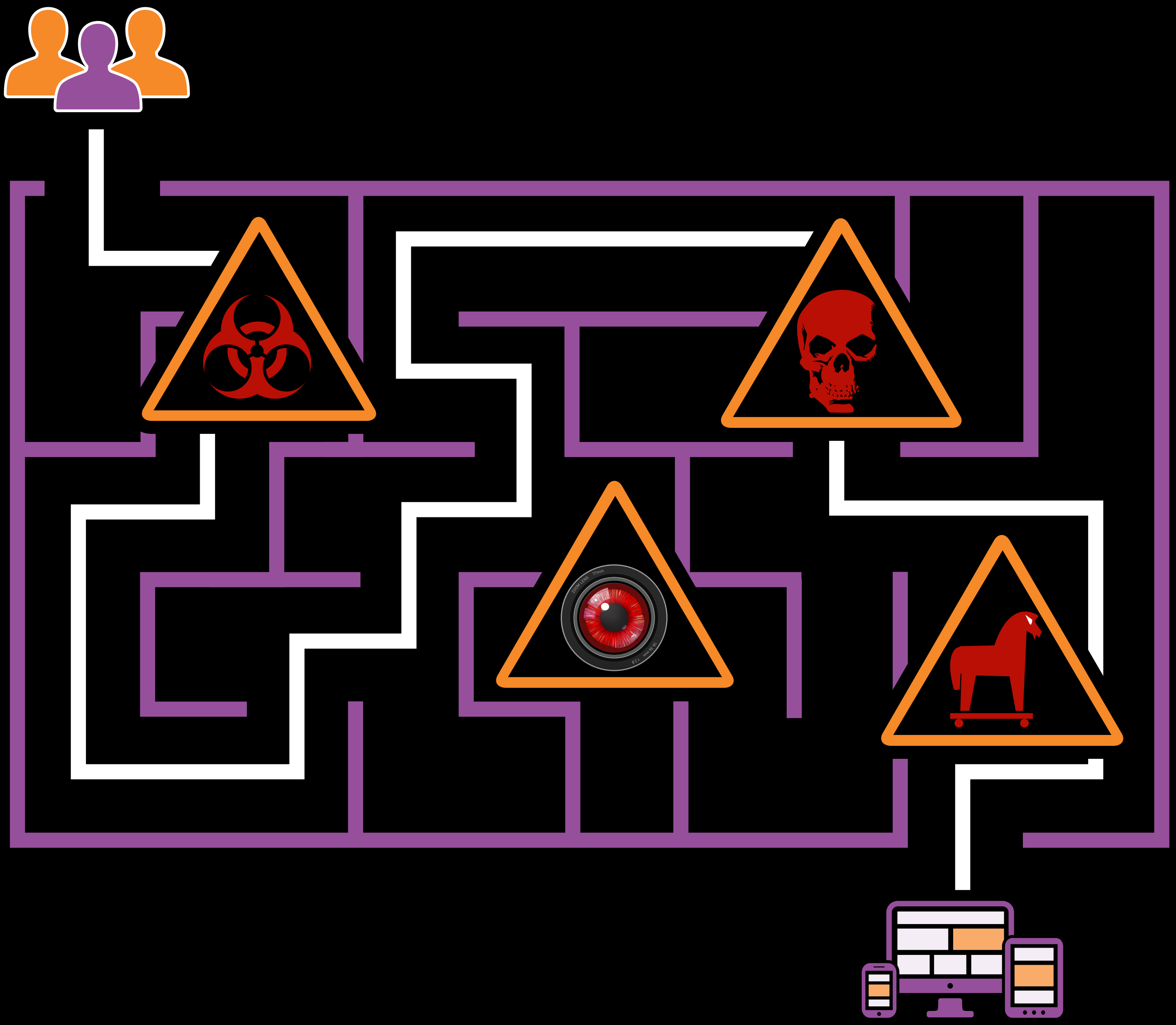
Trouble in Our Digital Midst

How Digital Platforms Are Being Overrun by Bad Actors and How the Internet Community Can Beat Them at Their Own Game



June 2017

digitalcitizens alliance

Table of Contents

Executive Summary

Cybercrime has shaken American's trust in the Internet. Digital Citizens Alliance polling shows that illegal and illicit activities online threaten consumers' faith in some of the largest and most profitable companies. These are just some of the responses we saw just this past April:

- 64 percent of Americans said their trust in digital platforms has dropped in the last year.
- When asked, "In your opinion, are digital platforms doing enough to keep the Internet safe and trustworthy, or are do they need to do more?" a staggering 75 percent responded that they need to do more to keep the Internet safe.
- Asked what role they want digital platforms to play when it comes to illicit activities, 59 percent responded that, "They should monitor their digital platforms to find these activities and remove them when they find them." That compares to 20 percent who said they shouldn't have to monitor but just remove them when notified and just 6 percent who said they should not remove them at all.
- Nearly three-quarters of respondents see the pairing of brand name advertising with offensive online content – like ISIS/terrorism recruiting videos – as a threat to the continued trust and integrity of the Internet.
- 64 percent of Americans say that the Fake News issue has made them less likely to trust the Internet as a source of information.

Consumers can take some comfort knowing that Facebook, Google and Twitter have taken important first steps to try to regain control of Fake News. Facebook, in early May, took another important step by hiring 3,000 people to monitor videos posted on the social network for violent activities. This action shows Facebook takes seriously the potential harm bad actors pose to Internet safety and consumers in particular.

We know it is complicated balancing concerns over free speech and responsible behavior, so it will take a while for the platforms to get this problem solved, but these are good first steps. However, we are at only the beginning of thinking through other kinds of illicit and illegal activity happening on digital platforms right now that we must gain or re-gain control over, such as:

- The sale of illicit goods such as drugs and stolen credit cards as well as new issues such as illicit streaming devices - which are a new way to traffic in stolen content - as well as an insidious yet effective delivery mechanism to infect computers with malware such as Remote Access Trojans.

