WANT TO KNOW MORE?

Research, links and articles…..

ARTICLES

https://www.consumer.ftc.gov/blog/free-movies-costly-malware
The US Federal Trade Commission issued a warning in April 2017 that sites and apps offering free downloads or streams of movies, TV shows, sports and games often hide malware. It's the hidden cost of "something for nothing". The threat is so real that Attorneys General from around the United States have recorded consumer messages about staying safe on the internet: https://www.youtube.com/user/4SaferInternet

https://www.consumer.ftc.gov/articles/0011-malware
The US Federal Trade Commission provides some consumer information about malware – what it is and how to avoid, detect report and get rid of it.

http://mistercopyright.org/
By Kevin Madigan.
Recent theft-based, blackmail cyberattacks are on the rise as more pirate-content sites shut down, discrediting hackers' claims of a commitment to benevolent sharing and revealing that it's always been all about the money.

http://www.huffingtonpost.co.uk/liz-bales/
By Liz Bales, CEO of the Industry Trust for IP Awareness
A warning for parents that, even when connecting a TV to an internet connected box or stick to access unauthorised entertainment online, they are likely to be exposed to many of the security and safety risks traditionally associated with pirate websites as well as inadvertent exposure to pornographic or age-inappropriate content.

Searching for free movie sites increases risks of malware
by David Newhoff
Research shows there is a one-in-three chance of downloading malicious software when people visit illegal sites.

How some websites are spreading malware
by Ellen Seidler
At least two U.S.-based companies are helping rogue websites to peddle malicious content, according to a 2016 report.

USEFUL LINKS…

Australia

http://www.contentcafe.org.au/
http://www.nothingbeatstherealthing.info/index
https://www.screenaustralia.gov.au/
https://www.esafety.gov.au/education-resources/classroom-resources
https://www.copyright.com.au/
http://www.copyright.org.au/
https://www.screenrights.org/
http://whymusicmatters.com.au/

Global

http://www.digitalcitizensalliance.org/index.php
http://www.copyrighthub.org/
http://www.industrytrust.co.uk/
http://www.creativecoalitioncampaign.org.uk/
https://www.creativefuture.org/
http://alliance4creativity.com/
http://crackingideas.com/

RESEARCH STUDIES

Below are links to published studies / academic papers on the use of malware and other potentially dangerous programs that proliferate on infringing sites, with a brief summary of the scope of the research paper.

The studies prove that, in addition to professionals in the creative industries, end users are also victims of the massive and growing cybercrime industry.

ILLEGAL STREAMING AND CYBER SECURITY RISKS: A DANGEROUS STATUS QUO?
Commissioned/Published by The Association of Internet Security Professionals
September 2014

Academic paper arguing that infringing video streaming has become the number one method to propagate malware on the Internet. The paper recommends mounting an awareness campaign targeted at computer users everywhere and informing individuals of the personal risks of illegal streaming.
The cyber security dangers that accessing unauthorized videos pose to individual computers mean that illegal streaming can be as damaging to the user as it is to the copyright holders of our most cherished sports, television and film content.
http://cryptome.org/2014/09/illegal-streaming-malware-epoch-times-full-14-0923.pdf

The 'Bogus Features' Lurking Behind Pirate Film and TV Sites

Commissioned/Published by: The Industry Trust
Released: April 2014

Highlights two studies: The first by Incopro found that 97% of the thirty most frequently used infringing film/ TV sites in the UK contained malware or credit card scams and 3 in 4 visitors to the sites experienced problems with their device after visiting the sites. The second study was a survey by ICM of 4,210 users in the UK aged 16+ which found that the top offenders encountered after accessing motion picture and TV series content from infringing sites were:

- **Pop-up ads:** Nearly 2 in 5 (39%) experienced pop-up adverts which are difficult to get rid of and can be used to generate revenue from click-throughs as part of an online scam
- **Viruses:** 1 in 3 (32%) downloaded a virus on to their device, often leading to their devices being unusable or having to be fixed
- **Malware:** More than a quarter (28%) downloaded malware on their device
- **Stolen data:** Almost 1 in 5 (17%) lost personal data or had personal information stolen
- **Illicit material:** 14% were exposed to material such as pornography or violent images

http://www.industrytrust.co.uk/

Malware Risks

Commissioned/Published by The Asia Digital Alliance
June 2016

A study explaining A RAT – Remote Access Trojan [a very appropriate acronym] - a malicious code that can be embedded and disguised within a trusted file attachment such as a PDF, Word or Excel document, or hidden within a movie or music torrent or file. Once a victim clicks on the attachment, or opens or streams the content file, the RAT malware will be downloaded.
RATs can and are used to steal passwords, credit card details and other personal data and to remotely activate a victim's webcam and audio functionality, browse through a victims private pictures or videos, and download and publicly share (or sell) the images and videos of their choosing.
http://www.asiadigitalalliance.com/malware-risks/

Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet users' Computers and Personal Data

Commissioned/Published by The Digital Citizens Alliance & RiskIQ
December 2015

After comparing a sample of approximately 800 infringing sites to a control group of 250 similarly situated non-infringing sites, this study found that:

- 1 out of every 3 infringing site surveyed contained malware
- Visitors were 28 times more likely to get malware from an infringing site than on a similarly situated non-infringing site
- 45% of the malware on the infringing sites surveyed were delivered passively (i.e., a process which infects a user's device without the user having to click a link after arriving on the page)

http://www.digitalcitizensalliance.org/

The Revenue Sources for Websites Making Available Copyright Content without Consent in the European Union

Commissioned/Published by Incopro
March 2015

This study found that approximately one third (31.5%) of the advertisements reviewed from 622 popular infringing sites across France, Germany, Italy, Spain, and the UK were identified as trick buttons or malware, where clicking the advertisement could potentially infect the user's computer with malware and bots.
http://www.incoproip.com/

Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business

Commissioned/Published by The Digital Citizens Alliance
February 2014

This study and survey shows that of 45 large infringing sites (greater than 5 million monthly unique visitors), over half contained (60%) contained malware download links. It reports that the public expects digital and social platforms to do more on illicit and/or illegal activities posing threats to safety – including scams, pirated content, drugs and stolen goods. It urges platforms to take more responsibility for what occurs on their sites or risk further eroding consumer trust in the Internet and its most popular companies.
http://media.digitalcitizensactionalliance.org/