Revealed: the trail of cyberheists and destruction made by North Korean hackers behind WannaCry

THE North Korean hackers believed responsible for the WannaCry ransomware that crippled computers around the world this week have been carrying out a series of targeted attacks on international major banks for months.

Computer security experts call WannaCry just the latest battle in the war of good versus evil and for a few days this week the bad guys were winning.

The malicious ransomware WannaCry spread around the world infected 200,000 computers in 150 countries, forced hospitals to turn away patients, factories to shut and sent transport systems sent into chaos.

But this latest attack that so far has delivered about $110,000 in ransom payments is just small change for the hackers who have been launching malicious cyber attacks for nearly a decade, including one of the world's largest cyberheists in which they almost got away with stealing $1.2 billion.

Symantec security says this year Lazarus launched an attack on more than 100 major banks and telecommunication companies in 31 countries.

The attack, first detected by Poland's financial regulator, worked by embedding malware on websites.

Staff monitoring the spread of ransomware cyber-attacks at the Korea internet and Security Agency (KISA) in Seoul. Picture: AFP

If someone using a computer on the list of targeted institutions connected to one of the infected websites, the program would try to infect that bank's network.

The revelation of the apparent Lazarus link means that WannaCry is not just another ransomware attack.

Security experts have called it the first government-sponsored ransomware attack and say there is more to come.

Bruce Bechtol, a professor of political science at Angelo State University in Texas and author of four books on North Korea, says 40 per cent of the North Korean economy comes through illicit activity such as cybercrime and underground arms trade.

Interpol is headed up the international manhunt for the group behind WannaCry but computer security experts have launched their own investigations, studying each line of code in the WannaCry program itself looking for clues for the shadowy figures behind it.

Google threat intelligence researcher Neel Mehta was the first to spot the breakthrough giveaway, which was confirmed by Symantec Corp and Kaspersky Lab researchers.

> Similitude between #WannaCry and Contopee from Lazarus Group ! thx @neelmehta - Is DPRK behind #WannaCry ?
>
> — Matthieu Suiche (@msuiche) 4:04 AM - 16 May 2017

The malicious computer program that infects people's computers with WannaCry has sections of code that are similar to programs written by the North Korean hacking group Lazarus.

The researchers do not believe it is coincidence.

As First Wave chief technology officer Simon Ryan says, the evidence is circumstantial but compelling.

"It makes sense when you look at it," Ryan says.

Lazarus, also known as Guardians of the Peace, is the same hacking group that launched the 2014 high-profile attack on Sony in the wake of the Seth Rogen and James Franco comedy *The Interview*.

Kim Jong-Rewrite: North Korea Upset With Hollywood

Last year it switched its attacks from political targets to financial, netting a jaw-dropping $110 million in a cyber heist from a Bangladeshi bank by exploiting the internal banking computer system Swift and siphoning money to untraceable accounts.

The Belgian head of the Swift Gottfried Leibbrandt called the digital heist "a watershed" for the banking industry.

The first hint the bank had of the theft was when someone noticed the printer that is supposed to print out a pile of papers detailing every transaction was not working.

The hackers had turned off the system to hide their tracks, after ordering the system to transfer $1.2 billion out of Bangladesh Bank's New York Federal Reserve account.

Most transactions were rejected by bank's security systems but $110 million was sent to an account in the Philippines before disappearing.

Computer security firm Kaspersky Lab last month published the results of a year-long investigation into Lazarus, which found the group has been

attacking manufacturing companies, media, and financial institutions in at least 18 countries since 2009.

There are few clues as to the makeup of the group, as they carefully remove all traces of their location from their digital trail, although Kaspersky Lab was able to track them on one day to a server in North Korea.

The Kaspersky Lab report shows the Lazarus hackers have patience, sometimes spending months after breaking into a network getting to know the internal system before launching an attack. And another conclusion in the report strikes a warning note about possible future variants of WannaCry: “the Lazarus group heavily invests in new variants of their malware”.

Ryan says the Lazarus hackers are “picking the low hanging fruit”.

Hospitals in the United Kingdom and Indonesia were hit by the WannaCry ransomware: Picture: AP Photo/Dita Alangkara.

“They’re trying to penetrate through the typically fairly well defended outer layers and they’re trying to get into those core networks that have less attention to them,” he said.

The startling thing about the WannaCry attack this week is that the North

Korean hackers did not have to find the backdoor in old Microsoft software.

The hackers just exploited a weakness reportedly leaked from the United States National Security Agency by another group of hackers called The Shadow Brokers.

Microsoft issued patches for its software two months ago, after The Shadow Brokers released the exploit on the Net. Microsoft's president Brad Smith this week lashed out at the NSA for stockpiling vulnerabilities in software, saying the leaking of them was like having a Tomahawk missile stolen.

Microsoft has lashed out at the National Security Agency for first hoarding software exploits and then losing them to hackers. Picture: AFP

The success of WannaCry is further proof that many people and organisations simply do not update their software with security patches.

The Shadow Brokers occasionally issue online rants written in broken English filled with racists and anarchist statements along with vows of support for President Donald Trump.

This week The Shadow Brokers announced it is launching a monthly

subscription service for hacking groups, like Lazarus, who needed a steady supply of security exploits.

The Shadow Brokers claim those who sign up to the service, to be launched next month, can expect to get compromised data from the global banking network software SWIFT, backdoors into Windows 10 and “compromised network data from Russian, Chinese, Iranian, or North Korean nukes and missile programs”.

Ryan says in the post-Edward Snowden era, there are hacking groups like The Shadow Brokers who feel all information should be released and the WannaCry attack should be a warning to us all.

A fast-moving wave of cyberattacks swept the globe this week, exploiting a flaw exposed in documents leaked from the US National Security Agency. Picture: AFP

“It’s a wake-up call to a lot of businesses,” he said.

“It’s not going to be the last attack. When we look at the attack strategy, if

they follow what they've just done then we could be heading for another disaster."

A likely target is the internet of Things, which includes everything from smart toasters to talking teddy bears, which often run on outdated or easy to hack software.

Mikko Hypponen, chief research officer with security company F-Secure, calls internet of Things "a clear and present danger for the internet."

Recently hackers launched a "zombie army" of smart TVs, security cameras and digital video cameras, compromised with the Mirai malware, to launch massive DDOS attacks.

Ryan says another major risk is the medical industry, with a lot of ageing medical equipment running on outdated software that has not, or cannot, be updated.

"We've seen a lot of internet Of Things attacks but nothing as devastating as WannaCry," he says.

"Maybe we will. Maybe that's the next step for them which is a bit scary.

"It's a war of the good guys against the bad guys and the bad guys are learning. It's a war and the battle is waging."