New technique completely protects internet pictures and videos from cyberattacks

13 March 2017

Credit: Wikipedia

A Ben-Gurion University of the Negev (BGU) researcher has developed a new technique that could provide virtually 100 percent protection against cyberattacks launched through internet videos or images, which are a growing threat.

"Any downloaded or streamed video or picture is a potential vehicle for a cyberattack," says Professor Ofer Hadar, chair of BGU's Department of Communication Systems Engineering. "Hackers like videos and pictures because they bypass the regular data transfer systems of highly secure systems, and there is significant space in which to implant malicious code."

Cyber security has become a high-profile issue, made even more so by recent WikiLeaks allegations against the Central Intelligence Agency, accusing them of bypassing security encryption on a variety of smart devices.

Yet, attacks on internet video and pictures are a broader, lesser-known threat. Internet video will comprise 82 percent of all global consumer internet traffic by 2020, according to the 2016 Cisco Visual Networking Index research report. As a result, downloaded and shared videos and images are a growing target for cyberattackers.

To counter this emerging threat, Prof. Hadar developed a series of algorithms that can completely prevent attackers from being able to infiltrate and extract information through videos or pictures.

His techniques combat steganography, a process that involves hiding a message in an appropriate carrier, such as an image file. Utilizing steganography, the carrier can be sent to a receiver without anyone else knowing that it contains a hidden message.

"We are dealing nowadays with the use of steganography to insert malicious codes within videos and photos to attack the viewer," explains Prof. Hadar. "We have developed algorithms to find a solution to that problem in the 'compressed domain.' The idea is to manipulate the file's 'payload' to remove the malicious code without damaging the data quality."

Prof. Hadar's approach, which he has dubbed The Coucou Project, addresses two potential attack scenarios. Both scenarios assume that basic malware has been planted on the victim's servers/hosts by means of social engineering, such as phishing scams or other means of exploiting data vulnerability. From there, the malware gathers classified information from the victim's data center.

In the first scenario, once the user uploads an image or a video to a social network, the malware embeds the classified information into the uploaded

content (making it accessible to the attacker). In the second scenario, the attacker uploads infected content to a social network or any other shared server where the malware can extract the malicious code and execute it.

"Preliminary experimental results show that a method based on a combination of Coucou Project techniques results in virtually 100 percent protection against cyberattacks," says Prof. Hadar. "We envision that firewall and antivirus companies will be able to utilize Coucou protection applications and techniques in their products."

The Coucou Project receives funding from the BGU Cyber Security Research Center and the BaseCamp Innovation Center at the Advanced Technologies Park adjacent to BGU, which is interested in developing the protective platform into a commercial enterprise.

Provided by American Associates, Ben-Gurion University of the Negev