- The abuse of advertising and brands to create an aura of credibility on illegal or sketchy activities. That includes the rise of objectionable content that is incentivized by brand name advertising. In 2015, when CNN found Budweiser ads showing up next to terrorist recruiting videos on YouTube, it was clear a problem existed. Still, it took nearly two years and hundreds of advertisers vowing to boycott YouTube advertising until Google addressed the advertisers' question: why are our ads showing up next to content pushing illicit and/or illegal activity? It also includes the $200 million in advertising that shows up on illegal content theft websites often unbeknownst to the brands.
- The new way in which hackers are using these content theft websites to lure consumers and then infect their computers. RiskIQ found 1 in 3 of these websites exposed consumers to malware, which can lead to identity theft, financial loss, ransomware and the so-called slaving discussed below to take over the computer cameras of young girls and boys.
- Our privacy across the myriad of platforms and providers who deliver content and services to us. Nearly 40 percent of Americans report that their online privacy has been violated at some point. Americans deserve confidence that they know what their privacy expectations should be – and they are met by all companies.
- The way certain users are taking advantage of the lack of policing in many of these platforms to showcase live sexual assaults, murders, and other illegal conduct.

75 percent said that when they see things such as a scam, Fake News, pirated content or illicit drugs for sale on a platform, they think "less of them as a reputable platform and a company."

Americans are looking for digital platforms to step up and help protect them. Specifically, Americans want digital platforms to take a more proactive and hands-on approach to protecting them – like they have done recently by taking steps to identity and warn users about Fake News. Consumers want to see more of that approach.

Digital Citizens wants to start this report by stating that most companies want to do the right thing and have good intentions. This report is not looking to criticize or call out: it wants to put a spotlight on emerging issues, look at potential solutions and hopefully spur a thoughtful discussion about the future of digital platforms. At the same time, digital platforms over the last year have shown a new willingness to intervene, impact, or even alter the content on their platforms on issues of national importance. Given that they have opened the door, they must take a fresh and holistic look at all illicit goods, services, content, and behavior on their platforms. The response, "we're just a platform," clearly is not the answer in response to the Fake News problem and objectionable content that has brand name advertising imprinted upon it, and it shouldn't be the answer when it comes to stolen credit cards, counterfeit goods, illicit drugs or pirated movies, TV shows and music, or the violation of our young.

We need a way forward that can restore trust that criminals and bad actors won't continue to have the upper hand. That means having faith that a combination of law enforcement, hands-on efforts by digital platforms, a new commitment by "commerce facilitators" such as search engines, the domain industry, payment processors, and delivery services to avoid assisting criminals and increased awareness by consumers will enable all of us to get the upper hand against those who wish to do us harm. What this report explores is what should be the "Platforms Principles" that guide digital platforms so Americans can once again trust the Internet.

Trouble in Our Digital Midst

Undermining Trust; Americans Want More Monitoring and Action to Stop Bad Actors and Criminals from Overrunning Popular Apps and Websites

64%

of consumers have **lost trust in digital platforms** over the past year.

3 in 4

consumers think less of a platform when they see:

- Scams
- Fake News
- Pirated Content
- Drugs for Sale

72%

percent say the pairing of brand name advertising with offensive online content like ISIS/terrorist recruiting videos **is a threat to their continued trust in the internet.**

60%

say **digital platforms should be responsible** for what people do on them.

3 in 4

consumers say **digital platforms need to do more** to keep the internet safe.

digitalcitizens alliance

Results from Digital Citizens Alliance poll conducted from April 12 – May 17 on Survey Monkey. There were 1,240 responses to the poll. The margin of error is ±/-3.6. Percent.

Visit **www.digitalcitizensalliance.org** to learn more.

The Scope of the Problem

By any measure, digital and social platforms have become an integral part of our society, and arguably the most important development in the still brief history of the Internet. For a moment, consider how they have transformed the way we live, work, play, and connect. The combination of Big Data, digital platforms and smart phones has:

- Transformed the way retail goods are bought and sold (Amazon).
- Changed the way we get around (Uber and Lyft) and how we decide to travel (Airbnb, Homeaway, Expedia).
- Altered how we market and connect with each other (Facebook, Google, Facetime).
- Evolved the way we network with colleagues and potential employers (LinkedIn, Network After Work).
- Reshaped how we are entertained (iTunes, Spotify, Hulu, Netflix).
- Revised how we approach fundraising and charitable giving (GoFundme).
- Localized international connections and increased our privacy conscience (WhatsApp, Viber).

Only two decades or so ago, none of these companies even existed. Combined with high bandwidth penetration and the awesome transformational power of the smartphone, the so-called Apps Economy has created more than 1.7 million jobs (and counting) in less than a decade (according to the Progressive Policy Institute).

But the skyrocketing amount of illegal and/or illicit activity online threatens all this growth and the potential for opportunity on the Internet. Time and time again, examples have surfaced that point to criminals and bad actors exploiting digital platforms to mislead, defraud, and steal from Americans. It's reached a point where we now face the risk that our digital platforms will be overrun by thieves, con artists, abusers and hackers. In just the last six months, we have seen:

- A presidential election turned upside down by a proliferation of Fake News that sowed uncertainty, fear, and hatred into our national debate.

- The increased attention on how brand advertising is increasingly showing up on inappropriate and objectionable content spouting hate speech and criminal acts – catching major brands off guard and in embarrassing positions.
- The continued sale of narcotics, stolen credit cards, stolen goods, and stolen content on our most popular social platforms.
- The rise of fraudulent charity pleas on popular platforms.
- The persistent dissemination of videos on how to sexually slave a teen.
- The Federal Trade Commission warn consumers for the first time that so-called pirate websites were exposing consumers to malware.

Over the last few years, the Digital Citizens Alliance has looked at many of these issues. We have demonstrated the ease by which dangerous narcotics and steroids can be bought by teens on the Internet, including:

- The robust market for millions of stolen credit cards.
- How 1 in 3 content theft websites expose consumers to malware.
- How these hackers use it to take over the computer cameras of young girls and boys to sextort them.
- The need for a national discussion on a thoughtful way forward to protect Americans' privacy.

