UNHOLY TRIANGLE

From Piracy to Ads to Ransomware: How Illicit Actors Use Digital Ads on Piracy Sites to Profit by Harming Internet Users

digitalcitizens alliance

whitebullet

UNIT 221B
GUIDED BY INTEGRITY DISCREET BY DESIGN

September 2022

Table of Contents

Executive Summary

Consumers are accustomed to seeing advertising when they visit legitimate services offering online entertainment. It is often the price a viewer accepts for not having to pay directly for a movie, TV show, or live event. But when consumers venture into the shadowy world of piracy for their entertainment, they expose themselves to a different kind of advertising: Malicious ads designed to infect their devices - including with ransomware that locks up their files until they pay a fee to regain access to them.

The scheme developed by piracy operators, distributors of malicious advertising, and facilitators in ad tech is as dangerous as it is clever.

Piracy operators lure users to their sites by offering them "free content," including the latest movies, music, and television shows. Once they come to the piracy site, users are subjected to a deluge of malicious ads – often called "malvertising" – that employ fear tactics and other deceptions to trick users into clicking on them. The fateful click then activates hidden malware that infects the user's computer.

Piracy operators are paid handsomely by the malvertisers for allowing access to their users – collectively, over $120 million a year. The malvertisers (some who appear to operate from Russia and target U.S. citizens), in turn, profit each time a user clicks on the malicious ads and is exposed to ransomware, theft of their personal and financial information, and tracking of their online activity.

Thus, piracy operators and malvertisers have created an unholy triangle with pirate site visitors, who have unwittingly entered a perilous game of "Pirate Roulette" by entrusting their cyber-safety to malicious actors.

There is one more key player in this scheme: the ad intermediaries who make money by assisting the malvertisers that place the ads on piracy sites. Legitimate ad intermediaries police the ads they place and the sites they place them on. But there are services that appear eager to cast

a blind eye to this illicit arrangement – or even to help the malvertisers reach their intended victims.

These are among the findings of a joint investigation undertaken by the consumer advocacy group Digital Citizens Alliance, piracy advertising expert White Bullet, and cybersecurity firm Unit 221B. White Bullet analyzed thousands of piracy sites, including well-known platforms such as Fmovie[.]to, Myflixer[.]to, and Dramacool9[.]co. Then the groups conducted an in-depth analysis on advertising and threats on the most-visited piracy sites or those that had the most malvertising.

The investigation found the consequences of piracy-instigated malware are wide-reaching, with an impact beyond the world of entertainment and piracy.

Among the key findings of this report:

- The impact of malvertising can be devastating. With just a few clicks on a piracy site, investigators were victimized by a ransomware attack that encrypted their computer files. The **criminals demanded payment** to unlock them. This cyber threat was observed across multiple piracy sites.

- Ransomware is a $20 billion annual scourge on consumers, small businesses, corporations, and non-profits. Even if a victim pays the ransom, there is no guarantee they will regain access to their data.

- Beyond ransomware, investigators found malware on piracy sites designed to gain access to a user's device to steal banking information, download spyware to track a user's activities, or flag it for a potential future attack.

- Malvertising generates enormous revenue for piracy operators. Malvertising accounted for **12 percent of the total ads** on piracy sites, generating a **minimum of $121 million annually in revenue**[1]. More than half of that, $68.3 million, came from U.S. visits to these sites. Malvertising accounts for roughly $1 out of every $4 these illicit actors make in advertising revenue.

[1] The $121 million annual figure for revenue from malvertising is considered a minimum as it was estimated from the relatively small dataset of 500 piracy sites included in this study (see appendix for methodology details). This figure was not extrapolated to the thousands of piracy sites known to be supported by advertising.

- Malvertising is widespread on piracy sites. Nearly eight out of ten pirate sites investigated served up malware-ridden ads to their users. And the volume of malvertising targeting pirate site users is significant. Visitors to piracy sites were bombarded with an estimated **321 million ads** designed to do them harm across a one-month period.

