Ransomware cyber-attack a wake-up call, Microsoft warns - 15 May 2017

A cyber-attack that has hit 150 countries since Friday should be treated by governments around the world as a "wake-up call", Microsoft says.

The **computing giant said** software vulnerabilities hoarded by governments had caused "widespread damage". The latest virus exploits a flaw in a version of Microsoft Windows first identified by US intelligence. There have been warnings of further "ransomware" attacks as people return to work on Monday. Many firms have had experts working over the weekend to prevent new infections. The virus took control of users' files and demanded $300 (£230) payments to restore access.

The spread of the virus slowed over the weekend but the respite might only be brief, experts have said. More than 200,000 computers have been affected so far. But on Monday South Korea said just nine cases of ransomware had been found, giving no further details.

Australian officials said so far only three small-to-medium sized businesses had reported being locked out of their systems while New Zealand's ministry of business said a small number of unconfirmed incidents were being investigated.

A statement from Microsoft president and chief legal officer Brad Smith on Sunday criticised the way governments store up information about security flaws in computer systems. "We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world," he wrote.

"An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen."

Firms must patch their systems before Monday morning, Europol chief warns. He added: "The governments of the world should treat this attack as a wake-up call."

Microsoft said it had released a Windows security update in March to tackle the problem involved in the latest attack, but many users were yet to run it. "As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems," Mr Smith said.

There are going to be some tough questions on Monday for those institutions which didn't do enough to keep their networks secure, as well as the organisations that were best placed to stop it happening in the first place - the NSA and Microsoft. The NSA keeps a chest of cyberweapons to itself so it can hit targets, but Microsoft has long argued that this is dangerous. If there is a flaw in Windows, the company said, surely the safest thing to do is to let its team know straight away so it can be fixed.

But then Microsoft also needs to consider what obligation it has to update all users - not just the ones who pay extra for security on older systems. Updating your computer if you're an individual is a piece of cake, but for a network the size of Britain's National Health Service? Tough - time-consuming, expensive and complex.

For a company like Microsoft to say it won't keep those systems safe unless they shell out more money, then that in itself is something of a ransom. Meanwhile Europol's chief told the BBC the ransomware was designed to allow "infection of one computer to quickly spread across the networks", adding: "That's why we're seeing these numbers increasing all the time." Although a temporary fix earlier slowed the infection rate, the attackers had now released a new version of the virus, he said.

A UK security researcher known as "MalwareTech", who helped to limit the ransomware attack, predicted "another one coming... quite likely on Monday". MalwareTech, who wants to remain anonymous, was hailed as an "accidental hero" after registering a domain name to track the spread of the virus, which actually ended up halting it.

Becky Pinkard, from Digital Shadows, a UK-based cyber-security firm, told AFP news agency that it would be easy for the initial attackers or "copy-cat authors" to change the virus code so it is difficult to guard against. "Even if a fresh attack does not materialise on Monday, we should expect it soon afterwards," she said.

In England, 48 National Health Service (NHS) trusts reported problems at hospitals, doctor surgeries or pharmacies, and 13 NHS organisations in Scotland were also affected. Other organisations targeted worldwide included Germany's rail network Deutsche Bahn, Spanish telecommunications operator Telefonica, French carmaker Renault, US logistics giant FedEx and Russia's Interior Ministry.

Ransomware attack 'like having a Tomahawk missile stolen', says Microsoft boss

Brad Smith says ‘Wannacry’ virus attack that locked up to 200,000 computers in 150 countries is a ‘wake-up call’ amid fears more will be hit as week begins. New versions of the worm are expected to hit and the cost of the damage is not yet known. The massive ransomware attack that caused damage across the globe over the weekend should be a “wake-up call” for governments, the president of Microsoft has said.

Security officials around the world are scrambling to find who was behind the attack which affected 200,000 computer users and closed factories, hospitals and schools by using malicious software that believed to have been stolen from the US National Security Agency.

Europol, the pan-European Union crime-fighting agency, said the threat was escalating and predicted the number of “ransomware” victims was likely to grow across the private and public sectors as people returned to work on Monday.

But Brad Smith, Microsoft president’s and chief legal officer, said on Sunday that it was the latest example of why the stockpiling of vulnerabilities by governments was such a problem.

Smith, whose company’s older system software such as Windows XP was exploited by the ransomware, wrote in a blog post : “The governments of the world should treat this attack as a wake-up call,” Smith wrote. “We need governments to consider the damage to civilians that comes from hoarding these vulnerabilities and the use of these exploits. An equivalent scenario with conventional weapons would be the US military having some of its Tomahawk missiles stolen.”

Cyber security experts said the spread of the virus dubbed WannaCry had slowed but that the respite might only be brief amid fears it could cause new havoc on Monday when employees return to work. New versions of the worm are expected, they said, and the extent – and economic cost – of the damage from Friday’s attack were unclear.

“It’s going to be big, but it’s too early to say how much it’s going to cost because we still don’t know the magnitude of the attacks,” said Mark Weatherford, an security executive whose previous jobs included a senior cyber post with the US Department of Homeland Security.

The investigations into the attack were in the early stages, and attribution for cyber attacks is notoriously difficult.

US President Donald Trump on Friday night ordered his homeland security adviser, Tom Bossert, to convene an “emergency meeting” to assess the threat posed by the global attack, a senior administration official told Reuters.

Senior US security officials held another meeting in the White House situation room on Saturday, and the FBI and the National Security Agency were working to help mitigate damage and identify the perpetrators of the attack, said the official, who spoke on condition of anonymity to discuss internal deliberations.

The NSA is widely believed to have developed the hacking tool that was leaked online in April and used as a catalyst for the ransomware attack. The original attack lost momentum late on Friday after a security researcher inadvertently took control of a server connected to the outbreak, which crippled a feature that caused the malware to rapidly spread across infected networks.

