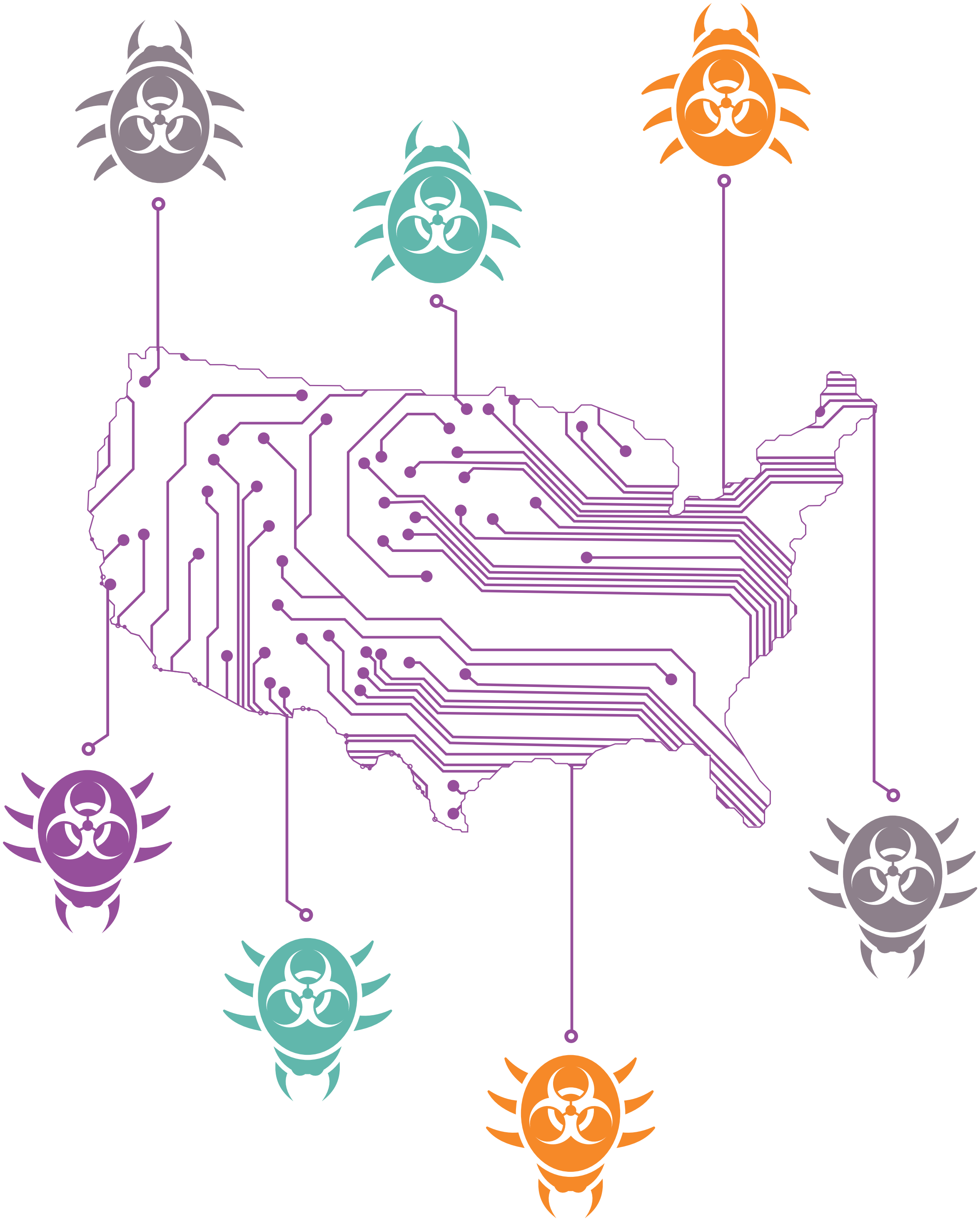
ENABLING MALWARE

HOW U.S.-BASED FIRMS ARE ENABLING MALWARE PEDDLERS TO BAIT CONSUMERS AND STEAL THEIR PERSONAL INFORMATION



July 2016

digitalcitizens alliance

Table of Contents

The Threat

When you think of Internet crime, you probably imagine shadowy individuals operating in Eastern Europe, China or Russia who come up with devious plans to steal your identity, trick you into turning over financial information or peddling counterfeits or stolen content. And you would be right.

But while many online criminals are based overseas, and often beyond the reach of U.S. prosecutors, they are aided by North American technology companies that ensure that overseas operators' lifeline to the public – their websites – are available.

A hosting company is an Internet service that allows companies, organizations and individuals to make their website accessible online. Through their servers and data centers, they ensure that websites are operational and available to Internet users.

A content delivery network (CDN) is an interconnected system of servers that use geographical proximity as criteria for delivering Web content. When website owners add content to their own servers, a CDN will then distribute that content across its network. A user visiting a website is served content from the server nearest their location. The end result is optimized bandwidth and faster performance leading to a better experience for a websites' users.

These two types of companies are vital to online criminals' efforts to lure consumers to content theft websites (also called pirate sites) so they can infect their computers with malware. Once infected, criminals can then gain access to personal or financial information or take over computers for botnet attacks.

In December, the Digital Citizens Alliance looked at the troubling trend of how content theft is being used as a bait to infect consumers' computers. Working with the Internet security firm RiskIQ, Digital Citizens found that 1 in 3 content theft sites exposed consumers to malware and other risks. This risk is serious: RiskIQ found that consumers were 28 times more likely to be exposed to malware on content theft sites than mainstream websites (such as espn.com or cnn.com).

In May, Digital Citizens and RiskIQ followed up on that research, and found that the risk of malware exposure remains high at 30 percent. But this time Digital Citizens delved into the websites that expose consumers to risk, and who is behind them.

What the research found is that while these shadowy content theft websites have overseas operators, many rely on North American companies to operate. Companies such as Hawk Host, which has a mailing address in Fergus, Ontario, Canada but has offices in Dallas, Los Angeles, and Washington DC.

Are these companies doing anything illegal? No more than the landlord of an apartment isn't doing anything illegal by renting to a drug dealer who has sellers showing up day and night. But just like that landlord, more often than not these companies either look the other way or just don't want to know.

For example, the company CloudFlare has repeatedly refused requests and efforts to crack down on websites that are clearly offering illegal products or engaged in scams that harm consumers.[1] For that, CloudFlare has earned the moniker "CrimeFlare" within the Internet community.[2]

But by looking the other way, these companies are now contributing to a growing issue for Americans: the threat of computer infections, the rise of identity theft and loss of financial information. The U.S. Department of Justice reports that 16.2 million U.S. consumers have been victimized by identity theft, with financial losses totaling over $24.7 billion.