And behind all of this are hackers looking for the opportunity to strike: either by stealing huge tranches of personally identifiable information such as credit card records or luring consumers to content theft websites so they can infect their computers with malware and open every door of the digital home.

If we don't get a handle on the way bad actors are trying to turn these platforms into their own version of the Dark Web, we risk hindering its growth and appeal to developers who work on it and consumers who use it.

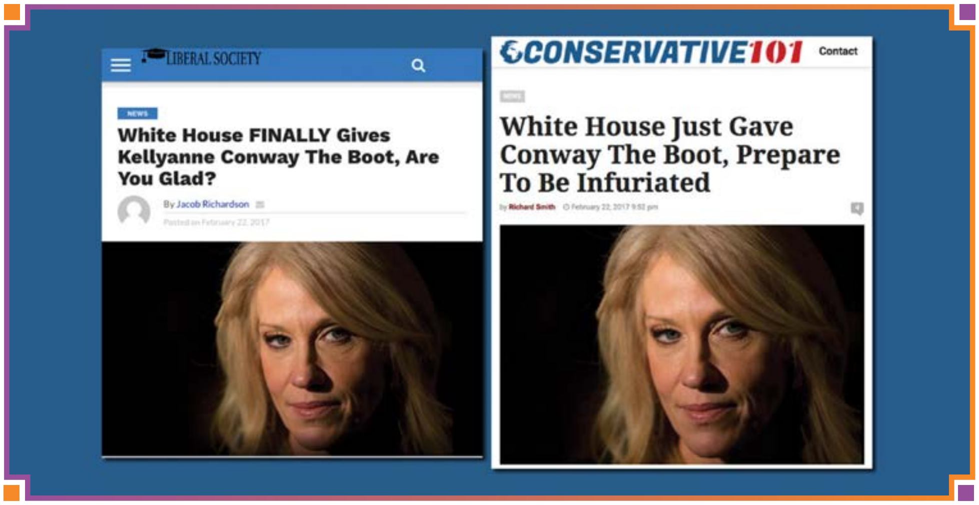
Fake News-Progress and a Template for Other Issues

In its "Fake Epidemic" report earlier this year, Digital Citizens labeled Fake News a cancer that has a corrosive effect on the Internet. The emergence of Fake News has led the majority of Internet users to report that it's made them less likely to rely on the Web as a reliable source of online news and information. This manipulation – whether to influence elections, steal money, or take control of your computer – is eroding trust because sometimes it is difficult to know whether a news story is fake or not.

And while most of the attention has been on Facebook, the reality is the problem goes well beyond that one platform. Digital Citizens acknowledges how difficult this issue can be. It has pushed these platforms out of their philosophical comfort zone of avoiding being a policeman for what appears on their platforms. When confronted with other issues – such as content theft or hate speech, platforms like Google say they rely on their user community to point out bad actors. But in the case of Fake News, these platforms have gone a step further by taking a more active role, even inviting experts to work with them.

We applaud digital platforms such as Google, Facebook, and Twitter for taking steps to identify and eradicate fake news on their sites – and urge them to use it as a template for how to combat other issues, such as content theft, stolen credit cards, the sale of illicit drugs, and the showcasing of assaults on innocent victims.

Digital Citizens has cited numerous examples of how Fake News is exploited for financial gain – in some cases using the same general story but creating two angles – one for liberal audiences and the other for conservatives.



LIBERAL SOCIETY

NEWS

White House FINALLY Gives Kellyanne Conway The Boot, Are You Glad?

By Jacob Richardson

Posted on February 22, 2017

CONSERVATIVE101 Contact

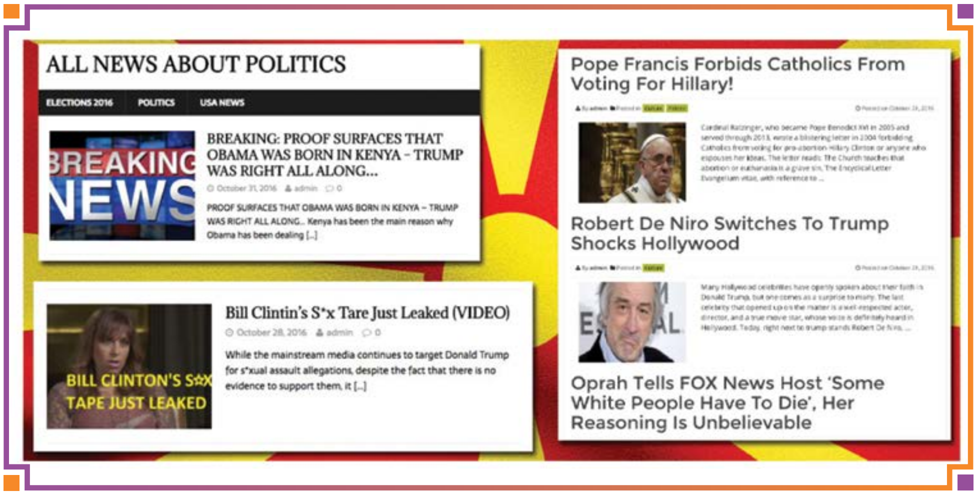
White House Just Gave Conway The Boot, Prepare To Be Infuriated

by Richard Smith February 22, 2017 9:52 pm

IMAGE 01

Source: BuzzFeed, February, 2017.

The DCA report also cited a Buzzfeed investigation that found how 140 political websites promoting mostly pro-Trump conspiracy theories all emanated from the town of Veles in Macedonia. DCA is curious whether or not the FBI's investigation into alleged Russian interference in the election will dig up additional information on who was behind these websites.



ALL NEWS ABOUT POLITICS

ELECTIONS 2016 | POLITICS | USA NEWS

BREAKING: PROOF SURFACES THAT OBAMA WAS BORN IN KENYA – TRUMP WAS RIGHT ALL ALONG...

