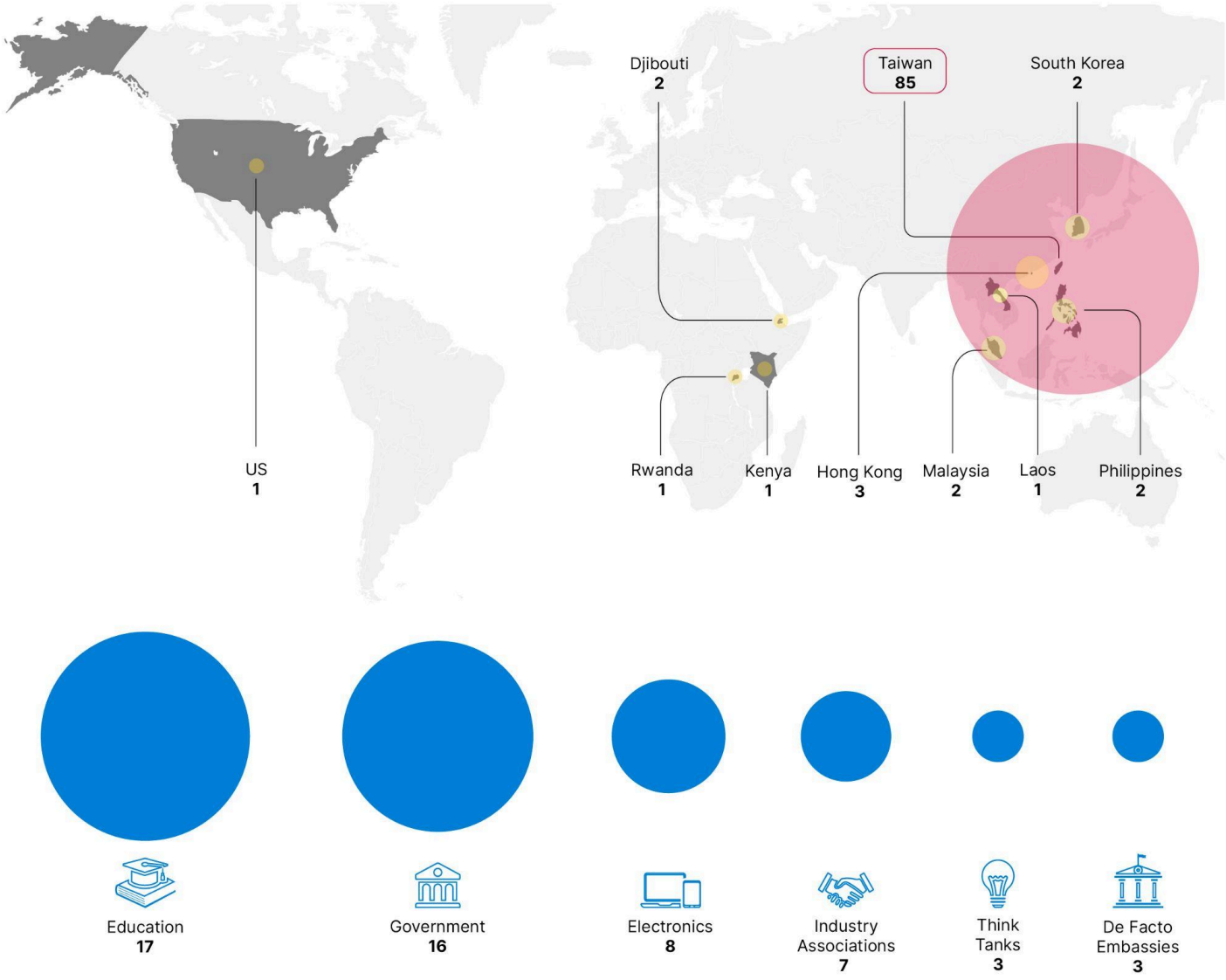

Figure 2: *Breakdown of RedJuliett targeting and victimology by geography and sector (Source: Recorded Future)*

Likely RedJuliett Victim Organizations Communicating with Threat Actor-Controlled SoftEther Servers

In early 2024, Insikt Group identified 24 suspected victim organizations regularly communicating to a RedJuliett SoftEther VPN server. This communication indicates that a SoftEther VPN bridge or client is running within these victim networks, which aligns with historical public reporting on RedJuliett activity. Victimology mainly consisted of government, education, and religious organizations, as well as software companies (see **Figure 3**). Approximately 60% of identified victim organizations were in Taiwan, with others in Hong Kong, South Korea, Laos, the United States, Rwanda, Kenya, and Djibouti.