In the case of content theft, the pirated movies, TV shows and music is the draw. Bad actors dangle free content, consumers take the bait, and the end result is millions of identities at risk and billions of dollars stolen. Then these computers are taken over to wreak more havoc, causing a nightmare for everyone from Internet users to advertisers who get defrauded, to corporations blackmailed into paying off hackers who threaten to use those rogue computers to launch attacks.

Digital Citizens research found that once hackers get into a computer, they can use it for a wide range of criminal schemes where the user of the computer is the victim. These include:

- Stealing bank and credit card information that is then sold on underground Internet exchanges. After the hack, consumers find their bank accounts depleted or suspicious charges on their credit cards. There is an underground market for credit card information that ranges from $2 to $135 per credit card credential.

[1] http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/

[2] This is not to be confused with the website crimeflare.com, which tracks abusive sites that hide behind CloudFlare's services

- Finding personal information that makes it easier to sell a person's identity to the highest bidder online. In July, the FBI added five online criminals to its "Most Wanted" list for creating computer programs that stole identities and financial information.

- Locking a user's computer and demanding a ransom fee before returning access to their files. Typically, hackers charge $100-$500 for consumers to regain access to their computers. The FBI reported in April, 2016 that consumers reported losses of $209 million in the first quarter of this year alone.[3]

In previous reports, Digital Citizens has looked at how credit card companies and the advertising industry have enabled criminals to peddle content theft. Now, with a look at how these websites are hosted and deliver their content, we are taking a snapshot into the world of the technology companies that criminals rely upon.

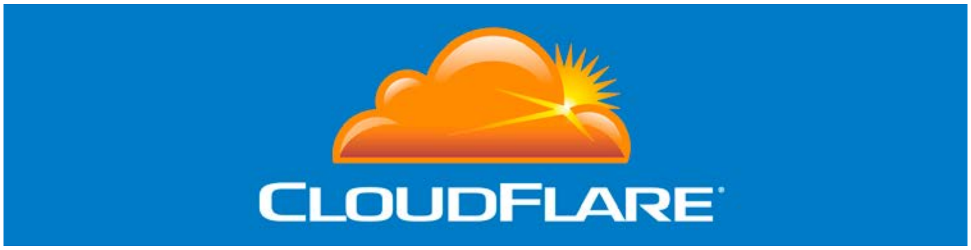
This report takes a look at these companies, the websites they enable and the malware that is spread from them. And perhaps most telling - how they reacted when presented with information that their customers were spreading malware.

In the last few years, consumers and businesses have fully grasped the threat that malware poses to their cyber and personal security. The companies that enable malware can't have it both ways – seeking legitimate customers while enabling criminals to prey on innocent consumers and businesses.

Through this report, Digital Citizens hopes to raise awareness on the connection between content theft and malware and put the spotlight on the companies that through their often-willful blindness put Internet users at grave risk.

[3] http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

Enabling Malware



On its website, CloudFlare touts itself as "a free global CDN, DNS, DDoS protection & web security provider that can speed up and protect any site online." It is headquartered in San Francisco, with additional offices in London, Singapore, Champaign and Austin.[4] Among the cyber security world, it's known for its willingness to support, or at least overlook, illicit activities.[5]

CloudFlare's services popped up the most in Digital Citizens' latest review of companies supporting content theft websites that expose consumers to malware.

When Digital Citizens' researchers ran Whois searches on the content theft sites serving malware, CloudFlare appeared as the host for numerous sites. We recognize, of course, that CloudFlare is not a traditional hosting company, but instead provides customers using its services with the ability to mask the true hosting company's information.

In order to utilize CloudFlare's CDN, DNS, and other protection services customers have to run all of their website traffic through the CloudFlare network. The end result of doing so is masked hosting information. Instead of the actual hosting provider, IP address, domain name server, etc., a Whois search provides the information for CloudFlare's network.

The company's blog puts it best, "Signing up for CloudFlare is like taking your number out of the phone book, and putting in CloudFlare's number under your name."[6] In the case of content theft sites examined for this report, CloudFlare is protecting the information of criminals who are peddling malware on consumers.

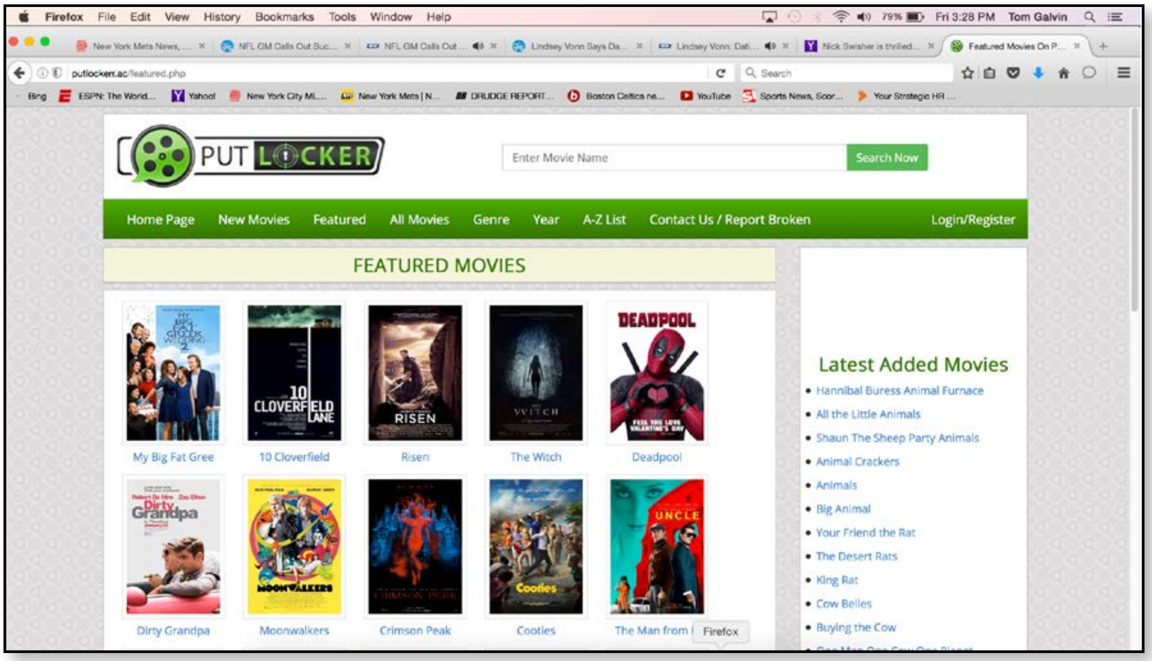
[4] https://www.cloudflare.com/overview/

[5] http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/

[6] https://blog.cloudflare.com/ddos-prevention-protecting-the-origin/

Take for example putlockerr.ac, a content theft website enabled by and utilizing CloudFlare's services.

