More evidence by Symantec links North Korea to WannaCry attack

23/05/2017 08:55 by admin

California: A fresh set of evidences by a cyber security firm have sought to link the this monthâ€™s â€˜WannaCryâ€™ ransomware attack to the Lazarus hackerâ€™s group, widely believed to be connected to North Korea.

Symantec, the worldâ€™s largest cyber intelligence company, said that the ransomware had many of the hallmarks, fingerprints of other Lazarus attacks that wiped off almost a terabyte worth of data from Sony Pictures and also siphoned a reported $81 million from the Bangladesh Central bank last year.

"Analysis... revealed substantial commonalities in the tools, techniques, and infrastructure used by the attackers and those seen in previous Lazarus attacks, making it highly likely that Lazarus was behind the spread of WannaCry."

Â

Last week, a researcher at Google had recognized an identical code originated in a WCry sample from February attack and also an early 2015 version of Cantopee, a backdoor used by Lazarus Group, a hacking group which has been operational since 2011.

Â

North Korea has dismissed earlier reports linking its isolated regime to the worm that crippled hundreds of thousands of computers, demanding payment in Bitcoin to return control to users.

Â

Researchers from security firm Symantec gave additional evidence which supplements the case that the ransomware bug WCry is closely linked to Lazarus Group.

Â

The evidence includes the discovery of three pieces of malware which were previously linked to Lazarus Group that were left out on a network first hit by WCry, in February.

Â

Â Â Â The malware included Trojan Volgmer and two variants of Backdoor. Destover, was the disk wiping tool used in this attack, the same tool used in the Sony Pictures attacks.

Â Â Â Trojan Alphanc, last used to spread WCry in attacks that took place in March and April attacks was a modified version of Backdoor.

Â Â Â Â Duzzer, which has previously been linked to Lazarus as well.

Â Â Â Â Bravonc, another Trojan used to install WCry in attacks on computers, used the same IP addresses for command and control as Duuzer and Destover.

Â

In a blog post by Symantec researchers, they also highlighted some points indicating the link to North Korea:

Â Â Â Â The earlier versions and WannaCry largely the same, with some minor changes, chiefly the incorporation of the EternalBlue exploit. The passwords used to encrypt the Zip files embedded in the WannaCry dropper are similar across both versions ("wcry@123", "wcry@2016", and "WNcry@2ol7") indicating that the author of both versions is

likely the same group.

Â Â Â The small number of Bitcoin wallets used by first version of WannaCry, and its limited spread, indicates that this was not a tool that was shared across cyber-crime groups. This provides further evidence that both versions of WannaCry were operated by a single group.

Â

Seoul internet security firm Hauri, known for its vast troves of data on Pyongyang's hacking activities, has been warning of ransomware attacks since last year.

Experts say the North appears to have stepped up cyber-attacks in recent years in a bid to earn hard foreign currency in the face of United Nations sanctions imposed over its nuclear and missile programmes.

- IT