Chinese State-Sponsored Activity Group TAG-22 Targets Nepal, the Philippines, and Taiwan Using Winnti and Other Tooling

recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan

Blog

Posted: 8th July 2021

By: INSIKT GROUP

Recorded Future has identified a suspected Chinese state-sponsored group that we track as Threat Activity Group 22 (TAG-22) targeting telecommunications, academia, research and development, and government organizations in Nepal, the Philippines, Taiwan, and more historically, Hong Kong. In this most recent activity, the group likely used compromised GlassFish servers and Cobalt Strike in initial access operations before switching to the bespoke Winnti, ShadowPad, and Spyder backdoors for long-term access using dedicated actor-provisioned command and control infrastructure.

Background

In September 2020, Recorded Future clients received a report on activity linked to a user of the shared custom backdoors Winnti and ShadowPad. This activity targeted a Hong Kong university and airport. The infrastructure and malware used in these intrusions directly overlap with previous reporting by ESET and NTT Group on Winnti Group activity. There are also numerous infrastructure and malware overlaps with activity recently reported by Avast, which described

an installer backdoored with Cobalt Strike found on the official website of MonPass, a major certification authority (CA) in Mongolia. Both the ShadowPad and Winnti backdoors are shared across multiple Chinese activity groups. Winnti in particular has been historically used by both APT41/Barium and APT17 and is commonly associated with activity linked to multiple groups of loosely connected private contractors operating on behalf of China's Ministry of State Security (MSS). In this case, Insikt Group tracks the cluster of activity described in this and our previous report using the temporary name Threat Activity Group 22 (TAG-22), while we note some historical overlap with activity clustered as APT41 and Barium by FireEye and Microsoft, respectively.

Victimology and Use of Compromised GlassFish Infrastructure

Insikt Group tracks known infrastructure and domains linked to TAG-22 using a combination of passive DNS data and adversary C2 detection techniques for ShadowPad, Winnti, and the Spyder Backdoor. In June 2021, we identified TAG-22 intrusions targeting the following organizations in Taiwan, Nepal, and the Philippines using Recorded Future Network Traffic Analysis (NTA) data:

- The Industrial Technology Research Institute (ITRI) in Taiwan
- Nepal Telecom
- Department of Information and Communications Technology (The Philippines)

In particular, the targeting of the ITRI is notable due to its role as a technology research and development institution that has set up and incubated multiple Taiwanese technology firms. According to the ITRI's website, the organization is particularly focused on research and development projects related to smart living, quality health, sustainable environment, and technology, many of which map to development priorities under China's 14th 5-year plan, previously highlighted by Insikt Group as likely areas of future Chinese economic espionage efforts. In recent years, Chinese groups have targeted multiple organizations across Taiwan's semiconductor industry to obtain source code, software development kits, and chip designs.

While we believe these 4 organizations were likely the intended end targets of TAG-22 intrusion activity, we also identified several suspected compromised GlassFish Servers communicating with TAG-22 C2 infrastructure. This is in line with recent NTT reporting, which identified the group exploiting GlassFish Server software version 3.1.2 and below and using the compromised infrastructure to conduct onward intrusion activity, specifically scanning using the Acunetix scanner and deploying the Cobalt Strike offensive security tool (OST). Per NTT researchers, the group likely used this infrastructure in the

early stages of intrusions before transitioning to dedicated infrastructure for controlling ShadowPad, Spyder, and Winnti implants. For its dedicated infrastructure, TAG-22 primarily used domains registered via Namecheap and Choopa (Vultr) virtual private servers (VPS) for hosting.

Nepal Telecom Tradecraft Case Study

By querying the TAG-22 C2 domain vt.livehost[.]live in the Recorded Future Threat Intelligence Platform, we identified links to the Shadowpad and Spyder backdoors that combine Recorded Future C2 detections and passive DNS data.

