THREAT ANALYSIS

CHINA

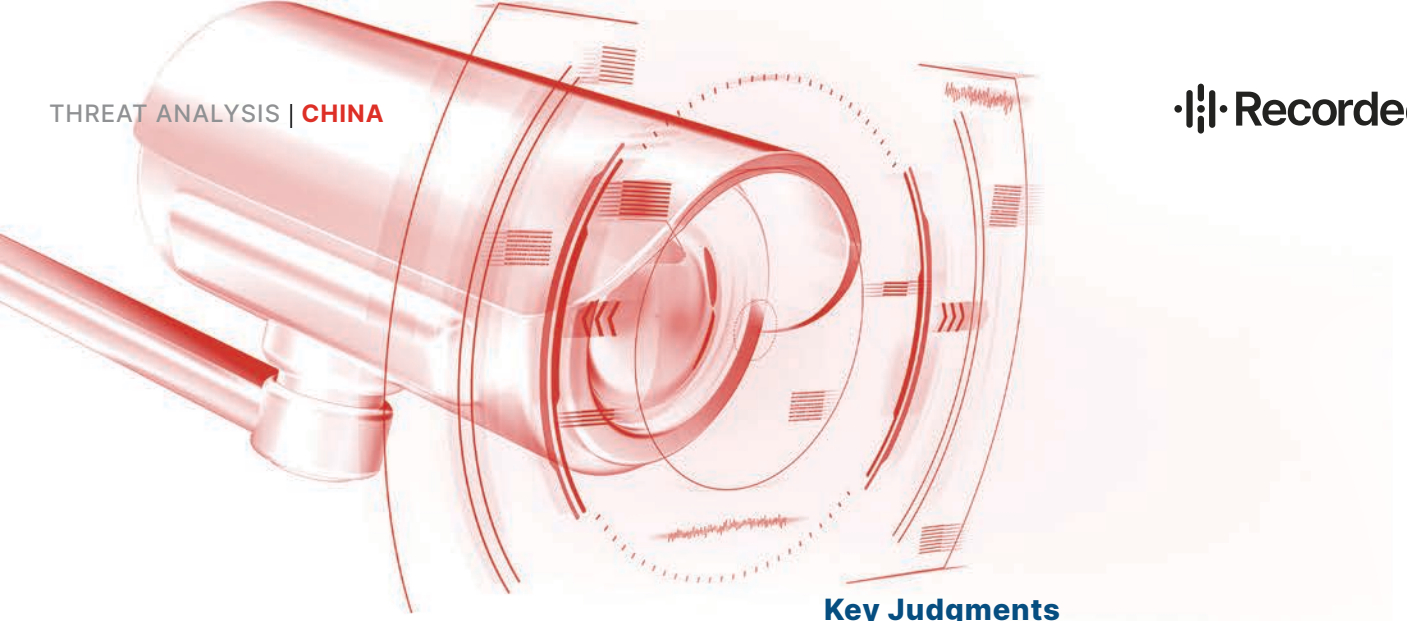
Recorded Future®

By Insikt Group®

August 16, 2022

RedAlpha Conducts Multi-Year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations

Recorded Future®



This report details multiple campaigns conducted by the likely Chinese state-sponsored threat activity group RedAlpha. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future® Platform, SecurityTrails, PolySwarm, DomainTools Iris, urlscan, and common open-source tools and techniques. It will be of most interest to individuals and organizations with strategic and operational intelligence requirements relating to Chinese cyber threat activity, as well as global humanitarian, think tank, and government organizations. Prior to the publication of this report, Recorded Future notified all affected organizations of the identified activity to support incident response and remediation investigations.

Executive Summary

In parallel with regular reporting from humanitarian and media organizations regarding human rights abuses orchestrated by the Chinese Communist Party (CCP), Recorded Future regularly observes Chinese state-sponsored cyber-espionage and surveillance campaigns likely intended to facilitate intelligence collection used in support of such abuses. Among these, we continue to track activity we attribute to the likely Chinese state-sponsored threat activity group RedAlpha (Deepcliff, Red Dev 3), as we previously reported in June 2018. Since this time, we have continued to observe the group engaging in mass credential theft activity primarily targeting humanitarian, think tank, and government organizations globally.