- Instead of prohibiting dangerous content, some ad intermediaries are willing to facilitate campaigns involving blatantly misleading ads, such as a false claim that the user has a computer virus, or coach illicit actors on effective tactics to frighten or otherwise entice users to click on ads.

- Using the lure of free content or fear tactics, illicit actors encourage users to take steps to undermine their device security, such as by changing their device settings or clicking on dangerous installs.

- While not every visit to a piracy site results in malware, the investigation found that on average 1 in 6 times, a visit to a piracy site leads to an attempt to serve malware to the user.

- That finding conforms with Digital Citizens' research that users who visit piracy sites are significantly more likely to report an issue with malware than those who don't.

Make no mistake about it, piracy is big business. It is a $2 billion-plus industry[2] fueled by illicit subscription services and by advertising, including both legitimate ads placed by reputable companies and malvertising. Malvertising ranges from the simply annoying, such as unwanted banner ads, to dangerous Trojan viruses that can inflict serious and sometimes catastrophic harm.

The screenshot on page 5 is an image from the ransomware attack triggered when investigators from Unit 221B clicked on an ad on a piracy site. The attack encrypted all the user's files so they could not be accessed. The criminals demanded the user pay a ransom of $980 to regain access to the locked files.

[2] This figure is the result of two pieces of prior research. DCA and White Bullet's 2021 "Breaking Bads" report found bad actors reaping an estimated $1.34 billion in annual revenues through advertising on websites and illicit streaming apps. DCA and NAGRA's 2020 "Money for Nothing" report found pirate subscription IPTV services generate subscription revenues of $1 billion annually in the U.S. alone.

