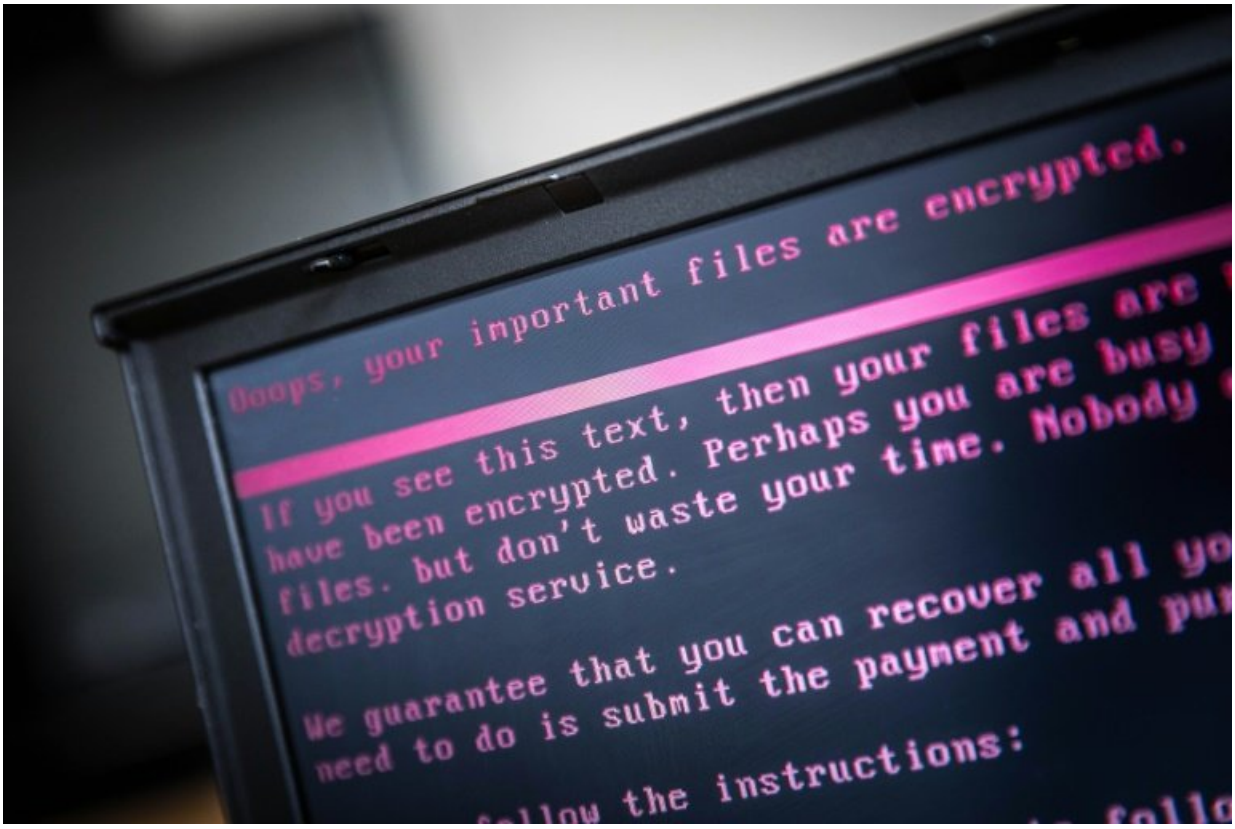
UK blames Russian military for 'NotPetya' cyber-attack (Update)

February 15 2018, by Dario Thuburn



The cyberattack in June 2017 contaminated thousands of computers worldwide

Britain on Thursday accused the Russian military of being behind last year's "NotPetya" cyber-attack, which started in Ukraine and Russia before spreading globally, affecting thousands of computers.

"The UK Government judges that the Russian Government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017," Foreign Office minister Tariq Ahmad said.

Defence Secretary Gavin Williamson said the attack was further evidence of a "new era of warfare" with "a destructive and deadly mix of conventional military might and malicious cyber attacks".

"Russia is ripping up the rule book by undermining democracy, wrecking livelihoods by targeting critical infrastructure and weaponising information," he said.

The accusation was immediately denied by the Kremlin.

"We categorically reject such accusations. We consider them unsubstantiated and groundless," Kremlin spokesman Dmitry Peskov told journalists.

"This is nothing but a continuation of a Russophobic campaign that is not based on any evidence," he said.

'More sophisticated attack'

The attack contaminated thousands of computers worldwide, particularly affecting multinational companies and critical infrastructure, such as radiation monitors at the old Chernobyl nuclear power plant and the ports of Mumbai and Amsterdam.

Companies hit included the Russian oil group Rosneft, Danish shipping company Maersk, US pharmaceutical giant Merck, French construction specialist Saint-Gobain and the British advertising firm WPP.

Ukraine, which is battling Russia-backed rebels in the east in a conflict

that has killed more than 10,000 people, was the worst affected country.

Banking operations were compromised in what authorities said was an unprecedented attack, which even disrupted arrivals and departures informations at the capital's main Boryspil airport.

The virus, which demanded a payment worth $300 as it locked up files at companies and government agencies, was reminiscent of the WannaCry ransomware attack that swept the world a month earlier in May 2017, hitting more than 200,000 users in more than 150 countries.

Britain and the US have blamed North Korea for the WannaCry attack, saying it may have been an attempt by the isolated communist regime to access foreign currency.

The NotPetya attack appeared much smaller in scale, with global cybersecurity firm Kaspersky Lab estimating there were thousands of victims.

Comparing it to WannaCry, the director of European police agency Europol, Rob Wainwright, said at the time that NotPetya showed "indications of a more sophisticated attack capability intended to exploit a range of vulnerabilities".

'Seeking to weaponise information'

The British government on Thursday said the attack "masqueraded as a criminal enterprise but its purpose was principally to disrupt".

"The UK and its allies will not tolerate malicious cyber activity," it added.

Minister Ahmad said the Kremlin had "positioned Russia in direct

opposition to the West", but that the country could still "be the responsible member of the international community that it claims to be rather than secretly trying to undermine it".

London has taken an aggressive stance against Moscow, with Prime Minister Theresa May last year accusing it of "seeking to weaponise information".

British army chief Nick Carter later said that Russian cyber-warfare presented a direct threat to Britain. He called for more investment in the armed forces to be able to deal with it.

Carter said Russia was engaging in "information warfare at its best".

Some British politicians have accused Russia of attempts to disrupt the democratic process in Britain by online interference in political campaigns such as the 2016 Brexit referendum and a 2017 general election.

Speaking on Wednesday, John Chipman, director of the International Institute of Strategic Studies, said Russia was engaged in "capabilities beyond conventional military force that are easier to develop and deploy unaccountably".

"There is still no effective response from the West either in the form of countermeasures or sanctions," he said.

© 2018 AFP

Citation: UK blames Russian military for 'NotPetya' cyber-attack (Update) (2018, February 15) retrieved 26 April 2024 from https://phys.org/news/2018-02-uk-blames-russian-military-malicious.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.