Putlockerr.ac offers dozens of pirated movies, and perhaps anticipating legal issues with copyright holders, abandons all responsibility: "All of the free movies found on this website are hosted on third-party servers that are freely available to watch online for all Internet users. Any legal issues regarding the free online movies on this website should be taken up with the actual file hosts themselves, as we're not affiliated with them."



FEATURED MOVIES

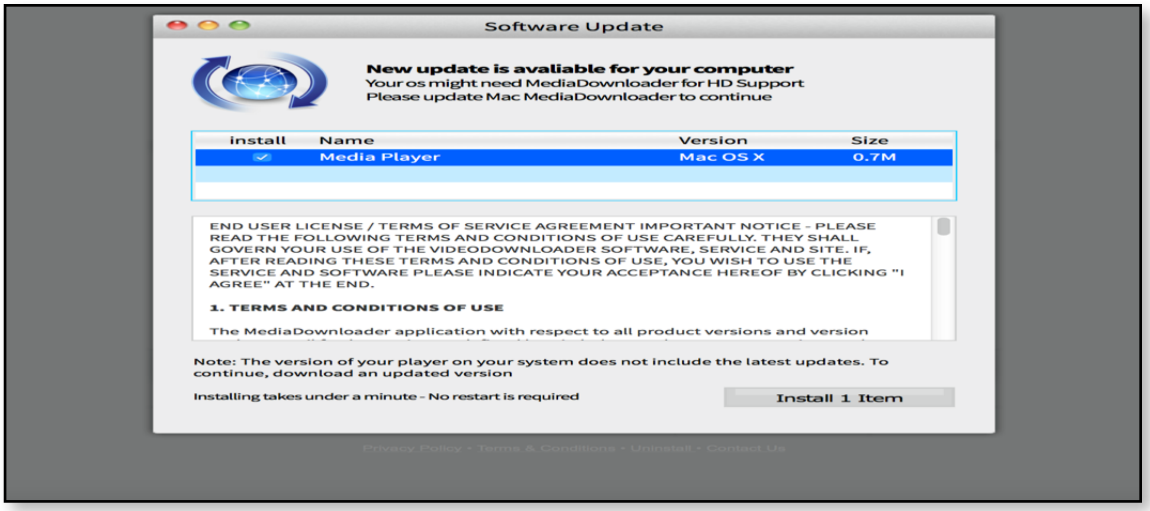
My Big Fat Gree
10 Cloverfield
Risen
The Witch
Deadpool
Dirty Grandpa
Moonwalkers
Crimson Peak
Cooties
The Man from

Latest Added Movies

- Hannibal Buress Animal Furnace
- All the Little Animals
- Shaun The Sheep Party Animals
- Animal Crackers
- Animals
- Big Animal
- Your Friend the Rat
- The Desert Rats
- King Rat
- Cow Belles
- Buying the Cow

IMAGE 01
The homepage for putlockerr.ac advertising unlicensed movies including *Deadpool, My Big Fat Greek Wedding 2,* and *The Man from U.N.C.L.E.*

But consumers download something else from putlockerr.ac besides free movies and/or television. From websites such as putlockerr.ac consumers are tricked into downloading malware. For example, when a consumer clicks to watch a movie, they are sent to a new screen in which they are told their video player is out of date and they must update it. The update, Digital Citizens' researchers found, is the malware delivery mechanism.



New update is avaliable for your computer
Your os might need MediaDownloader for HD Support
Please update Mac MediaDownloader to continue

install	Name	Version	Size
✓	Media Player	Mac OS X	0.7M

END USER LICENSE / TERMS OF SERVICE AGREEMENT IMPORTANT NOTICE - PLEASE READ THE FOLLOWING TERMS AND CONDITIONS OF USE CAREFULLY. THEY SHALL GOVERN YOUR USE OF THE VIDEODOWNLOADER SOFTWARE, SERVICE AND SITE. IF, AFTER READING THESE TERMS AND CONDITIONS OF USE, YOU WISH TO USE THE SERVICE AND SOFTWARE PLEASE INDICATE YOUR ACCEPTANCE HEREOF BY CLICKING "I AGREE" AT THE END.

1. TERMS AND CONDITIONS OF USE

The MediaDownloader application with respect to all product versions and version

Note: The version of your player on your system does not include the latest updates. To continue, download an updated version

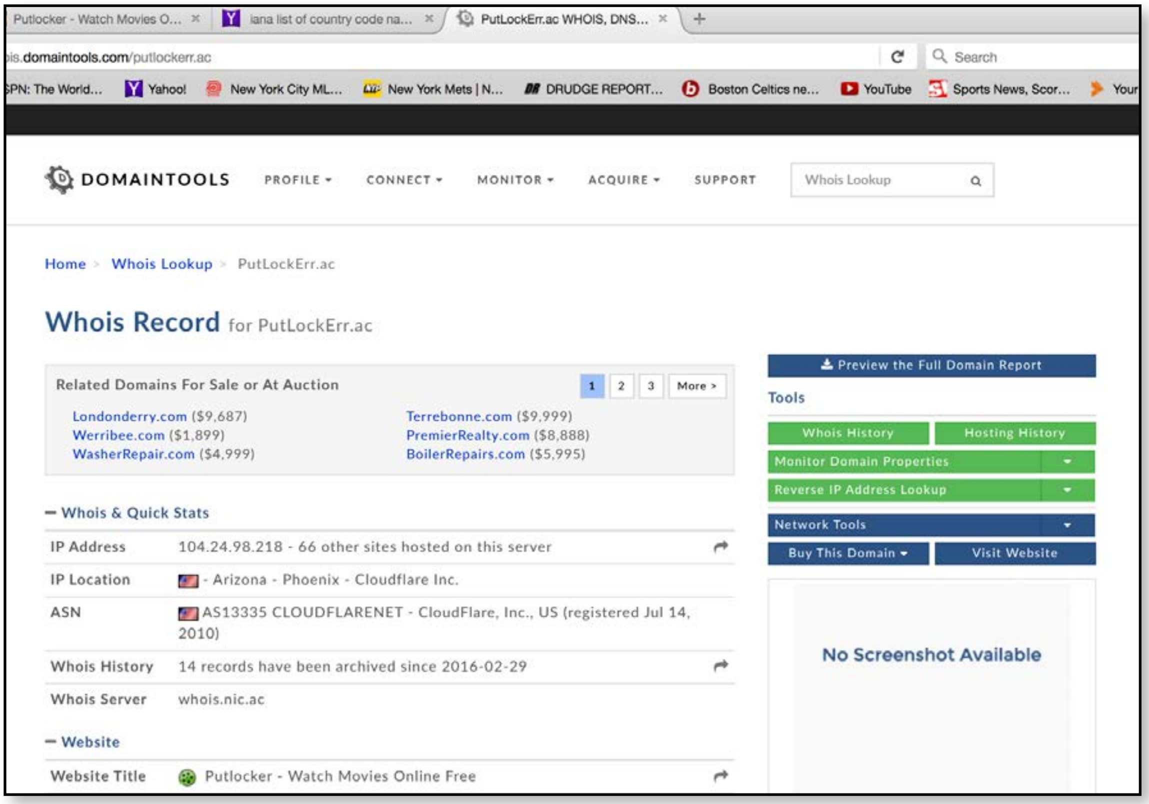
Installing takes under a minute - No restart is required

