Why is it so rare to hear about Western cyber-attacks?

By Joe Tidy ⋮⋮ 6/23/2023

A cyber-attack that took over iPhones at a Russian technology company is being blamed on US government hackers. Could the attack, and the response from the Russian government, be rewriting the narrative of who the good guys and bad guys are in cyber-space?

Camaro Dragon, Fancy Bear, Static Kitten and Stardust Chollima - these aren't the latest Marvel film superheroes but the names given to some of the most feared hacking groups in the world.

For years, these elite cyber teams have been tracked from hack to hack, stealing secrets and causing disruption allegedly under orders from their governments.

And cyber-security companies have even created cartoon images of them.

Image so

Image caption,

Camaro Dragon - Checkpoint's latest illustration for an alleged Chinese group hacking European foreign affairs workers

With dots on a world map, marketeers at these companies regularly warn customers about where these "advanced persistent threats" (APTs) are coming from - usually Russia, China, North Korea and Iran.

But parts of the map remain conspicuously empty.

So why is it so rare to hear about Western hacking teams and cyber-attacks?

A major hack in Russia, unearthed earlier this month, might provide some clues.

Defenders under attack

From his desk overlooking the Moscow Canal, the cyber-security worker watched as strange pings began to register on the company wi-fi network.

Dozens of staff mobile phones were simultaneously sending information to strange parts of the internet.

But this was no ordinary company.


Image so

Image caption,

Kaspersky HQ, in Moscow

This was Russia's biggest cyber company Kaspersky, investigating a potential attack on its own employees.

"Obviously our minds turned straight to spyware but we were pretty sceptical at first," chief security researcher Igor Kuznetsov says.

"Everyone's heard about powerful cyber tools which can turn mobile phones into spying devices but I thought of this as a kind of urban legend that happens to someone else, somewhere else."

After painstaking analysis of "several dozen" infected iPhones, Igor realised their hunch had been right - they had indeed unearthed a large sophisticated surveillance-hacking campaign against their own staff.

The type of attack they had found is the stuff of nightmares for cyber defenders.

The hackers had invented a way to infect iPhones simply by sending an iMessage that automatically deletes itself once the malicious software is injected into the device.

"Wham, you're infected - and you don't even see it," Igor says.

'Reconnaissance operation'

The victims' entire phone contents were now being pinged back to the attackers at regular intervals. Messages, emails and pictures were shared - even access to cameras and microphones.

Keeping to Kaspersky's long-standing rule of not pointing fingers, Igor says they are not interested in from where this digital espionage attack was launched.

"Bytes don't have nationalities - and anytime a cyber-attack is blamed on a certain country, then it's done with an agenda," he says.

But the Russian government is less concerned about that.

On the same day Kaspersky announced its discovery, Russian security services put out an urgent bulletin saying they had "uncovered a reconnaissance operation by American intelligence services carried out using Apple mobile devices".

- Albania severs ties with Iran over cyber-attack
- Inside US military cyber team's defence of Ukraine

The Russian cyber-intelligence service made no mention of Kaspersky but claimed "several thousand telephone sets" belonging to both Russians and foreign diplomats had been infected.

The bulletin even accused Apple of actively helping in the hacking campaign. Apple denies it was involved.

The alleged culprit - the United States National Security Agency (NSA) - told BBC News it had no comment.

Igor insists Kaspersky did not coordinate with the Russian security services and the government's bulletin took them by surprise.

Image so

Image caption,

The NSA has elite hackers working for the US

Some in the cyber-security world will be surprised by this - the Russian government had appeared to be issuing a joint announcement with Kaspersky, for maximum impact, the kind of tactic increasingly used by Western countries to expose hacking campaigns and loudly point fingers.

Only last month, the US government issued a joint announcement with Microsoft - Chinese government hackers had been found lurking inside energy networks in US territories.

And this announcement was swiftly and predictably followed by a chorus of agreement from America's allies in cyber-space - the UK, Australia, Canada and New Zealand - known as the Five Eyes.

China's response was a rapid denial saying the story was all part of a "collective disinformation campaign" from the Five Eyes countries.

Chinese Foreign Ministry official Mao Ning added China's regular response: "The fact is the United States is the empire of hacking."

'Targeting China'

But now, like Russia, China seems to be adopting a more aggressive approach to calling out Western hacking.

State-run news outlet China Daily has warned foreign-government-backed hackers are now the country's biggest cyber-security threat.

And that warning came with a statistic from Chinese company 360 Security Technology - it had discovered "51 hacker organisations targeting China".

The company did not respond to requests for comment.

Last September, China also accused the US of hacking a government-funded university responsible for aeronautics and space research programmes.

'Fair play'

"China and Russia have slowly figured out the Western model for cyber exposure is incredibly effective and I think we are seeing a shift," Rubrik Zero Labs head and former cyber intelligence worker Steve Stone says.

"I'll also say I think that's a good thing. I have zero issue with other countries revealing what Western countries are doing. I think it's fair play and I think it's appropriate."

Many brush off the Chinese charge of the US being the empire of hacking as hyperbole - but there is some truth in it.

According to the International Institute for Strategic Studies (IISS), the US is the only tier-one cyber power in the world, based on attack, defence and influence.

Tier two is made up of:

- China
- Russia
- the UK
- Australia
- France
- Israel
- Canada

The National Cyber Power Index, compiled by researchers at the Belfer Centre for Science and International Affairs, also deems the US the world's top cyber power.

The paper's lead researcher, Julia Voo, has also noticed a shift.

"Espionage is routine for governments and now it's so often in the form of cyber-attacks - but there's a battle of narrative going on and governments are asking who is behaving responsibly and irresponsibly in cyber-space," she says.

