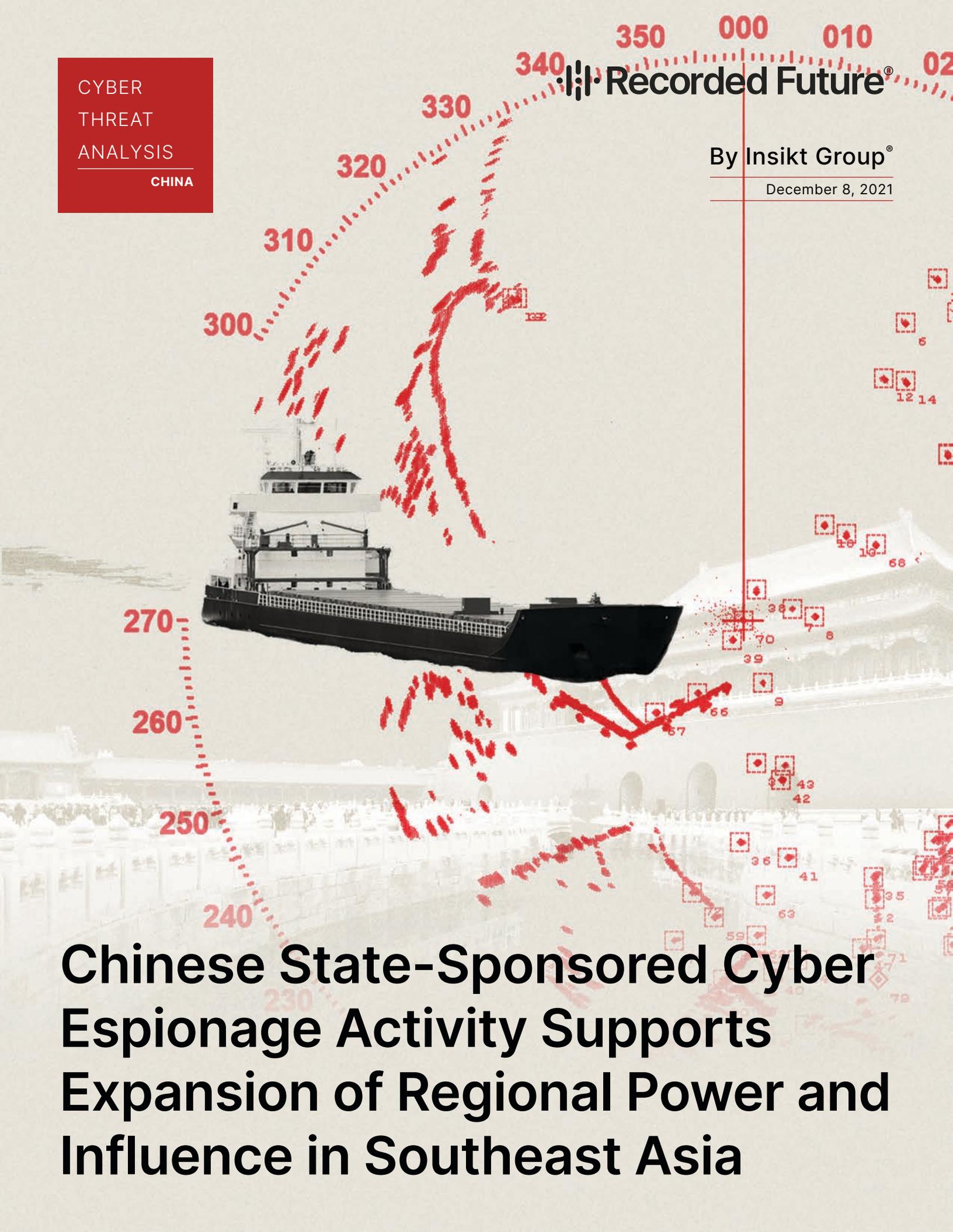


Chinese State-Sponsored Cyber Espionage Activity Supports Expansion of Regional Power and Influence in Southeast Asia





This report profiles trends in Chinese state-sponsored cyber espionage activity targeting Southeast Asian countries. The activity was identified through large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future Platform, SecurityTrails, DomainTools, PolySwarm, Farsight, Team Cymru, and common open-source tools and techniques. The research will be of most interest to individuals engaged in strategic and operational intelligence relating to the activities of Chinese military and foreign intelligence agencies in cyberspace and network defenders with a presence in Southeast Asia.

Executive Summary

Recorded Future's Insikt Group tracks Chinese state-sponsored cyber espionage operations targeting government and private sector organizations across Southeast Asia. In this report, we highlight multiple examples of activity reported to Recorded Future clients throughout 2021. The identified intrusion campaigns almost certainly support key strategic aims of the Chinese government, such as gathering intelligence on countries engaged in South China Sea territorial disputes or related to projects and countries strategically important to the Belt and Road Initiative (BRI).

