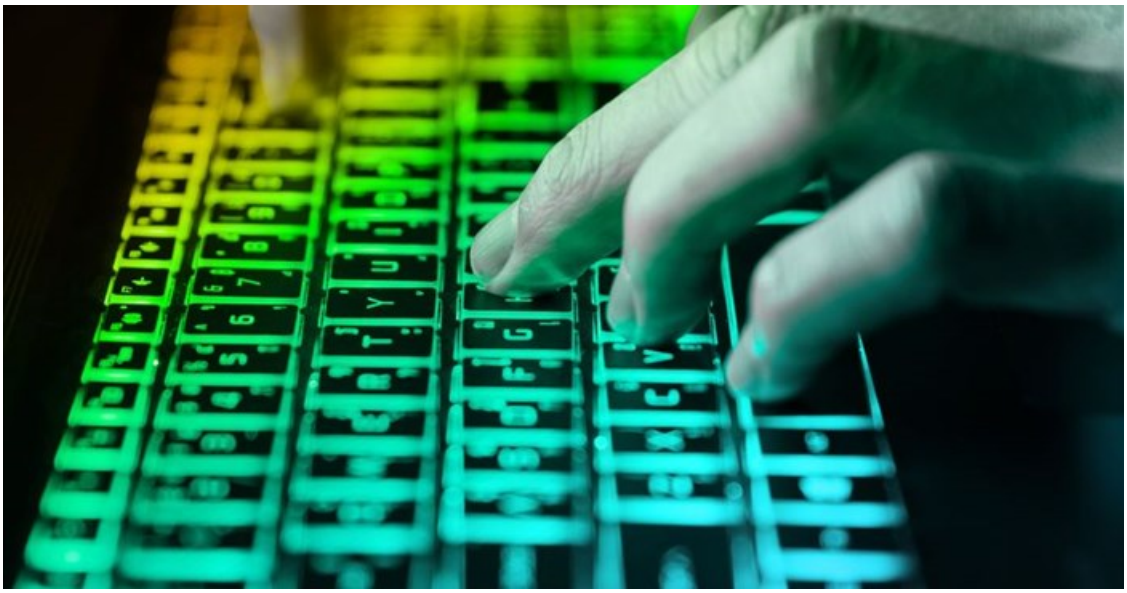
New global ransomware attack disrupts thousands of companies

By Ilse van den Berg

30 Jun 2017

NEWSWATCH: This week saw another global ransomware attack spread across the globe affecting big companies such as multinational advertising and public relations company WPP, Danish shipping company, Maersk, and FedEx, among many others...



© jes2ufoto via 123RF

According to a report on AdAge earlier this week, WPP employees arrived at work to locked PCs and a digital ransom note saying that files had been encrypted and that it would cost more than 300 in bitcoin (around $600,000) to restore them.

Comments Carol Gallarelli, chief marketing officer at Ogilvy & Mather South Africa - a WPP company: “As you will have seen, IT systems at a number of WPP companies, but not all, have been affected by the global cyberattack. WPP have taken appropriate precautionary measures and are continuing to assess the situation. We are doing everything possible to return to normal operations as quickly as possible.”

A number of Maersk's 76 container terminals were affected and were forced to run on manual systems, AP Moller Maersk chief operating officer Vincent Clerc told AFP, refusing to specify which terminals were impacted because of the "fluidity of the situation."

The company has since reported that most of its operations were now up and running again.

Shipping giant FedEx said on Wednesday that deliveries were slowed at its Dutch unit TNT Express after the firm was hit by the cyberattack.

FedEx said TNT's operations were "significantly affected" by the information system virus, which was causing delays at TNT Express' domestic, regional and inter-continental services.

"While TNT Express operations and communications systems have been disrupted, no data breach is known to have occurred," the company said in a statement.

Similarities with WannaCry

According to the European police agency, the wave of cyber attacks hitting Europe and North America is similar to last month's WannaCry ransomware havoc, but appears potentially "more sophisticated."

Describing it as "another serious ransomware attack," Europol said "critical infrastructure and business systems" were being targeted "with a new wave of ransomware, which is an updated version of Petya."

Fast-moving cyber attacks wreak havoc worldwide
15 May 2017

"There are clear similarities with the WannaCry attack, but also indications of a more sophisticated attack capability, intended to exploit a range of vulnerabilities," Europol director Rob Wainwright said in a statement.

Petya has been around since 2016, but it does not just encrypt files on infected devices it also overwrites the master boot record. This has the effect of rendering the computer useless and prevents users from recovering any information, Europol said. It warned that unlike WannaCry "this attack does not include any type of 'kill switch'."

Perhaps a completely new ransomware

Kaspersky Lab's analysts are investigating the new wave of ransomware attacks and its preliminary findings suggest that it is, in fact, not a variant of Petya ransomware as publicly reported, but a new ransomware that has not been seen before. While it has several strings similar to Petya, it possesses entirely different functionality. The company has named it ExPetr.

The company's telemetry data indicates around 2,000 attacked users so far. Organisations in Russia and the Ukraine are the most affected, and it has also registered hits in Poland, Italy, the UK, Germany, France, the US and several other countries.

This appears to be a complex attack, which involves several vectors of compromise. It has confirmed that modified EternalBlue and EternalRomance exploits are used by the criminals for propagation within the corporate network.

"The most significant discovery to date is that the Ukrainian website for the Bakhmut region was hacked and used to distribute the ransomware to visitors via a drive-by-download of the malicious file. To our knowledge, no specific exploits were used in order to infect victims. Instead, visitors were served with a malicious file that was disguised as a Windows update. We are investigating other leads in terms of distribution and initial attack vector."

Kaspersky Lab experts will continue to examine the issue to determine whether it is possible to decrypt data locked in the attack – with the intention of developing a decryption tool as soon as they can.

It advises all companies to update their Windows software: Windows XP and Windows 7 users can protect themselves by installing MS17-010 security patch.

Sources

- AdAge Pay Up or Lose Everything: What Madison Avenue Should Know About The WPP Ransom Hack
- AFP via I-Net Bridge
- Kaspersky Lab press statement

ABOUT ILSE VAN DEN BERG

Ilse is a freelance journalist and editor with a passion for people & their stories (check out Passing Stories). She is also the editor of Go & Travel, a platform connecting all the stakeholders in the travel & tourism industry. You can check out her work here and here. Contact Ilse through her website here.
- #StartupStory: Aura security app to aid beleaguered Uber drivers - 13 Jul 2018
- #StartupStory: BlockMesh - 12 Jun 2018
- Taking telecoms to the next level: Who needs a long-term contract? - 4 Jun 2018
- Nokia makes a comeback in South Africa with new phones - 24 Apr 2018
- New Cape Town/Brazil subsea cable to boost SA broadband - 18 Apr 2018

View my profile and articles...