And compiling a list of APT hacking groups and pretending there are no Western ones is not a truthful depiction of reality, she says.


Image so

Image caption,

UK hackers operate from Government Communications Headquarters (GCHQ), in Cheltenham

"Reading the same reports about hacking attacks from only one side adds to a general ignorance," Ms Voo says.

"A general education of the public is important, because this is basically where a lot of tensions between states are going to be playing out in the future."

And Ms Voo praises the UK government for publishing its inaugural transparency report into National Cyber Force operations.

"It's not super-detailed but more than other countries," she says.

'Data bias'

But the lack of transparency could also stem from cyber-security companies themselves.

Mr Stone calls it a "data bias" - Western cyber-security companies fail to see western hacks, because they have no customers in rival countries.

But there could also be a conscious decision to put less effort into some investigations.

"I don't doubt that there's likely some companies that may pull the punch and hide what they may know about a Western attack," Mr Stone says.

But he has never been part of a team that deliberately held back.

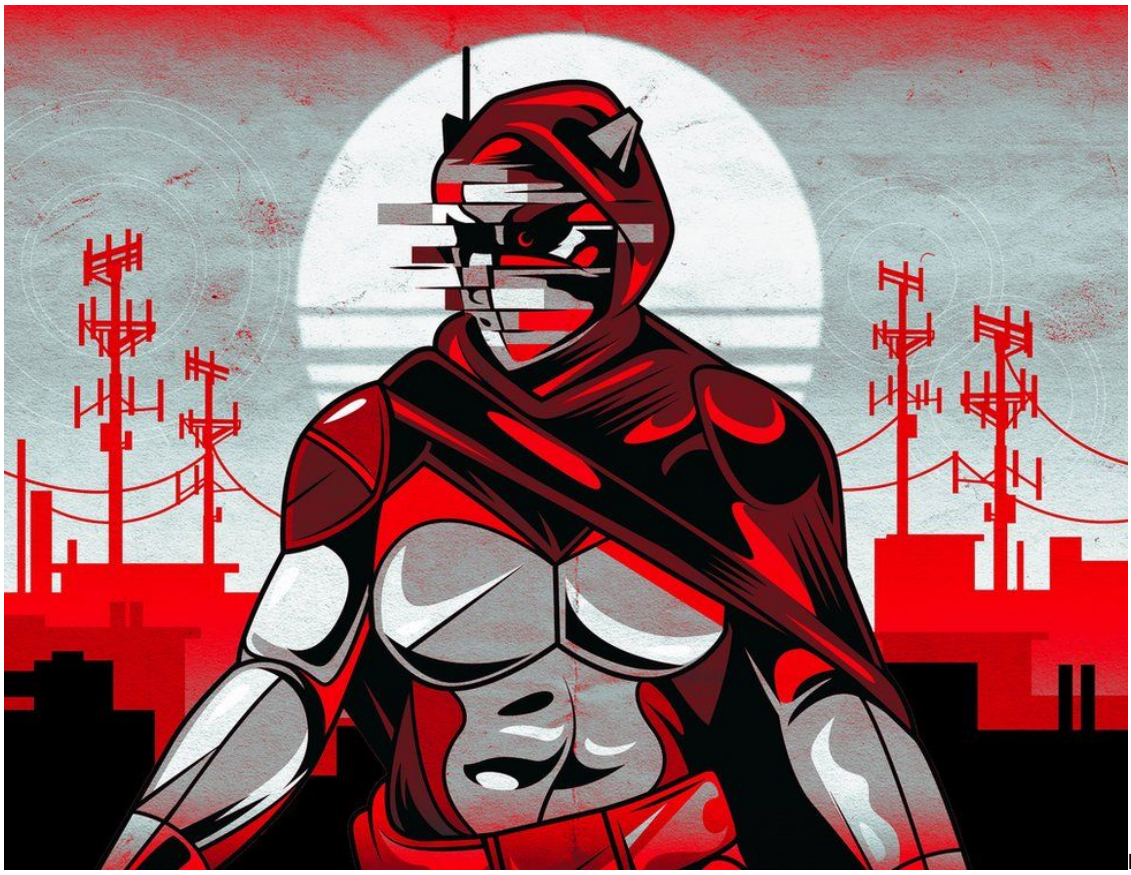

Image so

Crowdstrike
Image caption,

Static Kitten is the name given to an Iranian government-sponsored hacking group

Lucrative contracts from governments such as the UK or US are a major revenue stream for many cyber-security companies too.

As one Middle Eastern cyber-security researcher says: "The cyber-security intelligence sector is heavily represented by Western vendors and greatly influenced by their customers' interests and needs."

The expert, who asked to remain anonymous, is one of more than a dozen volunteers regularly contributing to the APT Google Sheet - a free-to-view online spreadsheet tracking all known instances of threat-actor activities, irrespective of their origins.

It has a tab for "Nato" APTs, with monikers such as Longhorn, Snowglobe and Gossip Girl, but the expert admits it is pretty empty compared with tabs for other regions and countries.

'Less noise'

He says another reason for the lack of information on Western cyber-attacks could be because they are often stealthier and cause less collateral damage.

"Western nations tend to conduct their cyber operations in a more precise and strategic manner, contrasting with the more aggressive and broad attacks associated with nations like Iran and Russia," the expert says.

"As a result, Western cyber operations often yield less noise."

The other aspect to a lack of reporting could be trust.

It is easy to brush off Russian or Chinese hacking allegations because they often lack evidence.

But Western governments, when they loudly and regularly point the finger, rarely, if ever, provide any evidence either.