Over the past 3 years, we have observed RedAlpha registering and weaponizing hundreds of domains spoofing organizations such as the International Federation for Human Rights (FIDH), Amnesty International, the Mercator Institute for China Studies (MERICS), Radio Free Asia (RFA), the American Institute in Taiwan (AIT), and other global government, think tank, and humanitarian organizations that fall within the strategic interests of the Chinese government. Historically, the group has also engaged in direct targeting of ethnic and religious minorities, including individuals and organizations within Tibetan and Uyghur communities. As highlighted within this report, in recent years RedAlpha has also displayed a particular interest in spoofing political, government, and think tank organizations in Taiwan, likely in an effort to gather political intelligence.

Key Judgments

- RedAlpha is likely attributable to contractors conducting cyber-espionage activity on behalf of the Chinese state. This assessment is based on the group's consistent targeting in line with the strategic interests of the CCP, historical links to personas and a private company situated in the People's Republic of China (PRC), and the wider regularly documented use of private contractors by Chinese intelligence agencies.
- In this activity, RedAlpha very likely sought to gain access to email accounts and other online communications of targeted individuals and organizations.
- RedAlpha's humanitarian and human rights-linked targeting and spoofing of organizations such as Amnesty International and FIDH is particularly concerning given the CCP's reported human rights abuses in relation to Uyghurs, Tibetans, and other ethnic and religious minority groups in China.

Background

Although it has been controlling large amounts of operational infrastructure and maintaining a high operational tempo since at least 2015, there has been minimal public reporting on RedAlpha activity over the past several years. First identified by CitizenLab in 2018, the group was observed conducting credential-phishing operations targeting the Tibetan community and other ethnic minorities, as well as social movements, a media group, and government agencies in South and Southeast Asia. In June 2018, we published activity linked to 2 RedAlpha campaigns that also targeted the Tibetan community to ultimately deploy the open-source malware family NjRAT. These 2 campaigns overlapped with the CitizenLab reporting based on matching WHOIS registrant data, common targeting of the Tibetan community, and hosting overlaps. RedAlpha activity explored in this report is also referenced in PWC's 2021 year in review, in which they track the group under the name Red Dev 3.

Historical RedAlpha activity targeted multiple ethnic and religious minority communities that have been persecuted within China, including Tibetans, Uyghurs, and Falun Gong supporters. More generally, organizations and individuals associated with ethnic and religious minorities within the PRC, particularly those within the so-called "Five Poisons", have been a frequent target for cyber threat activity groups linked to Chinese intelligence agencies over many years. This has included RedDelta (Mustang Panda, TA416) targeting the Vatican and organizations linked to Tibetan and Hong Kong Catholic communities; Chinese Ministry of State Security (MSS) contractors targeting emails belonging to Chinese Christian religious figures; APT41 (Barium) conducting reconnaissance on activists and other individuals associated with Hong Kong's pro-democracy movement; and the use of zero-day vulnerabilities to target members of the Uyghur community.

Threat Analysis

Over the past 3 years, Recorded Future has observed RedAlpha continuing to conduct credential-phishing activity using large clusters of operational infrastructure to support campaigns. Over this period, the group displayed a consistent set of tactics, techniques, and procedures (TTPs). In late 2019 and early 2020, the group likely shifted away from older infrastructure TTPs exhibited in public reporting, such as the registration of domains through GoDaddy and hosting on Choopa (Vultr) and Forewin Telecom infrastructure, and toward those described in the following section.

RedAlpha Infrastructure Tactics, Techniques, and Procedures

Since at least 2015, RedAlpha has consistently registered and weaponized large amounts of domains for use in credential-theft campaigns. These domains typically imitate well-known email service providers and spoof specific organizations that are either directly targeted in RedAlpha activity or that can be used to impersonate those organizations in activity targeting proximate organizations and individuals. In 2021, we noted a significant uptick in the volume of domains registered by the group, totalling over 350. Over this period, the group's infrastructure TTPs were characterized by the following criteria that allowed us to cluster this activity together:

- Use of *resellerclub[.]com nameservers
- Use of the virtual private server (VPS) hosting provider Virtual Machine Solutions LLC (VirMach)
- Consistent domain naming conventions, such as the use of "mydrive-", "accounts-", "mail-", "drive-", and "files-" strings across hundreds of domains
- Overlapping WHOIS registrant names, email addresses, phone numbers, and organizations
- The use of specific server-side technology components and fake HTTP 404 Not Found errors