The activity highlighted includes a group we track as Threat Activity Group 16 (TAG-16¹), which has compromised several high-profile military and government organizations across Southeast Asia throughout 2021 using custom malware families such as FunnyDream and Chinox. Many of the governments targeted by TAG-16 are engaged in ongoing disputes with China over territorial claims in the South China Sea. Additionally, we highlight 2 separate suspected Chinese state-sponsored intrusion campaigns targeting entities in Laos and Cambodia. Both are likely intended to support BRI objectives. Victims in these 2 respective campaigns include the National Committee for Special Economic Zones (SEZs) and National Enterprise Database (NED) in Laos and Cambodia's Sihanoukville Autonomous Port (PAS).

¹ Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, typically when analysts have data corresponding to at least 3 points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-16, where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group.

Key Judgments

- Our research highlights China's continued strategic and tactical interest in government and private sector organizations in Southeast Asia. This targeting is almost certainly linked to a range of objectives intended to support a deepening of regional influence, including traditional intelligence gathering against regional rivals and allies, economic intelligence gathering against BRI-linked targets, and the South China Sea disputes.
- The operational tasking of TAG-16 is likely linked, in part, to gathering intelligence on South China Sea-related issues. Notably, Insikt Group identified the compromise of navies, prime minister's offices, ministries of defense, and ministries of foreign affairs across several countries with a presence in the South China Sea.
- The targeting of Cambodia's Sihanoukville Autonomous Port and Laos's National Committee for SEZs is likely linked to China's wider strategic objectives under the BRI. PAS has high strategic significance given its location along the Maritime Silk Road route, while the Lao government has promoted the development of SEZs as an entry point for private sector development, including domestic and foreign direct investment (FDI).

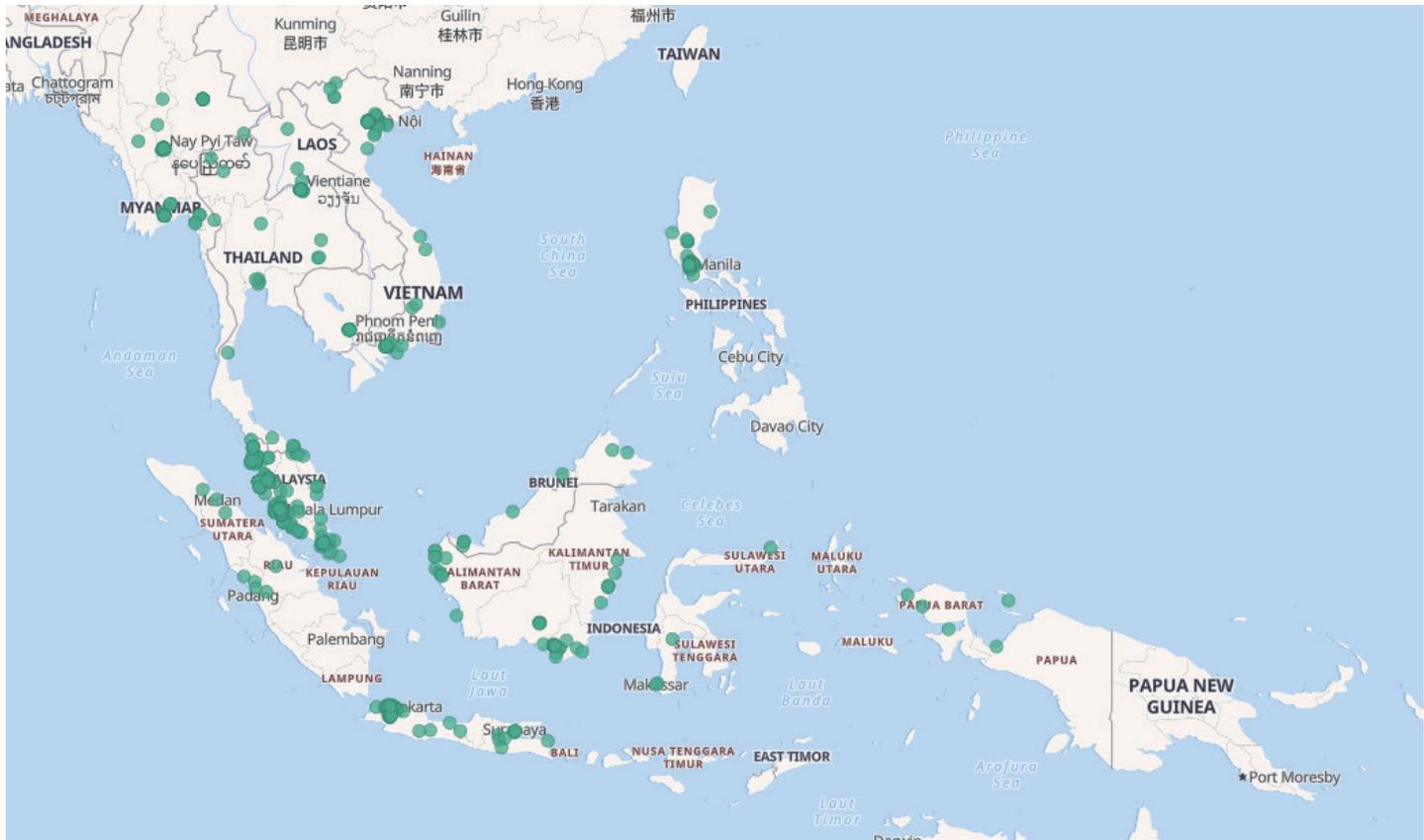


Figure 1: Suspected Chinese state-sponsored intrusions targeting Southeast Asia (past 9 months) (Source: Recorded Future)