Install 1 Item
Privacy Policy • Terms & Conditions • Uninstall • Contact Us

IMAGE 02

Pictured is the software update prompt given to users when they click to watch a movie on putlockerr.ac. The update, Digital Citizens researchers found, is the malware delivery system.

But putlockerr.ac can't do this all itself. To be available to consumers online and deliver content with minimal interruption, a rogue website such as putlockerr.ac needs a company like CloudFlare. Here is the whois record that shows CloudFlare's support of the putlockerr.ac website.



Whois Record for PutLockErr.ac

Related Domains For Sale or At Auction

Londonderry.com ($9,687)
Werribee.com ($1,899)
WasherRepair.com ($4,999)
Terrebonne.com ($9,999)
PremierRealty.com ($8,888)
BoilerRepairs.com ($5,995)

– Whois & Quick Stats

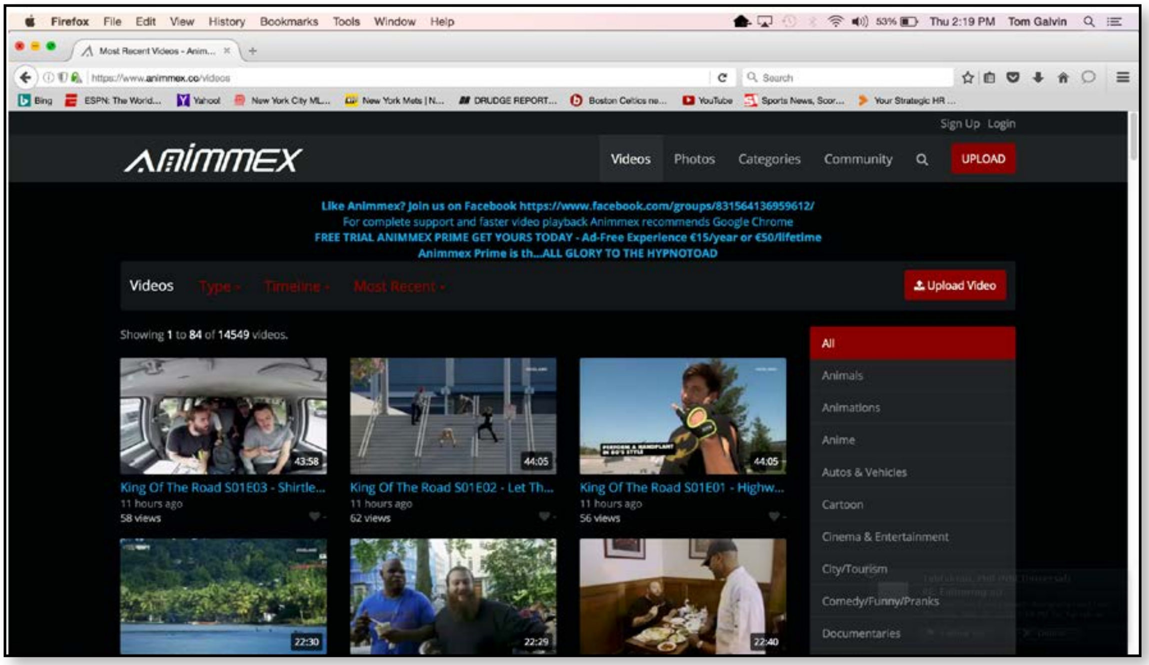
IP Address	104.24.98.218 - 66 other sites hosted on this server
IP Location	- Arizona - Phoenix - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - CloudFlare, Inc., US (registered Jul 14, 2010)
Whois History	14 records have been archived since 2016-02-29
Whois Server	whois.nic.ac

– Website

Website Title	Putlocker - Watch Movies Online Free

IMAGE 03

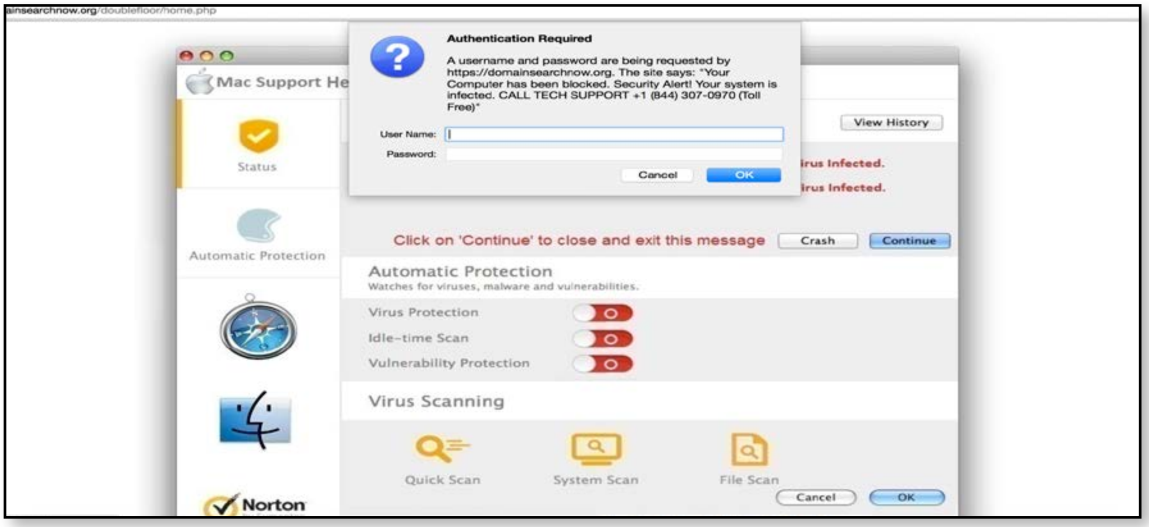
Another CloudFlare-supported website that poses dangers to consumers is animmex.co. That website offers TV shows and other pirated programs. But when you click on a link, it sends an "alert" that your computer may be infected and that you need to put in your user name and password – all common tactics by malware operators to gain your personal information to hack into your computer records.


