Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Examining the Cybersecurity Impact of State-Linked Threat Actors in African Digital Infrastructure

Ciré SALL
Centre de Formation Africain du Sénégal, Dakar, Senegal.

Manuscript received 7 Feb. 2026; accepted 19 Apr. 2026; published online 19 May 2026.

Abstract

Our paper presents results from a review of impacts of foreign threat actors on African cyberspace, with a focus on Chinese nationals between 2007 and 2025. We identified three case in which, on demand of African officials, Chinese actors helped to access to citizen data and privacy or used citizen data without clear agreement. We also identified 21 threat actor groups involved in 55 incidents, acting on their own and targeting about 21 countries. Those 55 incidents were analyzed with respect to their frequency, perpetrator type, motivation, and victim type. We found that incidents related to hacking-on-demand of African countries are marginal compared to threat actor groups' intrusions that are increasingly targeting Africa; that most frequent perpetrators are advanced persistent threat (APT) groups; that most incidents are motivated by information theft and espionage; that the more countries have close partnership with China, the more they are likely to be targeted; and that South Africa is the most targeted country. Based on findings, the author suggests that African Computer Security Incident Response Teams (CSIRT) should follow up on activities of threat actor groups globally and locally, and release reports allowing authorities to better understand the global and specific country's cyber-threat landscapes. For example, those teams should be able to investigate and flush out hidden malwares in devices before these latter reach low-income households.

I. Introduction

With more than 604 million Internet users [1], Africa has one of the fastest growing Internet network in the world. This increase in connectivity made Africa an emerging market for foreign companies looking to expand their user bases. Among foreign companies, those from China like Huawei, ZTE and Hikvision, are notable. This presence is in line with the China Going Global Policy (CGGP) which can be applied bilaterally or through the Forum on Cooperation (FOCAC). CGGP was aimed at enabling Chinese companies to install themselves around the world in order to guarantee natural resources, access to technology and further their competitiveness for export. The policy has evolved since then to encompass other forms of investment as part of the framework of the Belt and Road Initiative (BRI) [2]. FOCAC is an important forum which however suffers from a certain disequilibrium as it is dominated by a donor-

Keywords: Campaigns and advanced persistent threat (APT) groups, Chinese threat actors, information security, information theft and espionage.

Production and hosting by NAUSS

* Corresponding author: Ciré SALL
Email: sallcire@gmail.com
doi: 10.26735/HKKU4292

recipient dynamic. Because of African countries' weaknesses in strategic planning, the agenda often originates from China. By engaging in Africa, Beijing seeks to move forward its ambition of reaching a great power status [3]. As a consequence, China has a real footprint in Africa's digital infrastructure. Huawei has built more than 70% of the 4G telecom networks in Africa [4], and is engaged in the deployment of 5G by partnering, for example, with Mobile Telephone Network (MTN) in South Africa [5], and with Orange in Egypt [6]. Huawei, ZTE, and other companies from China have built or equipped at least 14 government networks, including dedicated military and police telecoms systems. Furthermore, the Chinese government has donated office equipment, including computers, to at least 35 African governments [4].

It is clear that China's investments in African digital infrastructure have improved this latter in terms of quality and have increased the Internet penetration. However, events like the reported espionage on the African Union (AU) attributed to China [7] suggest that there should be a real concern about the presence and negative impact, on Africa cyberspace, of such Chinese companies which are compelled by law to help the government collect intelligence [4]. This is clearly stated in the seventh article of the People's Republic of China (PRC)'s intelligence law [8].

This paper is an attempt to give an insight into such an impact, based on reported incidents that occurred in the African cyberspace. At least two reasons make the African countries susceptible to cyberattacks. The first one is the Internet penetration which ranges from 12.5% for Burundi to 92.2% for Morocco [9]. As a consequence, given that 10-15% Internet penetration is the threshold level for the generation of important hacking activities [10], African countries, all of which have reached this threshold, are experiencing numerous cyber-incidents. The second reason is that African countries are lagging behind in dealing with cybersecurity concerns [11]. For example, despite the African Union Convention on Cybersecurity and Personal Data Protection [12] was adopted in 2014, this latter entered into force only in June 2023, i.e., nine years after its adoption. According to the International Telecommunication Union Global Cybersecurity Index [13], only 55% of countries in Africa have a Computer Incident Response Team (CIRT) which role is to detect, prevent, respond to and mitigate cyber-threats and incidents. This percentage falls down to 25% when it comes to consider countries that have CIRT and cyberdrills. The report also underscores that in order to guarantee that the Domain Name System (DNS) is safe and authenticates responses to domain name lookups, only 0.43% of African providers have implemented DNS Security Extensions, compared to a higher adoption rate of 11.28% in Europe.

This study investigates Chinese actors' impact on African cyberspace by discriminating two situations:

1) When Chinese nationals help with espionage, to have access to citizen data, or use citizen data themselves, upon the request of African countries, we call it hacking-on-demand (HOD);
2) When espionage or hacking occurs from Chinese adversaries on their own initiative, we call it spontaneous hacking (SH).

Our aim to uncover the breadth of Chinese threat actors' intrusions in the continent cyberspace, and understand the distribution of these cyberattacks. To that end, we will need to answer the following questions:

1) Which of the HOD and SH is more prevalent.
2) What is the global trend of incidents over years.
3) What is the distribution of incidents with respect to targeted countries or perpetrator types; and why some countries are more targeted than others.

The total number of campaigns (or groups) reported is 21 and the aggregate number of incidents that targeted African countries is 55, as far as SH is considered. Three incidents related to HOD have also been reported. All incidents were identified between 2007 and 2025. Data were gathered by reviewing online media reports from, inter alia, Financial Times, Reuters, World Street Journal, Le Monde, Al Jazeera; or reports from cybersecurity firms like Trend Micro, ESET, Kaspersky, Mandiant, Palo Alto Networks, Recorded Future, and so on.

We used research terms like "Chinese APT group", "Chinese espionage" along with "Africa",

to identify incidents that occurred in the continent. We also used targeted online searches, typing, for example, the name of a specific campaign or APT group to gather more information.

Notice that most of the incidents reported here do not target African countries specifically; hence specific details about a particular attack that targeted a given African country may not be available. When a campaign targets the same country multiple times, we considered this to be a single incident.

While this study focus on Chinese threat actors, these latter are not alone in targeting Africa. For example, ProjectSauron [14] and Equation APT [15] campaigns attributed to US nationals, have been reported as targeting African countries, among others in the globe. The same holds for the Spanish Mask APT group [16] and the Agrius campaign [17] from Iranian threat actors, which also targeted Africa. However, this is out of this paper's scope.

II. Hacking-on-Demand

The first case study belonging to HOD emphasizes how Huawei employees assisted the Zambian government spy on political adversaries [18], [19]. According to senior officials, Huawei technicians helped to hack into the phones and Facebook pages of a group of bloggers running a key opposition website known for its criticism against the then-President Edgar. At least two Huawei experts based in a cybersurveillance unit of Zambia's telecoms regulator were in constant contact with police units dispatched to arrest the bloggers.