October 31, 2016 admin 0

PROOF SURFACES THAT OBAMA WAS BORN IN KENYA – TRUMP WAS RIGHT ALL ALONG... Kenya has been the main reason why Obama has been dealing [...]

Bill Clintin's S*x Tare Just Leaked (VIDEO)

October 28, 2016 admin 0

While the mainstream media continues to target Donald Trump for s*xual assault allegations, despite the fact that there is no evidence to support them, it [...]

Pope Francis Forbids Catholics From Voting For Hillary!

Cardinal Ratzinger, who became Pope Benedict XVI in 2005 and served through 2013, wrote a blistering letter in 2004 forbidding Catholics from voting for pro-abortion Hillary Clinton or anyone who espouses her ideas. The letter reads: The Church teaches that abortion or euthanasia is a grave sin. The Encyclical Letter Evangelium vitae, with reference to ...

Robert De Niro Switches To Trump Shocks Hollywood

Many Hollywood celebrities have openly spoken about their faith in Donald Trump, but one comes as a surprise to many. The last celebrity that opened up on the matter is a well-respected actor, director, and a true movie star, whose voice is definitely heard in Hollywood. Today, right next to trump stands Robert De Niro. ...

Oprah Tells FOX News Host 'Some White People Have To Die', Her Reasoning Is Unbelievable

IMAGE 02

Source: The "Fake" Epidemic, March, 2017

The disturbing issue is that half of Americans report they can't necessarily tell whether some news stories are fake or not. But the impact is real: Sixty-one of Americans said, in a research survey conducted by DCA in February, that Fake News has made them less likely to rely on the Internet as a source of news and information.

Later in this report, Digital Citizens proposes a neighborhood watch approach that would combine a greater level of diligence by platforms and users to identify bad actors. That information would then be passed along to other users and platforms through a clearinghouse that could send out alerts.

Content Theft: How Bad Actors Make Millions by Hacking Consumers

For two decades, the narrative around content theft has been this: creators complain that criminals are ripping them off by stealing their movies, TV shows, music and games and offering them to online users. And some tech giants and other advocates fire back by saying the problem would go away if the creative industry updated their business model – while others simply believe that all content deserves to be "free."

But over the last two years the risks have grown exponentially – and it's gotten the attention of government and law enforcement. While we've seen new efforts from federal and state regulators to crack down on criminal activity online, digital platforms that have been reluctant to delve into this issue have shown some willingness to move toward greater efforts to stop the content thieves.

The brewing sea of change seem to be the result of a growing concern about a new threat to consumers: criminals using content theft websites to lure consumers to their websites so they can infect their computers with dangerous malware. The danger is significant: 1 in 3 content theft websites expose consumers to malware just by visiting them, according to research by the security group RiskIQ. Consider this: Internet users who visited content theft sites were 28 times more likely to get malware from these sites than from mainstream websites or licensed content providers.

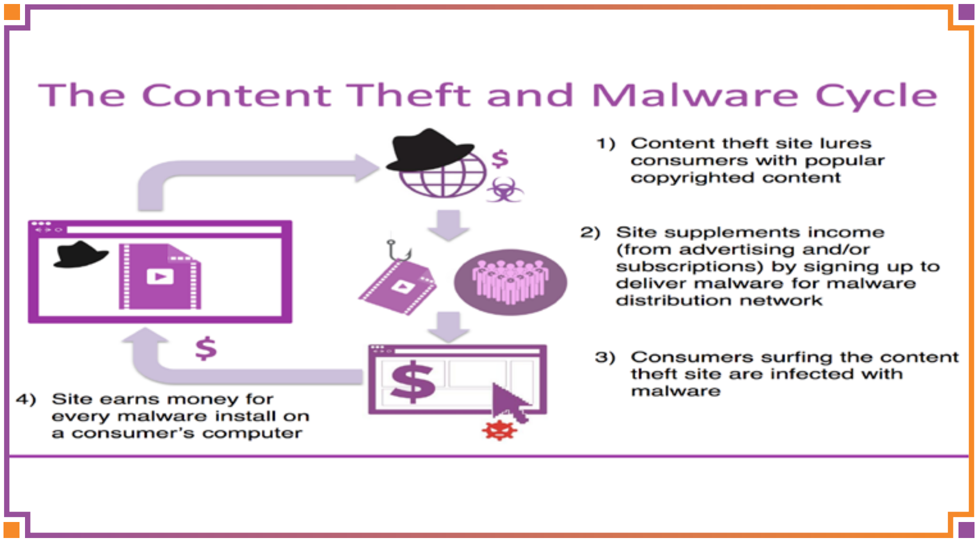
Once infected, criminals use the malware to:

- Steal ID and financial information.
- Engage in ransomware.
- Take over the video cameras of teen girls and boys (called slaving, Remote Access Trojans enable hackers to control the cameras without the teens' knowledge).

Just like Fake News, this is big business. The RiskIQ research found that piracy/malware is bought and sold between pirates and hackers on the dark web: this is a $70 million-plus business. Take a moment to think about that – if hackers are paying content theft websites $70 million to drop malware on their sites that infect visitor computers, how much are they making?

By penetrating the crime forums to document how hackers and malware developers work together, RiskIQ laid out both how the pirates and hackers lure consumers so they can infect their computers and the pricing that serves as the bargaining template among the criminals.

