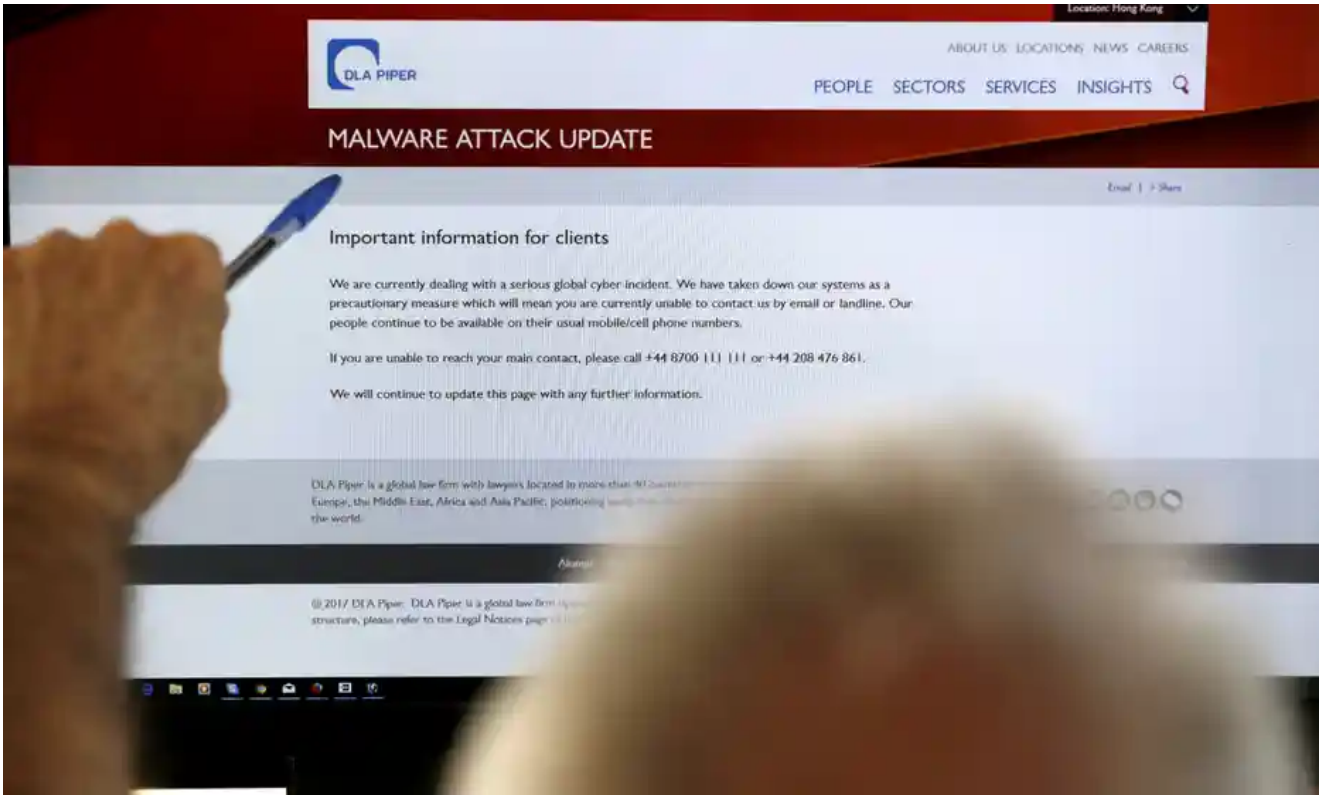
'NotPetya' malware attacks could warrant retaliation, says Nato affiliated-researcher

theguardian.com/technology/2017/jul/03/notpetya-malware-attacks-ukraine-warrant-retaliation-nato-researcher-tomas-minarik

Alex Hern July 3, 2017

If malware outbreak was state sponsored it could count as violation of sovereignty and open possibility of countermeasures, says Tomáš Minárik



While a cyberattack can trigger an armed response from Nato, Minárik cautioned that the damage caused by NotPetya in Ukraine and elsewhere was not sufficient for such an escalation. Photograph: Barbara Walton/EPA
While a cyberattack can trigger an armed response from Nato, Minárik cautioned that the damage caused by NotPetya in Ukraine and elsewhere was not sufficient for such an escalation. Photograph: Barbara Walton/EPA
The NotPetya malware that wiped computers at organisations including Maersk, Merck and the Ukrainian government in June “could count as a violation of sovereignty”, according to a legal researcher at a Nato-affiliated cybersecurity organisation.

If the malware outbreak was state-sponsored, the researcher says, it could open the possiblity of “countermeasures”. Those could come through retaliatory cyber--attacks, or more conventional means such as sanctions, but they must fall short of a military use of force.

Tomáš Minárik, a researcher at the Nato Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, made the comments after the Centre concluded that the malware outbreak, which overwhelmingly hit Ukraine but also affected more than 60 other countries, can most likely be attributed to a state actor.

While a cyber-attack can trigger an armed response from Nato, Minárik cautioned that the damage caused by NotPetya was not sufficient for such an escalation. The law of armed conflict applies only if a cyber-attack causes damage “with consequences comparable to an armed attack”, during an ongoing international armed conflict, “but so far there are reports of neither,” he said.

However, Minárik, added, “as important government systems have been targeted, then in case the operation is attributed to a state this could count as a violation of sovereignty. Consequently, this could be an internationally wrongful act, which might give the targeted states several options to respond with countermeasures.”

A countermeasure is any state response which would be illegal in typical circumstances, but can be authorised as a reaction to an internationally wrongful act by another state. A “hack back” response, for instance, could be a countermeasure, but Nato CCDCOE says that such responses “do not necessarily have to be conducted by cyber means”; they cannot, however, affect third countries, nor can they amount to a use of force.

The suspicion that NotPetya – so called because the malware is superficially similar to an earlier ransomware variant called Petya – may be the work of a state sponsored actor arose shortly after the outbreak began in late June.

While the malware appears to be ransomware (a type of program which holds critical files hostage in exchange for payment), it contained several flaws that prevented it from ever being an effective moneymaker for its creators. Among other things, the payment infrastructure was tied to one email address outside their control, which was promptly blocked by the webmail provider, preventing victims form ever receiving their decryption key and unlocking their files.

But the malware, which was overwhelmingly seeded to victims through a compromised Ukrainian accounting program, did function well as a “wiper”, designed simply to render systems unusable and cause economic damage. It spread rapidly inside business networks, using a combination of exploits stolen from the NSA and more common weaknesses in older versions of Windows, ensuring that whole organisations found themselves unable to operate for days on end.

Unlike WannaCry, an earlier piece of ransomware also suspected of being the work of state-sponsored attackers (in that case, explicitly linked to North Korea by intelligence agencies including the NSA and GCHQ), NotPetya did not contain any functionality enabling it to spread unconstrained across the internet, limiting the vast majority of its damage to those organisations directly infected by the compromised accounting software.