Outside of generic spoofing of major email and storage service providers like Yahoo (135 typosquat domains), Google (91 typosquat domains), and Microsoft (70 typosquat domains), we observed the use of large numbers of domains typosquatting humanitarian, think tank, and government organizations including:

- Radio Free Asia
- Mercator Institute for China Studies
- Amnesty International
- International Federation for Human Rights
- American Chamber of Commerce (including AmCham Taiwan)
- Purdue University
- India's National Informatics Centre
- Taiwan's Democratic Progressive Party
- American Institute in Taiwan
- Ministries of foreign affairs in multiple countries globally

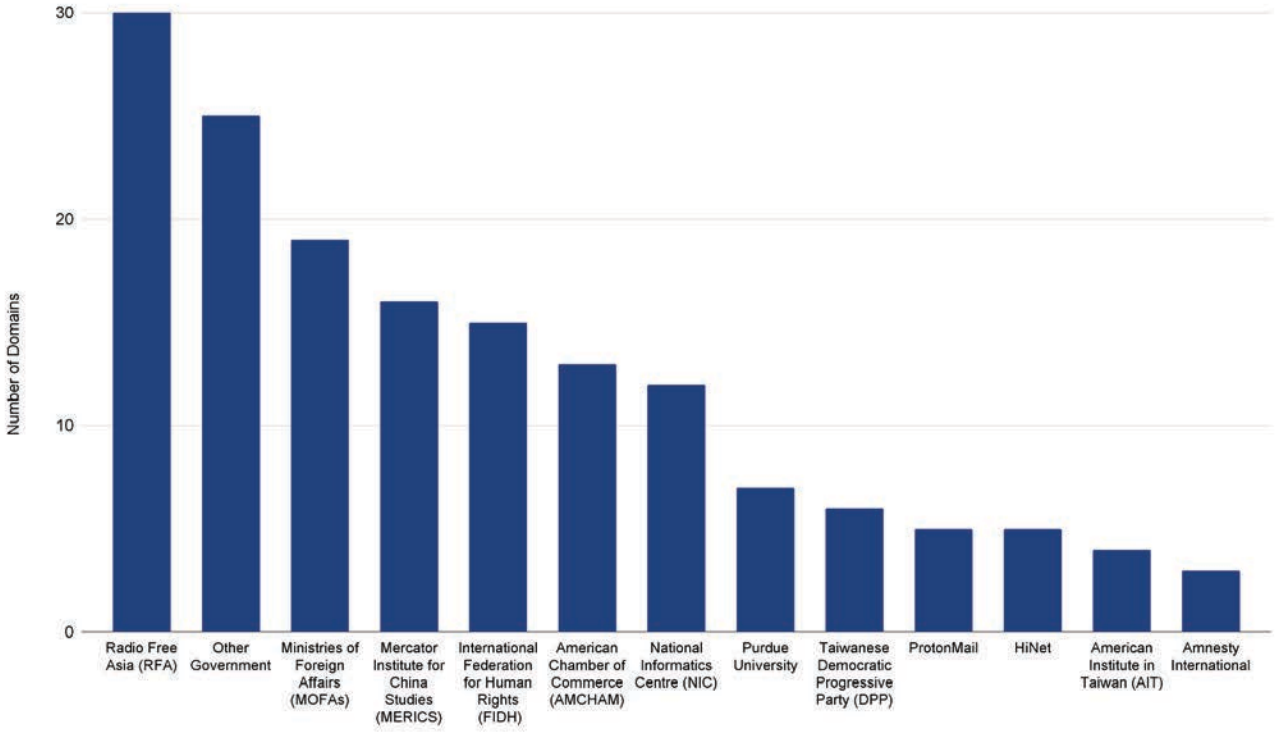


Figure 1: Number of RedAlpha typosquat domains by spoofed organization

Historical Typosquat Similarity - Typo or Homograph • Identified by Recorded Future as potential typosquatting
Typo or Homograph similarity found between amcham.space and 5 possible targets including **amcham.com.ar**, **amcham.co.il**, **amcham.com.br**.

