

Experts, Microsoft push for global anti-hacking NGO

AGENCE FRANCE-PRESSE

Tallinn, Estonia June 8

As cyber attacks sow ever greater chaos worldwide, IT titan Microsoft and independent experts are pushing for a new global NGO tasked with the tricky job of unmasking the hackers behind them.

Dubbed the 'Global Cyber Attribution Consortium', according to a recent report by Rand Corporation think-tank, the NGO will probe major cyber attacks and publish, when possible, the identities of their perpetrators, whether they be criminals, global hacker networks or States.

"This is something that we don't have today: a trusted international organisation for cyber-attribution," Paul Nicholas, Director of Microsoft's Global Security Strategy, told NATO's Cycon cyber security conference here last week.

With State and private companies having "skills and technologies scattered around the globe", Nicholas admits it becomes "really difficult when you have certain types of complex international offensives occur-

Cyber Attribution Consortium would probe major cyber attacks and publish, when possible, the identities of their perpetrators, whether they be criminals, global hacker networks or States

ring." "The main actors look at each other and they sort of know who they think it was, but nobody wants to make an affirmation."

Microsoft already floated the idea of an anti-hacking NGO in a June 2016 report that urged the adoption of international standards on cyber security.

The report by Rand commissioned by Microsoft called 'Stateless Attribution - Toward international accountability in Cyberspace' analyses a string of major cyber attacks.

They include offensives on Ukraine's electricity grid, the Stuxnet virus that ravaged an Iranian nuclear facility, the theft of tens of millions of confidential



Pinning down the identity of hackers in cyberspace can be next to impossible, according to experts SHUTTERSTOCK.COM

files from the US Office of Personnel Management (OPM) or the notorious WannaCry ransomware virus.

Duping Investigators

"In the absence of credible institutional mechanisms to contain hazards in cyberspace, there are risks that an incident could threaten international peace and the global economy," the report's authors conclude.

They recommend the creation of an NGO bringing together independent ex-

perts and computer scientists that specifically excludes State actors, who could be bound by policy or politics to conceal their methods and sources.

Rand experts suggest funding for the consortium could come from international philanthropic organisations, institutions like the United Nations, or major computer or telecommunications firms.

Pinning down the identity of hackers in cyberspace can be next to impossible, according to

experts who attended Cycon.

"There are ways to refurbish an attack in a way that 98 per cent of the digital traces point to someone else," Sandro Gaycken, founder and Director of the Digital Society Institute at ESMT Berlin, told AFP in Tallinn.

"There is a strong interest from criminals to look like nation-states, a strong interest from nation-states to look like criminals," he said.

"It's quite easy to make your attack look like it comes from North Korea."

According to experts at Cycon, hackers need only include three lines of code in Cyrillic script in a virus in order to make investigators wrongly believe it came from Russian hackers.

Similarly, launching attacks during working hours in China raises suspicions about Chinese involvement.

Hackers can also cover their tracks by copying and pasting bits and pieces of well known Trojan viruses, something that points the finger at their original authors.

