Mercenary APTs – An Exploration

cyjax.com/2021/10/26/mercenary-apts-an-exploration/

October 26, 2021

Blog

By William Thomas 26th October 2021

Mercenary advanced persistent threat (APT) groups, sometimes called “hackers-for-hire” – and dubbed private-sector offensive actors (PSOAs) by Microsoft – have become a significant part of the threat landscape in recent years. These cyber-soldiers of fortune have been executing increasing numbers of attack campaigns for their clients, usually nation-states, that are looking for surveillance capabilities. Not all countries have the technical capability to launch their own attacks: many, however, have the financial resources to pay someone who does.

Over the last decade, more than a dozen mercenary APT campaigns have been disclosed. Many of these have been both highly sophisticated and highly persistent. Victims often include politicians, human rights activists, journalists, academics, embassy workers, and dissidents from around the world. They frequently target end-to-end encrypted (E2EE) applications, such as Signal, WhatsApp, and Telegram, that are used to thwart traditional government surveillance tactics. A growing number of these mercenary APT campaigns are now also actively infiltrating and stealing intellectual property and other sensitive information from enterprises.

These campaigns are supported by a significant market for 0day exploits and malware developers. As such, nation-states that want to begin hacking campaigns no longer need the technical expertise of years gone by: they just need to be well-resourced. Furthermore, even though these APTs have existed for decades, the capabilities previously associated uniquely with them are more accessible than ever before. And, in the case of nation-state APTs, it has become easier to predict which companies and sectors are most likely to be attacked, meaning defence has also been made, marginally, easier.

If the threat landscape is evolving in the way these mercenary groups suggest, however, where anyone can hire mercenaries for a broad spectrum of intrusion campaigns, even this minor advantage may have been lost.

Hackers For Hire – A Line-Up

In the following section, we will outline the pre-eminent mercenary APT groups that have engaged in malicious activity over the past few years: CostaRicto, Bahamut, DarkBasin, and DeathStalker. First, we explore the intriguing case of the DarkMatter espionage unit.

In September 2021, the US Department of Justice revealed that three former US intelligence agency employees had been fined $1.69 million and barred from ever again receiving security clearance. The employees violated US computer abuse laws by spying for the government of the UAE. The three men admitted to selling sensitive military technology while working for Project Raven: the codename for a secretive company, DarkMatter, that acted as a clandestine spying unit for the UAE.

Project Raven leveraged computer network exploitation (CNE) to compromise the accounts of human rights activists, journalists, and rival governments. Whilst engaged in Project Raven, the three men reportedly targeted the US and exported spying software to a foreign government without gaining the required permission from the US State Department’s Directorate of Defense Trade Controls (DDTC). As noted in a Reuters investigation, the three men are former US National Security Agency (NSA) employees and worked for DarkMatter in the UAE between January 2016 and November 2019. While working for DarkMatter, the ex-NSA employees helped develop and deploy two iOS zero-click exploits called Karma and Karma 2. These were reportedly used against iPhones belonging to dissidents, reporters, and government opposition leaders. The US Department of Justice also noted that this

agreement was the first resolution of its kind for two types of criminal activity: providing unlicensed export-controlled services in support of hacking campaigns; and a commercial company supporting a foreign government to access networks and devices of computers worldwide, including in Qatar, Yemen, and the US. [1, 2]

In November 2020, BlackBerry researchers disclosed a new mercenary APT, dubbed CostaRicto. This group was targeting organisations around the world but predominantly in South Asia – India, Bangladesh, and Singapore – Africa, Europe, and the Americas. The victims were spread across several verticals, with many in the financial sector. It is unclear where these hackers-for-hire are located. However, as they mainly focused on South Asian targets, the researchers believe they are most likely to be based there. For many of its campaigns, CostaRicto uses spear-phishing attacks to drop a custom backdoor, dubbed SombRAT, that has rarely been seen in the wild. The code suggests there are multiple versions, indicating the backdoor can be flexibly adapted for different attacks. The earliest compilation timestamps for SombRAT date back to 2017. The group has also compromised its targets via stolen credentials, reportedly purchased on the darknet. [1, 2]