RedJuliett compromised government organizations in Taiwan, Laos, Kenya, and Rwanda. The group also targeted the technology industry in Taiwan, including an optoelectronics company, a large Taiwanese facial recognition company that has held contracts with the Taiwanese government, and four software companies. Multiple universities were also compromised, including three Taiwanese universities, an American university, and a Djiboutian university. The group also targeted religious organizations in Taiwan, Hong Kong, and South Korea. Additionally, RedJuliett compromised a geological engineering company in Hong Kong, a Taiwanese waste and pollution treatment company, and a Taiwanese publishing house.

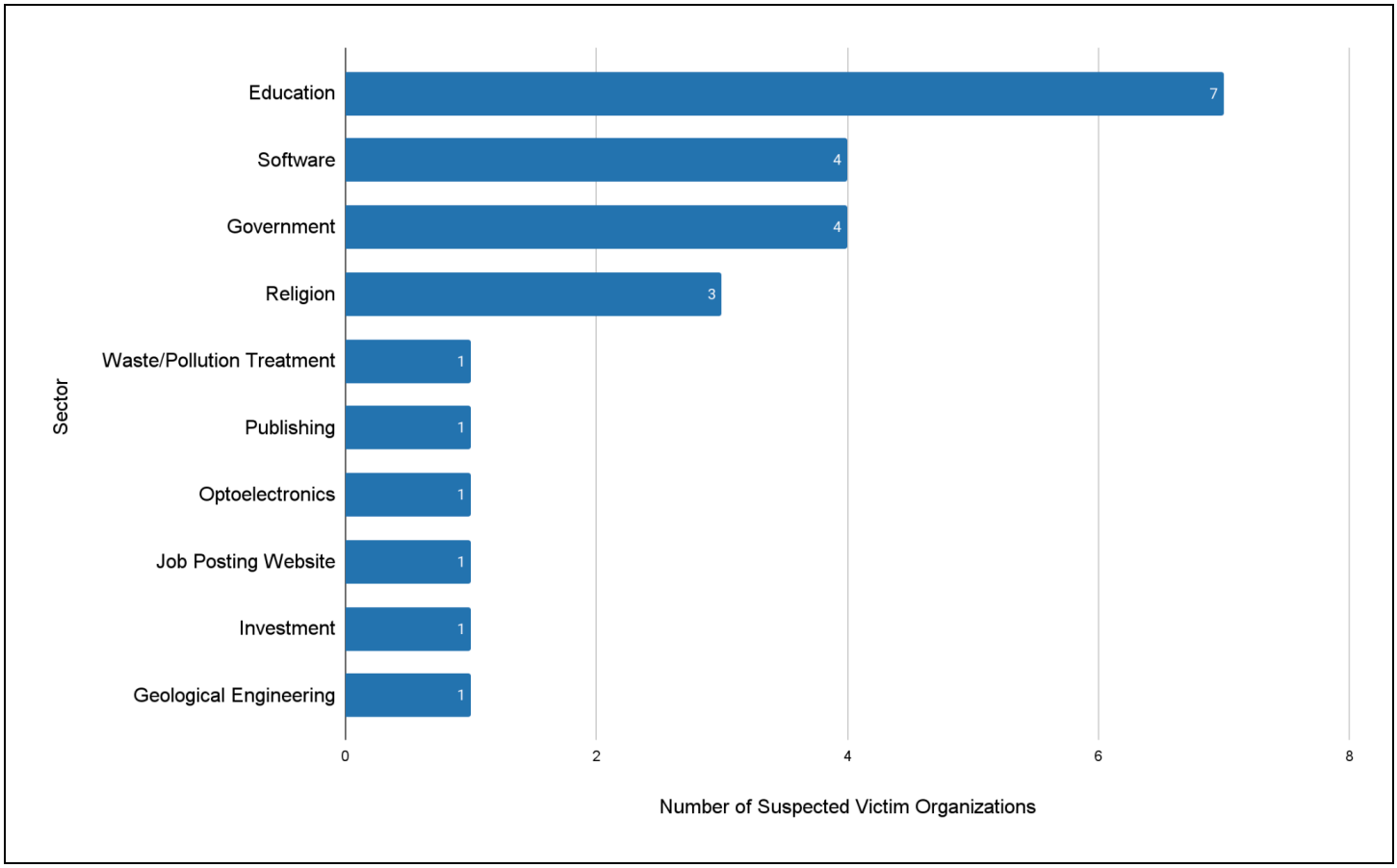

Figure 3: *Suspected RedJuliett victims by sector (Source: Recorded Future)*

RedJuliett Targets Internet-Facing Web Servers and Appliances

Using Recorded Future® Network Intelligence, Insikt Group observed RedJuliett using dedicated threat actor-controlled SoftEther VPN servers to conduct reconnaissance and attempted exploitation activity targeting a wide range of predominantly Taiwanese organizations from November 2023 to April 2024. In addition to acting as SoftEther VPN nodes, multiple RedJuliett IP addresses have been concurrently configured as Acunetix Web Application Security Scanners. Insikt Group has regularly observed vulnerability scanning and exploitation activity from these servers targeting web servers associated

with multiple Taiwanese organizations, predominantly in the government, education, and technology sectors.

Most recently, Insikt Group observed RedJuliett attempt SQL injection, directory traversal, and other exploits targeting web applications of target entities in multiple cases. In a small number of cases, we observed the group conduct post-exploitation activity using the open-source web shells devilzShell and AntSword and exploiting the Linux elevation of privilege vulnerability DirtyCow (CVE-2016-5195).

Insikt Group also observed the group display an interest in probing internet-facing F5 BIG-IP and Fortinet FortiGate devices, both of which are commonly exploited for initial access by a range of Chinese state-sponsored groups. In multiple cases in late 2023, we also observed RedJuliett communicating with ZyXEL ZyWALL firewall devices located within Taiwan. While Insikt Group is unable to confirm the nature of these communications, we note recent reporting from TeamT5 detailing suspected Chinese threat actors exploiting two vulnerabilities in ZyXEL ZyWALL devices in Taiwan since at least July 2023, likely for use as operational infrastructure in follow-on intrusion activity.