The second case study focuses on Uganda where in 2019, Kampala police procured $126 million worth of closed circuit television camera (CCTV) surveillance technology from Huawei in order to monitor the city's growing crime problem [20]. This made the opposition and civil society contend that the surveillance tools that are based on facial recognition technology, will be used instead to track opponents. This claim seems to be justified as it has been reported that in 2018, senior intelligence officials benefited from Huawei technicians' help in penetrating the digital communications of Bobi Wine, an opposition leader. This led to the arrest of this latter as well as many of his partisans [18], [19].

The third case study is not a formal hacking, but is related to the use of citizenry data without their input. In fact, the Australian Strategic Policy Institute reported that in March 2018, CloudWalk Technology, a giant of Artificial Intelligence (AI) in China, concluded an agreement with the Zimbabwean government to build a national facial recognition database and monitoring system as part of China's BRI program [21]. Zimbabwe had to provide CloudWalk with biometric data on millions of its citizenry to help in the development of facial recognition algorithms intended to perform well with different ethnicities; and this without any consultation of ordinary citizens. What makes this deal vital for the Chinese firm is the fact that facial recognition technology is known to perform poorly in detecting people with dark skin; which makes the biometric data from Zimbabwean nationals highly valued. The ultimate goal of the company is to improve its facial recognition systems for people with dark skin, hence promoting the use of its technology worldwide. As a reward, CloudWalk's technology would be deployed in many vital entities of the country including financial industry, airports, bus stations, railway stations as well as any other locations requiring face recognition to ensure public security. The institute hence considered this arrangement as a data colonialism. The author in [22] went further by focusing on three concepts which are algorithmic oppression, algorithmic exploitation, and algorithmic dispossession. The study emphasized that the deployment of Chinese AI surveillance technology in Zimbabwe leads to algorithmic oppression due the extension of the unjust subservience of social groups and the privileging of the ruling party; that algorithmic exploitation occurs because the development of the technology involves the exploitation of data and labor; and that algorithmic dispossession also happens because the policies related to the importation of the technology facilitate the centralization of Chinese economic power, in presence of unfit national legal framework and environment.

III. Spontaneous Hacking

Our investigation identified the following reported campaigns that targeted African countries and involved Chinese threat actors:

A. NetTraveler (One Incident; 2013)

In June 2013, Kaspersky experts published a report about the NetTraveler group which compromised hundreds of high-profile victims in 40 countries, among which Morocco [23]. Victims were infected via clever spear-phishing emails with malicious Microsoft Office attachments exploiting two vulnerabilities, CVE-2012-0158[1] and CVE-2010-3333[2]. Experts were able to gain access to, and obtain infection logs from many of the group's command and control (C2) servers that allow to install additional malware on infected machines and exfiltrate stolen data. The stolen data exfiltrated from infected machines and estimated to 22 gigabytes typically included file system listings, keystrokes, and various types of files like PDF, Excel and Word.

B. Safe (Three Incidents; 2013)

In 2013 Trend Micro released a report on the operations of a campaign they referred to as Safe [26]. The Safe campaign compromised many organisations including government ministries, academic research institutions, technology companies, non-governmental organisations (NGO) and media outlets. Taking advantage of the mistakes the attackers made, researchers gained a deeper understanding of the group activities. For example, the contents of the directories of one of the C2 servers were viewable to anyone who accessed them, without any restriction. This allowed them to determine the campaign's victims and to download the PHP source code used for the C2 server as well as the C code used to generate the malware used in attacks. The Safe campaign used spear-phishing emails containing a malicious attachment that exploited the CVE-2012-0158 vulnerability. If opened with an obsolete version of Microsoft Word, a malicious payload is installed on the unsuspecting user's machine. As a consequence, the attackers could take control of the system and steal data. Following initial compromise, affected systems may be instructed to download additional malware and tools. Those tools that were found on the C2 servers are off-the-shelf programs able to extract saved passwords from browsers like Internet Explorer and Mozilla Firefox or stored Remote Desktop Protocol credentials. The list of Safe campaign's victims includes Algeria, Egypt and South Sudan.

[1] CVE-2012-0158 allows remote attackers to execute arbitrary code via a crafted web site, Office document, or RTF file that triggers system state corruption [24].

[2] CVE-2010-3333 is a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code via crafted RTF data [25].

C. APT1 (One Incident; 2013)

In the same year, it was also reported that an organization in South Africa fell victim to the APT1 espionage group of Chinese hackers [27]. APT1 is considered to be the second Bureau of the People's Liberation Army General Staff Department's third department, also known as Unit 61398. The group is known to steal many types of information including those related to product development and use, manufacturing procedures, business plans, policy positions and analysis, e-mails of prominent employees, user credentials or information related to network architecture.

D. PNRC Attack (One Incident; 2007)

In 2015, the Al Jazeera cables alleged that South African spies suspected that Beijing was involved in break-ins at a major nuclear facility. According to secret documents leaked to Al Jazeera's Investigative Unit [28], the dispatched agents stole technology in order to gain the advantage in a then-new kind of nuclear power generation. The attackers climbed up a fence surrounding the nuclear facility, disabled alarms, shot a man who interrupted them, and then ran away with a laptop computer stolen from a control room. It is noteworthy that this contradicts the narration of South African government and nuclear officials considering the 2007 incidents at the Pelindaba Nuclear Research Center (PNRC) as a piece of random criminality and a simple burglary attempt. This is the only incident where intellectual property theft is evident; and also the only one that involved physical hacking.

E. HummingBad (Two Incidents; 2016)

By early 2016, researchers at Check Point discovered HummingBad which is a malware that installs a persistent rootkit on Android devices, generates fraudulent advertisement incomes, and sets up other fraudulent applications [29]. Their investigation focused on the C2 servers used by

the group revealed that the attackers' repositories belong to Yingmob, a mobile advertisement company in China, which develops legitimate platforms along with malicious ones. To obfuscate their action, the HummingBad campaign was run together with a legitimate advertising analytics business, allowing the company to share its technology and resources, and consequently enabling it to control tens of millions of Android devices. The fraudulent advertisement revenue achieved by the campaign per month reached $300,000. With these devices under control, threat actors could create a botnet used for further attacks or even sell the access to other cybercriminals on the black market. According to the report, both Egypt and Algeria were from the victims of the campaign.

F. Red Apollo (One Incident; 2017)

South Africa was the target of Red Apollo known as APT10 and considered as a cyberespionage group from China, within the Cloud Hopper espionage campaign [30]. According to the Federal Bureau of Investigation (FBI), two members of the group who have been indicted for conspiracy to commit computer intrusion, wire fraud, and aggravated identity theft, were identified. The threat actors worked for a company located in Tianjin, China, and are believed to act in association with the Chinese Ministry of State Security's Tianjin State Security Bureau. The victims of the group, active from at least 2006, include companies in many fields like aviation, space and satellite, manufacturing, oil and gas exploration, production, communications, computer processor and maritime [31].