Active since 2016, a mercenary APT known as Bahamut (connected to WindShift) has launched multiple highly targeted ongoing campaigns against Android users in the Middle East. Individuals targeted by the group have usually been human rights activists, military officers, members of royal families, diplomats, religious leaders, and business executives. Bahamut's targets have also been located in other parts of the globe, such as the US. The group usually uses malicious mobile applications distributed via legitimate application stores, masquerading as fitness trackers or password managers. Once downloaded by a victim, an array of personal information is extracted which can then be used for a wide spectrum of malicious activities, with potentially serious implications. [1, 2, 3]

In June 2020, researchers from Citizen Lab disclosed that thousands of individuals and hundreds of institutions had been targeted by a mercenary group known as DarkBasin. Targets included advocacy groups, journalists, and senior government officials, as well as hedge funds and other organisations from various sectors. The group mainly targeted American non-profits, especially those working on a campaign operating under the hashtag #ExxonKnew, which claims ExxonMobil hid information concerning climate change for decades. DarkBasin was also linked to phishing campaigns targeting net-neutrality advocates. Further investigation into the group uncovered several ties to an Indian cybersecurity company, called BellTroX InfoTech Services, which subsequently disappeared once the investigation was made public. Analysis of DarkBasin's phishing infrastructure, which used a custom URL shortener, revealed 28,000 additional URLs containing emails of targets. [1, 2]

In August 2020, Kaspersky researchers disclosed an unusual Russian-speaking mercenary APT group called DeathStalker (originally named Deceptikons). Unlike the other groups mentioned above, DeathStalker primarily focuses on law firms and financial institutions. These threat actors are reportedly tasked with gathering sensitive business information in

what are believed to be corporate espionage campaigns. DeathStalker uses custom malware distributed in highly targeted spear-phishing emails. For C&C communication, the malware uses “dead drop” resolvers: using safe websites, such as GitHub, Facebook, YouTube, Reddit, and Twitter, to host the locations of C&C servers. This means the communication is camouflaged amongst legitimate traffic, in much the same way as spies use a dead drop to pass messages undercover. DeathStalker’s victims are spread around the world in countries such as the UK, Switzerland, the UAE, India, China, Taiwan, Israel, Lebanon, Jordan, Cyprus, Argentina, and Turkey. [1, 2]