Targets of RedJuliett Reconnaissance or Attempted Exploitation Activity

Between December 2023 and April 2024, Insikt Group observed RedJuliett reconnaissance or attempted exploitation activity targeting at least 75 organizations, predominantly in Taiwan and across the government, education, and technology sectors (see **Figure 4** for a full breakdown of targeting by sector). While we observed RedJuliett likely attempting to target all of these organizations, we could only confirm post-exploitation activity in a small number of cases.

Within Taiwan, we observed RedJuliett heavily target the technology industry, including organizations in critical technology fields. RedJuliett conducted vulnerability scanning or attempted exploitation against a semiconductor company and two Taiwanese aerospace companies that have contracts with the Taiwanese military. The group also targeted eight electronics manufacturers, two universities focused on technology, an industrial embedded systems company, a technology-focused research and development institute, and seven computing industry associations.

RedJuliett also displayed an interest in Taiwan's economic and trade policy and international affairs. The group targeted three de facto embassies from South and Southeast Asian countries, two government departments focused on economic policy, two think tanks conducting research on Taiwanese economic policy, and a trade promotion organization. Additionally, RedJuliett conducted scanning or attempted exploitation against infrastructure associated with a multinational logistics company and two airlines. RedJuliett also targeted civil society, including two media organizations, a charity, and a non-governmental organization (NGO) focused on human rights. Insikt Group observed RedJuliett target eight universities and eleven government entities in total.

RedJuliett also conducted reconnaissance scanning or attempted exploitation of four organizations outside of Taiwan, including two government organizations in the Philippines, a government department in Djibouti, and a Malaysian airline.