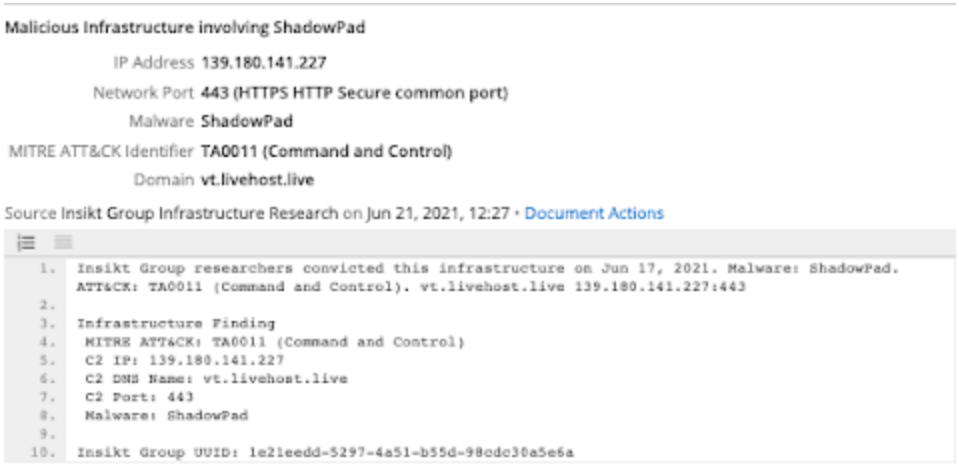


Figure 1: *Malicious Infrastructure Verdict for vt.livehost[.]com (Source: Recorded Future)*

This allows us to pivot and identify the TAG-22 IP address 139.180.141[.]227, which we have detected being used by the group for both Shadowpad and Spyder command and control.