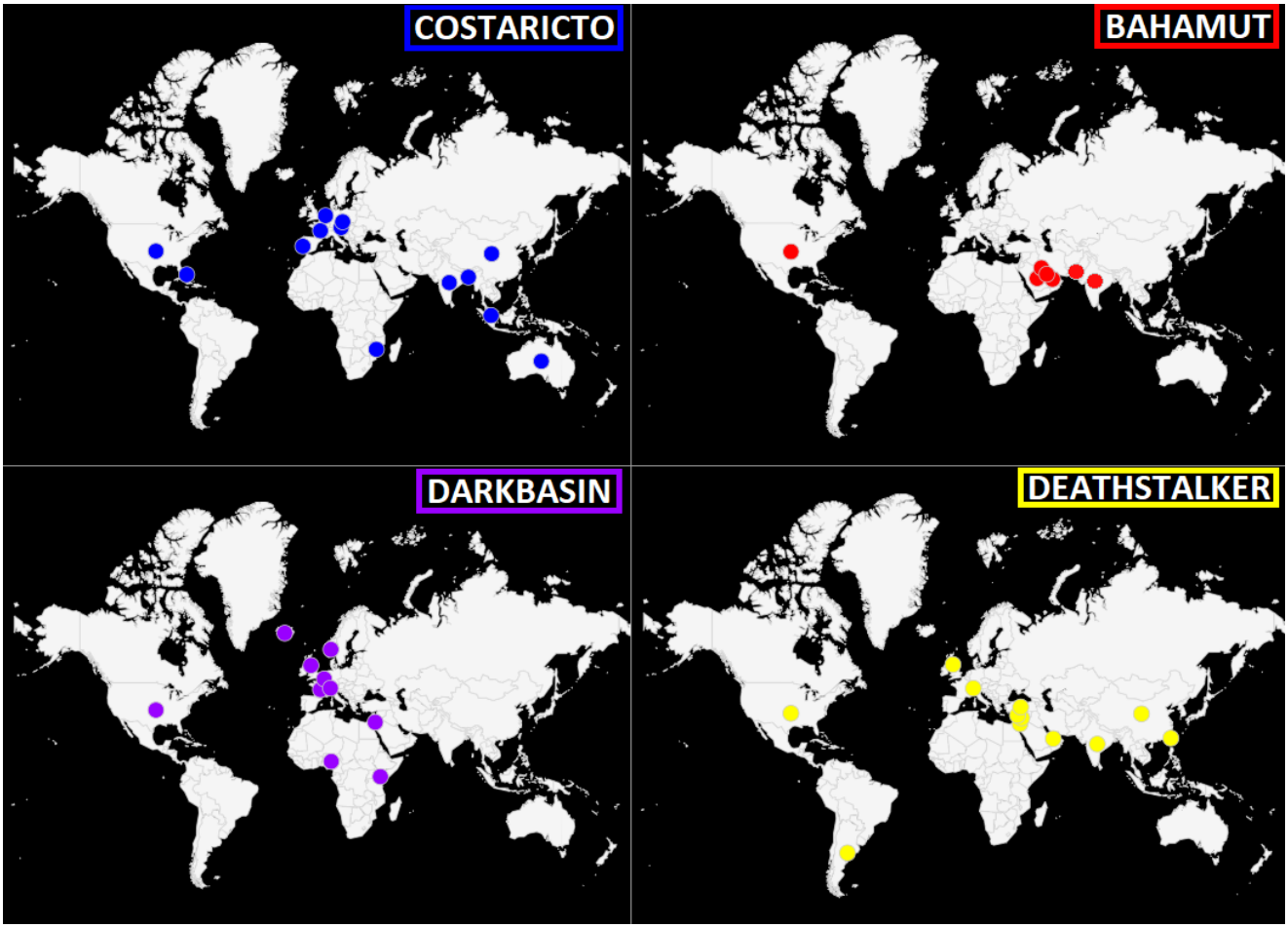

Fig. 1 – Geographic targeting of known Mercenary APTs

Hacking-as-a-Service

While Mercenary APTs carry out their criminal activity with no action needed on their clients’ behalf, there are also a growing number of licensed companies selling offensive software that can be bought and deployed by anyone with malicious intent. Intelligence agencies, law enforcement, and military units around the world are increasingly acquiring these off-the-shelf hacking software, buying exploits for 0day vulnerabilities, and paying others to develop spying tools.

The standard defence of ethically dubious products is that their software is used to fight terrorism and organised crime. More often than not, however, their products end up being used to target human rights defenders, journalists, lawyers, activists, and dissidents. FinFisher, also known as FinSpy, is a surveillance software created and distributed by Gamma International. The company was breached in 2014 by an individual working under the moniker Phineas Fisher, who stole and leaked an archive containing 40GB of data from Gamma International servers. This information included price lists, source code, invoices, and other private data able to link the purchase of spyware to specific clients.

Another company that was hacked by Phineas Fisher was Hacking Team, which suffered a much more serious attack than Gamma International and went out of business. The attack on HackingTeam left a gap in the market, from mid-2015 onwards, for surveillance tools. This was filled by Gamma International with its FinFisher spyware suite. Although Gamma International was breached by the same individual, the incident was not as serious and the spyware firm was able to recover, operating in the vacuum left by HackingTeam. The Phineas Fisher leaks unveiled what many suspected about these commercial spyware developers: they were knowingly selling surveillance tools to authoritarian regimes who used them to spy on civilians. [1, 2, 3]