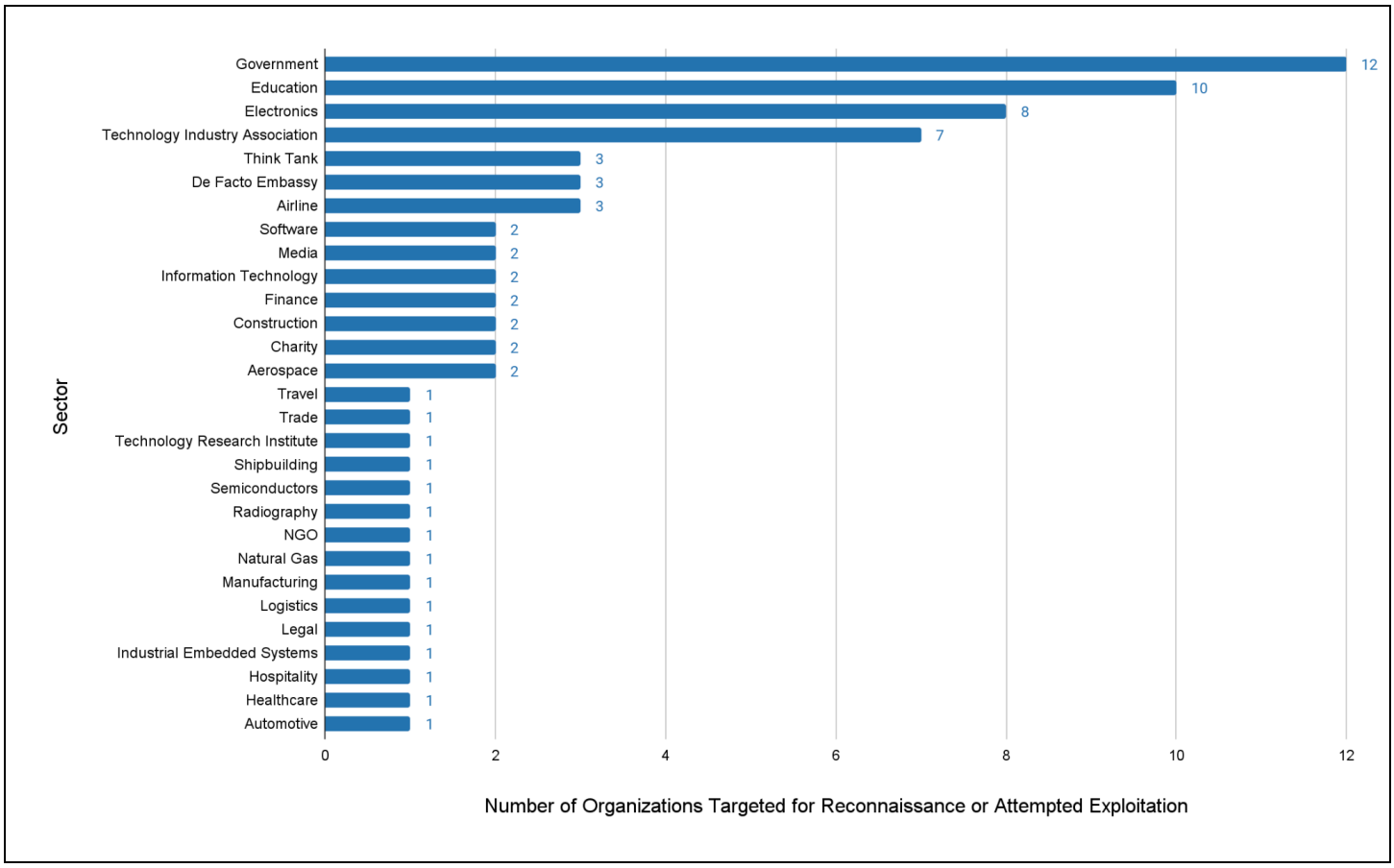

Figure 4: *RedJuliett reconnaissance or attempted exploitation targeting by sector (Source: Recorded Future)*

Suspected Source Range Administration Activity from Fuzhou, Fujian Province

Using Recorded Future Network Intelligence, Insikt Group observed suspected administration activity from Chinanet IP addresses geolocating to Fuzhou, Fujian province, to multiple RedJuliett SoftEther servers. This traffic was consistent with established SoftEther VPN connections and interaction with an internet-exposed Acunetix login panel. While RedJuliett's potential affiliation with either China's Ministry of State Security (MSS) or People's Liberation Army (PLA) is currently unknown, an operating location within Fuzhou is consistent with the group's persistent focus on Taiwan. Regional specialization has been observed in the operations of both civilian and military intelligence organizations in China. Fuzhou falls within the PLA Eastern Theater Command, which heavily focuses on targeting Taiwan.