Firefox File Edit View History Bookmarks Tools Window Help
Thu 2:19 PM Tom Galvin
Most Recent Videos - Anim...
https://www.animmex.co/videos
Search
Bing ESPN: The World... Yahoo! New York City ML... New York Mets | N... DRUDGE REPORT... Boston Celtics ne... YouTube Sports News, Scor... Your Strategic HR ...
Sign Up Login
ANIMMEX
Videos Photos Categories Community UPLOAD
Videos Type Timeline Most Recent
Upload Video
Showing 1 to 84 of 14549 videos.
King Of The Road S01E03 - Shirtle...
11 hours ago
58 views
King Of The Road S01E02 - Let Th...
11 hours ago
62 views
King Of The Road S01E01 - Highw...
11 hours ago
56 views
43:58
44:05
44:05
22:30
22:29
22:40
All
Animals
Animations
Anime
Autos & Vehicles
Cartoon
Cinema & Entertainment
City/Tourism
Comedy/Funny/Pranks
Documentaries

Like Animmex? Join us on Facebook https://www.facebook.com/groups/831564136959612/
For complete support and faster video playback Animmex recommends Google Chrome
FREE TRIAL ANIMMEX PRIME GET YOURS TODAY - Ad-Free Experience €15/year or €50/lifetime
Animmex Prime is th...ALL GLORY TO THE HYPNOTOAD

IMAGE 04

Here's the "alert" you get when you try to click on a program:



Authentication Required

A username and password are being requested by https://domainsearchnow.org. The site says: "Your Computer has been blocked. Security Alert! Your system is infected. CALL TECH SUPPORT +1 (844) 307-0970 (Toll Free)"

User Name:

Password:

Cancel OK

Click on 'Continue' to close and exit this message

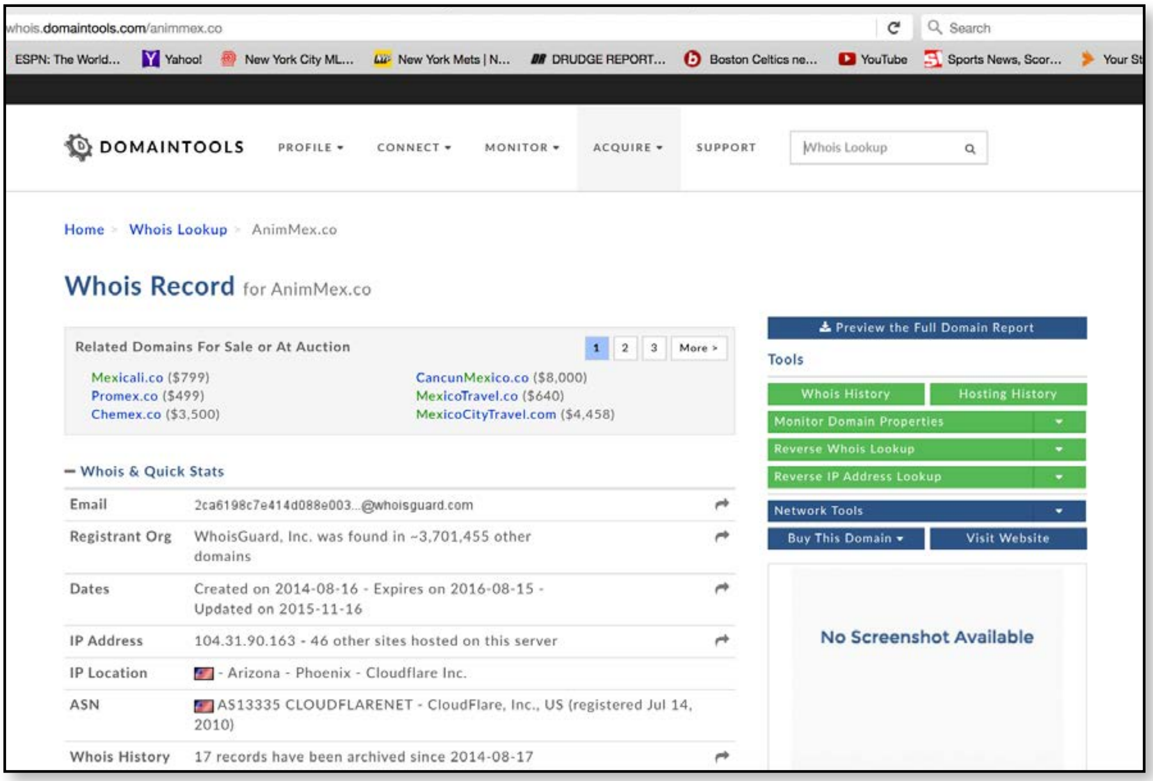
Automatic Protection

Watches for viruses, malware and vulnerabilities.

IMAGE 05

The scareware dialogue box prompt users of animmex.co are given when they click on a link in the hopes they will hand over their username and password. A common tactic employed by online criminals.

Here is the Whois record that shows that CloudFlare provides services to the website:


whois.domaintools.com/animmex.co
Search
ESPN: The World... | Yahoo! | New York City ML... | New York Mets | N... | DRUDGE REPORT... | Boston Celtics ne... | YouTube | Sports News, Scor... | Your St
DOMAINTOOLS
PROFILE ▾ | CONNECT ▾ | MONITOR ▾ | ACQUIRE ▾ | SUPPORT
Whois Lookup
Home > Whois Lookup > AnimMex.co

Whois Record for AnimMex.co

Related Domains For Sale or At Auction

Mexicali.co ($799)	CancunMexico.co ($8,000)
Promex.co ($499)	MexicoTravel.co ($640)
Chemex.co ($3,500)	MexicoCityTravel.com ($4,458)

– Whois & Quick Stats

Email	2ca6198c7e414d088e003...@whoisguard.com
Registrant Org	WhoisGuard, Inc. was found in ~3,701,455 other domains
Dates	Created on 2014-08-16 - Expires on 2016-08-15 - Updated on 2015-11-16
IP Address	104.31.90.163 - 46 other sites hosted on this server
IP Location	- Arizona - Phoenix - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET - CloudFlare, Inc., US (registered Jul 14, 2010)
Whois History	17 records have been archived since 2014-08-17

IMAGE 06

CloudFlare Response to DCA Findings

The Digital Citizens Alliance contacted CloudFlare via email to inform the company of the key findings from this report. A representative from CloudFlare's communications team responded:

"CloudFlare's service protects and accelerates websites and applications. Because CloudFlare is not a host, we cannot control or remove customer content from the Internet. CloudFlare leaves the removal of online content to law enforcement agencies and complies with any legal requests made by the authorities. If we believe that one of our customers' websites is distributing malware, CloudFlare will post an interstitial page that warns site visitors and asks them if they would like to proceed despite the warning. This practice follows established industry norms."