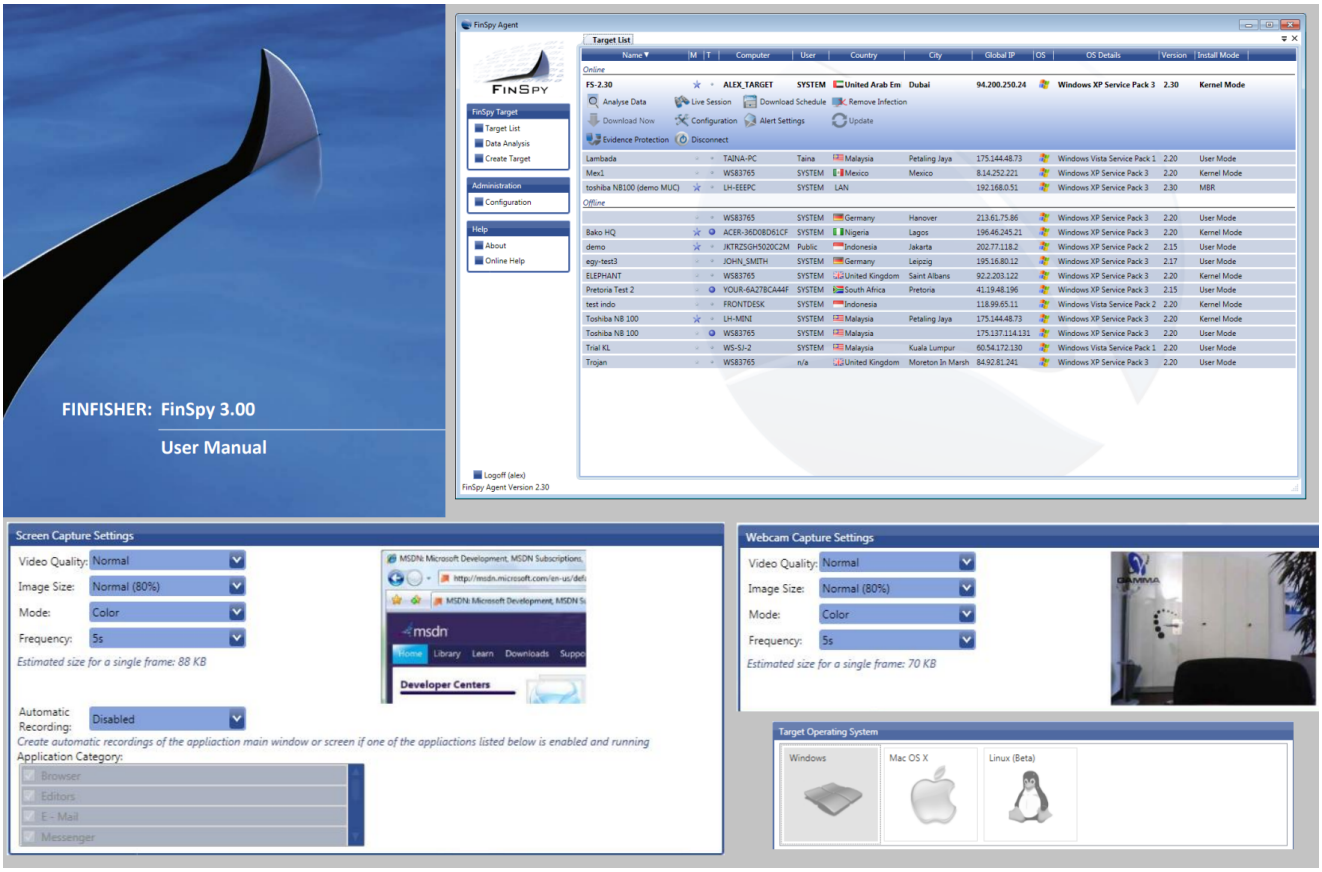

Fig. 2 – Graphical User Interface of FinSpy (circa 2011)

In July, Microsoft released new information regarding a private-sector offensive actor (PSOA) it tracks as Sourgum, which reportedly belongs to an Israel-based company called Candiru. The organisation has targeted over 100 victims around the world, including politicians, human rights activists, journalists, academics, embassy workers, and political dissidents with a malware family called DevilsTongue. Approximately half of the victims were found in the Palestinian Authority, with others in Israel, Iran, Lebanon, Yemen, Spain (specifically Catalonia), the UK, Turkey, Armenia, and Singapore. It should be noted that the identification of victims of the malware in a country is not indicative that an agency in that country is a Candiru customer, as international targeting is common. Nonetheless, this is not proof that the country in question is not a Candiru customer, either.