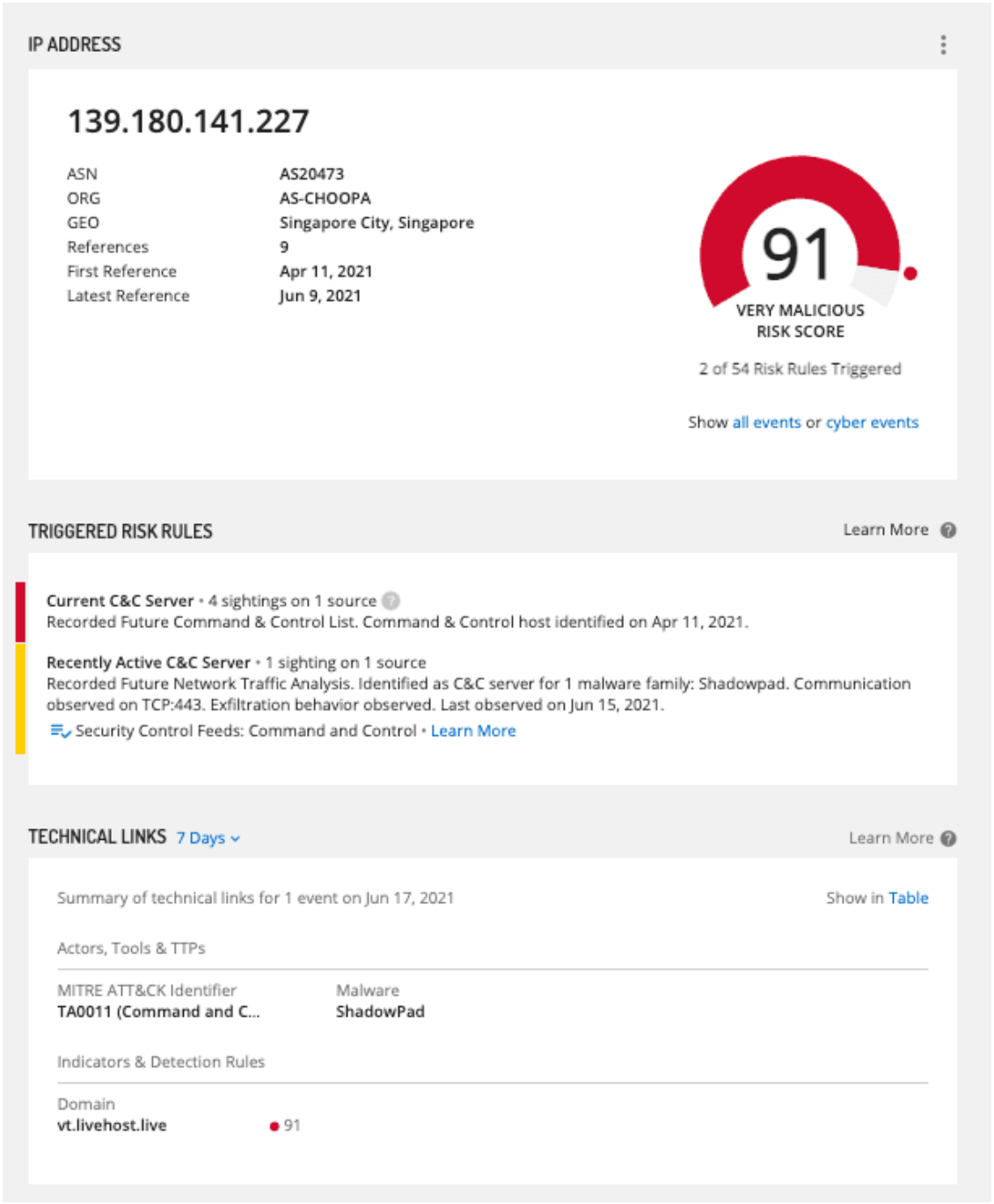


Figure 2: *Intelligence Card for TAG-22 C2 139.180.141[.]227 (Source: Recorded Future)*