Background

Insikt Group has reported extensively on Chinese state-sponsored threat activity groups targeting countries surrounding the People's Republic of China (PRC). In the past year, much of this activity has focused on India, with groups such as [RedEcho](#), [RedFoxtrot](#), and [TAG-28](#) heavily targeting government and private sector organizations following a significant increase in tensions between the Indian and PRC governments. Alongside this concentration on India, other Asian countries are also prime targets of many PRC-sponsored groups. Much of this is likely driven by traditional espionage goals, as well as supporting strategic policy objectives like the Belt and Road Initiative and Five-Year Plans. Southeast Asia is no exception to this, and the South China Sea territorial disputes very likely constitute another driver of China's cyber espionage activity.

Based on Recorded Future adversary infrastructure detection and Network Traffic Analysis (NTA) techniques, in the past 9 months, Insikt Group identified over 400 unique victim servers located in Southeast Asia communicating with malware command and control (C2) infrastructure with likely links to Chinese state-sponsored actors. The top 3 targeted countries within our data set were Malaysia, Indonesia, and Vietnam, with known groups active in the region including RedDelta, Naikon, and Goblin Panda, as well as temporary clusters we group as TAG-16 and TAG-22.

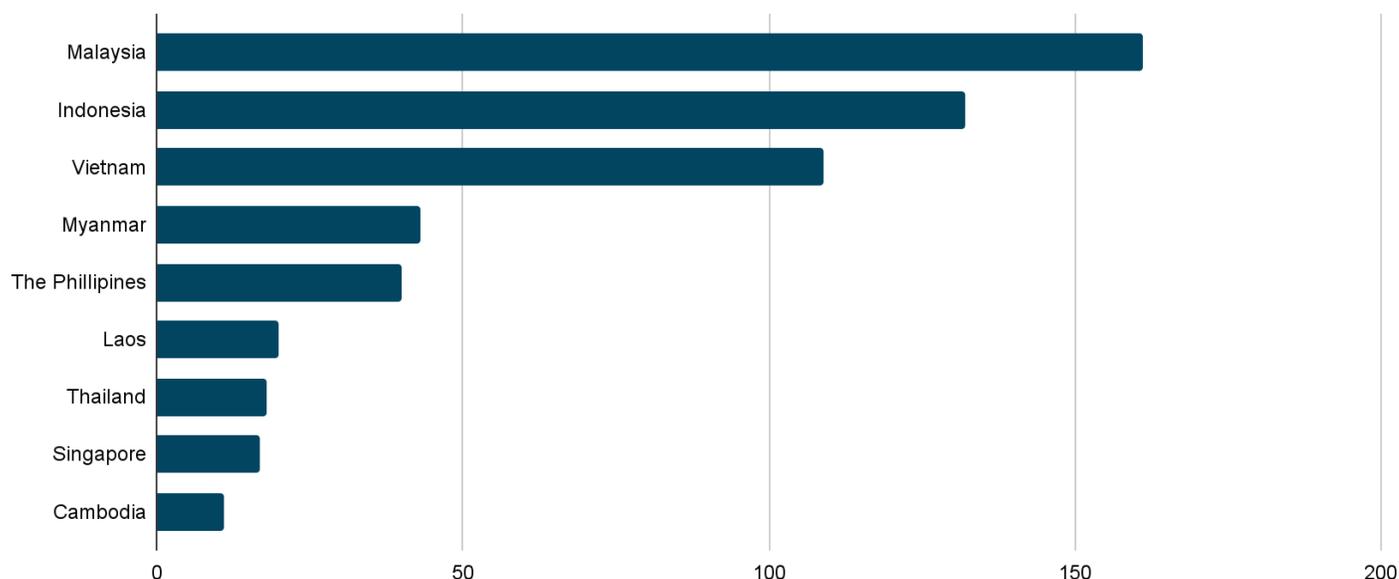


Figure 2: Suspected Chinese state-sponsored intrusions targeting Southeast Asia by country in the past 9 months. The number of victim organizations is likely smaller than the number of victim IPs listed due to IP reassignment and other technical considerations. (Source: Recorded Future)

China State-Sponsored Activity in the South China Sea

Chinese state-sponsored groups have traditionally been highly active in targeting the PRC's rival claimants in the South China Sea, with the operational tempo often mirroring increased geopolitical tensions. For instance, escalating tensions related to China's [development](#) of artificial islands containing [port facilities, airstrips, and military buildings](#) within the disputed Spratly Islands archipelago [reportedly](#) led to increased activity from Chinese state-affiliated groups in 2015. This activity entailed reconnaissance and phishing campaigns targeting rival claimants throughout the development of the artificial islands, which intensified as the PRC's progress was increasingly reported in local media throughout the region. Multiple Chinese APT groups were observed conducting this activity, including Vixen Panda, Naikon, and Goblin Panda (Cycldek).