Here is the approach the hackers use to lure and infect consumers:



The Content Theft and Malware Cycle

1) Content theft site lures consumers with popular copyrighted content

2) Site supplements income (from advertising and/or subscriptions) by signing up to deliver malware for malware distribution network

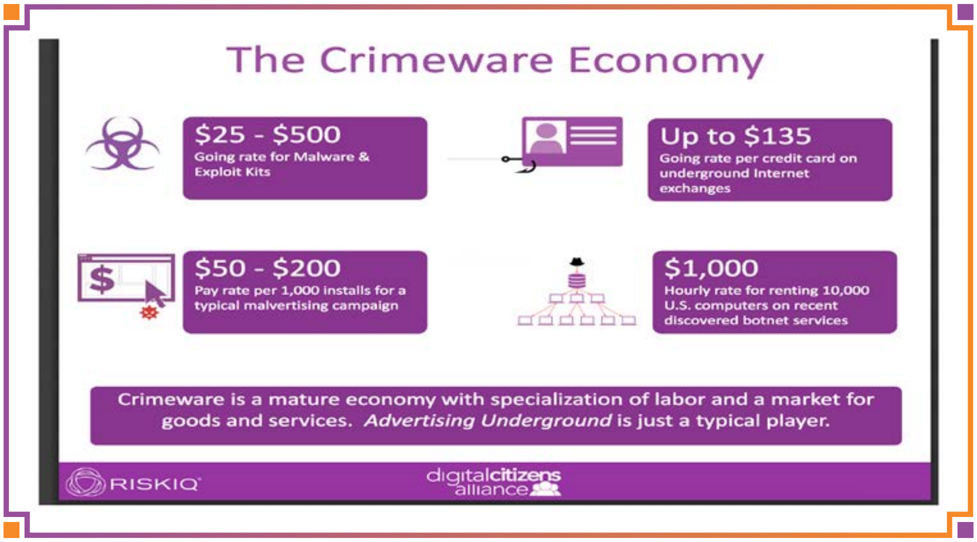
3) Consumers surfing the content theft site are infected with malware

4) Site earns money for every malware install on a consumer's computer

IMAGE 03

Source: Digital Citizens and RiskIQ Digital Bait Presentation, December, 2015

And this was the financial "menu" that hackers offered to entice content theft websites owners to allow them to put malware on the websites so they could infect the computers of visitors tempted by free content.



The Crimeware Economy

$25 - $500
Going rate for Malware & Exploit Kits

Up to $135
Going rate per credit card on underground Internet exchanges

$50 - $200
Pay rate per 1,000 installs for a typical malvertising campaign

$1,000
Hourly rate for renting 10,000 U.S. computers on recent discovered botnet services

Crimeware is a mature economy with specialization of labor and a market for goods and services. *Advertising Underground* is just a typical player.

IMAGE 04

Source: Digital Citizens and RiskIQ Digital Bait Presentation, December, 2015

The clear takeaway from this is that these are organized criminals – with business models, investments and an effective network – who are targeting unknowing consumers who really don't stand a chance.

But now law enforcement and consumer protection agencies are paying attention. In an alert called "Free Movies, Costly Malware," the Federal Trade Commission warned consumers in April 2017 about how bad actors are using these websites to infect consumers' computers. Here is what the FTC wrote: "If the something is a site or app offering free downloads or streams of well-known movies, popular TV shows, big-league sports, and absorbing games, the hidden cost is probably malware. Sites offering free content often hide malware that can bombard you with ads, take over your computer, or steal your personal information. We recently downloaded movies from five sites that offered them for free. In all five cases, we ended up with malware on our computer."

And it's not just the FTC taking action. More than a dozen state attorneys general are warning their constituents about the dangers that content theft websites pose to consumers. We are faced with a serious, long-term threat to millions of Internet users and consumers, and it will take a long-term effort to stop them.

Our best hope is both greater coordination among law enforcement and digital platforms – for example when a digital pirate is caught on Facebook, all other platforms should be alerted to be on the lookout for him or her so they can take action to block the pirate quickly.

The most effective approach is raising public awareness. In a December 2015 research survey, Digital Citizens found that 63 percent of Americans aged 18-29 years old would "definitely steer clear" of content theft websites if they thought those sites would expose them to malware. This is telling because it is that age group that is most likely to visit content theft websites without thinking through the impact of visiting unsavory sites. That is why the public awareness efforts of the FTC and state attorneys general are so vital.

Among the central tenets of that awareness campaign should be two issues that hit home for young Americans and parents who run a small business.

The so-called "slaving" issue is a disturbing trend because the camera on your computer, when hacked, can become a tool to spy on you in the privacy of your own home. And it's easy. And it can happen to anyone. In 2013, it happened to Cassidy Wolf just as she was getting ready to compete in the Miss Teen USA pageant. A hacker took control of her computer's webcam and took private pictures of her in her bedroom as part of what is commonly called a "sextortion" attempt. Miss Wolf would go on to win the Miss Teen USA pageant and tell her story to the world. "I had not one clue of having someone watching me," she told Digital Citizens. "It never passed my mind for the entire year." As is common with these slaving hackers, they sextort numerous teens at any given time.

The other disturbing development is ransomware. According to security firm Sonic Wall, in 2016 there were 638 *million* instances of ransomware, which is when a hacker takes over or locks a computer until the computer's owner pays a ransom to the criminal to give back control. Because hackers are overseas and out of the reach of U.S. law enforcement, many are forced to pay it. Small businesses are a popular target because they usually don't have the expertise or money for strong security systems and they can go out of business quickly if their systems are down.

Perhaps most alarming, the Dark Web – the shadowy marketplace for illicit goods and services – has become a hub for content theft and malware. As noted above, RiskIQ penetrated Dark Web forums and found hackers and criminals openly bargaining over the prices for malware and the number of computers the viruses would infect.

Given the seriousness of the issues, and challenges from hackers and criminals being outside the United States, we have to as an Internet community invest more time and money warning consumers. This should be a collaborative effort by all stakeholders – law enforcement, consumer protection agencies, consumer groups, small business advocacy organizations, and those operating the digital platforms themselves.