Figure 2: Recorded Future typosquat risk rule for RedAlpha credential-phishing domain amcham[.]space spoofing American Chamber of Commerce (AMCHAM)

In many cases highlighted over the following sections, observed phishing pages mirrored legitimate email login portals for the specific organizations named above. We suspect that this means they were intended to target individuals directly affiliated with these organizations rather than simply imitating these organizations to target other third parties. In other cases, the phishing pages used generic login pages for popular mail providers and the intended targeting was ambiguous. The group has used basic PDF files containing links to the identified phishing sites, typically stating that a user needs to click the link to preview or download files.

Figure 3: Sample PDFs linking to RedAlpha credential-phishing domains - Top: Translation (Traditional Chinese): "Preview or Download Files" with link to milfiles[.]download; Bottom: Phishing link to RedAlpha domain outlookfiles[.]download

Targeting of Humanitarian Organizations and Think Tanks

As noted, RedAlpha has regularly registered domains imitating humanitarian organizations and think tanks, including MERICS, FIDH, Amnesty International, RFA, and multiple Taiwanese think tanks. Of particular note, the registration of at least 16 domains spoofing MERICS from early to mid-2021 coincided with the Chinese Ministry of Foreign Affairs (MOFA) imposing sanctions on the Berlin-based think tank in March 2021.

Figure 4: Fake Roundcube login page spoofing International Federation for Human Rights (FIDH) email login hosted on RedAlpha domain files-fidh[.]org

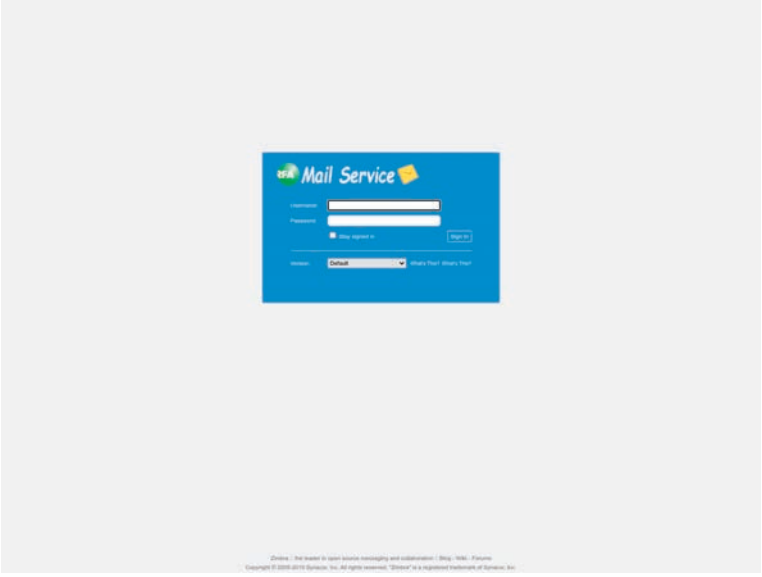


Figure 5: Fake Zimbra login page spoofing Radio Free Asia email login hosted on RedAlpha domain my-rfa[.]org

RedAlpha's Consistent Focus on Taiwan

Over the past 3 years, we observed RedAlpha consistently register domains spoofing Taiwanese or Taiwan-based government, think tank, and political organizations. Notably, this included the registration of multiple domains imitating the AIT, the de facto embassy of the United States of America in Taiwan, during a time of increasing US-China tension regarding Taiwan over the past year. Similar to wider activity, these domains were used in credential-phishing activity using fake login pages for popular email providers such as Outlook, as well as emulating other email software such as Zimbra used by these particular organizations (see Figure 6). A sample list of typosquat domains seen spoofing Taiwanese organizations is included in Table 1.

