Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
43/17

WHERE'S THE MONEY HONEY? ARE INDIAN ATMS VULNERABLE TO CYBER ATTACK

Wg Cdr A Shrivastava
Research Fellow, CAPS

India was among the countries worst affected by the '*WannaCry*' attack, as per data shared by Kaspersky, a Russian anti-virus company. According to initial calculations performed soon after the malware struck on early morning of May 12, 2017, around five per cent of all computers affected in the attack were in India[1]. Helsinki-based cyber security company F-Secure, identified this as the biggest ransomware outbreak in history and estimated that 130,000 systems in more than 100 countries had been affected. According to news reports, Russia, China and India were hit because Microsoft's Windows XP was one of the operating systems still widely used in these countries.

The first indications of the *'WannaCry'* cyber attack surfaced in Spain and Britain, where it caused disruptions in many IT networks. The ransomware affected computer networks across hospitals in United Kingdom causing them to lose access to patient data. Hospitals and clinics were unable to attend to patients, including those suffering from serious ailments as their treatment history was inaccessible to doctors. '*WannaCry'* works by encrypting all the data on a computer system by changing file extension names to '.WNCRY'. The malware then displays a window informing users that their files have been encrypted and that they can be recovered in lieu of a payment made in bitcoin[2]. As on May 12, night, six out of the 48 National Health Service (NHS) trusts computer networks were down. However, British Prime Minster Theresa May, said that the NHS weren't deliberately targeted but the denial of services on British hospitals networks were follow through of an international attack.

Chronology of Attack

- On May 12, 2017, media reports started highlighting that a ransomware attack had brought down computer systems in UK hospitals. It soon emerged that the attack was global with

reports of affected computers coming in from all over the globe.

- By midnight of May 12, 2017, the ransomware '*WannaCry*' had infected thousands of computers in UK and encrypted all the data stored on the hard drives. In lieu of decrypting the data, *WannaCry* demanded payment ranging between $300 (around Rs 19,000) to $600 (around Rs 39,000) in bitcoin.
- The Indian Computer Emergency Response Team (CERT-In) is said to be monitoring the situation continuously. On May 13, 2017, CERT-In issued advisory asking computer users in India to upgrade their systems to the latest Windows patch level.
- By the morning of May 14, 2017, government agencies of Russia, Germany, Sweden, Brazil, France and other European nations acknowledged the attack but insisted that all issues have been resolved and attacks were "effectively repelled".
- China's information security watchdog said "a portion" of Windows systems users in the country were infected, according to a notice posted on the official Weibo page of the Beijing branch of the Public Security Bureau on Saturday. Xinhua News Agency reports that over 29,000 institutions had been infected along with hundreds of thousands of devices still running on Windows XP. It cited the Threat Intelligence Center of Qihoo 360, a Chinese internet security services company.
- As on May 15, 2017, no hacker or hacker group has come forward to claim responsibility for the cyber-attack. The recent attack is at an unprecedented level and will require a complex international investigation to identify the culprits.

Architecture of the Attack

WannaCry, researchers say, uses an exploit first developed by the United States National Security Agency. The exploit called Eternal Blue was first made public in April 2017, after a group of hackers called Shadow Brokers released data and hacking tools purportedly belonging to the NSA. NSA is the US' premier signals intelligence agency that has for long been associated with both offensive as well as defensive cyber capabilities. The attack fuelled concerns that the international intelligence community-especially the US' NSA-often does not make public information about vulnerabilities in technology products so that such vulnerabilities can be used by the agencies for offensive purposes. Taking leads from this, hackers exploited the vulnerability of windows XP operating system (an old operating system developed in early 2000) and developed the *'WannaCry'* virus. The program denies user access to data drives of their own computer and thereafter demands a ransom, to be paid in BitCoin, for return of control.