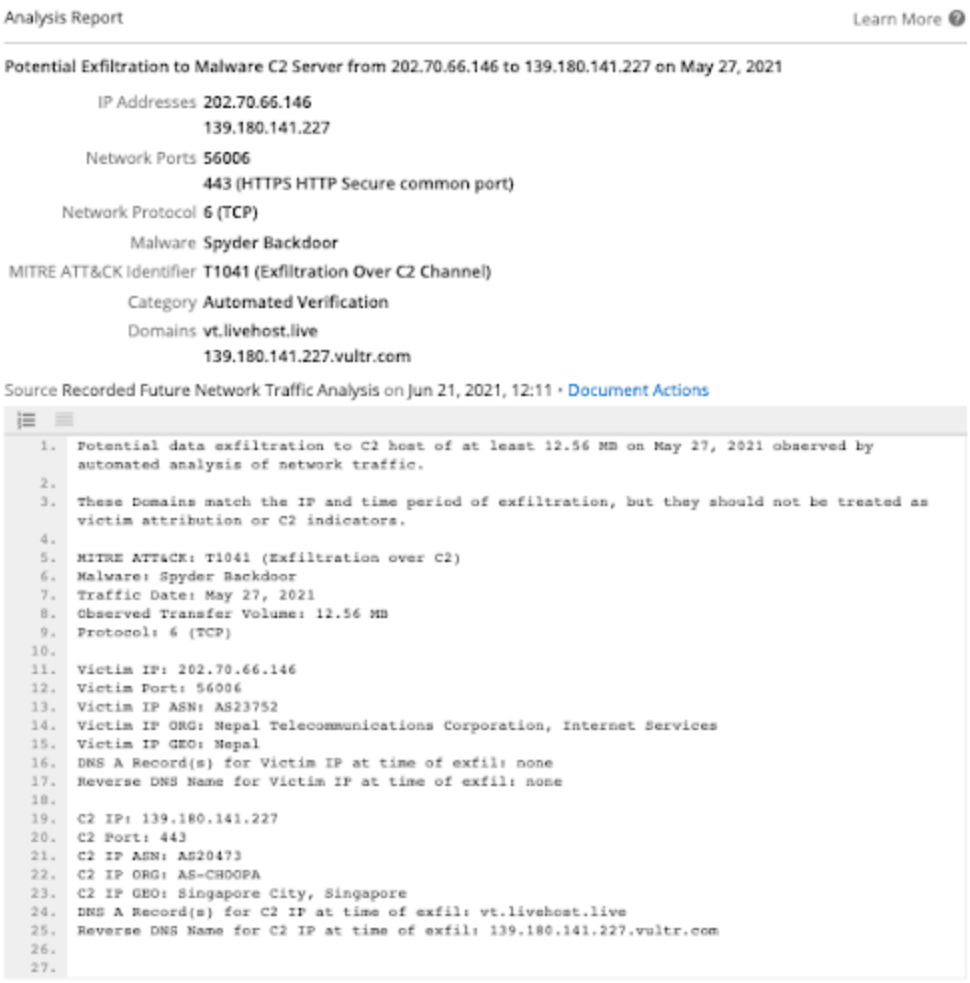


Figure 3: *Sample exfiltration event from Nepal Telecom to TAG-22 C2 Infrastructure (Source: Recorded Future)*

In addition to identifying additional related malicious infrastructure, using Network Traffic Analysis Exfiltration Events, we were also able to pinpoint specific victims of TAG-22 activity. The screenshot above shows an exfiltration event from the Nepal Telecom IP to the Shadowpad and Spyder backdoor C2 139.180.141[.]227, which hosted the domain vt.livehost[.]live at the time of exfiltration. While the victim IP address is assigned to Nepal Telecom, for telecommunication companies, this is often insufficient for attributing the true victim organization because the majority of infrastructure owned by those entities is leased or provided to its customers. In this case, we can use the new, proprietary VPN and Geographical Information extension alongside other enrichments to try to pinpoint the victim of this activity.

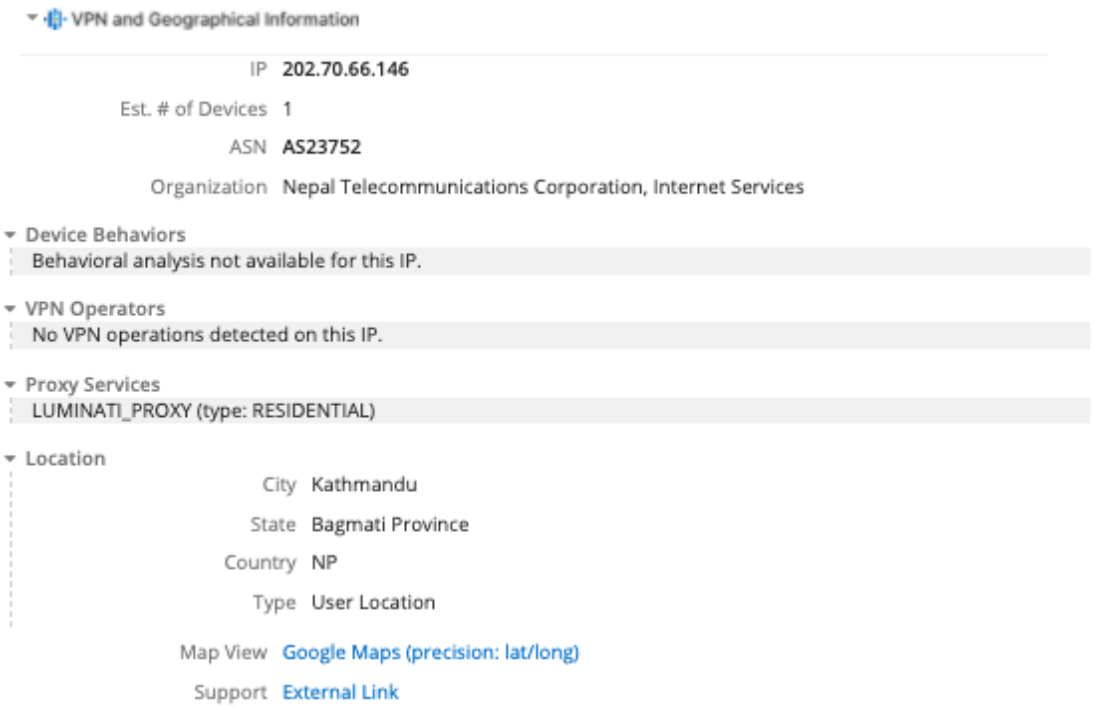


Figure 4: *VPN and Geographical Information extension for Nepal Telecom IP 202.70.66[.]146 (Source: Recorded Future)*

By clicking on the Google Maps view within the VPN and Geographical Information extension for this IP address, we can pinpoint a location and confirm that Nepal Telecom is likely the victim of this activity — the location directly points to Nepal Telecom's head office in Kathmandu.