Figure 6: Fake Zimbra login page spoofing Taiwan External Trade Development Council (TAITRA) email login hosted on RedAlpha domain mydrive-taitra[.]link

RedAlpha Domain	Spoofed Organization
ait-org[.]tw	American Institute in Taiwan
files-ait[.]link	American Institute in Taiwan
files-ait[.]org	American Institute in Taiwan
my-ait[.]link	American Institute in Taiwan
files-taitra[.]org	Taiwan External Trade Development Council (TAITRA)
mydrive-taitra[.]link	Taiwan External Trade Development Council (TAITRA)
myfiles-dpp[.]link	Democratic Progressive Party
my-dpp[.]org	Democratic Progressive Party
dppmail[.]download	Democratic Progressive Party
files-dpp[.]org	Democratic Progressive Party
files-dpp[.]space	Democratic Progressive Party
files-cier-edu[.]link	Chung-Hua Institution for Economic Research (CIER)
files-cier[.]link	Chung-Hua Institution for Economic Research (CIER)
files-mail-indsr[.]link	Institute for National Defense and Security Research (國防安全研究院)
moea[.]site	Ministry of Economic Affairs (MOEA)

Table 1: RedAlpha credential-phishing domains spoofing organizations in Taiwan

RedAlpha's Targeting of Ministries of Foreign Affairs and Embassies

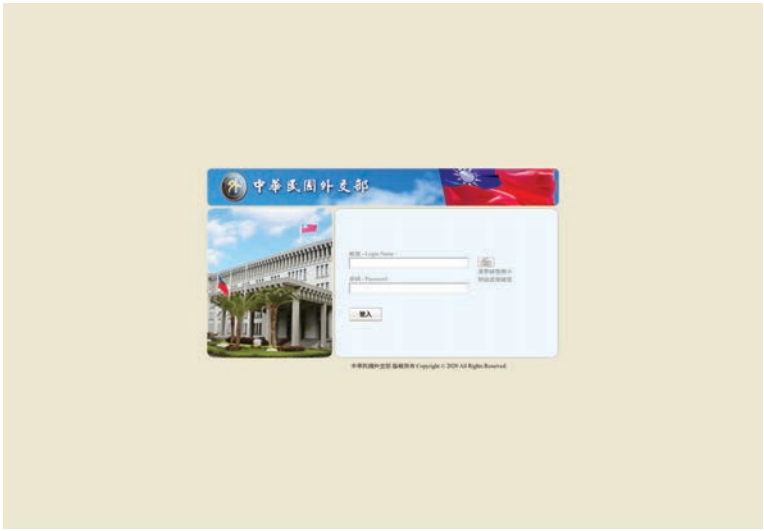


Figure 7: Fake Taiwanese Ministry of Foreign Affairs email login page seen on RedAlpha domain drive-mofa[.]com

As noted in PWC's 2021 year-in-review report, RedAlpha's activity has expanded over the past several years to include credential-phishing campaigns spoofing ministries of foreign affairs in multiple countries. We observed phishing pages imitating webmail login portals for Taiwan and Portugal's MOFAs (see Figures 7 and 8), as well as multiple domains spoofing Brazil and Vietnam's MOFAs. The previous section also highlighted consistent use of domains imitating the AIT. The group has also consistently spoofed login pages for India's National Informatics Centre (NIC), which manages wider IT infrastructure and services for the Indian government.

RedAlpha Domain	Spoofed Ministry of Foreign Affairs
files-itamaraty-gov[.]space	Brazil
itamaraty-gov[.]com	Brazil
files-mne[.]space	Portugal
mydrive-mne-pt[.]space	Portugal
mofa-vn[.]online	Vietnam
settings-mofavn[.]online	Vietnam
drive-mofa-vn[.]online	Vietnam
files-mfa[.]link filesmofa-gov[.]com mydrive-mofa[.]space drive-mofa[.]com my-mofa[.]space files-mofa[.]space mofa-gov[.]site mofasec[.]site files-mofa[.]com files-mofa[.]link	Generic MOFA Domains

Table 2: RedAlpha credential-phishing domains spoofing ministries of foreign affairs