Hawk Host

According to its website, Hawk Host was founded in 2004 and provides shared hosting, reseller hosting, semi-dedicated and virtual hosting in Dallas, Los Angeles, Washington DC, Amsterdam, and Singapore.[7]

While Hawk Host offers customers services to combat malware and spam, it is actually hosting companies that spread infection among its viewers.

Among the websites Hawk Host was found to support was watchfreemovieonline.top, which was among the worst purveyors of malware found by RiskIQ when it conducted research for this report on how content theft websites are spreading infections. RiskIQ found that watchfreemovieonline.top's malware exposure rate was 32 percent – meaning consumers who went to the site had a 1 in 3 chance of infecting their computers.

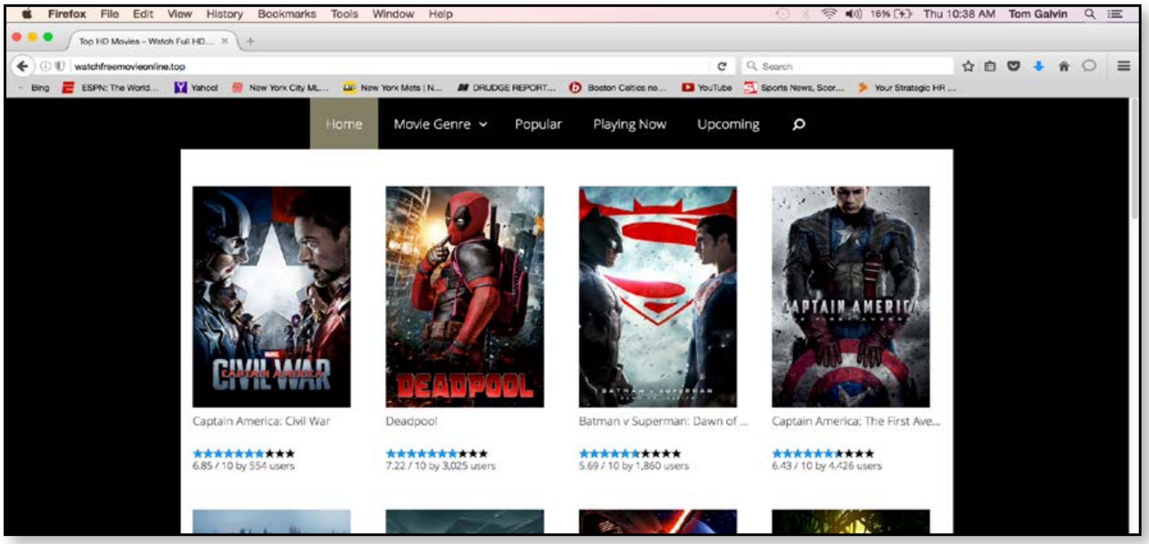

Firefox File Edit View History Bookmarks Tools Window Help
16% Thu 10:38 AM Tom Galvin
Top HD Movies – Watch Full HD...
watchfreemovieonline.top
Search
Bing ESPN: The World... Yahoo! New York City ML... New York Mets | N... DRUDGE REPORT... Boston Celtics ne... YouTube Sports News, Scor... Your Strategic HR ...
Home
Movie Genre
Popular
Playing Now
Upcoming
CIVIL WAR
CAPTAIN AMERICA
DEADPOOL
BATMAN v SUPERMAN
CAPTAIN AMERICA
Captain America: Civil War
6.85 / 10 by 554 users
Deadpool
7.22 / 10 by 3,025 users
Batman v Superman: Dawn of ...
5.69 / 10 by 1,860 users
Captain America: The First Ave...
6.43 / 10 by 4,426 users

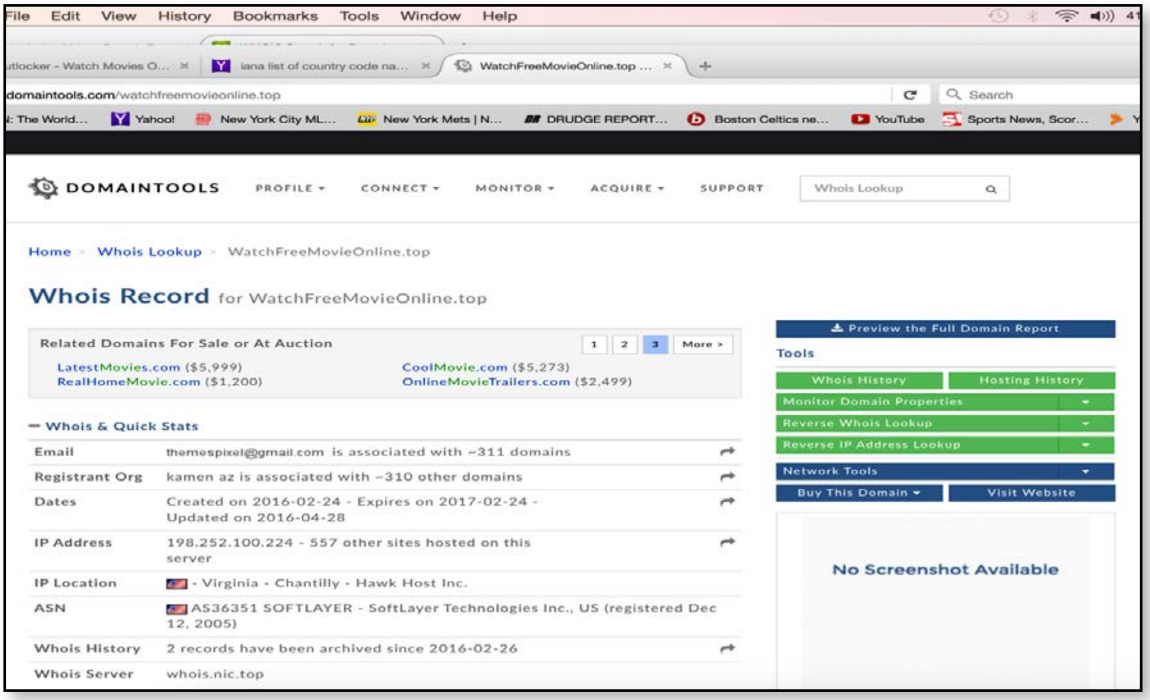
IMAGE 07

The homepage for watchfreemovieonline.top advertising unlicensed movies such as *Deadpool, Batman V Superman: Dawn of Justice, and Captain America: Civil War.*

[7] https://www.hawkhost.com/About

The website watchfreemovieonline.top was offering the movie "Captain America: Civil War" at least a day in advance of the film's release on May 6, 2016. Whether the movie was actually available on the site is unknown as content theft websites have dangled movies that are not available as a means to bait consumers to download malware.