Infected computers appear to largely be out-of-date devices that organisations deemed not worth the price of upgrading or, in some cases, machines involved in manufacturing or hospital functions that proved too difficult to patch without possibly disrupting crucial operations, security experts said.

Marin Ivezic, cyber security partner at PwC, said that some clients had been "working around the clock since the story broke" to restore systems and install software updates, or patches, or restore systems from backups.

Microsoft released patches last month and on Friday to fix a vulnerability that allowed the worm to spread across networks, a rare and powerful feature that caused infections to surge on Friday.

Code for exploiting that bug, which is known as "Eternal Blue", was released on the internet in March by a hacking group known as the Shadow Brokers. The group said it was stolen from a repository of NSA hacking tools. The agency has not responded to requests for comment.

Hong Kong-based Ivezic said that the ransomware was forcing some more "mature" clients affected by the worm to abandon their usual cautious testing of patches "to do unscheduled downtime and urgent patching, which is causing some inconvenience". He declined to identify clients that had been affected.

The head of the European Union police agency said on Sunday the cyber assault hit 200,000 victims in at least 150 countries and that number would grow when people return to work on Monday.

"At the moment, we are in the face of an escalating threat. The numbers are going up, I am worried about how the numbers will continue to grow when people go to work and turn (on) their machines on Monday morning," Europol director Rob Wainwright told Britain's ITV.

Monday was expected to be a busy day, especially in Asia which may not have seen the worst of the impact yet, as companies and organisations turned on their computers.

"Expect to hear a lot more about this tomorrow morning when users are back in their offices and might fall for phishing emails" or other as yet unconfirmed ways the worm may propagate, said Christian Karam, a Singapore-based security researcher.

WannaCry ransomware – The details 14 May 2017

The ransomware is believed to be based on tools stolen from the US National Security Agency. Avast said it had seen over 75,000 cases of the ransomware as of this weekend. It is reported that WannaCry, and variants of it, have hit organisations in 99 countries.

The details:

The WannaCry ransomware – also known as WannaCrypt, WanaCrypt0r, WCrypt, and WCRY – has been detailed in a post on **GitHubGist**. It can affect all versions of Windows before Windows 10, unless they have been patched for MS-17-010. The ransom demand from the attack is between $300 to $600, and the post noted that there is code to "delete files" in the ransomware.

"The worm loops through every RDP session on a system to run the ransomware as that user. It also installs the DOUBLEPULSAR backdoor. It corrupts shadow volumes to make recovery harder," stated the post.

As discovered by a security researcher, the ransomware's killswitch is the website "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com". If the website is up and running, the attack stops spreading.

Tens of thousands of PCs at large institutions and companies have been infected, including the NHS in the UK and FedEx, stated the post.

Warning from Wits

Wits University sent the following email to its students regarding the WannaCry ransomware:

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. Users of all versions of Microsoft Windows operating system are notified and need to take immediate measures to install the relevant security updates. Important information can be found from the Microsoft Security Bulletin MS17-010.

On the 12th of May 2017, a new strain of the Ransom.CryptXXX (WannaCry) strain of ransomware began spreading, impacting a large number of organisations in Europe, demanding a ransom of $300 to $600 in Bitcoin to be paid by the 15th of May 2017.

What needs to be done?

If you are already infected then there is not much you can do. You will have to format and reinstall your software from offline unaffected backups. If you have not been infected, make sure your security patches are up to date by using the Windows Update Service. Do not open any emails or attachments from unknown sources.

Global cyber ransom attack spreads to South Africa 13 May 2017

A cyber security expert has warned people not to open any unknown emails and to urgently update their security software as a global cyber ransom attack spread to South Africa on Saturday.

"We need people to understand that they must not open mail or attachments from senders they do not know," said Roi Shaposhnik of Johannesburg-based Gold N' Links Cyber.

He said his company had seen the attack coming, and was currently helping local clients defend themselves against the attack. The global courier company FedEx were among the first victims of the attack. Official comment from FedEx in South Africa was not available, but a call centre operator said: "We can't even track anything".

Describing it as the biggest cyber attack in history, Shaposhnik said syndicates around the world targeted a weak spot in Microsoft security updates which lead to a massive crash. The Guardian online reported that at least 99 countries have been hit, including Spain, Russia and China.

In the UK, patient files at the UK National Health Services were locked and patients could not be treated.

A demand for a ransom to be paid in the cyber crypto-currency Bitcoin was demanded. Microsoft confirmed the ”painful” attack by the malicious “WannaCrypt” software, which it said did not affect customers using Windows 10.

”Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers,” a statement released via Twitter said.

It proved an urgent security update for customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. It noted that ”phishing” was a component of the attacks and also urged vigilance when opening documents from untrusted or unknown sources. Phishing involves an attempt to get private information from users, including their passwords and credit card numbers.

Phillip Misner, Principal Security Group Manager of Microsoft Security Response Center warned that the method of attack may evolve, and the company would provide updates. He said in March the company released a security update which addresses the ”vulnerability that these attacks are exploiting”, so those who have Windows Update enabled are protected.

Organisations who have not yet applied the security update, should deploy Microsoft Security Bulletin MS17-010. For customers using Windows Defender, the company released an update which detects this threat. Shaposhnik added that people should be cautious on social media because it is not uncommon to track Twitter or Facebook posts to tailor an attack on those platforms.

He explained that a posting about a simple thing like a trip to the hairdresser could expose a person to being phished with an enticing offer to redeem a discount voucher at another hairdresser. Once the link was opened, the attack could start. He urged Facebook and Twitter users to keep their accounts closed to all but friends they know, and to not open links from unknown sources.