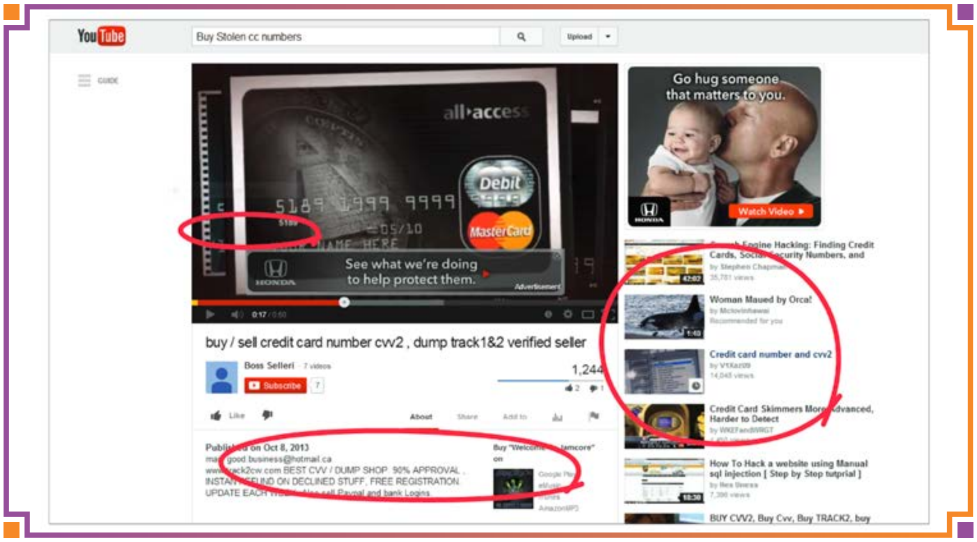
The Veneer of Credibility: Brand-Name Ads on Illicit Websites

Advertising has always been the lifeblood of sports, news, and entertainment programming. Whether it's iconic ads during the Super Bowl or short ads prior to online videos, we understand the content we view doesn't come for free. Without advertising (or a subscriber fee) there would be no sports, entertainment, or other programming.

But brand advertising is also being distorted to give the aura of respectability to shady activities. Or, in some other instances, its appearance next to offensive content is simply outrageous.

In 2015, a public furor erupted over Budweiser ads showing up next to terrorist recruiting videos on YouTube. And it wasn't just Budweiser: ads for Aveeno (featuring Jennifer Aniston), Secret, and even the NYC Police Department appeared on ISIS videos.

In other instances, brand name advertising enhanced the "credibility" of illicit activities such as the sale of stolen credit cards, counterfeit passports or driver's licenses, narcotics without a prescription, underage escort services, and content theft.



buy / sell credit card number cvv2 , dump track1&2 verified seller

Published on Oct 8, 2013
ma good business@hotmail.ca
www.track2cw.com BEST CVV / DUMP SHOP 90% APPROVAL , INSTANT REFUND ON DECLINED STUFF, FREE REGISTRATION UPDATE EACH WEEK Also sell Paypal and bank Logins

Buy "Welcome ... Hardcore" on

Search Engine Hacking: Finding Credit Cards, Social Security Numbers, and
by Stephen Chapman
35,781 views

Woman Maued by Orca!
Recommended for you

Credit card number and cvv2
14,043 views

Credit Card Skimmers More Advanced, Harder to Detect
by WKEFandWRGT

How To Hack a website using Manual sql injection [Step by Step tutprial]
7,398 views

BUY CVV2, Buy Cvv, Buy TRACK2, buy

IMAGE 05

Source:
Digital Weeds: How Google Continues to Allow Bad Actors to Flourish on YouTube,
March, 2014

These ads appear because of a breakdown in the advertiser system. And it will take stepped up efforts by brand advertisers, the ad networks that work to place ads, and the digital platforms that rely upon them to remedy the problem. On some of the larger digital platforms, the platforms own the ingestion, placement, and delivery vehicles altogether.

In recent weeks, faced with an advertising boycott by dozens of brand owners – among them McDonald's, AT&T, L'Oreal - over their ads appearing around objectionable content, Google announced steps to address the issue. Promising "a tougher stance on hateful, offensive and derogatory content," Google has imposed new controls and rules to make sure content is "advertiser friendly." It has also set some criteria for 10,000 views on YouTube videos before it's eligible for advertising.

The steps are new, so it will take some time to determine if they are effective, but the advertising giant deserves some credit for acting – even if it took several years to do so. And again, these laudable steps are proof that Google and other digital platforms can discard their "hands-off" policy on what appears on their platforms when they choose to do so.

But brand name advertising next to illicit content and websites online is still a $200 million-plus business. Addressing that will take a holistic approach by the advertising networks and digital platforms. A study two years ago by Digital Citizens Alliance and MediaLink found that 1 in 3 large content theft websites featured premium advertising. Seventy-two percent of Americans said this issue is a threat to trust in the Internet. Efforts that have been made by the advertising ecosystem can be trusted through the Trustworthy Accountability Group, which is a cross-advertising industry initiative to eliminate fraudulent digital advertising traffic, combat malware and identify and fight ad-supported Internet piracy.

Though today the advertising networks may strive to isolate bad actors willing to look the other way at illicit content, digital platforms could share information by collaborating about bad actors and refusing to include their content on their platforms. This neighborhood watch framework is detailed below, and while it could have challenges, it at least would negate bad actors' ability to hop from platform to platform.

Americans see it as a group problem that needs a group solution. Asked who should be responsible for monitoring where ads are placed so they don't appear on hate speech or illegal activities, they placed the responsibility in this order: digital platforms, the advertising networks and the advertiser themselves. Only 1 in 20 Americans said no one should be responsible for monitoring where ads are placed.

The Illicit Market: Combatting the Sale of Illegal Goods and Services

When people think of the sale of illicit goods and services online, they may think of the Dark Web, the shadowy marketplace where everything from escorts, drugs, and murder-for-hire can be bought and sold.

But in fact, illicit goods and services end up being sold on mainstream digital platforms all the time. Everything from stolen credit cards, counterfeit goods, illicit drugs, sex slaves, and stolen content have been peddled on social media and online retail websites.