G. Bronze President (Three Incidents; 2018, 2022)

In 2018, China was accused of hacking the headquarters of the AU funded ($200 million) by Beijing and built by a state-owned company. The Continental organization computer systems were under persistent intrusion for five years, and confidential data were stolen. Data exfiltration was at its maximum every night between midnight and 2am from January 2012, upon the building inauguration, to January 2017 [7]. Furthermore, four nationals from Algeria, along with Ethiopian cyber experts discovered, after inspection, some listening devices under desks and in the walls. As consequence, the AU set up its own servers and all electronic communications were encrypted and no longer passed through Ethio Telecom, the domestic operator [32]. Despite this, later on, the organization was again targeted [33]. In fact, the AU's technology staffers received a message from Koichiro Komiyama, the deputy director of the global coordination division of Japan's Computer Emergency Response Team (CERT), who sent an e-mail after his team discovered a malicious traffic while investigating a hacking group's old infrastructure.

Within days of Komiyama's alert, AU's staff was able to locate the suspicious traffic to a set of servers in the basement of the organization's Building C, part of an older complex. The security breach was carried out by a Chinese hacking group nicknamed Bronze President. Hackers were able to steal a large amount of data from the servers, hiding it in the regular flow leaving the AU's network during business hours, even stopping their data stealing temporarily during lunch. This espionage is due, in part, to China's role in providing the AU with Information and Communication Technology infrastructure; which allowed Beijing to establish backdoors into AU servers and put listening devices. South Sudan and South Africa have also been reported as victims of the same group [34].

H. xHelper/Triada (Five Incidents; 2020)

In August 2020, an alarming release of Upstream [35], unveiled xHelper/Triada malware that was seen on thousands of low cost devices made by Transsion, a Chinese manufacturer. The malicious agent comes pre-installed on mobile users' devices and signs them up to subscription services without their permission. Secure-D which is an Upstream anti-fraud platform, caught and blocked an unusually large number of transactions coming from Transsion Tecno W2 handsets mainly in Ethiopia, Cameroon, Egypt, Ghana and South Africa. Following their investigation, they found pieces of the xHelper/Triada malware preinstalled on 53,000 Transsion's smartphones.

Technically, Triada is a backdoor and malware downloader. It installs xHelper which a trojan onto compromised devices. Notably, xHelper is able to persist after reboots, application removals and even factory resets. This makes it extremely difficult to remove even for experienced professionals. In presence of a phone network, xHelper can make queries to find new subscription targets and submit fraudulent subscription requests on behalf of the phone's owner automatically without any input from him, and does so hiddenly. If successful, all user's pre-paid airtime will be consumed.

I. Gelsemium (Six Incidents; 2021, 2022)

In mid-2020, researchers at ESET began to track multiple campaigns, later attributed to the Gelsemium cyberespionage group, and found the earliest version of the malware going back to 2014 [36]. Victims of these campaigns are located in East Asia as well as the Middle East, specifically Egypt, and include governments, religious organisations, electronics manufacturers and universities. ESET researchers found a new version of Gelsemium which is complex and modular, with components they dubbed Gelsemine, Gelsenicine and Gelsevirine. Gelsemine is the first stage of Gelsemium and acts as a dropper that drops both Gelsenicine and Gelsevirine. Gelsenicine is a loader that searchs for Gelsevirine in order to execute it. Gelsevirine is the last stage of the chain that will be in contact with the C2 server. Kenya, Djibouti, Swaziland, Equatorial Guinea and Nigeria have also been targeted by the group [37].

J. Back Door Diplomacy (Nine Incidents; 2020, 2021, 2023)

As threat intelligence analyst at ESET, Adam Burgher released a report in 2021 stating that an APT group called BackdoorDiplomacy, was active in Africa and the Middle East, targeting ministries of foreign affairs and telecommunication companies since at least 2017 [38]. Initial access was accomplished via vulnerable Internet-exposed devices such as web servers and management interfaces for networking equipment. Then, threat actors used open-source tools for scanning the environment and lateral movement. Interactive access was achieved via Turian backdoor or open-source remote access tools. Interestingly, they focused on targeting removable media for data collection and exfiltration and targeted both Windows and Linux operating systems. Using a map, the author reported that the group targeted Libya, Nigeria, Ghana, South Africa and Namibia. Moreover, SentinelOne also noted that the group had carried out campaigns in Africa, targeting other countries like Kenya, Senegal and Ethiopia [39]. Egypt has also been reported as a target of the same APT group [40].

Specifically for Kenya, Reuters reported that Kenya's government was victim of large and persistent intrusions from Chinese threat actors who targeted key ministries and state institutions [41]. By late 2019, Kenyan authorities enlisted the services of a national cybersecurity expert to analyze a government-wide network hacking. This happened in a context where Kenya's financial issues were showing, and Beijing was decreasing his lending that went over $9 billion, and used to build or upgrade railways, ports and highways. The intrusion began with a spear-phishing attack at the end of 2019, when an unsuspecting government employee downloaded an infected document, allowing threat actors to infiltrate the network and access other agencies. As a consequence, a huge volume of documents were exfiltrated from the ministries of foreign affairs and finance. The attacks focused on the debt situation. Notably, according to documents provided by the analyst, the cyberespionage also reached the office of Kenya's president, the ministries of defense, information, health, land and interior, the counter-terrorism center and other institutions which were victim of persistent and prolonged hacking activity.

In early July 2021, the research reports shared by an intelligence analyst in the region documented how the intruders hacked into an e-mail server used by Kenya's National Intelligence Service (NIS); and Reuters was able to verify that the victim's IP address belonged to the NIS. Due to identical tools and techniques used in other hacking campaigns, Reuters provided Palo Alto Networks, with the IP address used by the hackers. The firm confirmed it as belonging to BackdoorDiplomacy and that this latter is sponsored by Beijing.

In addition, Reuters was also able to confirm that a server controlled by the Chinese hackers accessed a shared Kenyan government webmail service from December 2022 to February 2023.

K. Worok (Three Incidents; 2022)

In 2022, an ESET report uncovered attacks that used unknown tools targeting prominent companies and governments [42]. Dubbed Worok, the espionage group was active since at least 2020 and targeted entities in various countries, among which a private company in southern Africa. The targets' profiles and the tools used against victims suggest that Worok's main objective is to steal information. In some cases, initial accesses was obtained using exploits targeting the ProxyShell vulnerabilities. Once on a system, hackers deployed publicly available tools for reconnaissance like Mimikatz, EarthWorm, ReGeorg, and NBTscan, and then deployed their custom implants: a first stage loader, followed by a second one. The first stage loader CLRLoad is written in C++ and loads the next stage PNGLoad. CLRLoad may have been replaced, in subsequent Worok campaigns, by PowHeartBeat, a full-featured backdoor written in PowerShell. PNGLoad, the second stage payload deployed by Worok on compromised systems, which can be loaded either by PowHeartBeat or CLRLoad, is a loader that uses steganography to extract hidden malicious payloads to execute, from PNG files. Through a map, the report located the victims in Botswana, Namibia and South Africa.

L. Earth Lusca (One Incident; 2022)

In 2022, Trend Micro released a report about a threat actor from China they dubbed Earth Lusca [43]. The type of targets and the evidence found suggest that the goal of the group is cyberespionage, according to authors. However, cyber actors appeared also to be financially motivated considering their target of gambling companies and cryptocurrency platforms. The victims are from diverse regions and countries in the globe, including Nigeria. Earth Lusca's infrastructure included two clusters. The first one was set up with virtual private servers and the second one was a set of compromised web servers. In order to hide the IP addresses of their compromised servers, Cloudflare was used as a proxy for these latter. The first cluster is a C2 server for malware with tools like Cobalt Strike, ShadowPad, FunnySwitch, and Winnti, used by the threat actors to compromise victims. The second cluster is also a Cobalt Strike C2 server, but that additionally scans for vulnerabilities in targeted public-facing servers or builds traffic tunnels within the victim's network. Investigating Secure Shell access logs unveiled that a suspect IP address traced back to a region near Sichuan, Chengdu, China, was connected to a compromised server.