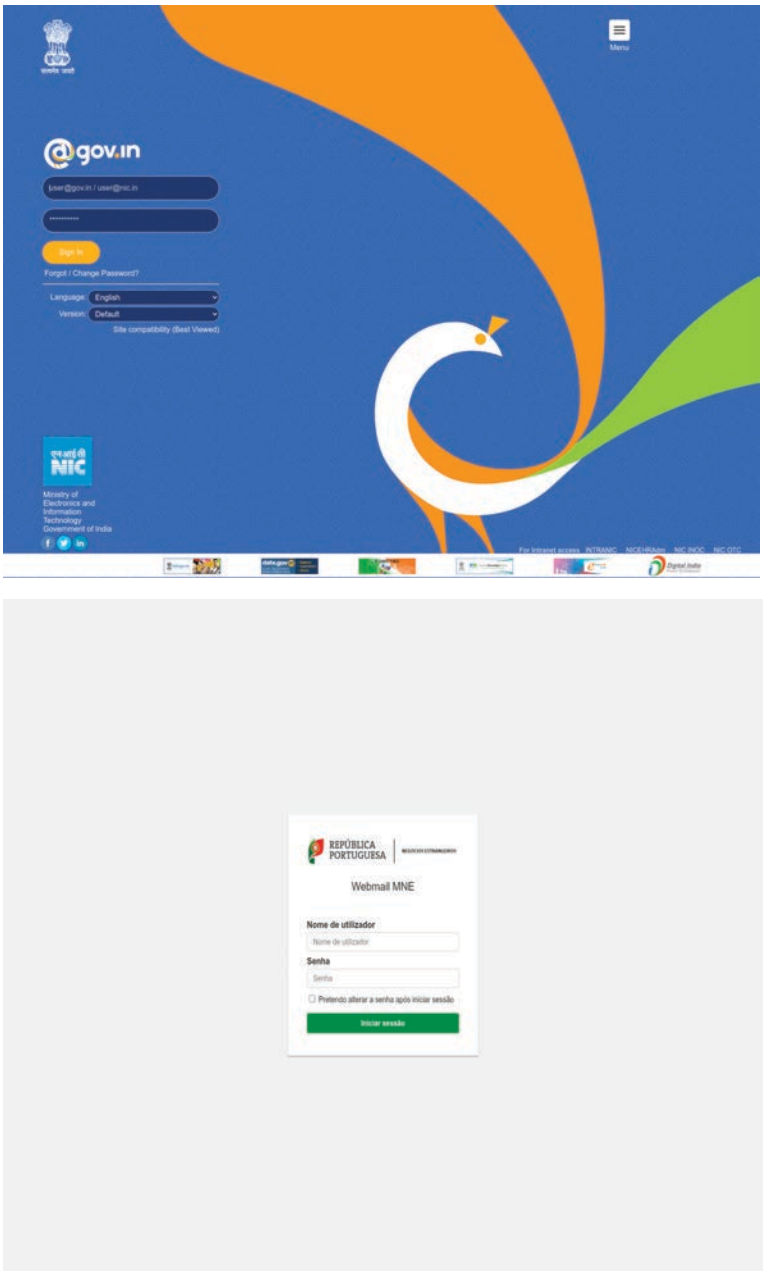


Figure 8: Fake Indian Government email login page seen on RedAlpha domain files-nic[.]online (left) and fake Portuguese Ministry of Foreign Affairs (MNE) email login page seen on RedAlpha domain files-mne[.]online (right)

Attribution

We identified multiple overlaps with previous publicly reported RedAlpha campaigns that allowed us to assess this is very likely a continuation of the group's activity. Of note, in at least 5 instances the group appeared to re-register previously owned domains after expiry. An alternative hypothesis we considered is whether a separate actor registered these domains in an attempt to emulate RedAlpha activity and conduct similar credential-theft targeting in line with Chinese state interests. However, based on additional evidence linking this more recent activity to historically reported campaigns, we believe that this is unlikely and that it instead constitutes a continuation of RedAlpha activity. The re-registration of previously owned domains may instead be a product of multiple factors such as the sheer volume of domains registered by the group, poor infrastructure management, and the repetitive nature of naming conventions used. Some of the attribution evidence we observed is summarized below and displayed in Figure 9.

- The domain mydrive-google[.]online was observed in Citizen Lab's original reporting on the group and was originally registered using the email address deepcliff@sina[.]com . This same domain was observed in more 2021 RedAlpha activity and was hosted on the VirMach IP address 172.245.81[.]180 alongside a host of other RedAlpha domains spoofing entities such as MERICS and FIDH.
- The domain edit-yahoo[.]space was also originally referenced in Citizen Lab and Recorded Future reporting on RedAlpha activity, and was later hosted on VirMach IP address 107.172.39[.]25 in 2021 alongside additional RedAlpha domains spoofing organizations such as Radio Free Asia.
- Another domain seen in earlier RedAlpha activity, mail-protect[.]space , was reregistered and hosted on then-dedicated infrastructure on 45.114.125[.]130 in 2018. This IP concurrently hosted the similarly named mail-method[.]space . Mail-method[.]space was later hosted on the Forewin Telecom IP address 118.99.51[.]31 in mid-2018. This IP address is used for command and control (C2) by the malware sample SHA256 2c03d3f3e6d8c08db2322153d95262f6ace9288bff6d7e4c729517aecc2713af compiled and submitted to public malware repositories during that time. We identified 2 additional samples belonging to this same custom malware family which share matching import hashes and use the respective C2 domains phpinfo[.]pw and microbug[.]info . Both of these domains are linked to original reporting on RedAlpha activity.