In more recent years, Insikt Group has [observed](#) continued targeting of South China Sea claimants by additional Chinese state-sponsored groups, notably APT40, a [group linked](#) to the Ministry of State Security's Hainan State Security Department. APT40 has typically [targeted](#) maritime and engineering entities, as well as organizations with operations in Southeast Asia or involved in South China Sea disputes. Of particular note was the group's [targeting](#) of multiple Cambodian entities related to the country's electoral system ahead of the country's 2018 election. Given the [historical support](#) of Cambodia's incumbent government for China in the South China Sea, this has been [interpreted](#) as a possible step to monitor and avoid an election upset that could weaken China's influence in the region.

Activity Spotlight: TAG-16 Targets Southeast Asian Governments with South China Sea Focus

Throughout 2021, Insikt Group tracked a persistent cyber espionage campaign targeting the prime minister's offices, military entities, and government departments of rival South China Sea claimants Vietnam, Malaysia, and the Philippines, as listed in Table 1. Additional victims during the same period include organizations in Indonesia and Thailand. We attribute this activity to a Chinese state-sponsored group that we track as Threat Activity Group 16 (TAG-16). We also identified evidence suggesting that TAG-16 shares custom capabilities with the People's Liberation Army (PLA)-linked activity group RedFoxtrot.

In November 2020, Bitdefender [reported](#) on a TAG-16 campaign targeting Southeast Asian government institutions using the Chinoxy, FunnyDream, and PCShare backdoors. While the group behind this activity was unnamed, [Kaspersky](#) and [PWC](#) have also briefly referenced this FunnyDream campaign, with PWC tracking the group as Red Hariasa. In April 2021, we reported on multiple government organizations across Vietnam, Malaysia, Indonesia, Thailand, and the Philippines communicating with TAG-16 C2 infrastructure. In more recent activity, we identified a swath of additional high-value victims following this same targeting pattern within Southeast Asia and continued intrusions targeting organizations identified as victims within our previous research. Victim organizations include the following:

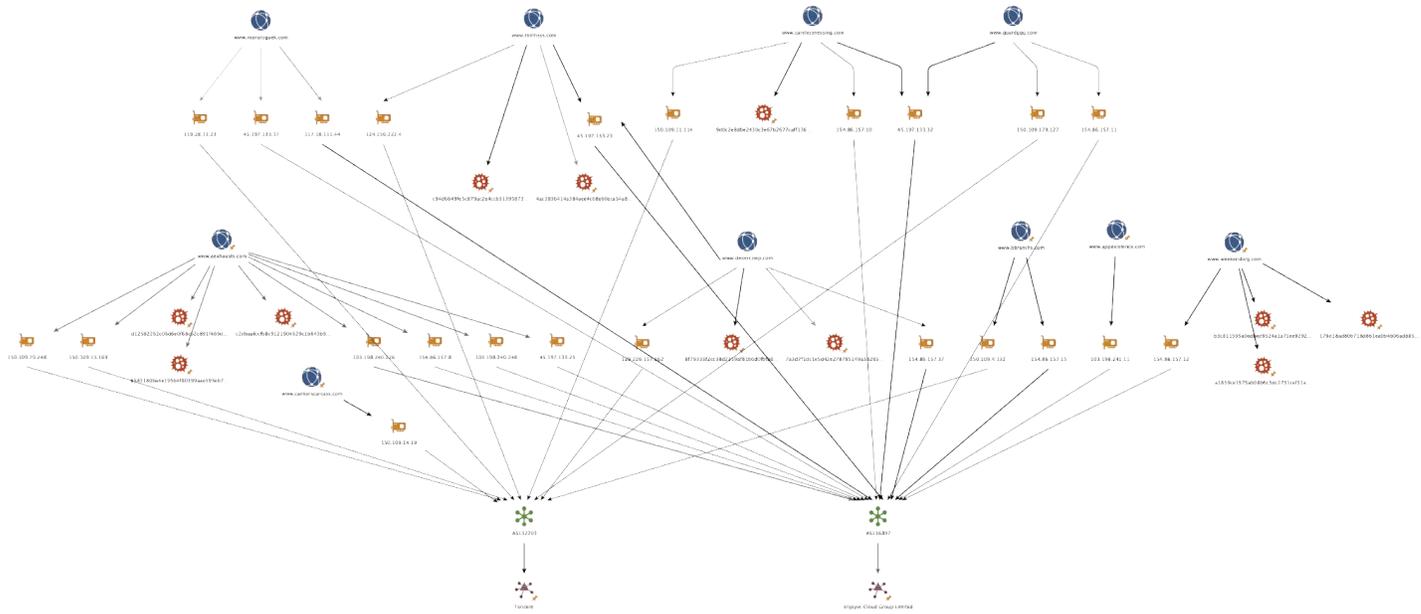


Figure 3: TAG-16 infrastructure cluster observed in targeting of SEA

| Organization | Country |
|---|-----------------|
| Ministry of Defense | Malaysia |
| Prime Minister's Office | |
| Royal Malaysia Police | |
| Anti-Corruption Commission (Suruhanjaya Pencegahan Rasuah Malaysia) | |
| Ministry of Foreign Affairs | |
| Philippine Navy | The Philippines |
| Armed Forces of the Philippines (AFP) | |
| Presidential Management Staff | |
| Department of Foreign Affairs | Vietnam |
| Ministry of Natural Resources and Environment (Department of Information Technology and Environment Resources Data (DINTE)) | |
| Vietnam National Assembly | |
| Central Office of the Communist Party of Vietnam | Thailand |
| Prime Minister's Office | |
| Royal Thai Army | |
| Indonesian Navy | Indonesia |
| Ministry of Foreign Affairs (Kementerian Luar Negeri Republik Indonesia) | |
| Cabinet Secretariat of the Republic of Indonesia | |
| Coordinating Ministry for Maritime and Investment Affairs | |