Candiru uses a chain of vulnerabilities in web browsers and Windows to install its DevilsTongue modular multi-threaded backdoor. This custom malware is written and can steal credentials from web browsers, such as Chrome or Firefox. It also decrypts and exfiltrates conversations from Signal, the E2EE messaging app. The attacks begin with a single-use URL that is sent via messaging applications, such as WhatsApp. These threat actors have also weaponised Windows 0day vulnerabilities, tracked as CVE-2021-31979 and CVE-2021-33771, to support delivery. Successful exploitation led to privilege escalation, giving an attacker the ability to escape browser sandboxes and gain kernel code execution. Spy agencies in Uzbekistan, the UAE, and Saudi Arabia are among the list of Candiru's alleged previous customers. [1, 2]

In August, CitizenLab revealed that the infamous NSO Group, an Israeli spyware developer, had once again been implicated in an unethical surveillance campaign. The latest Pegasus spyware campaign targeted at least nine Bahraini activists, a French Lawyer, and an Indian journalist via a new iOS exploit, dubbed FORCEDENTRY. This was a highly sophisticated zero-click, 0day vulnerability in iMessage, meaning it could be triggered without the intended victim either viewing the message sent by the threat actors or clicking the link contained in the message.

The NSO Group, however, allegedly does not carry out hacking itself: the most recent campaign having been orchestrated by a Pegasus customer and operator, dubbed LULU, linked to the government of Bahrain. The technically impressive part of the FORCEDENTRY exploit is that it could bypass BlastDoor, which Apple recently developed to protect from such attacks. It places parts of iMessage inside a sandbox to isolate malicious code from interacting with the underlying operating system (OS). Interestingly, four of the victims' phone numbers were present in the list of 50,000 potential Pegasus targets obtained by Forbidden Stories and Amnesty International in July. The leaked phone numbers belong to hundreds of business executives, religious figures, academics, NGO employees, union officials, and government officials. Also shown in the leak are NSO Group clients from at least 11 countries, including Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the UAE. [1, 2]