- Another notable aspect of the mail-protect[.]space domain is that it was originally registered by evalliang@163[.]com. We associated this email address with a persona using the moniker Mr. Liang (full name omitted for the purposes of this report), who was observed registering domains seen in earlier RedAlpha activity. Notably, this domain was later reregistered after expiry using the email address girder1992@hotmail[.]com . This "girder" handle also has links to historical RedAlpha activity (see next section on RedAlpha's Links to Private Contractor). This, coupled with the malware connection outlined in the previous point, provides evidence that the observed cases of domain re-registration were likely conducted by the same actor.
- The domain drive-mail[.]space was also registered using the deepcliff@sina[.]com email address and referenced in public reporting on the group's activity. This domain was later hosted on 115.126.25[.]13 in 2019 alongside RedAlpha domains spoofing entities such as Purdue University and Indonesia's National Counter Terrorism Agency. The spoofing of Purdue University was observed on multiple other occasions from 2019 onwards.
- Other similarities observed include overlapping domain-naming conventions seen in historical and more recent activity. An example of this is the use of domains spoofing Thailand's Department of Special Investigation (DSI), where mail-dsi-go[.]space was identified in CitizenLab's reporting and both files-dsi-go-th[.]link and files-dsi-go[.]space were observed in more recent 2021 activity.
- Similarly, the use of the string mg followed by 1 or 2 digits was a common trait seen in historical and more recent activity spoofing Yahoo mail services, such as mail-mg16-yahoo[.]cf referenced in CitizenLabs's reporting and mg12-mail[.]link seen in 2021 activity.
- The use of non-exclusive domain-naming tendencies (such as the inclusion of the strings "mydrive-", "accounts-", "mail-", "drive-", and "files-") was also common across both sets of activity.

RedAlpha's Links to Private Contractor

In our previous public reporting, we identified a link between RedAlpha and a Chinese information security company. A specific QQ email address that was used to register multiple RedAlpha domains also appeared on a job listing for an "information security engineer" for a company called "Nanjing Qinglan Information Technology Co., Ltd." (南京青苜信息技术有限公司) several years prior. This company, now known as "Jiangsu Cimer Information Security Technology Co. Ltd." (江苏君立华域信息安全技术股份), reportedly provides "security assessment, security reinforcement, penetration testing, security consulting, offensive and defensive drills, security training". The associated persona linked to the QQ account and on the job listing was listed as "Mr. Liang/Leung". Notably, multiple email addresses used to register early RedAlpha domains referenced in CitizenLab reporting featured the string "Liang" or "Leung" and a full registrant name which matches the owner of the linked QQ account.

We identified 3 Chinese-language blog sites registered by the Mr. Liang persona over several years, which featured frequent posts on information security and hacking topics. One of these linked directly to Mr. Liang's QQ page, which referenced both their full-name moniker and the same QQ number. Historical versions of Mr. Liang's QQ page revealed they are a "network security expert" and a former member of the Chinese underground hacking group Green Corps (绿色兵团).

Notably, one of Mr. Liang's personal blog domains was also linked to an additional registrant email address featuring the moniker "girder" in 2014. At this time, the page also displayed the header "girder's blog". In the previous section, we noted that the email address girder1992@hotmail[.]com was later used to register a batch of RedAlpha operational domains in 2018.