Table 1: Sample of identified TAG-16 victims

| SHA256 Hash | C2 Domain |
|--|---------------------------|
| c94d6649fe5c879ac2e4ccb313958736ac4c86f217c3a68c799f9641b6ac9f2a | www.rnihsss[.]com |
| 4ac3836414a384aee4c68e60eca54a848c8727a9e548de2b7ab76ecbd520107a | www.rnihsss[.]com |
| 9d0c2e8d0e2430c3e67b2677caff136e562570da162a371e9cfa6602c70b03bb | www.carelessnessing[.]com |
| b3c811595a0edbed9524a1a71ee9292c19792370c99f856f765a39f80a437418 | www.weekendorg[.]com |
| a1859ce1575ab08b6c3dc2731cef31e358dd3ccfc7d6febaccb6a730bc1d58c0 | www.weekendorg[.]com |
| 179d18ad80b718d861ea0b4b06ad885e0a7760051497db6eb87315f92dd24b53 | www.weekendorg[.]com |
| 8f79333f2cc38d2259af81b6d0fbfb0731f1e3442c187b19a6538d0e7daf85df | www.dexercisep[.]com |
| 7a3d7f1dc1e5d42e278785149a382651c70a8f967a153e1960cffff5f92eaa33 | www.dexercisep[.]com |
| d12582262c06d6e0f68c62c891f469d819e18e0498fa2e9d277981f25eee93a1 | www.aexhausts[.]com |
| 6543180ba4e195b4f80399aae593eb7554588b61e651fce81b91fefa56baec30 | www.aexhausts[.]com |
| c2dbaafccfb8c9121904629c1b643b99dfa934a2ec9f4bd8754ba3cad38b9a90 | www.aexhausts[.]com |

Table 2: TAG-16 FunnyDream backdoor samples

We identified multiple FunnyDream backdoor samples configured to communicate with the group's C2 infrastructure. These samples closely resemble FunnyDream samples previously reported by [Bitdefender](#) and [NTT Security](#). Other researchers have [noted](#) a possible link between TAG-16 and the SManager backdoor (also known as PhantomNet).

Specifically, an SManager sample referenced in [NTT Security reporting](#) (SHA256: 00badf016953ec740b61f4ba27c5886a6460f6abba98819e00bde51574e0ebf4), was identified containing appended FunnyDream code and artifacts, such as the hardcoded TAG-16 C2 domain `lotus.wmiprvse[.]com`, PDB path overlap, and “funnydream” and “prettygirl” strings characteristic of older FunnyDream samples. However, the file name “igfx.exe.bak” suggests this sample may have been tampered with, leaving an assessment on the group's possible access to SManager inconclusive at this time.

Publicly reported activity related to SManager primarily describes campaigns targeting Vietnam, which also aligns to TAG-16 activity described in [Insikt Group's findings](#). Notably, [ESET identified](#) a supply chain compromise targeting the Vietnam Government Certification Authority (VGCA), where a digital signature toolkit installer located on the VGCA website was compromised to serve the SManager backdoor. However, despite TAG-16's potential access to SManager, there is not sufficient evidence to link this supply chain compromise to this group at this time given the prevalence of tool sharing across disparate Chinese groups.

TAG-16 also [shares](#) a custom PCShare loader with the Chinese activity group RedFoxtrot, which [Insikt Group](#) linked to People's Liberation Army (PLA) Unit 69010 in June 2021. Both groups have used the same loader to inject the open source PCShare backdoor into memory. Despite this, the group's targeting and wider toolset are distinct, and this very likely further reflects the continued sharing of capabilities across Chinese threat activity groups.

Belt and Road Initiative-Linked Targeting

Historically, many Chinese cyber espionage operations have [heavily overlapped](#) with projects and countries strategically important to the BRI. The BRI (also known as One Belt, One Road) is a global infrastructure development and connectivity project launched by China in 2013. Under the initiative, China [assists](#) countries seeking to improve their overland and maritime transportation networks, telecommunications systems, and energy infrastructure, among other types of projects, through financial assistance and other development activities. Although purely economic on the surface, the BRI almost certainly serves China's [geopolitical influence](#) and [military aims](#) as well. [Insikt Group](#) has previously [reported](#) on China's Digital Silk Road Initiative, the digital infrastructure component of the BRI, which we assess poses both a critical cybersecurity threat to the world and a growing threat to competitors' markets.