M. Daggerfly (One Incident; 2023)

In April 2023, experts from the Threat Hunter Team at Symantec and Carbon Black reported that a telecommunications organization in Africa was among the victims of the Daggerfly APT group, using undocumented plugins from the MgBot[3] malware framework [45]. The cyberespionage group also used a PlugX loader which is a remote access tool with modular plugins, and profited from AnyDesk which is a common remote desktop software. Authors noticed that the use of the MgBot modular malware framework and PlugX loader had been associated in the past with China-linked APTs. At least, Nigeria was from the list of victims [46].

N. Operation Tainted Love (One Incident; 2023)

In September 2023, SentinelOne released an update about a previous campaign named Operation Tainted Love that previously targeted telecommunication providers in the Middle East. The updated report identified the compromise of a telecommunications entity based in North Africa by the same group [39]. Author assessed it as part of an operation supporting China's soft power efforts.

O. Earth Krahang (Five Incidents; 2024)

In March 2024, researchers at Trend Micro issued a report on an APT campaign nicknamed

[3] MgBot is a modular malware framework known to be used by Daggerfly since at least 2012. It includes a large range of modules that allow to identify local administrator accounts on victim systems, to collect information on Active Directory domain accounts, to steal stored credentials from Outlook and Foxmail email client software, to dump and capture credentials from process memory and so on [44].

Earth Krahang suspected to be from China, they had been monitoring since early 2022 [47]. The campaign focused on Southeast Asia, but was also seen targeting Europe, America, and Africa. The APT group infected public-facing servers and distributed spear-phishing e-mails to spread backdoors. Notably, the hackers used their initial access to government infrastructure to attack other government entities. This was achieved by using the compromised infrastructure to host malicious payloads, proxy attack traffic, and using compromised government e-mail accounts to send spear-phishing e-mails to government-linked targets. Another tactic of the group was to build VPN servers on compromised public-facing servers to gain access to the private network of victims. Subsequently, brute-force attack is used to obtain e-mail credentials which are then used to exfiltrate victim's data within the cyberespionage campaign. The map of victims given by the report shows that five African countries were targeted, including Nigeria, Morocco, Rwanda, Egypt and South Africa.

P. Flax Typhoon (Four Incidents; 2024)

In September 2024, the FBI, Cyber National Mission Force, National Security Agency and allied partners published a joint report on a threat group linked to the PRC and known as Flax Typhoon, RedJuliett and Ethereal Panda [48]. The group compromised thousands of devices, including SOHO routers, firewalls, network-attached storage and IoT gadgets with the goal of creating a botnet. To enrol a new device in the botnet, the system first compromises this latter using a known vulnerability exploit. Then, the victim device executes a Mirai-based malware payload from a remote server. Next, the compromised device establishes a connection with a C2 server using Transport Layer Security. The system information gathered from the device, that includes the operating system version and processor, memory and bandwidth details, is sent to the C2 server for enumeration. By June 2024, the botnet included more than 260,000 devices. Victim devices which are part of the botnet have been observed in many countries among which South Africa. Kenya, Rwanda and Djibouti have also been the target of the group [49].

Q. Earth Estries (Four Incidents; 2021, 2024)

In November 2024, Trend Micro reported that, since 2023, Earth Estries, a Chinese APT group, has compromised various entities belonging to various sectors like telecommunications, technology, consulting, chemical, and transportation industries, along with government agencies and NGOs, in several countries including South Africa [50]. Earth Estries exploits public-facing server N-day vulnerabilities (i.e. known vulnerabilities), to establish initial access. Then, living-off-the-land binaries[4] are used for lateral movement, and backdoors like Snappybee, Masol Rat and Ghostspider, and the Demodex rootkit are deployed to conduct persistent espionage activities. Along with South Africa, Burkina Faso, Egypt and Ethiopia have also been targeted by the APT group [51], [52].

R. TAG-100 (One Incident; 2024)

Recorded Future's Insikt Group [53] uncovered a suspected cyberespionage group targeting high-ranking entities belonging to government, intergovernmental and private sector, worldwide. At least ten countries among which Djibouti have been likely victim of the group of cyber actors tracked as TAG-100. To achieve initial access, they took advantage of Internet-facing appliances like enterprise VPN, firewall, and e-mail appliances. Then, TAG-100 used Pantegana and SparkRAT, two open source Go backdoors, for remote access capabilities. Victim entities in Djibouti and other countries were seen communicating with the C2 infrastructure of the group, since at least February 2024.

S. Phantom Taurus (One Incident; 2025)

Palo Alto Networks reported that a Chinese APT group had been carrying out a campaign called Operation Diplomatic Specter, temporarily [54]. The group was active since at least late 2022 and targeted political entities in the Middle East, Africa and Asia. The malicious actors first infiltrate targets' mail servers and then search them to obtain sensitive and classified information about entities like diplomatic and economic missions,

[4] Allow to use legitimate and native binaries of the victim's system to disguise malicious activity.

TABLE I
CYBER-INCIDENT CLASSIFICATION TAXONOMY INCLUDING INCIDENT TYPE, PERPETRATOR TYPE, MOTIVATION TYPE, AND VICTIM TYPE

Incident Type	Perpetrator Type	Motivation Type	Victim Type
Hacking-on-demand (HOD) Spontaneous hacking (SH)	APT Non-APT	Information theft and espionage Financial gain	Comprehensive strategic partnership Strategic partnership Other

embassies, military operations, political meetings, ministries, and high-profile officials. Continuing their monitoring till late 2025, the researchers renamed the group as Phantom Taurus and observed its tactical evolution, shifting from theft from email servers to a direct targeting of databases [55].

T. RedDelta (One Incident; 2025)

In early 2025, Insikt Group at Recorded Future released a report about a Chinese state-sponsored threat group RedDelta that was active since at least 2012 and regularly adapted its intrusions based on global geopolitical events [56]. The group used LNK and Microsoft Management Console Snap-in control files as its first-stage components and then loaded PlugX backdoor by search order hijacking[5]. From September to December 2024, victims in many countries among which Ethiopia were identified, with malicious traffic observed between RedDelta PlugX C2 servers and IP addresses from these countries. Insikt Group could confirm that ten IP addresses from Henan province in China were used to manage those C2 servers.