Mitigations

We recommend that users conduct the following measures to detect and mitigate observed TTPs associated with RedJuliett activity:

- Ensure a risk-based approach for patching vulnerabilities, prioritizing high-risk vulnerabilities and those being exploited in the wild as determined through the Recorded Future Vulnerability Intelligence module. Regarding Chinese state-sponsored groups, prioritize addressing remote code execution (RCE) vulnerabilities in popular VPN, mail server, firewall, and load-balancing appliances. Pay particular attention to F5 BIG-IP, Fortinet FortiGate, and ZyXEL ZyWALL devices, as they were targeted by RedJuliett.
- Recorded Future Third-Party Intelligence module users can monitor real-time output to identify suspected targeted intrusion activity involving key vendors and partners within physical, network, and software supply chains.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future clients can alert on and proactively monitor infrastructure that may be involved in notable communication to known RedJuliett command-and-control (C2) IP addresses.
- Install the Recorded Future® Threat Intelligence Browser Extension to get instant access to threat intelligence from any web-based resource. This extension enables users to process alerts faster within their security information and event management (SIEM) and prioritize vulnerabilities for patching.
- Ensure security monitoring and detection capabilities are in place for all external-facing services and devices. Monitor for follow-on activity likely to occur following exploitation of these external-facing services, such as the deployment of web shells, backdoors, or reverse shells and subsequent lateral movement to internal networks.
- Practice network segmentation, such as isolating internet-facing services in a network demilitarized zone (DMZ).
- Review public guidance on mitigating common TTPs used by Chinese state-sponsored groups (1, 2, 3, 4). Review Insikt Group's report Charting China's Climb as a Leading Global Cyber Power for trends and recommendations for mitigating Chinese advanced persistent threat (APT) activity more broadly.

Outlook

Insikt Group anticipates that RedJuliett and other Chinese state-sponsored threat actors will continue to target Taiwan for intelligence-gathering at a high operational tempo, focusing on universities, government departments, think tanks, and technology companies. We also anticipate that Chinese state-sponsored groups will continue to focus on conducting reconnaissance against and exploiting public-facing devices, as this has proved a successful tactic in scaling initial access against a wide range of global targets.

Appendix A — Indicators of Compromise

Active RedJuliett servers as of May 21, 2024:

38.147.190[.]192 (since 2024-04-07)
61.238.103[.]155 (since 2024-02-23)
122.10.89[.]230 (since 2024-01-24)
137.220.36[.]87 (since 2024-05-09)
140.120.98[.]115 (since 2023-11-14)
154.197.98[.]3 (since 2023-11-14)
154.197.99[.]202 (since 2023-12-16)
176.119.150[.]92 (since 2024-04-01)

Known RedJuliett SoftEther TLS Certificates (SHA-1 Fingerprint)

7992c0a816246b287d991c4ecf68f2d32e4bca18
5437d0195c31bf7cedc9d90b8cb0074272bc55df
cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1
2c95b971aa47dc4d94a3c52db74a3de11d9ba658
0cc0ba859981e0c8142a4877f3af99d98dc0b707
9f01fc7cad8cdd8d934e2d2f033d7199a5e96e4a

Domains:

cktime.ooguy[.]com
www.sofeter[.]ml
www.dns361[.]tk

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Virtual Private Server	T1583.003
Resource Development: Compromise Infrastructure: Server	T1584
Reconnaissance: Active Scanning: Vulnerability Scanning	T1595.002
Initial Access: Exploit Public-Facing Application	T1190
Persistence: External Remote Services	T1133
Persistence: Server Software Component: Web Shell	T1505.003
Privilege Escalation: Exploitation for Privilege Escalation	T1068

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com