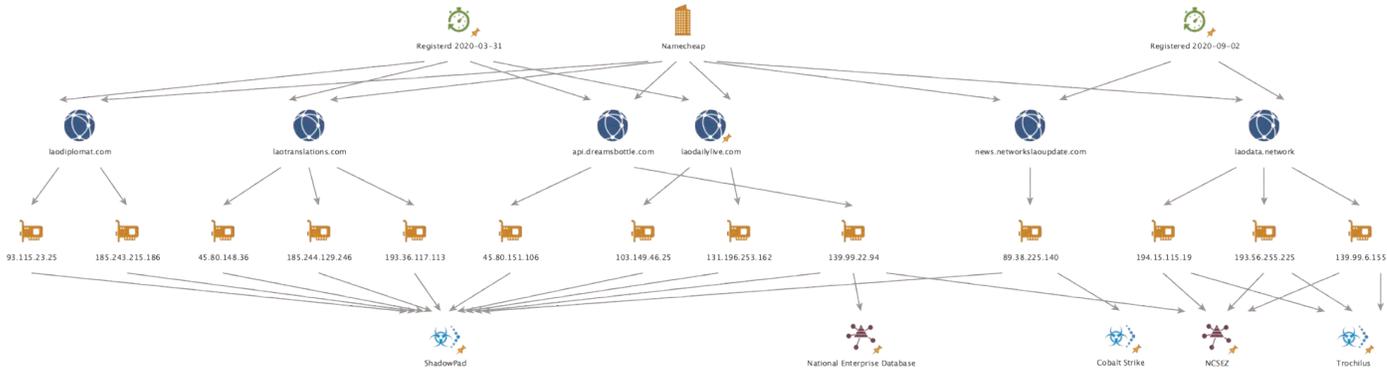


Figure 4: TAG-33 infrastructure cluster used in targeting of Laos entities

Activity Spotlight: TAG-33 BRI-Linked Targeting in Laos

In May 2021, Insikt Group identified a cluster of ShadowPad, Cobalt Strike, and Trochilus infrastructure used in suspected Chinese state-sponsored network intrusion activity targeting telecommunications, government, and state-owned organizations within Laos. Of particular note, we identified the targeting of both the Lao National Committee for Special Economic Zones and the National Enterprise Database, which likely [aligns](#) with wider Chinese government economic and policy objectives under the BRI. We currently track this activity using the temporary group designator TAG-33. The Lao government has promoted the development of SEZs as an entry point for private sector development, including domestic and foreign direct investment (FDI). Notably, China has [invested](#) more than \$1.5 billion in Laos’s SEZs, reportedly as part of the BRI, which Laos [joined](#) in 2018. Today, 4 of Laos’s 14 SEZs are [operated](#) by Chinese firms.

In addition to the multiple cases of overlapping victimology across this cluster, all of the identified C2 domains were registered through Namecheap, are Laos-themed, and many were registered on the same day. Across this series of intrusions, there were some historical overlaps with activity attributed to the Chinese state-sponsored group Goblin Panda (also known as Conimes and Cycldek). In addition to infrastructure overlap, the [targeting](#) of Laos and the use of [Laos-themed domains](#) is also in line with historical Goblin Panda activity. However, as the identified infrastructure overlaps were non-concurrent, we continue to track this TAG-33 activity as a distinct cluster.

TAG-33 Goblin Panda Overlaps

Insikt Group first identified the Trochilus C2 IP address 139.99.6[.]155 hosting the domain laodata[.]network and its subdomain cdn.laodata[.]network on March 5, 2021. This domain has historical non-concurrent hosting overlaps with the suspected Goblin Panda domain viengchannews[.]com in 2019, through the New Zealand IP address 103.209.194[.]149. The subdomain cdn.viengchannews[.]com is linked to a RoyalRoad RTF sample which drops a NewCore RAT sample, both of which have previously been [linked](#) to Goblin Panda activity. The use of a .cdn subdomain and the popular registrar Namecheap is an additional link between these 2 indicators.

The Cobalt Strike and ShadowPad C2 89.38.225[.]140 hosting the domain networkslaoupdate[.]com was also identified in relation to this activity due to shared victimology. Both networkslaoupdate[.]com and laodata[.]network were registered on the same day through Namecheap. This server was configured with the [Cobalt Strike Amazon malleable C2 profile](#) and used news.networkslaoupdate[.]com for C2. Similar to the laodata[.]network domain, this domain features historical non-concurrent infrastructure overlap with a [publicly reported](#) Goblin Panda domain, laovoanew[.]com, with both domains hosted on the Singapore IP address 103.253.25[.]158 several months apart in 2019.

| SHA256 Hash | Description |
|--|--|
| 130daacff74d57bb2319fc5cf815e783c6505883f69e4adcd4c2b1cac3e598ce | Royal Road RTF sample written in Lao |
| 207e66a3b0f1abfd4721f1b3e9fed8ac89be51e1ec13dd407b4e08fad52113e3 | NewCore RAT sample dropped from Royal Road |

Table 3: Historical Goblin Panda malware samples

Activity Spotlight: TAG-34 Targeting of Cambodian Port Facility

In September 2021, Insikt Group identified intrusion activity linked to a suspected Chinese state-sponsored threat activity group targeting the Cambodian Ministry of Foreign Affairs (MOFA) and the country’s sole international and commercial deep seaport, Sihanoukville Autonomous Port. Using Recorded Future Network Traffic Analysis (NTA), we detected infrastructure linked to both of these entities communicating with a ShadowPad C2 cluster over a sustained period, which we currently track using the temporary group designator TAG-34. While we do not attribute this activity to a known threat activity group at this time, ShadowPad is a custom backdoor shared across multiple Chinese state-sponsored groups.