U. APT41 (One Incident; 2025)

In a 2025 report, Kaspersky analysts detected a targeted attack against government IT services in a Southern African organization [57], [58]. They determined that the threat actor behind the activity was APT41. The cyberespionage group known to be active in 42 countries, targets entities like telecommunications providers, educational and healthcare institutions, as well as IT and energy sectors. The FBI formally identified five China nationals as members of the group [59]. Initial access was achieved thanks to a breach through an unmonitored host (a SharePoint server), which was used to run Impacket modules (Atexec and WmiExec), taking advantage of a compromised service account. This allowed them to achieve reconnaissance and determine their C2 server availability. Next, they collected privileged credentials using tools like Mimikatz, and performed lateral movement through the network. Cobalt Strike was then deployed using DLL side-loading[6] with malicious DLLs scheduled to prevent from execution on systems using East Asian language packs (Japanese, Korean and Chinese) showing that the group was targeting a specific region in the world. Two trojans agents.exe and agentx.exe were uploaded to victim hosts. These agents' role is to execute commands received from a web shell named CommandHandler.aspx uploaded to the SharePoint server, effectively turning this latter to a C2 server. Then, the group downloaded a malicious HTML application file which delivered a reverse shell, allowing remote command execution. The last step of the attack was the collection of sensitive data using tools like stealers and credential-harvesting utilities, before being exfiltrated via the compromised SharePoint server.

IV. ANALYSIS

In order to analyze the data gathered, we used four classifications: incident type, perpetrator type, motivation type, and victim type. Table I gives a summary of the elements in each classification.

[5] Allows hackers to execute malicious payloads by abusing the search order used by Windows to load DLLs.

[6] Allows a hacker to trick a native or uploaded program into loading a malicious DLL from an unsafe location.

TABLE II
SUMMARY OF CHINESE THREAT ACTOR GROUPS THAT TARGETED AFRICAN COUNTRIES, INCLUDING VICTIM COUNTRIES, ALTERNATIVE GROUP NAMES, ACTOR TYPE (APT/NON-APT), AND PRIMARY MOTIVATION

Threat actor group/campaign	Victim countries/regions and reporting year	Alternative names	Is APT	Motivation
NetTraveler (Kaspersky)	2013: Morocco	APT21, Hammer Panda	Yes	IT&E
Safe (Trend Micro)	2013: Algeria, Egypt, South Sudan	No other name	Yes	IT&E
APT1 (Mandiant)	2013: South Africa	Comment Crew, Comment Panda	Yes	IT&E
Armed groups dispatched by China	2007: South Africa	No other name	N/A	IT&E
Yingmob (Real name)	2016: Egypt, Algeria	HummingBad	No	IT&E and financial crime
Red Apollo (PwC)	2017: South Africa	APT10, Earth Kasha	Yes	IT&E
Bronze President (Secure-Works)	2018: Ethiopia 2022: South Africa, South Sudan	Mustang Panda, Earth Preta	Yes	IT&E
Transsion (Real name)	2020: Ethiopia, Cameroon, Egypt, Ghana, South Africa	xHelper/Triada (malware)	No	Financial crime
Gelsemium (ESET)	2021: Egypt 2022: Djibouti, Equatorial Guinea, Kenya, Nigeria, Swaziland	No other name	Yes	IT&E
BackdoorDiplomacy (ESET)	2020: Egypt 2021: Libya, Nigeria, Ghana, South Africa, Namibia 2023: Kenya, Senegal, Ethiopia	APT15, Bronze Idlewood	Yes	IT&E
Worok (ESET)	2022: Botswana, Namibia, South Africa	No other name	Yes	IT&E
Earth Lusca (Trend Micro)	2022: Nigeria	Bronze University, Chromium	Yes	IT&E and financial crime
Daggerfly (Symantec)	2023: Nigeria	Bronze Highland, Evasive Panda	Yes	IT&E
Operation Tainted Love (SentinelLabs)	2023: North Africa	No other name	Yes	IT&E
Earth Krahang (Trend Micro)	2024: Egypt, Morocco, Nigeria, Rwanda, South Africa	No other name	Yes	IT&E
Integrity Tech (Real name)	2024: Djibouti, Kenya, Rwanda, South Africa	Flax Typhoon, RedJuliett	Yes	IT&E
Earth Estries (Trend Micro)	2021: Burkina Faso, Egypt, Ethiopia 2024: South Africa	GhostEmperor, FamousSparrow	Yes	IT&E
TAG-100 (Recorded Future)	2024: Djibouti	Storm-2077	Yes	IT&E
Phantom Taurus (Palo Alto)	2025: Africa	Operation Diplomatic Specter, TGR-STA-0043	Yes	IT&E
RedDelta (Recorded Future)	2025: Ethiopia	TA416	Yes	IT&E
APT41 (FireEye)	2025: South Africa	Wicked Panda, Barium	Yes	IT&E and financial crime

Note: APT = advanced persistent threat; IT&E = information theft and espionage; N/A = not applicable

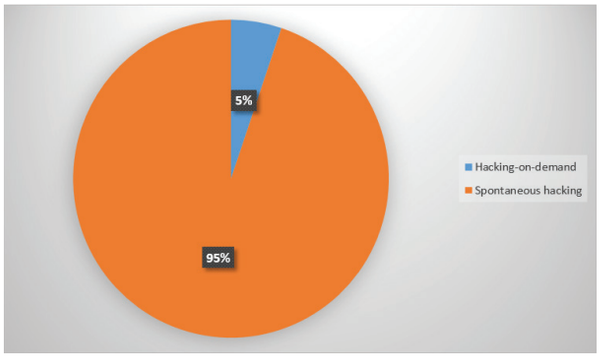

Fig. 1. Distribution of cyber incidents by type: hacking-on-demand (HOD) versus spontaneous hacking (SH) (total=58).

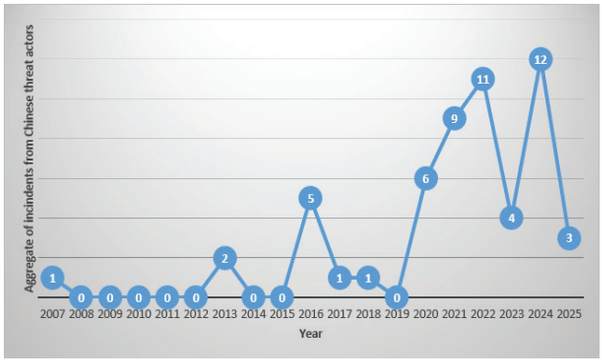

Fig. 2. Annual trend of reported cyber incidents from Chinese threat actors targeting African countries (2007–2025).

Fig. 1 presents the percentage distribution of the incidents by type, showing that those related to hacking-on-demand from African countries (5%) are marginal with respect to those from independent Chinese cyber actors (95%). Hence, even if surveillance tools provided by China along with possible help from Chinese dispatched technicians may be a real concern for African citizenry, the focus should be on independent Chinese threat actors that are analyzed in the rest of the paper.

Table II gives a summary of Chinese threat actor groups that targeted African countries. For every incident, the threat actor group along with the reporting source that dubbed it, the victim countries, and two other names of the group if any, are given based on reports and the summary provided by [60]. When the malware involved in an incident is from a known Chinese company, we give the real name of the company and the malware (application) is given as other name, as it is the case for Transsion. Also, the nature of groups involved (APT or not) and their motivation are given.