Image 1. Pirate Site Visit Leads to a Ransomware Attack

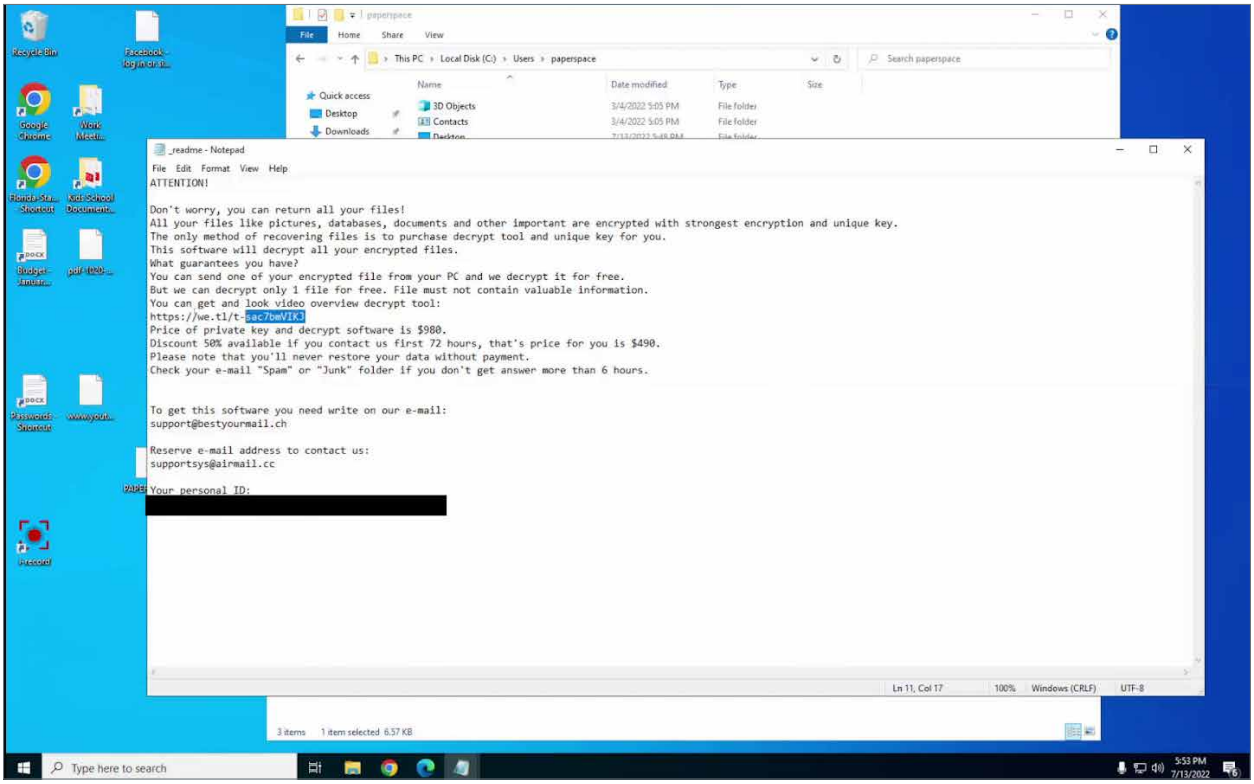


Image 1

When visiting the sites, investigators mimicked the behavior of a typical user by clicking on ads, viewing a media file, or downloading a file such as a media or torrent. The ransomware attack was just one of the examples of pirate site visitors being targeted by malware.

Ransomware and other malicious code have been a challenge for law enforcement to combat. Nevertheless, the role of unscrupulous ad intermediaries in facilitating the spread of this malware should also be looked at by authorities.

The ad industry has made important progress in reducing the number of ads for reputable companies on piracy sites, particularly since key U.S. advertising associations created the Trustworthy Accountability Group (TAG) to combat malicious activity and increase trust in the digital advertising industry. As those efforts have succeeded in reducing revenue from legitimate advertisers, pirate operators appear to be increasingly turning to malvertising facilitated by the bottom feeders of the advertising ecosystem.

The investigation found that while some ad intermediaries claim to have policies against deceptive or maliciously manipulative ads, they appear to turn a blind eye to ads clearly designed to trick users.

For example, ad intermediary RichAds told investigators (posing as would-be shady advertisers) that it would have no issue serving up the overtly malicious ad below that falsely "warns" users that their device has a virus in order to trick them into downloading "a security tool" that is actually malware.