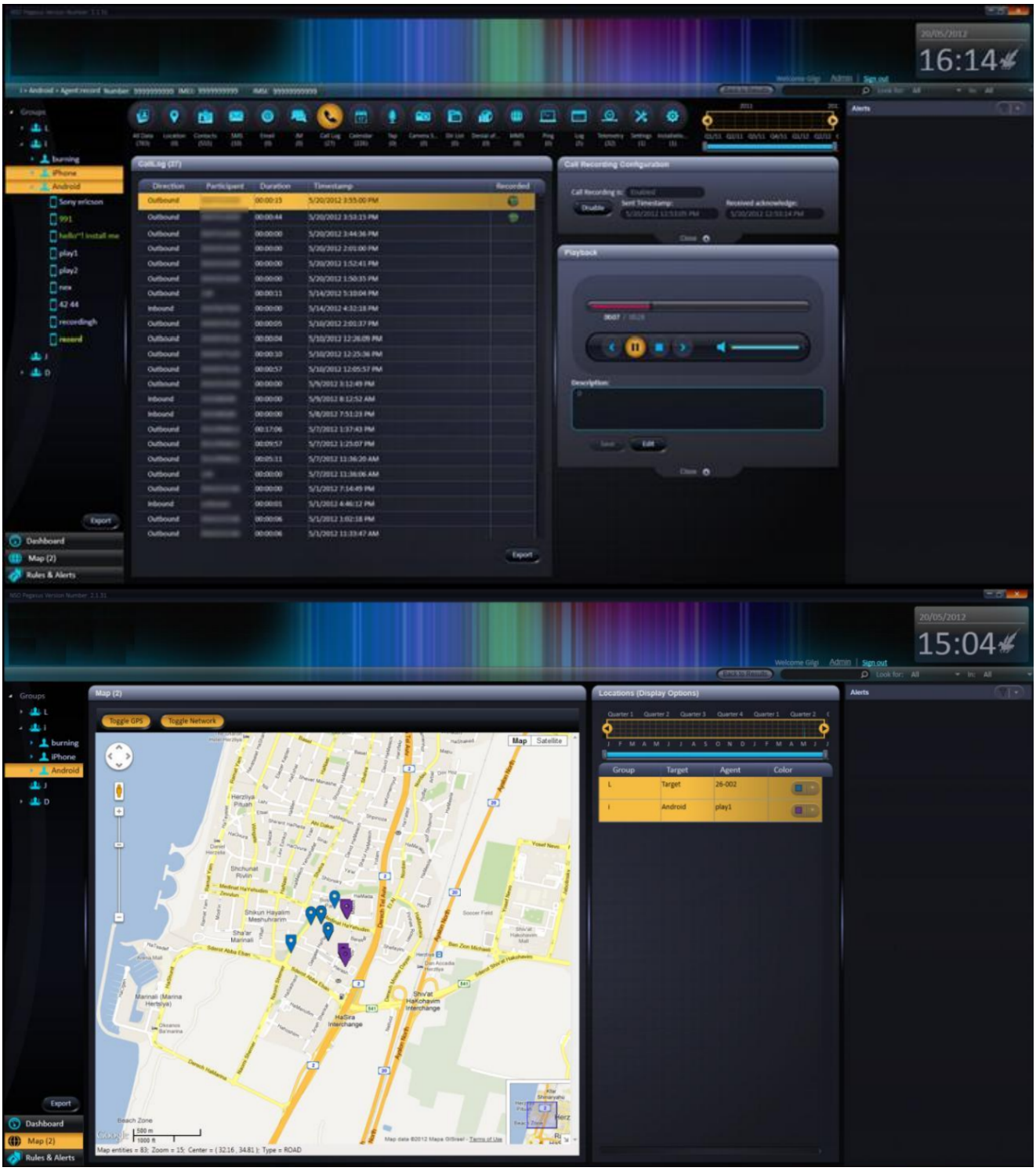

Fig. 3 – Graphical User Interface of Pegasus spyware (circa 2012)

A Mercenary Future

Mercenary APTs, malicious software developers, and 0day brokers significantly lower the barrier to entry for launching advanced hacking campaigns. Technical expertise and a small army of highly skilled individuals are no longer required to perform such attacks. Now, all that is needed, are resources: of which many nation-states have a lot. The previously technically

impossible is made available through 0day exploits worth millions of dollars on underground markets. Mercenary APTs develop bespoke malware tooling, manage their own infrastructure, perform their own reconnaissance, and execute all phases of the intrusion. This is the effective outsourcing of many of the most nefarious parts of the playbook for despotic regimes.

A mercenary APT's tactics, techniques, and procedures (TTPs) often resemble highly sophisticated state-sponsored campaigns, but the profiles and geography of their victims are far too diverse to be aligned with one state's interests. Therefore, these cybercriminals must carefully choose their targets to avoid the risk of being exposed and having their operations shut down: consequently, many go undetected for several years. Even notorious adversaries, experienced in cyber-espionage, can benefit from adding a layer of obfuscation to their campaigns. By using a mercenary group as a proxy, therefore, the real attacker can better protect their identity and frustrate attempts at attribution by the cybersecurity community.

Defending against these powerful and disaggregated threats, however, can lead to a sort of "security nihilism", wherein it seems that nothing can be done to prevent these sophisticated attacks. We content that this conclusion, however, is incorrect. The majority of these attacks rely on victims making simple mistakes, such as clicking on a link, opening a document, or leaving devices unpatched. As such, by practising proper security awareness, using password managers and multi-factor authentication, keeping devices and applications updated, and investing in security software, attackers' campaigns will be frustrated to the point that they will eventually move on to softer targets.