Sensing the unprecedented danger and loss of business worldwide, Microsoft on May 13,

2017, took the unusual step of releasing free software patches for older, unsupported Windows XP system. The US software giant had already developed a patch for the Eternal Blue exploit and had released it as part of an optional security upgrade for Windows users a few weeks back. However, several computers and networks failed to install the new patch as it was not adequately publicised by cyber experts then. The 'ransomware' attacks targeted PCs which use Windows. Many organisations worldwide have still not upgraded from XP to Windows 7 or 10 – which is a logistical nightmare, very expensive and takes years. Microsoft had stopped issuing security patches (updates) for XP in 2014, which means that organisations that still use XP are at security risks.

The Virus Kill Switch

A 22-year-old cybersecurity analyst accidentally shut down vast numbers of attacks by the devastating *'WannaCry'* ransomware by buying a domain name hidden in the program. The domain name is believed to have been written into the software by the hackers to act as a kill switch. Each time the program tried to infect a computer; it would try to contact the webpage. If it failed, *'WannaCry'* would carry on with the attack, but if it succeeded it would stop. The analyst, who tweets as Malware Tech and works for Kryptos Logic, a security firm, admitted he had not realised that buying the domain name, would have this fortunate effect. Dan Goodin, security editor at the Ars Technica blog, wrote: "The virally spreading worm was ultimately stopped when Malware Tech took control of a domain name that was hard-coded into the self-replicating exploit. As a result, the number of infection detections plateaued dramatically in the hours following the registration."

India's Concern

Kaspersky[3], a Russian company which provides antivirus patches for banking sector clients across India had warned in October last year, that most ATMs in India were at risk since they still used Windows XP operating system. However, only few banks took the advice seriously and ordered for software upgrades. Sensing the urgency and scale of the attack, RBI has given clear directives to banks to restrict services on their ATM networks and operate them only after installing the Windows update. The directive was made by the apex bank in response to the *'WannaCry'* ransomware. ATM machines are seen as being vulnerable since almost all of them run on Windows software. Public sector Banks have acknowledged that over 60% of the 2.25 lakh ATMs in the country run on the outdated Windows XP. Updating all ATMs with the latest patch is likely to take some time. In the unforeseen condition of the virus affecting the ATMs, banks and customers could be denied access to banking data of their own accounts leading to catastrophic collapse of the entire banking sector. Our savings may suddenly

disappear from our own bank accounts as the software running on the banks cashier terminal (Tellers) or ATM would not be able to fetch the customers' details from its own server.

Lessons Learnt

India is a world acknowledged software development giant. It is the world's largest sourcing destination for the information technology (IT) industry, accounting for approximately 67 per cent of the US$ 124-130 billion market [4]. The industry employs a workforce of about 10 million. Further, with the present government pushing hard for e-commerce and cashless transactions, it is pertinent to re-start developing the highly secure OS, called Bharat Operating System Solutions or 'BOSS'. The system had successfully passed a crash test in Sep 2015. According to the Centre for Development of Advanced Computing (C-DAC)[5] the software has already been tested by DRDO, Indian Army and other state entities. It's time we develop it as a standard platform for financial transactions.

Cybercriminals and hackers have no international boundaries; it would be naive for us to think that we can be immune to cyber-attack since we are geographically kilometres away from Europe, US or other developed nations. It is time that all organisations whether government run or privately owned, need to understand the fast changing e-networked working environment. It is now important to continuously invest in technology and knowledge to survive.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] http://indiatoday.intoday.in/story/cyberattack-downs-computers-across-countries-including-india/1/9528, May 13, 2017

[2]The word 'Bitcoin' was created by Satoshi Nakamoto, on 31 October 2008 in a research paper called "Bitcoin: A Peer-to-Peer Electronic Cash System". Later, he implemented bitcoin as open source code, presently Bitcoins are used as a source of transactions in the cyberworld.

[3] http://indiatoday.intoday.in/technology/story/indian-banks-use-insecure-atm-machines-still-cling-to-outdated-windows-xp-report/1/7943, October 24, 2016

[4] https://www.ibef.org/industry/information-technology-india.aspx, April 20, 2017

[5] http://www.indiatimes.com/news/india/indian-government-is-launching-its-own-operating-system-boss-to-replace-microsoft-windows-245255.html, September 16, 2015