Image 2. Malware Disguised as a Security Warning

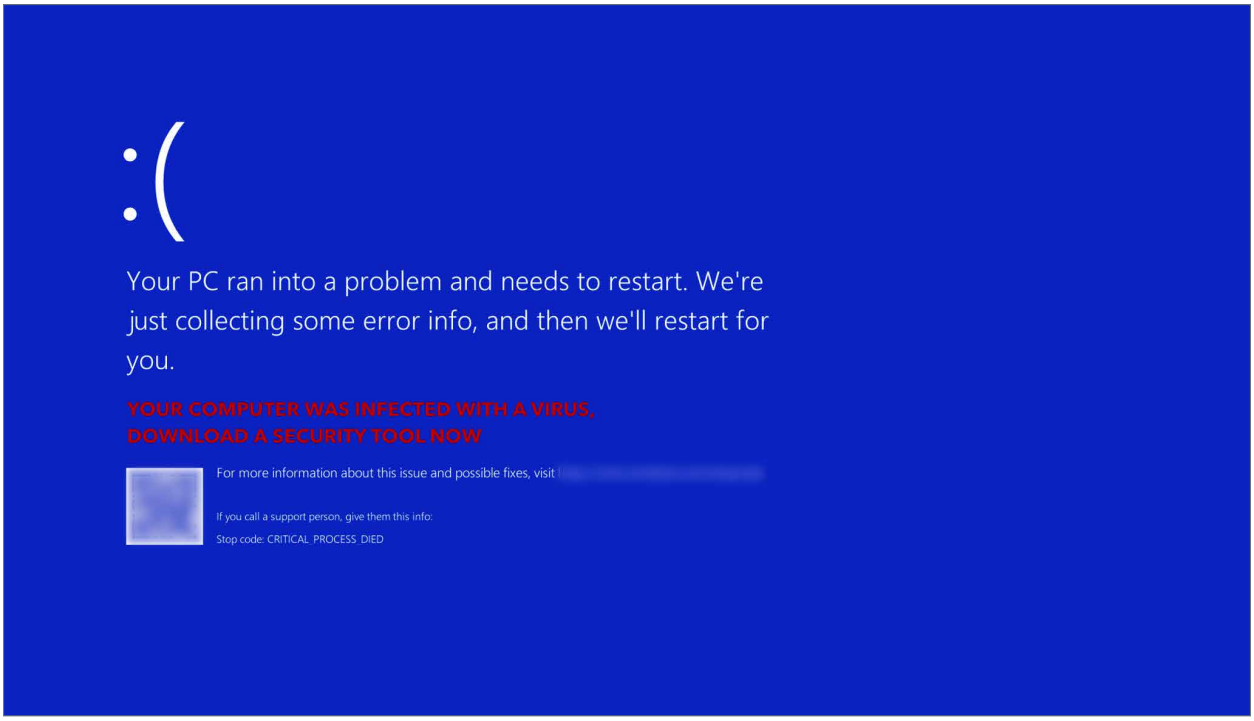


Image 2

And ad intermediary PropellerAds, found to be among the biggest facilitators of malvertising on piracy sites, advises its customers peddling ads that its content can "frighten users" to entice them to click on ads.

This report shows that piracy leads to malware and malware equals harm to Internet users. These risks reinforce why law enforcement must make investigating and prosecuting piracy a priority. And the ad ecosystem must make clear that its members can't play in both the legitimate ad world and those illicit corners of the industry that enable piracy and malvertising.

Dishonor Among Thieves: Piracy and Malvertising

The $2 billion-plus piracy ecosystem is a sophisticated network of operators and enablers that illicitly supply content to millions of users. Piracy site operators aren't in business to share content among the masses out of a sense of principle; to paraphrase the bank robber Willie Sutton, they create piracy services because that's where the money is.

The top websites that offer stolen content generate $1.08 billion in annual ad revenue, while the top apps generate another $259 million from ads, as shown by a 2021 report by Digital Citizens and White Bullet.

The current report grew out of that prior research. At the time, investigators uncovered numerous incidences of malicious ads on piracy sites. That meant that not only was the piracy industry generating revenues from offering subscription and ad-supported piracy services but from malware purveyors as well.

The business model behind malvertising on piracy sites is straightforward. Malicious actors buy ad space from advertising networks that are sloppy or uninterested in policing the ads submitted. Once approved, the malvertising is placed on piracy sites willing to accept the dangerous ads. In effect, piracy operators, in their quest to make money, sell the safety of the visitors to their sites. In some cases, users are bombarded with virus-laden advertising - with as many as 11 malicious ads per page on a piracy site.

To shed light on the risks consumers face when they visit pirate sites, in the spring of 2022 Digital Citizens and White Bullet teamed up with cybersecurity firm Unit 221B to closely look at the relationship among piracy, advertising, and malicious ads. With piracy, the scope of the problem often correlates to the financial size of the ecosystem, so the initial effort evaluated the extent of malvertising on these illicit sites.

The answer is a lot – a minimum of $121 million per year.

The United States makes up more than half of that amount ($68.2 million). Given that activity is generating more than half the annual malvertising revenue, it's a fair assumption that U.S. users are also more likely the most at risk.

How Illicit Actors Trick Users to Click on Malware

There are thousands of piracy sites on the Internet and a prospective user often learns about them from a friend, an online resource, or through a search engine. By just visiting a piracy site, the user has done the hard part for the illicit actor: *Instead of the actor having to find a target, the target has come to them.*

Now that their prey is in their territory, the malicious actor needs to entice the target to do just one thing: click.

Why is the "click" so important? A few years ago, computers could be infected simply by the user visiting a site, which would attack the computer with malicious malware as soon as the page started loading. Browser security has improved so "drive-by" attacks of this kind have become more difficult to carry out. Thus, a successful attack now typically requires a user to actually click on a particular place on a webpage to permit the malware to download.