While the targeting of Cambodia’s MOFA likely falls within the scope of traditional cyber espionage, the activity aimed at PAS is more likely linked to China’s objectives under the BRI. Although the port is government owned, it is largely financed by Japanese investment and is located near the China-owned Sihanoukville Special Economic Zone (SSEZ), a key location for China’s BRI-linked projects within Cambodia. PAS also has high strategic significance given its location along the Maritime Silk Road route, along which Chinese companies have financed and built multiple deep sea ports under the banner of the BRI. China and Japan have historically vied for influence within Sihanoukville, with the targeting of the PAS potentially supporting an effort to offset Japanese influence within the province.

From at least June until October 2021, infrastructure associated with these Cambodian organizations were identified communicating with the ShadowPad C2 cluster highlighted in Figure 5. As well as hosting overlaps, all of the identified domains were registered through GoDaddy and use 1984 Hosting nameservers. Originally considered unique to APT41 activity, in recent years ShadowPad use has drastically expanded across Chinese state-sponsored groups, with Insikt Group tracking at least 7 distinct activity groups using the malware family.

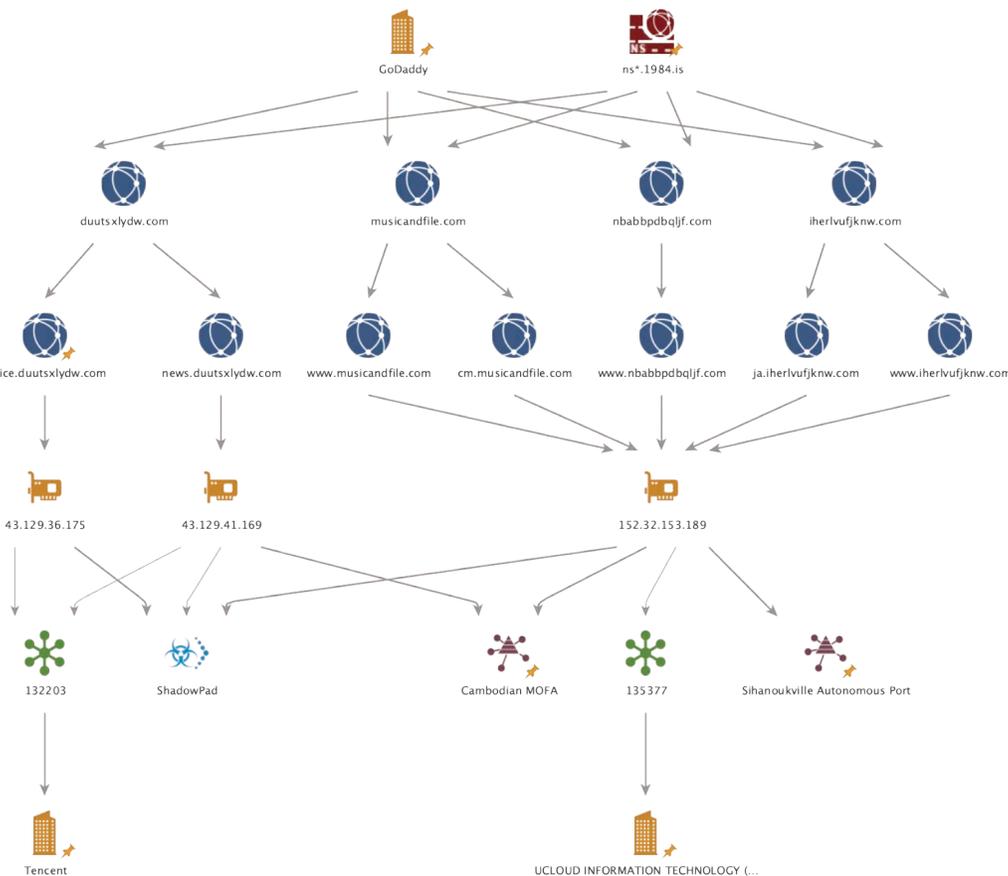


Figure 5: ShadowPad infrastructure cluster used in the targeting of Cambodian entities

Outlook

Our research highlights China's continued strategic and tactical interest in government and private sector organizations in Southeast Asia. This targeting likely serves several objectives, including traditional intelligence gathering against regional rivals and allies, economic intelligence gathering against BRI-linked targets, and the South China Sea disputes. Future activity targeting rival South China Sea claimants is likely to increase in line with geopolitical tensions.

The scale and scope of China's cyber espionage program remain unrivaled, exemplified by the large number of distinct actors with operational taskings within specific geographic regions. The countries surrounding China bear the brunt of this activity and are prime targets of many PLA Strategic Support Force (SSF) and Ministry of State Security (MSS)-linked threat activity groups.