And it's a complicated issue for the digital platforms because the bad actors can come and go, popping up when they are left alone only to disappear when they are scrutinized. In this way, these operators are no different than the criminals who move from street corner to street corner any time the local police pay attention to them. That was certainly the case with Google several years ago. Google allowed some overseas operators to illegally market prescription drugs in the United States. After that crackdown – which cost Google $500 million in a government fine – those drugs were no longer showing up on Google proper, but illicit drugs – painkillers and steroids – popped up for sale on YouTube. Once those sales were scrutinized, Google took some steps to remove them from YouTube.

For as long as there is a free market, there will be underground sale of illicit goods and services. But clearly more can be done to make the Internet a safer place, and turn back the tide against the bad actors who have gained the upper hand due to a lack of coordinated enforcement by the digital platform industry.

Americans are under siege. Last summer, Digital Citizens reported that nearly half of Americans said they had been tricked or defrauded online. That includes 1 in 5 Americans who reported that they have purchased something online, but never received it nor got a refund of their money.

Part of the issue is the growth of illicit goods and services for sale. In a way it's an extension of the "broken window theory" – that is, a breakdown in the maintenance of the safety of a neighborhood contributes to the growth of social disorder, crime and ultimately the decline of the area.

When illicit goods and services are sold on mainstream websites, it gives bad actors a license to use them as well to trick and defraud consumers. The link between content theft and malware is not an accident, but rather the natural extension of bad actors building on their illicit activities.

For that reason, digital platforms must take a stand against the sale of illicit goods and services on their platforms. That includes stolen credit cards, illegally sold narcotics and steroids, counterfeits, and content theft. It's in the interest of the digital platforms. Two years ago, Etsy's stock plunged over reports that as many as 2 million items for sale on the platform were counterfeit or in violation of trademark laws. eBay has issues with a myriad of goods coming from China being fake – prompting some to call on the retailer not to sell goods from that country.

In recent months, Amazon has grappled with the sale of illicit streaming devices on its retail platform. These devices are a variation of set-top boxes, except the software or content is configured to provide pirated material such as illicit movies, TV shows, music or games. Kodi extensions, for example, will connect the devices to illegal content through streaming websites and file lockers.

To its credit, Amazon implemented policy changes and in April announced that it suspended the accounts of people selling pre-loaded Kodi TV boxes. Amazon acted to address the concerns of content creators and stem the growth of shady goods on its platforms. In late May, Facebook followed suit, announcing changes in policies for advertising and Commerce to prohibit the sale of Kodi boxes and ban the sale of any streaming device that facilitates access to unauthorized digital media. And though this issue underscores the challenges faced by digital platforms – not all of which act with the same level of responsibility – it also highlights the fact digital platforms can and will step up when their own brands are at stake.

What is clear is that there is a slippery slope for platforms, and lack of vigilance could lead to a decline in the quality of the platform, or cause investor heartburn, as both Etsy and Google have experienced.

Finding the Right Balance on Privacy on our Digital Platforms

The recent congressional debate on data privacy underscored an issue facing Americans: they rely on a slew of digital platforms, each of which has its own privacy policies and settings. As a result, for many consumers, it is difficult to make heads or tails of what each platform is doing to protect their privacy. And that lack of understanding is having an impact on how they view the platforms they use.

An April Digital Citizens Alliance survey of over 1200 consumers found that this should be a growing area of concern for digital platforms. The survey found that nearly 40 percent of Americans have experienced an issue where their online privacy was violated.

Worse, 61 percent said they lack the confidence that their online privacy will be protected and not breached or misused. And if the last several years are any indication, consumers have every right to be concerned. Threats are getting more severe as government-sponsored hackers continue to make their presence felt. Last fall, Yahoo reported that data associated with at 1 billion accounts in two breaches, including at least one in which it was suspected the hacker was a "state-sponsored actor." In the first breach, according to Yahoo, names, email addresses, telephone numbers, dates of birth, unencrypted passwords and security questions and answers were stolen.

Breaches are a booming business. Two years ago, Digital Citizens conducted an undercover investigation in which it reached out to credit card thieves peddling stolen cards online. The thieves walked DCA investigators through the prices for stolen cards, offered guidance on what online retailers to avoid (they told us to stay away from large retailers) and even offered to sell a credit card-making machine. ABC News followed up on Digital Citizens' work with their own investigation, with the "carder" offering a manual to ABC News reporter Byron Pitts on how to exploit stolen credit cards.

As threats to Americans continue to mount and their confidence in their online privacy wanes, it is becoming increasingly clear that the platforms must work together to restore the faith of their users. Too often, consumers are confused about how their privacy is being protected and lack understanding of just how personal information is collected, used, shared, or disclosed by platforms. While privacy policies are always present and available for review, it is clear that consumers are not 'getting it'. Instead, they are often bombarded with disparate messages from privacy advocates and government officials who have the best interest of consumers in mind, but such is lost in the rhetoric. As such, now is the time for companies to work together to better educate their users on their platforms' existing privacy protections so that they can better protect themselves. At the same time, in the face of large scale data breaches like those that struck Yahoo, it is imperative that consumers understand what impact these breaches can have on them and how they should navigate the online world going forward.

In such a complicated digital ecosystem, a one size fits all privacy approach may not be feasible. That said, platforms need to take the initiative to help users understand and protect their privacy or risk further eroding their trust.

As a baseline, Americans should have confidence that:

- Digital platforms are a proponent of, and not a threat to, their online privacy.
- Regardless of whether they are using a service provider or on a social media website, a retail ecommerce website or entertainment platform, they can understand how their privacy is being protected and what mechanisms they have to impact information collected and shared about them, not through one size fits all privacy regulation, but industry led best practices and consumer education.
- They will be promptly notified if an issue or breach occurs in accordance with existing state data breach notification requirements.

Protecting our privacy is a fundamental thing that the businesses we use must do. There is now an opportunity for those same businesses to lead the way in educating and empowering Americans to protect themselves in the new digital economy. Let's make it happen.