Here's the Whois record of how Hawk Host provides essential services to the website.



Whois Record for WatchFreeMovieOnline.top

Related Domains For Sale or At Auction

LatestMovies.com ($5,999)
RealHomeMovie.com ($1,200)
CoolMovie.com ($5,273)
OnlineMovieTrailers.com ($2,499)

— Whois & Quick Stats

Email	themespixel@gmail.com is associated with ~311 domains
Registrant Org	kamen az is associated with ~310 other domains
Dates	Created on 2016-02-24 - Expires on 2017-02-24 - Updated on 2016-04-28
IP Address	198.252.100.224 - 557 other sites hosted on this server
IP Location	- Virginia - Chantilly - Hawk Host Inc.
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc., US (registered Dec 12, 2005)
Whois History	2 records have been archived since 2016-02-26
Whois Server	whois.nic.top

No Screenshot Available

IMAGE 08

Another content theft website that is notorious for exposing consumers to malware is movietubeonline.top - another Hawk Host client. According to RiskIQ, visitors to movietubeonline.top were exposed to malware during 73 percent of visits.

Notice that nearly every movie highlighted by the website is a first-run movie that is either in or was recently in the theaters. By offering Internet users first-run movies, it provides the perfect bait for malware operators to gain new victims.

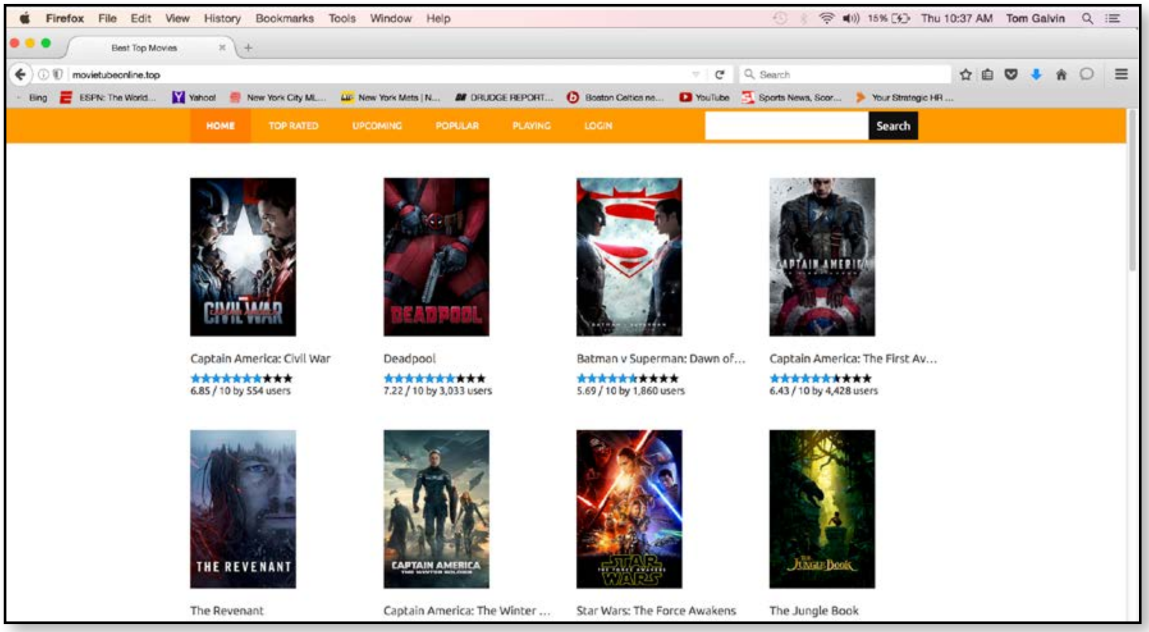
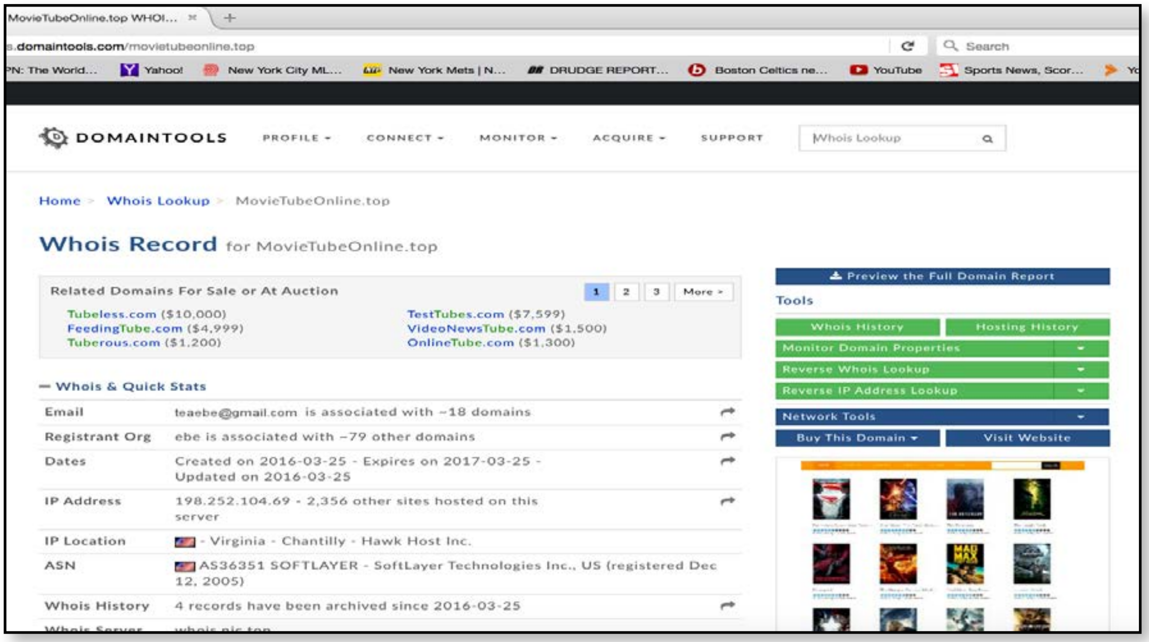


