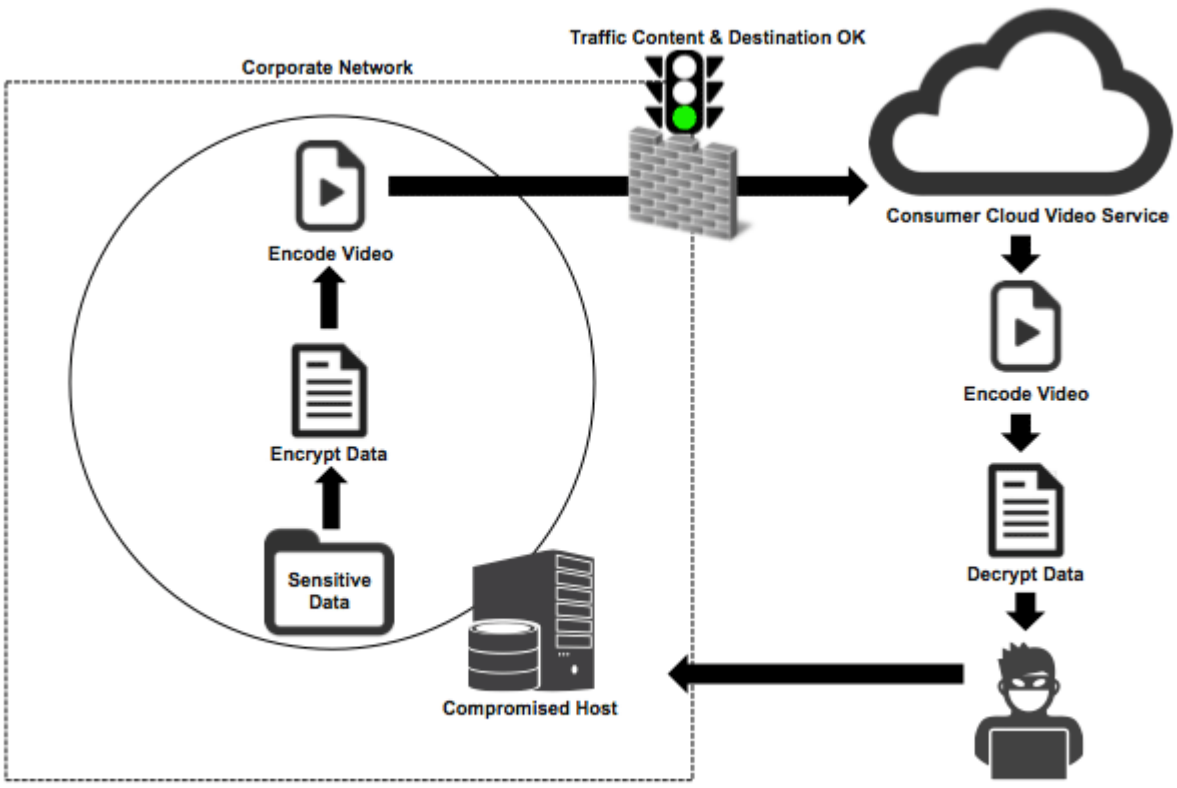
Hackers Exfiltrating Data with Video Steganography via Cloud Video Services

KEN WESTIN

NOV 24, 2014 | INCIDENT DETECTION

A new technique for data exfiltration has been seen in the wild using video uploaded to cloud services as a way to move data out of compromised networks without detection. The technique utilizes steganography where encrypted data is encoded into video files and uploaded to trusted or unmonitored video sharing services.



This particular attack vector has been theoretically possible for some time. However, this is the first time that such an attack has been seen in use as a way to exfiltrate data out of an organization to avoid detection by conventional security tools, such as intrusion detection/prevention systems.

There are a number of commercial and open source (eg. OpenSego, OpenPuff) steganography tools that can be used in this particular attack. The use of steganography is usually a technique reserved for spycraft, as a means of passing communications to another party with the goal of avoiding interception. An Al-Qaeda operative was arrested in Germany a few years ago and it was discovered he was using this technique to hide plain text files containing operations and other data into pornographic videos.

A Fortune 500 company was recently hit by this particular exploit and had sensitive data exfiltrated from their network. The data exfiltration went undetected by perimeter defenses and intrusion detection systems, until the company received an alert the revealed multiple duplicate video files had been uploaded from their network to a video sharing website.

MITIGATION

There are a number of tools available that can detect the presence of steganography in images on a network, such as software to appliances designed specifically for detecting signatures of common steganography tools and techniques. The problem is they are generally designed to detect the use of steganography in images, not video. The groups using this as an exfiltration technique are well aware of this, hence why they are using video instead of images which would be an easier transport mechanism.

In most cases the attackers will need to utilize a third-party tool or custom built binary to encode data into an image, as well as have a video itself. Administrators should already be monitoring assets for new binaries on hosts. This is trivial with tools like Tripwire Enterprise; however, they may not think a video file appearing on a host is suspicious. It is important to note that not all potentially malicious applications installed on a host may be flagged as malware in various threat intelligence data sources.

A scan of host systems for video files may also be a good idea—there is generally no good reason for any video files to be present on critical assets, or servers in the data center unless the services are serving some sort of media function.

Also, by monitoring connections of a host system to external services administrators can monitor suspicious activity. Although it is not odd for a laptop in marketing to upload a video to YouTube, the same activity from a server asset, or from anywhere in the data center or secured area of a network could be an indicator you have a problem.

In the case of the Fortune 500 company that was targeted, the videos were the same, but with different pieces of data in each video uploaded, which could be another indicator.