Figure 5: *VPN and Geographical Information extension for Nepal Telecom IP 202.70.66[.]146 (Source: Recorded Future)*

Malware Analysis

Through analyzing the identified TAG-22 operational infrastructure, we identified several Cobalt Strike samples likely used by the group to gain an initial foothold in the target environment. The group also used a custom Cobalt

Strike loader the malware authors appear to have called Fishmaster based on a debugging string present within several samples:

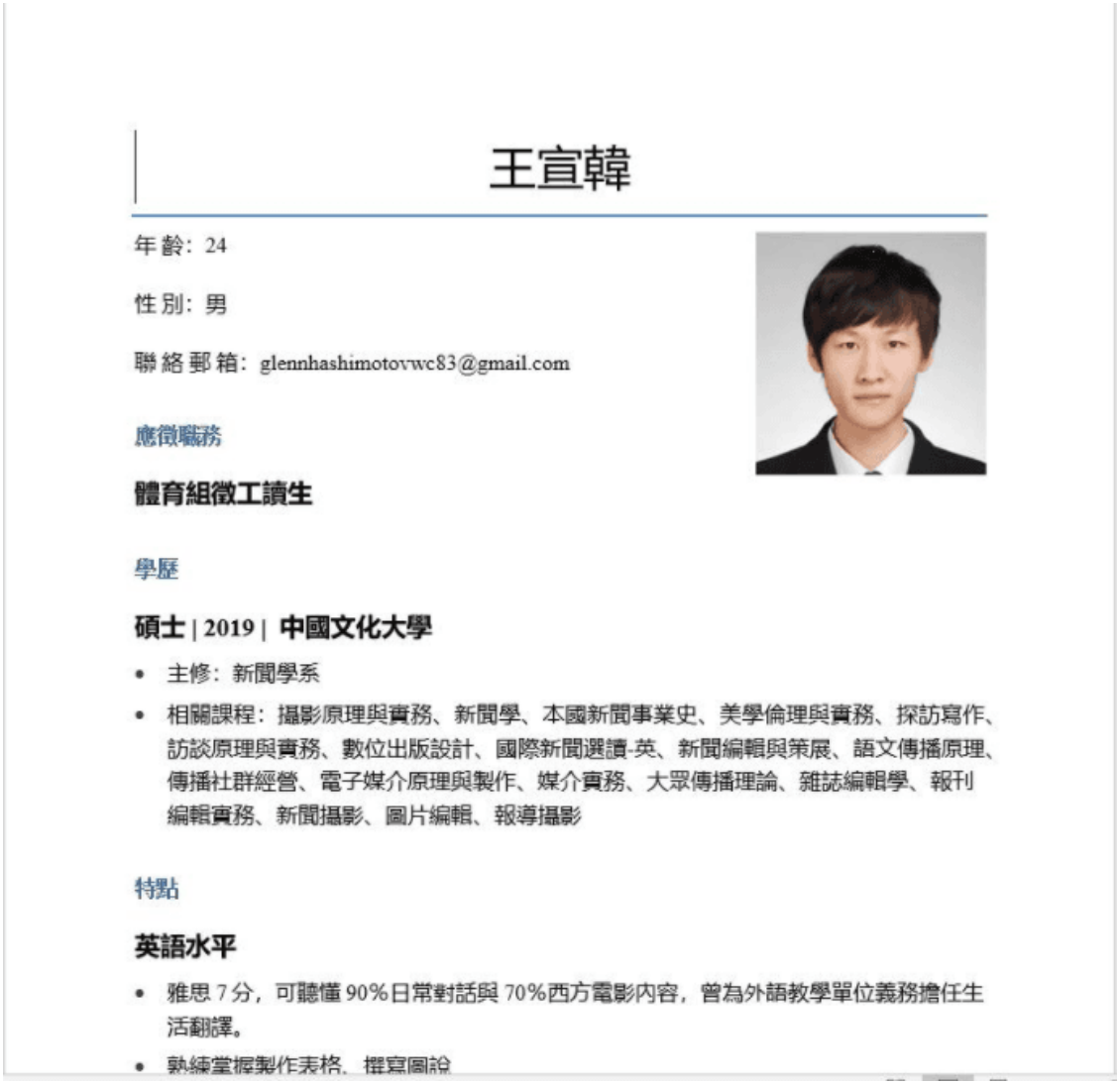
(C:\Users\test\Desktop\fishmaster\x64\Release\fishmaster.pdb)

