# Cyber-espionage is more difficult to pin to a state than spying in the physical world

October 21 2014, by Siraj Ahmed Shaikh

Credit: AI-generated image (disclaimer)

Who's in your network, checking out your data? The latest invasive digital creature is Sandworm, a piece of malware discovered to be using a previously unknown Windows vulnerability to infiltrate government networks, spying on systems at NATO, the European Union, the Ukrainian government and others.

In recent years a number of such attacks have been about espionage: stealing sensitive information, or disrupting the critical infrastructure that nations depend on. Making use of sophisticated techniques and zero-day exploits (security vulnerabilities that have not been publicly announced), they are the result of considerable skills and resources.

With targets more political than commercial or criminal in nature, the suspicion is that, due to their deliberate and persistent pursuit of goals aligned with national interests, the attacks have state sponsors.

This is a worrying trend. Cyber-attacks can be launched with relatively little software, hardware and skills, but can have an enormous impact in terms of cost and disruption. As global networks grow in terms of traffic, speed and reach, the situation is only going to get worse.

One serious problem is the difficulty in attributing with any confidence a particular attack to its nation of origin. The internet's technical architecture was built to provide open connectivity, not accountability.

This is complicated by how multi-stage attacks, which most modern cyber-attacks are, make it near-impossible to assert any reliable attribution. These operations are set up so that the attacker first compromises a third party's computer in order to use it as a proxy platform to launch an attack on the final target.

There may be several such machines, each used to compromise another, creating a complex web of connections that obscure the attack's origin. This chain can be sustained in order to allow data to be extracted from the target and brought back, undercover, to the attacker.

## Pointing the finger

Some nations including Russia, China, and Israel are thought to maintain

cyber-warfare teams and carry out state-sponsored attacks. For example, the security research firm Mandiant recently identified a suspected Chinese military cyberwarfare team, Unit 61398, down to the location of its building. This led the US government to file criminal charges for hacking against five named Chinese military officers.

Attributing cyber-attacks follows the principle of sophistication, examining the level of skills and resources required to pull off the attack. The use of zero-day exploits, for example, demonstrates considerable time and effort has gone into testing for an unknown vulnerability against which the target will have little protection. This is not likely to be something a bedroom hacker could achieve.

Attacks that are persistent, trying to overcome defences rather than looking elsewhere for easier targets, are also a sign of possible state backing. This is especially when the target is to steal sensitive information – such as the details of the US F-35 stealth fighter apparently lost to Chinese cyber-espionage – rather than just financial gain.

In the case of Sandworm the context of the conflict in Ukraine is a further giveaway, judging by the military and political organisations targeted and the intelligence-related documents sought.

## Signals in the noise

The characteristics of internet traffic make its attribution more difficult still. The rising volume of non-productive traffic, such as network scanning, worms, traffic resulting from misconfigured routers or systems, and web indexing crawlers such as Googlebot, creates background noise.

The problem is that this background noise may also resemble genuine

malicious attacks – in fact, it's difficult to determine what is accidental and what is deliberate. This leaves a great number of false positives recorded in firewall logs which only makes pinpointing genuine attacks harder.

At the political level, any accusation of state-sponsored hacking needs to be backed up with proof. More often than not, however, the proxy launch pads for most multi-stage attacks are based in non-hostile states. The Tallinn Manual, the most comprehensive legal cyberwarfare rulebook, states that those on the receiving end of any cyber-attack can only respond by applying the "unwilling or unable" test. This is an underlying principle of international law which asserts that retaliation against an intermediary state used by an enemy to launch an attack is only permissible if the intermediary is either unwilling or unable to prevent the aggressor responsible from doing so.

Perhaps the greatest difficulty posed by any retaliatory cyber-attack is the geopolitics of the day. Political alliances, intelligence sharing, legal and ethical considerations, and potential sensitivity of offensive operations, all make it very difficult for nation states to launch such operations. The result is that the sort of public accusations of cyber attacks seen in the press and meant as a tool of deterrence are almost entirely useless – as can be seen Russia and China's frequent and easy denials.



Source: The Conversation

espionage-difficult-pin-state-spying.html