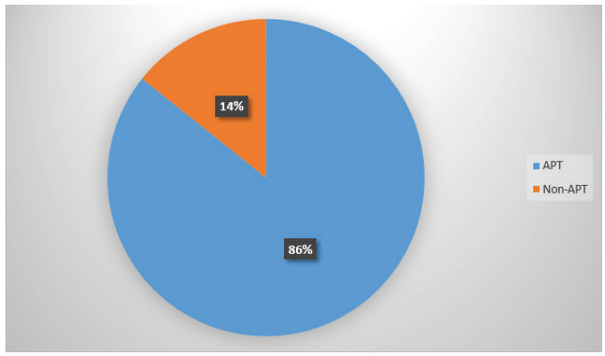

Fig. 3. Distribution of perpetrator types: advanced persistent threat (APT) groups versus non-APT actors.

Because a particular campaign from an APT group may last for months or years, reports on one particular campaign targeting African countries may spread over years.

Table II emphasizes that no one of the cyber-incidents targeting African countries has been reported by a cybersecurity firm from the country targeted. Even for Bronze President that targeted the AU headquarters, investigation from local information technology team began after a tip from Japan's CERT. This shows to which extent African cyberspace is vulnerable.

Fig. 2 shows the annual total cyber-incident trend from Chinese threat actors targeting African countries. Notice that we took the reporting year as a reference, except for the PNRC attack that was uncovered following leak of hundreds of secret intelligence papers, instead of a common report from cybersecurity firms. Fig. 2 demonstrates that incidents are reported at least three times a year from 2020 onwards; and that the average of incidents has drastically increased in the period of 2020 to 2025 (around seven incidents per year) compared to the period of 2013 to 2019 (around one incident per year) where incidents began to be notable. This suggests that Chinese threat actors are focusing more on African countries.

Fig. 3 presents the percentage distribution of the perpetrator types, with a predominance of APT groups (86%) with respect to non-APT (14%). According to US Cybersecurity and Infrastructure Security Agency, "APT actors are well-resourced and engage in sophisticated malicious cyber activity that is targeted and aimed at prolonged network/system intrusion" [61]. Hence, it is challenging to

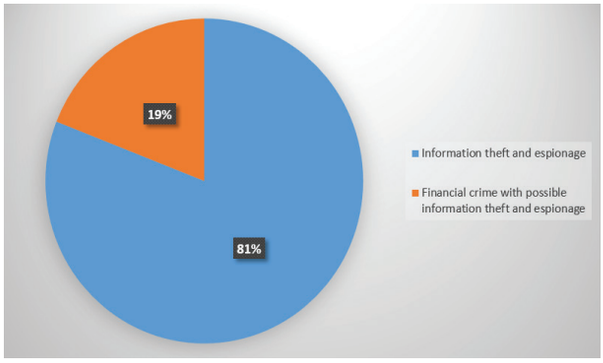

Fig. 4. Distribution of incident motivations: information theft and espionage versus. financial crime.

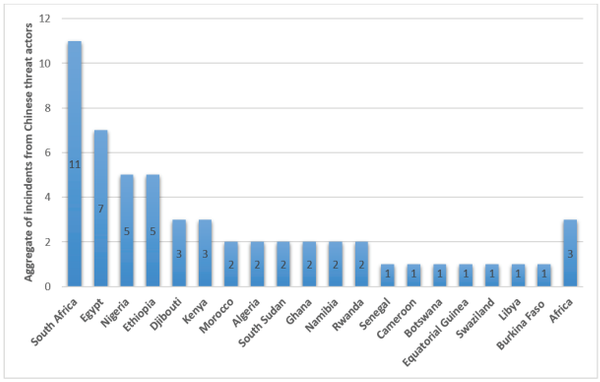

Fig. 5. Cumulative number of reported cyber incidents per targeted African country.

deal with APT groups even for countries with mature CSIRTs, let alone those with less experienced teams as it is the case in Africa, if they exist.

Fig. 4 shows the share of each incident motivation. Information theft and espionage that is likely to be state-sponsored is more prevalent (81%) than financial crime (19%) which can possibly be accompanied by information theft and espionage. This suggests that most of incidents that targeted African countries from Chinese threat actors, during the period of study, are likely to be state sponsored.

Fig. 5 depicts the cumulative number of incidents that targeted each country. For three of the incidents belonging respectively to Phantom Taurus and Operation Tainted Love campaigns, reports did not name a particular country, thus justifying the three incidents attributed to Africa. South Africa (11) is the most targeted country being victim of more than half of the campaigns reported in this study, followed by Egypt (7), Nigeria (5) and Ethiopia (5). Then, come Djibouti (3) and Kenya (3), followed by six countries

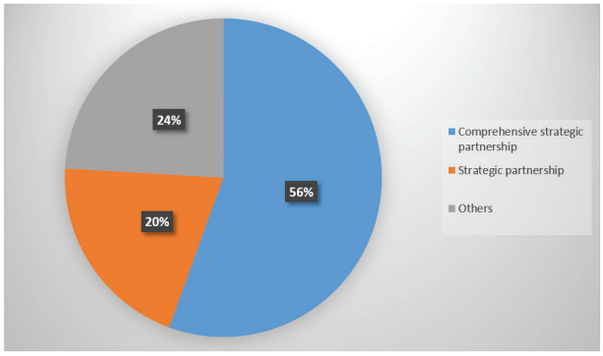

Fig. 6. Distribution of incidents by China–Africa partnership level: comprehensive strategic partnership, strategic partnership, and other countries.

which recorded 2 incidents, which are Algeria, South Sudan, Ghana, Morocco, Namibia and Rwanda. Finally, seven countries Senegal, Botswana, Burkina Faso, Swaziland, Libya, Cameroon and Equatorial Guinea experienced only one incident.

To justify, at least partially, why these countries are targeted among 54 and why some of them experienced by far more incidents than others, we assess that this is due to China's interest in these countries. Recall that Beijing classifies countries by their category of partnership [62]. For Africa, the first category is comprehensive strategic partnership that involves the AU as well as nine other countries which are South Africa, Egypt, Ethiopia, Kenya, Algeria, Namibia, Mozambique, Zimbabwe and Sierra Leone. China funded the AU building and is an important trading partner for all nine countries.

Beijing has a second level that is strategic partnership that involves Nigeria, Djibouti, Morocco, Senegal, Angola, Sudan, Gabon, Republic of Congo, Guinea and Tanzania. Except Senegal, Tanzania and Djibouti, these countries have significant quantities of natural resources of interest to China. Senegal is an important country in West Africa due to its recognized political stability. Moreover, the country recently began gas and oil production. Tanzania has a long historical and military relationship with Beijing. Djibouti holds China's only military base in Africa.

Fig. 6 shows the share of incidents targeting each group of countries with respect to its level of partnership with China. As expected, the six countries belonging to the first level of partnership are largely targeted (56%), hence emphasizing the

focus of Chinese threat actors on this group. Then follow 4 countries from the second level with 20%; the rest (24%) being the share of the 44 remaining countries. Therefore, ten countries from the two first levels are victim of 76% of all the incidents reported in this study, most of which are motivated by information theft and espionage typical of state-sponsored groups. China objectives in such intrusions are likely due to interest in business awareness on negotiations, aimed at granting competitive advantage, geopolitical affairs or national policies related to debts, for example. This is particularly notable for campaigns like Phantom Taurus, Operation Tainted Love and BackdoorDiplomacy. It is noteworthy that, among all the incidents reported here, only the PNRC attack was evidently related to intellectual property theft targeting an African country.