IMAGE 09

The homepage of movietubeonline.top advertising unlicensed movies including *The Jungle Book, Star Wars: The Force Awakens, and Captain America: Civil War.*

Here is the Whois record showing Hawk Host's role with movietubeonline.top:



Home > Whois Lookup > MovieTubeOnline.top

Whois Record for MovieTubeOnline.top

Related Domains For Sale or At Auction

Tubeless.com ($10,000)
FeedingTube.com ($4,999)
Tuberous.com ($1,200)
TestTubes.com ($7,599)
VideoNewsTube.com ($1,500)
OnlineTube.com ($1,300)

— Whois & Quick Stats

Email	teaebe@gmail.com is associated with ~18 domains
Registrant Org	ebe is associated with ~79 other domains
Dates	Created on 2016-03-25 - Expires on 2017-03-25 - Updated on 2016-03-25
IP Address	198.252.104.69 - 2,356 other sites hosted on this server
IP Location	- Virginia - Chantilly - Hawk Host Inc.
ASN	AS36351 SOFTLAYER - SoftLayer Technologies Inc., US (registered Dec 12, 2005)
Whois History	4 records have been archived since 2016-03-25
Whois Server	whois.nic.top

IMAGE 10

Hawk Host Response To DCA Findings

As with CloudFlare, the Digital Citizens Alliance contacted Hawk Host via email to inform the company of the key findings from this report.

Two Hawk Host employees, including the company's Chief Technology Officer, responded to the email:

"As part of our normal operating procedures we do investigate all valid abuse complaints/reports sent to our abuse team. After investigation if the reported sites are in violation of any US laws or our TOS/AUP we will forward the complaint to our customer for resolution. If after a set period of time (generally 24-48 hours) our customer does not resolve the reported issue we'll suspend their website so the content is no longer accessible.".

–Brian F.
Operations Manager, Hawk Host

"While we actively scan for malware on accounts one thing that's difficult for us (and other providers) is actively detecting phishing websites before they get used. Currently we rely on reports sent to us (phishing websites are suspended and or terminated immediately). In the last two years we also proactively invested in enterprise E-Mail filtering for all outbound e-mail on our network to help curb UCE which often contains malicious content."

–Cody Robertson
Chief Technical Officer, Hawk Host

After an exchange of information, Hawk Host agreed the sites did violate their policies and told Digital Citizens the sites would come down. Cody Robertson said the sites "clearly violate our TOS / AUP." He did add that it would be impossible for Hawk Host to audit all of the 100,000-plus sites they host and that they would continue to rely on abuse reports. Hawk Host's swift action is an encouraging sign and Digital Citizens is hopeful that the company will continue to take steps to protect Internet users from malicious content.

Additionally, Digital Citizens' researchers and Hawk Host's staff are scheduling a briefing to further discuss the findings from this report.

What Can be Done?

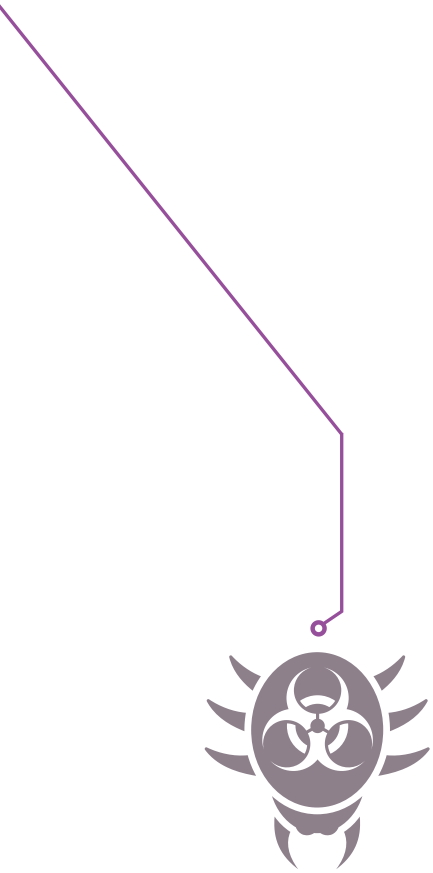
When authorities try to track down online criminal operators, more often than not they are frustrated to find they are based overseas. But at times the authorities have found that outreach to “facilitators”- the companies that enable websites to process payments or market themselves-is helpful because these companies don’t want to be associated with illicit or dangerous activities.

For example, payment processors such as PayPal, and more recently, Visa and MasterCard, have done a commendable job refusing to provide payment services to online criminals. In other instances, companies have been charged with helping criminals – most notably FedEx which faced criminal charges in 2014 that it allegedly aided online pharmacies ship illegal drugs.

In the cases of Hawk Host and CloudFlare, both have offices in the United States, and there is nothing to stop federal or state authorities from inquiring whether the company knowingly aids content thieves and malware peddlers.

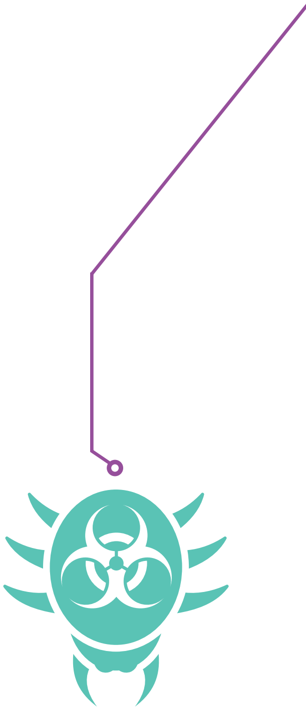
Government can also take an active role in raising awareness among consumers about the malware dangers associated with visiting content theft websites. In particular, the Federal Trade Commission has been a tireless advocate on behalf of consumers and could play an appropriate role here warning consumers. In addition, state Attorneys General – who often serve as the de facto consumer protection arm in their respective states – can play a strong role in warning their consumers.

We remain at an early stage of building consumer awareness about the dangers of malware – both how it can affect a person’s identity or financial situation and also what activities can expose consumers to harm. Digital Citizens intends to be a voice to raise that awareness, and hopes that government and other organizations play the vital role they can in protecting citizens against a very 21st century risk.



About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer- oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on 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. Visit us at digitalcitizensalliance.org