Dangerous Partners: Digital Citizens Investigation Finds That Malware Operators and Content Theft Websites – Assisted by U.S.-based Tech Firms – are Targeting Millions of Consumers

Pirated Movies and TV Shows Used as Bait to Lure Consumers, Who are Then Infected with Malware That Leads to ID Theft, Financial Loss, Ransomware

1 in 3 Content Theft Websites Expose Consumers to Malware, According to Latest RiskIQ Research of Rogue Sites

Washington, DC, July 20, 2016 – A Digital Citizens investigation has found that malware operators and content theft website owners are teaming up to target consumers – with an unexpected assist from U.S.-base tech firms. The research found that 1 in 3 content theft websites expose consumers to dangerous malware that can lead to serious issues such as ID theft, financial loss and ransomware.

And disturbingly, U.S.-based tech firms – such as hosting companies that enable websites to remain up and running – play a vital role in enabling these websites to operate. The Digital Citizens report, *Enabling Malware*, found that among content theft websites analyzed that are spreading malware, two tech firms – Hawk Host and CloudFlare – were the most often used by these rogue websites.

The research, done in collaboration with respected cyber security firm RiskIQ, built on earlier research that found that malware operators and content theft website owners were collaborating to target and harm consumers. Ongoing research has found that 1 in 3 of these websites expose consumers to malware. And RiskIQ went undercover in December to scrutinize the DarkNet chat rooms where malware operators meet and negotiate prices for how to infect consumers.

"Given that our research shows that 12 million Americans are exposed to malware through content theft websites, we are approaching a cyber epidemic that poses serious concerns about the long-term security of Americans' computers," said Tom Galvin, Executive Director of the Digital Citizens Alliance.

"These rogue operators are using pirated movies and TV shows to lure consumers so they can infect their computers and steal their money, their identity or hold access to the computer for ransom," said Galvin. "It's time for government authorities – from the Federal Trade Commission to Congress to state attorneys general – to warn consumers about the risk content theft poses to their well-being."

In this latest research, RiskIQ looked at hundreds of content theft websites and checked for malware. Here is what RiskIQ found:

- Thirty percent of content theft websites exposed consumers to malware. The type of malware and technique was constantly changing. In some cases, rogue operators tricked consumers with a prompt to update a movie player or through an infected ad. In other cases, malware was downloaded simply by visiting a content theft website.

- RiskIQ has found that based on its research, 12 million Americans are exposed on a monthly basis to malware from content theft websites. RiskIQ has found that consumers are 28 times more likely to get exposed to malware on content theft websites than mainstream websites.

- Once infected, the hackers can access and steal personal and financial data. In some cases, it enables hackers to install a Remote Access Trojan, enabling criminals to gain access to the video camera on a laptop and secretly tape the activities of unknowing people, usually young girls. In some cases, these videos are then resold online on DarkNet websites (and even in some instances, are made available on the popular video website YouTube, which is owned by Google).

- Hawk Host and CloudFlare were the go-to tech firms for content theft websites spreading malware, according to the new research. Digital Citizens researchers reached out to both companies and received sharply different responses. Hawk Host reported that it conducted its own investigation, and found that the websites violated its terms of service and therefor the company suspended them. CloudFlare, in its response, said it leaves the removal of content to law enforcement. It added that in some instances if it believes that malware is spread by a customer, it will warn site visitors. But Digital Citizens to date has seen no warning on the websites found to spread malware.

  "For Digital Citizens, the key test of companies is what it does once it learns that one of its customers is engaged in wrongdoing and spreading malware. For that reason, we applaud Hawk Host for the responsible manner in which it took quick action to protect internet users from risk," said Galvin.

In recent months, Digital Citizens has presented findings on malware and content theft websites to Congress, the FTC and state attorneys general. DCA research found that government awareness programs can be an effective tool in alerting consumers, 72 percent of whom reported in a recent poll that if they knew that content theft websites exposed them to malware, they would avoid such sites.

"The DarkNet marriage of malware operators and content theft websites is ominous for consumers who already face a tough task in protecting their cyber security," added Galvin. "We need to raise awareness among consumers, and no one is in a better position to do that than government entities who already provide the important public service of alerting consumers to online risks."

About Digital Citizens

Digital Citizens is a consumer-oriented coalition focused on educating the public and policy makers on the threats that consumers face on the internet and the importance for internet stakeholders – individuals, government and industry - to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on internet safety.

The Digital Citizens Alliance will be an active voice in promoting a better and safer internet, working with governments, policy makers, security experts, and the businesses that operate the internet. We will carry your voice – that of the consumer – to ensure that the internet is a place we can trust. For more information please visit http://www.digitalcitizensalliance.org/.

-30-