V. Conclusion

The key findings from this study are that incidents related to hacking requested by African countries are insignificant compared to those from Chinese threat actor groups that are increasingly focusing on Africa; that most frequent perpetrators are APT groups ; that most incidents are motivated by information theft and espionage ; that countries belonging to the first and second levels of partnership with China are more likely to be victim than others; and that South Africa is the most targeted country.

The frequency of incidents from Chinese threat actor groups is expected to increase due to steady interest of Beijing in Africa, along with an increasing Internet penetration in the continent which expands its attack surface.

African authorities should know that the reporting an analysis of cyber incidents via their CSIRT, will improve their understanding of local and global cyber-threat landscapes, resulting in a better monitoring of their cyberspace.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The author declares no conflict of interest.

References

[1] Statista. “Number of internet users in Africa as of February 2025, by country.” Statista.com. https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/ (accessed Jan. 27, 2026).

[2] R. K. Reddy. “China’s going global policy: a prelude to the BRI.” Orcasia.org. https://orcasia.org/chinas-going-global-policy-a-prelude-to-the-bri (accessed Jan. 27, 2026).

[3] P. Nantulya. “FOCAC 2024: elevating African interests beyond the Africa-China summit.” Africacenter.org. https://africacenter.org/spotlight/focac-2024-elevating-african-interests-africa-china-summit/ (accessed Jan. 27, 2026).

[4] J. Meservey. “Government buildings in Africa are a likely vector for Chinese spying.” Heritage.org. https://www.heritage.org/sites/default/files/2020-06/BG3476.pdf (accessed Jan. 27, 2026).

[5] Digwatch. “MTN and Huawei to launch Africa’s first 5.5G trial.” Dig.watch. https://dig.watch/updates/mtn-and-huawei-to-launch-africas-first-5-5g-trial (accessed Jan. 27, 2026).

[6] J. Barton. “Orange partners with Huawei to deploy 5G in Egypt.” Developingtelecoms.com. https://developingtelecoms.com/telecom-technology/wireless-networks/18635-orange-partners-with-huawei-to-deploy-5g-in-egypt.html (accessed Jan. 27, 2026).

[7] J. Aglionby, E. Feng and Y. Yang. “African Union accuses China of hacking headquarters.” FT.com. https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5 (accessed Jan. 27, 2026).

[8] China Law Translate. “PRC National Intelligence Law (as amended in 2018).” Chinalawtranslate.com. https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/ (accessed Jan. 27, 2026).

[9] Statista. “Share of internet users in Africa as of February 2025, by country.” Statista.com. https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/ (accessed Jan. 27, 2026).

[10] N. Kshetri. *Cybercrime and cybersecurity in the Global South*. Palgrave Macmillan, 2013.

[11] C. Sall, “Analysis of cyber incidents in Senegal from 2005 to 2023.” Afr J. Inf Commun, no 34, pp. 1–19, Dec. 2024, https://doi.org/10.23962/ajic.i34.17851.

[12] African Union. "African Union Convention on Cyber Security and Personal Data Protection." AU.int. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed Jan. 28, 2026).

[13] International Telecommunication Union. "Global Cybersecurity Index 2024." ITU.int. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf (accessed Jan. 28, 2026).

[14] Kaspersky. "ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms." Securelist.com. https://securelist.com/faq-the-projectsauron-apt/75533/ (accessed Apr. 09, 2026).

[15] Kaspersky. "Equation Group: questions and answers." Media.kasperskycontenthub.com. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf (accessed Apr. 09, 2026).

[16] Kaspersky. "Unveiling Careto, the Masked APT." Media.kasperskycontenthub.com. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20133638/unveilingthemask_v1.0.pdf (accessed Apr. 09, 2026).

[17] A. Burgher. "Fantasy: a new Agrius wiper deployed through a supply-chain attack." Welivesecurity.com. https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/ (accessed Apr. 09, 2026).

[18] U.S.-China Economic and Security Review Commission. "Section 3: China's strategic aims in Africa." USCC.gov https://www.uscc.gov/sites/default/files/2020-12/Chapter_1_Section_3--Chinas_Strategic_Aims_in_Africa.pdf (accessed Jan. 28, 2026).

[19] J. Parkinson, N. Bariyo and J. Chin. "Huawei technicians helped African governments spy on political opponents." WSJ.com. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017 (accessed Jan. 28, 2026).

[20] B. Jili. "The Spread of surveillance technology in Africa stirs security concerns." Africacenter.org. https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/ (accessed Jan. 28, 2026).

[21] D. Cave, F. Ryan and V. X. Xu. "Mapping more of China's tech giants: AI and surveillance." ASPI.org https://www.aspi.org.au/report/mapping-more-chinas-tech-giants/ (accessed Jan. 28, 2026).

[22] L. Travers, "Algorithmic coloniality? The case of Chinese artificial intelligence technology and Zimbabwean surveillance." Transcience J., vol. 15, no 2, pp. 48-82, 2024, https://www2.hu-berlin.de/transcience/Vol15_No2_S48_S82.pdf.

[23] Kaspersky. "Kaspersky Lab uncovers operation NetTraveler, a global cyberespionage campaign targeting government-affiliated organizations and research institutes." Kaspersky.com. https://www.kaspersky.com/about/press-releases/kaspersky-lab-uncovers-operation-nettraveler-a-global-cyberespionage-campaign-targeting-government-affiliated-organizations-and-research-institutes (accessed Jan. 28, 2026).

[24] Common Vulnerabilities and Exposures. "CVE-2012-0158." CVE.org. https://www.cve.org/CVERecord?id=CVE-2012-0158 (accessed Jan. 28, 2026).

[25] Common Vulnerabilities and Exposures. "CVE-2010-3333." CVE.org. https://www.cve.org/CVERecord?id=CVE-2010-3333 (accessed Apr. 09, 2026).

[26] N. Villeneuve and K. Wilhoit. "Safe a targeted threat." Cybercampaigns.net. http://cybercampaigns.net/wp-content/uploads/2013/05/Safe-A-Targeted-Threat.pdf (accessed Jan. 28, 2026).

[27] Mandiant. "APT1: exposing one of China's cyber espionage units." Services.google.com. https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf (accessed Jan. 29, 2026).

[28] J. Jordan and Al Jazeera Investigative Unit. "Spy cables: China behind South Africa nuclear break-ins." Aljazeera.com. https://www.aljazeera.com/news/2015/2/25/spy-cables-china-behind-s-africa-nuclear-break-ins (accessed Jan. 29, 2026).

[29] Check Point. "From HummingBad to worse: new details and an in-depth analysis of the Hummingbad android malware campaign." Blog.checkpoint.com. https://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf (accessed Jan. 29, 2026).

[30] PwC and BAE Systems. "Operation Cloud Hopper: exposing a systematic hacking operation with an unprecedented web of global victims." PwC.com. https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf (accessed Jan. 29, 2026).

[31] Federal Bureau of Investigation (FBI). "APT10 group: conspiracy to commit computer intrusions; conspiracy to commit wire fraud; and aggravated identity theft." FBI.gov. https://www.fbi.gov/wanted/cyber/apt-10-group (accessed Jan. 29, 2026).