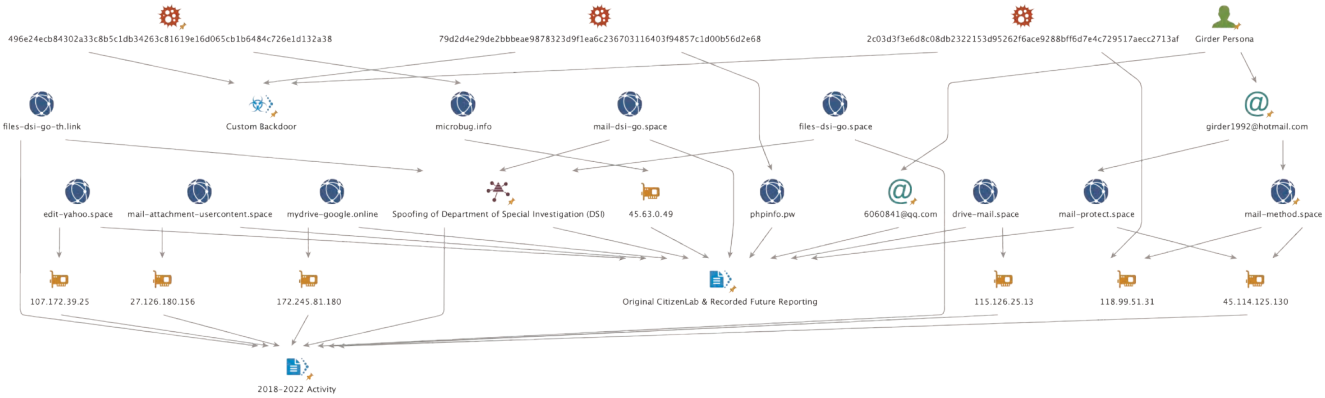


Figure 9: Connections between publicly reported RedAlpha campaigns and observed 2018-2022 activity (Source: Recorded Future)

Figure 10: Screenshot from one of Mr. Liang's personal blogs in 2014 displaying "Girder" moniker (subheading translated from Simplified Chinese)

Based on these findings and wider activity examined, it is very likely that RedAlpha operators are located within the PRC. Chinese intelligence services' use of private contractors is also an established trend, with groups such as APT3, APT10, RedBravo (APT31), and APT40 all identified as contractors working for China's Ministry of State Security (MSS) (1,2,3,4). In the case of RedAlpha, the group's targeting closely aligns with the strategic interests of the Chinese government, such as the observed emphasis on China-focused think tanks, civil society organizations, and Taiwanese government and political entities. This targeting, coupled with the identification of likely China-based operators, indicates a likely Chinese state-nexus to RedAlpha activity.

Mitigations

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

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains linked in the Outlook section below.
- Use strong passwords, in conjunction with multi-factor authentication (MFA) enabled where possible, to limit the potential damage of credential theft.
- Monitor for domain abuse, such as typosquat domains spoofing your organization and vendors, through the Recorded Future® Brand Intelligence module.
- Enforce strong security awareness through interactive exercises; train users to recognize phishing emails and exercise caution when clicking on links or opening attachments in emails to make accounts less susceptible to unauthorized logins.
- Monitor for unusual and anomalous account login patterns through methods such as monitoring for the unexpected use of anonymization services such as Tor or commercial VPNs.
- For high-profile individuals likely to be targeted by state-sponsored actors, such as activists, journalists, or human rights campaigners, consider employing extra precautionary measures such as Gmail's Advanced Protection Program.

Outlook

Our research uncovered the suspected China state-sponsored group RedAlpha conducting credential-harvesting activity targeting individuals and organizations globally, with a particular focus on civil society and government sectors. The group has used a consistent set of TTPs to register and manage large clusters of operational phishing infrastructure, using a mixture of pages impersonating popular email provider logins and custom webmail login pages to mimic specific providers and organizations. Since 2015, the group has engaged in consistent targeting of individual citizens and groups associated with minority communities, many of which are subject to reported human rights abuses within China. More generally, Chinese state-sponsored groups continue to aggressively target dissident and minority groups and individuals, both domestically through state surveillance and internationally through cyber-enabled intrusion activity. This targeting of sensitive and vulnerable communities, many of which have security budget and resources constraints, is particularly concerning.

Readers can access the RedAlpha indicators observed through our public Insikt Group Github repository: https://github.com/Insikt-Group/Research **(RedAlpha Conducts Multi-year Credential Theft Campaign Targeting Global Humanitarian, Think Tank, and Government Organizations - June 2022).**

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 intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.