Solutions: A Community Problem Demands a Community Answer

The compartmentalized approach in which digital platforms and the law enforcement community take to combatting abusive or exploitive behavior is inefficient and ultimately plays into the hands of bad actors. While digital platforms collaborate on policy and technical issues, there is no evidence that they are sharing information about the bad actors themselves. That enables criminals and bad actors to move seamlessly from platform to platform.

There are numerous examples of industry working together to identify and share information about exploitive behavior. For example, casinos share information about card sharks and cheats, and for decades the retail industry has shared information about fraudulent credit cards. A similar model would enable digital platforms and law enforcement to more quickly identify and combat those seeking to leverage the platforms to harm consumers.

It is worth noting that the industry has already engaged in sharing of security threats, providing, for example, knowledge of links to malware or phishing sites to working groups that other members can use to block their users from reaching. While these activities are not identifying the actual bad actor, it is a step that proves sharing even bad conduct can help protect consumers.

While there are technical, legal and policy issues to address, an industry effort to share and disseminate information should be pursued.

Platforms Can No Longer Say It's Not Their Job to Monitor Their Sites

In the last year, due to the controversies over Fake News and brand name advertising associated with objectionable content, we've seen a significant change in what consumers, brands, investors and government expects from digital platforms. In short, they expect more responsibility.

And thus far, while it's early, many of the digital platforms have stepped up, and deserve credit for doing so. However, since these platforms are so widely relied upon, it is clear that more needs to be done. If only Fake News is addressed, that won't change consumers' angst in feeling that bad actors have the upper hand when it comes to our digital world. That is reflected in the grade that consumers give digital platforms in keeping the Internet safe.

Asked, "what grade would you give digital platforms for ensuring that these platforms are not overrun by those trying to deceive, scam or trick consumers?" the average grade was a C-. Taking it one step further, 75 percent of consumers from the same Digital Citizens' poll said platforms need to do more to keep the Internet safe and trustworthy.

Clearly, these responses are a call to do better by the very people using these platforms. And collectively, we can all successively step up to this challenge. Law enforcement must not throw up its hands just because so many of the bad actors are overseas and beyond their reach. Consumer groups must do more to raise awareness on threats to Internet users. And digital platforms must continue to widen their circle of issues that they will interject themselves, beyond just Fake News and objectionable content.

There is no question that it's in the interests of digital platforms to take responsible steps, or risk backlash that could threaten their standing. Consider these findings from Digital Citizens' research:

- 66 percent of consumers polled have lost trust in digital platforms over the last year.
- When asked, "What role should digital platforms play in ensuring the Internet remains safe and trusted?" 3 in 5 consumers responded that digital platforms are an essential part of life now and should be responsible for what people do on them.
- 72 percent of respondents say the issue of brand name advertising showing up on offensive online content like ISIS/terrorism recruiting videos is a serious threat to the continued trust and integrity of the Internet. 56 percent think digital platforms should be responsible for where ads are placed so they don't appear on hate speech or illegal activities.
- When it comes to bad actors and criminals using platforms to illegally sell drugs, scam consumers and offer illicit goods and services, nearly 60 percent said companies should monitor their platforms to find these activities and remove them when found. 3 in 4 said they think platforms less reputable when they see these shady activities on them.

Digital Citizens' survey results show that a potentially toxic combination for these platforms is a perception that they are all-powerful but lack the moral compass or commitment to prevent being overrun by bad actors, which will no doubt force legislators and regulators to take steps to check their power. Before we get to such an extreme and potentially devastating step, there are other ways to demonstrate that digital platforms are on the side of consumers.

First, digital platforms should, where they aren't already, leverage "Big Data" to address the threats posed by criminals and other bad actors. Digital Citizens believes digital platforms could isolate certain terms that consistently lead to illicit goods and services. For example, a posting with the phrase "buy stolen credit cards," could be sent into a higher priority review queue for human moderation. Facebook recently took a similar step; hiring 3,000 new employees to monitor videos posted on the social network for violent activities. These human reviews could also take place based on user flagging, something that is done as a limited solution today, but could be employed with a greater impact.

Next, platforms could also better analyze usage data that they already collect to highlight behavior that is anomalous and suggests illicit, unlawful, or illegal conduct. And with a little help from engineers, digital platforms could create fingerprints of unlawful conduct that is shared across platforms to proactively block such conduct, as is done in a limited capacity with child pornography. If these and other newly developed measures were adopted, digital platforms would have the information to enable them to make decisions whether to de-list or demote websites offering illicit goods and services, and the ability to stop the spread of illegal behavior that victimizes its users.

Finally, a greater investment in public awareness is also essential regardless of what other steps are taken. Society has been successful in the past with public awareness campaigns for smoking, drinking and driving, and littering, and should adopt a similar comprehensive multi-stakeholder approach to improving consumer capabilities to know when they are being tricked, the dangers from illicit goods and services, and when and how they should report such behavior rather than spreading it to others.

Conclusion

Digital and social platforms have become an integral part of our society and the most popular destination for consumers using the Internet. But as users have adopted these platforms and the technologies they have introduced, so too have bad actors looking to scam and defraud unsuspected consumers, sell illicit and illegal goods, and spread false information and malware.

While some platforms have taken positive initial steps to address the issue of Fake News, Digital Citizens' consumer attitudes survey shows the public expects them to do more on other illicit and/or illegal activities posing threats to their safety – including scams, pirated content, drugs, and stolen goods. We are at a tipping point where digital platforms must take more responsibility for what occurs on their sites or risk further eroding consumer trust in the Internet and its most popular companies.

Digital platforms should seek out opportunities to collaborate with law enforcement, cybersecurity experts, consumer protection groups, and civil rights organizations to explore a new approach to protect consumers. These groups have come together numerous times in the past when new challenges have arisen in other settings, and Digital Citizens calls upon them to do it again.

A holistic approach is a necessary component of prevention and enforcement, whether is it in the physical world or the online world. Digital platforms have a responsibility to their users, and the society that now relies upon them, to explore every possible solution to better protect their privacy and security.

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

digitalcitizens alliance