[32] G. Kadiri and J. Tilouine. "At Addis Ababa, the headquarters of the African Union spied on by Beijing (in French)." Lemonde.fr. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html (accessed Jan. 29, 2026).

[33] R. Satter. "Exclusive: suspected Chinese hackers stole camera footage from African Union–memo." Reuters.com. https://www.reuters.com/world/china/exclusive-suspected-chinese-hackers-stole-camera-footage-african-union-memo-2020-12-16/ (accessed Jan. 29, 2026).

[34] A. C. Cyr. "Mustang Panda's hodur: old tricks, new Korplug variant." https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/ (accessed Jan. 29, 2026).

[35] Upstream. "xHelper/Triada malware pre-installed on thousands of low cost Chinese Android devices in emerging markets." Upstreamsystems.com https://www.upstreamsystems.com/press/press-releases/xhelper-triada-malware-pre-installed-on-thousands-of-low-cost-chinese-android-devices-in-emerging-markets/ (accessed Jan. 29, 2026).

[36] M. Faou and T. Dupuy. "Gelsemium: when threat actors go gardening." Welivesecurity.com. https://www.welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/ (accessed Jan. 29, 2026).

[37] Kaspersky. "Kaspersky discovers poorly detected backdoor, targeting governments and NGOs around the globe." Kaspersky.com. https://www.kaspersky.com/about/press-releases/kaspersky-discovers-poorly-detected-backdoor-targeting-governments-and-ngos-around-the-globe (accessed Jan. 29, 2026).

[38] A. Burgher. "BackdoorDiplomacy: upgrading from Quarian to Turian." Welivesecurity.com. https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/ (accessed Jan. 29, 2026).

[39] T. Hegel. "Cyber soft power: China's continental takeover." https://www.sentinelone.com/labs/cyber-soft-power-chinas-continental-takeover/ (accessed Jan. 29, 2026).

[40] Lookout. "Mobile APT surveillance campaigns targeting Uyghurs: a collection of long-running android tooling connected to a Chinese mAPT actor." Lookout.com. https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf (accessed Jan. 29, 2026).

[41] A. Ross, J. Pearson and C. Bing. "Exclusive: Chinese hackers attacked Kenyan government as debt strains grew." Reuters.com. https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/ (accessed Jan. 29, 2026).

[42] T. Passilly. "Worok: the big picture." Welivesecurity.com. https://www.welivesecurity.com/2022/09/06/worok-big-picture/ (accessed Jan. 29, 2026).

[43] J. C. Chen, K. Lu, G. Chen, J. Horejsi, D. Lunghi and C. Pernet. "Delving deep: an analysis of Earth Lusca's operations." Trendmicro.com. https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf (accessed Jan. 29, 2026).

[44] Mitre Att&ck. "MgBot." Attack.mitre. https://attack.mitre.org/software/S1146/ (accessed Jan. 29, 2026).

[45] Threat Hunter Team. "Daggerfly: APT actor targets telecoms company in Africa." Security.com. https://www.security.com/threat-intelligence/apt-attacks-telecoms-africa-mgbot (accessed Jan. 29, 2026).

[46] F. Muñoz. "Evasive Panda APT group delivers malware via updates for popular Chinese software." Welivesecurity.com. https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/ (accessed Jan. 29, 2026).

[47] J. C. Chen and D. Lunghi. "Trend Micro. Earth Krahang exploits intergovernmental trust to launch cross-government attacks." Trendmicro. https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html (accessed Jan. 29, 2026).

[48] FBI, CNMF, NSA et al. "People's Republic of China-linked actors compromise routers and IoT devices for botnet operations." IC3.gov. https://www.ic3.gov/CSA/2024/240918.pdf (accessed Jan. 29, 2026).

[49] Recorded Future. "Chinese state-sponsored RedJuliett intensifies Taiwanese cyber espionage via network perimeter exploitation." Assets.recordedfuture.com. https://assets.recordedfuture.com/insikt-report-pdfs/2024/cta-cn-2024-0624.pdf (accessed Jan. 29, 2026).

[50] L. M. Chang, T. Chen, L. Bermejo and T. Lee. "Game of emperor: unveiling long term Earth Estries cyber intrusions." Trendmicro.com. https://www.trendmicro.com/en_us/research/24/k/earth-estries.html (accessed Jan. 29, 2026).

[51] M. Faou and T. Bin Taj. "FamousSparrow: a suspicious hotel guest." Welivesecurity.com. https://www.welivesecurity.com/2021/09/23/famoussparrow-suspicious-hotel-guest/ (accessed Jan. 29, 2026).

[52] M. Lechtik, A. Kayal, P. Rascagneres and V. Berdnikov. "GhostEmperor: from ProxyLogon to kernel mode." Securelist.com. https://securelist.com/ghostemperor-from-proxylogon-to-kernel-mode/104407 (accessed Jan. 29, 2026).

[53] Recorded Future. "TAG-100 uses open-source tools in suspected global espionage campaign, compromising two Asia-Pacific intergovernmental bodies." Go.recordedfuture.com. https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf (accessed Jan. 29, 2026).

[54] L. Rochberger and D. Frank. "Operation Diplomatic Specter: an active Chinese cyberespionage campaign leverages rare tool set to target governmental entities in the Middle East, Africa and Asia." https://unit42.paloaltonetworks.com/operation-diplomatic-specter/ (accessed Feb. 07, 2026).

[55] L. Rochberger. "Phantom Taurus: a new Chinese Nexus APT and the discovery of the NET-STAR malware suite." Unit42.paloaltonetworks.com. https://unit42.paloaltonetworks.com/phantom-taurus/#post-158604-_7mib773okdxz (accessed Jan. 24 2026).

[56] Recorded Future. "Chinese state-sponsored RedDelta targeted Taiwan, Mongolia, and Southeast Asia with adapted PlugX infection chain." Go.recordedfuture.com. https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0109.pdf (accessed Jan. 29 2026).

[57] Kaspersky. "APT41 targets Southern African organization in espionage attack." Kaspersky.com. https://www.kaspersky.com/about/press-releases/kaspersky-apt41-targets-southern-african-organization-in-espionage-attack (accessed Jan. 29 2026).

[58] D. Kulik and D. Pogorelov. "The SOC files: rumble in the jungle or APT41's new target in Africa incidents." Securelist.com https://securelist.com/apt41-in-africa/116986/ (accessed Jan. 29 2026).

[59] FBI. "Most wanted: APT41 group." https://www.fbi.gov/wanted/cyber/apt-41-group (accessed Jan. 29 2026).

[60] Electronic Transactions Development Agency, Jan. 2026, "Threat group cards: a threat actor encyclopedia," Electronic Transactions Development Agency. [Online]. Available: https://apt.etda.or.th/cgi-bin/aptsearch.cgi (accessed Apr. 09 2026).

[61] Cybersecurity and Infrastructure Security Agency. "Nation-state threats." CISA.gov. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (accessed Jan. 29 2026).

[62] U.S.-China Economic and Security Review Commission. "Hearing on China's strategic aims in Africa." USCC.gov. https://www.uscc.gov/sites/default/files/2020-06/May_8_2020_Hearing_Transcript.pdf (accessed Jan. 29 2026).