The string “fish_master” was also present across others.

For initial access, the group typically used double extensions for Fishmaster Portable Executable (PE) files to make them appear like Microsoft Office or PDF files:

- 2af96606c285542cb970d50d4740233d2cddf3e0fe165d1989afa29636ea11db - Advertising Cooperation- DUKOU ICU.pdf.exe
- C2df9f77b7c823543a0528a28de3ca7acb2b1d587789abfe40f799282c279f7d - 履歷-王宣韓.docx.exe

In each case, following execution, the user is shown a decoy document, such as the resume shown below for a likely Taiwanese national. In other instances, the group used malicious macros to drop the Fishmaster loader. As both sample lure documents are written in traditional Chinese characters and the CV features a Taiwanese university, and because the group has more widely targeted Taiwan, we believe that Taiwanese organizations were likely the targets for these particular lures.



王宣韓

年齡：24

性別：男

聯絡郵箱：glennhashimotovwc83@gmail.com

應徵職務

體育組徵工讀生

學歷

碩士 | 2019 | 中國文化大學

- 主修：新聞學系
- 相關課程：攝影原理與實務、新聞學、本國新聞事業史、美學倫理與實務、採訪寫作、訪談原理與實務、數位出版設計、國際新聞選讀-英、新聞編輯與策展、語文傳播原理、傳播社群經營、電子媒介原理與製作、媒介實務、大眾傳播理論、雜誌編輯學、報刊編輯實務、新聞攝影、圖片編輯、報導攝影

特點

英語水平

- 雅思 7 分，可聽懂 90%日常對話與 70%西方電影內容，曾為外語教學單位義務擔任生活翻譯。
- 熟練掌握製作表格、撰寫圖說

Figure 6: *Decoy documents used in TAG-22 activity*

Many of the Cobalt Strike beacon payloads used by TAG-22 across this campaign were configured using the Backoff malleable C2 profile, which contains the following high level network traffic characteristics:

User Agent: “Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0"
HTTP POST URI (multiple choices):

/windebug/updcheck.php

/aircanada/dark.php

/aero2/fly.php

/windowsxp/updcheck.php

/hello/flash.php

HTTP GET URI:

/updates

All of the configurations contain the watermark 305419896, which is associated with a cracked version of Cobalt Strike.

Outlook

At this time, Insikt Group continues to track TAG-22 activity as an independent activity cluster that overlaps with the wider group defined as Winnti Group by ESET. TAG-22 uses shared custom backdoors likely unique to Chinese state-sponsored groups, including ShadowPad and Winnti, while also employing open-source or offensive security tools such as Cobalt Strike and Acunetix. TAG-22’s continued use of publicly reported infrastructure is indicative of a group experiencing a high degree of operational success despite a breadth of public reporting regarding its operations. Insikt Group has primarily identified TAG-22 operating within Asia. However, apart from this campaign, the group has a relatively broad targeting scope both geographically and by industry. This wider targeting scope, coupled with the use of the Winnti backdoor, is typical of several suspected MSS contractors, including APT17 and APT41.

For a full list of indicators of compromise, please refer to Insikt Group’s Github repository.