Appendix A

TAG-16 Activity

TAG-16 C2 Domains

www.cankerscarcass[.]com
www.appexistence[.]com
www.rnihhsss[.]com
www.aexhausts[.]com
ttxs.aexhausts[.]com
cdn.aexhausts[.]com
www.bbranches[.]com
www.carelessnessing[.]com
www.dexercisep[.]com
www.weekendorg[.]com
www.manaloguek[.]com
www.guardggg[.]com

Recently Active C2 IPs (last 1 month)

150.109.14[.]19
103.198.241[.]11
103.198.241[.]55
103.198.241[.]58
121.78.139[.]168
121.78.139[.]169
154.86.157[.]12
154.86.157[.]15
154.86.157[.]16
154.86.157[.]17
45.197.133[.]23
45.197.133[.]25
45.197.133[.]44

FunnyDream Backdoor Samples

8f79333f2cc38d2259af81b6d0fbfb0731f1e3442c187b19a6538d0e7daf85df
c2dbaafccfb8c9121904629c1b643b99dfa934a2ec9f4bd8754ba3cad38b9a90
7a3d7f1dc1e5d42e278785149a382651c70a8f967a153e1960cffff5f92eaa33
6543180ba4e195b4f80399aae593eb7554588b61e651fce81b91fefa56baec30
4ac3836414a384aee4c68e60eca54a848c8727a9e548de2b7ab76ecbd520107a
9d0c2e8d0e2430c3e67b2677caff136e562570da162a371e9cfa6602c70b03bb
c94d6649fe5c879ac2e4ccb313958736ac4c86f217c3a68c799f9641b6ac9f2a
a1859ce1575ab08b6c3dc2731cef31e358dd3ccfc7d6febaccb6a730bc1d58c0
179d18ad80b718d861ea0b4b06ad885e0a7760051497db6eb87315f92dd24b53
b3c811595a0edbed9524a1a71ee9292c19792370c99f856f765a39f80a437418
d12582262c06d6e0f68c62c891f469d819e18e0498fa2e9d277981f25eee93a1

TAG-33 Laos Campaign

ShadowPad, Cobalt Strike, and Trochilus C2 Infrastructure

laodailylive[.]com
laodiplomat[.]com
api.dreamsbottle[.]com
news.networkslaoupdate[.]com
laodata[.]network
laotranslations[.]com
193.56.255[.]225
139.99.22[.]94

RoyalRoad

130daacff74d57bb2319fc5cf815e783c6505883f69e4adcd4c2b1cac3e598ce

Newcore RAT

207e66a3b0f1abfd4721f1b3e9fed8ac89be51e1ec13dd407b4e08fad52113e3

Cobalt Strike

47b12169eb9933b8481327a9775d1efd4fa077881f023892938056ff06e4f2b4

TAG-34 Cambodian Campaign

ShadowPad C2 IP Addresses & Associated Domains:

nbabbpbdqljf[.]com
www.nbabbpbdqljf[.]com
iherlvufjknw[.]com
ja.iherlvufjknw[.]com
www.iherlvufjknw[.]com
musicandfile[.]com
www.musicandfile[.]com
cm.musicandfile[.]com
duutsxlydw[.]com
news.duutsxlydw[.]com
office.duutsxlydw[.]com
43.129.41[.]169
43.129.36[.]175
152.32.153[.]189

Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cybercriminals — individuals and groups — from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

Our coverage includes:

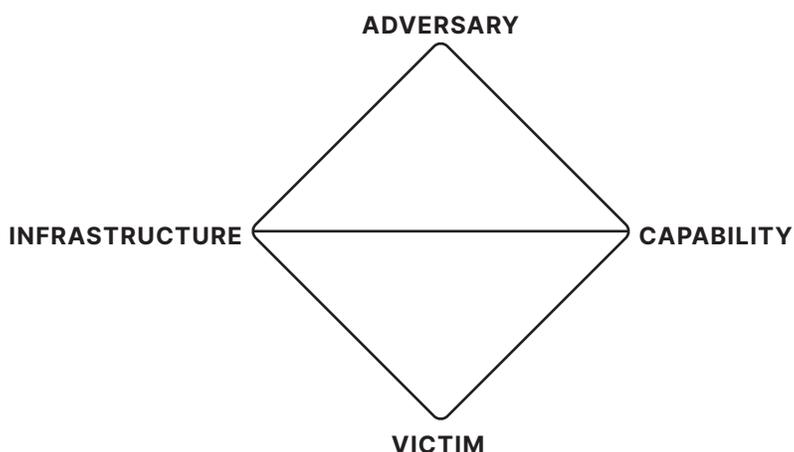
- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors
- Recorded Future-identified, suspected nation-state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific, persistent commodity malware

Insikt Group publicly names a new threat activity group or campaign, such as RedFoxtrot, when analysts typically have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence. We will occasionally report on significant activity using a temporary activity clustering name such as TAG-21 where the activity is new and significant but doesn't map to existing groupings and hasn't yet graduated or merged into an established activity group. We tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely used or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.

Insikt Group uses a simple color and phonetic alphabet naming convention for new nation-state threat actor groups or campaigns. The color generally corresponds to that nation's flag colors, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.

For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.



About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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