Of course, the malicious ads on these piracy sites don't reveal the real reason users are asked to click. Instead, users may be told they need new anti-virus software, to update a media player, or are the "lucky" winners of a promotion.

Those behind malvertising engage in a concerted effort of social engineering – relying on fear (ironically of malware) and desire (getting free content) – to get users to take steps that make their devices more vulnerable to attack.

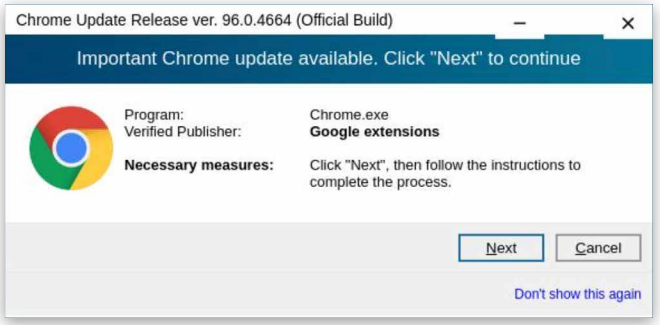
With a fateful click by an unwitting visitor, the game of Piracy Roulette begins, with users having a 1 in 6 chance of being served a malicious ad designed to do harm. A report, *Time to Compromise*, commissioned by the Asia Video Industry Association (AVIA) and authored by Dr. Paul Watters, found it typically takes just 42 seconds for an "advanced persistent threat" such as malware to infect a Windows device and 78 seconds to infect an Android device.

Malvertisers rely on a variety of tricks to get the user to click.

The most popular technique to get malicious software installed on a target's device are so-called *pop-under ads.* While pop-up ads appear on a user's screen, pop-under ads linger behind a browser window. In doing so, they serve ads in the background while the user views the content they choose.

Here's an example:

Image 3. Pop-Under Ads Trick Users to Click



GENERIC SYSTEM DECEPTION: Pop-under ads that trick users into installing malicious software including adware, browser hijackers, and other.

Image 3

Pop-under ads are lucrative for piracy operators, accounting for $88 million of the $121 million they make a year from malvertising placed on their sites.

Another go-to malvertising approach is *click-to-play ads* whose intent is to entice users looking to stream content. When users click, they are redirected to malicious sites that increase their risk of a malware infection.

Here's an example:

Image 4. Click-to-play Ads Designed to Deceive Users

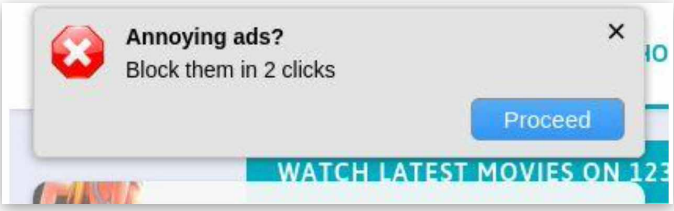
GENERIC DOWNLOAD: Various click-to-play or download ads appear on pirate streaming and IPTV websites to confuse users looking to stream content from the website. Clicking results in the installation of malicious software including adware.

Image 4

Click-to-play ads are also lucrative for piracy operators, who are paid an estimated $21 million to let them appear on their sites.

Other techniques, such as *generic click-scams*, are designed to initiate downloads of malicious software by playing off a user's fear of getting infected or annoyance at advertising. Piracy operators generate an estimated $5.5 million a year through these ads. The example below shows an ad that promises to get rid of "annoying ads" but actually redirects a user's browser to websites, generates *more* ads or installs malware:

Image 5. Generic Click-scams Play on Users' Security Concerns



GENERIC CLICK SCAM: The message varies but the click-through leads to downloads of malicious adware and other unwanted programs. An ad intermediary may redirect the browser to unwanted websites and generate large volumes of ads, with further user clicks that install unwanted and malicious software.

Image 5

In other instances, a visitor may be enticed to download a "helpful" consumer service. In the example below, photo recovery software is offered:

Image 6. Photo Recovery Software Advertisement

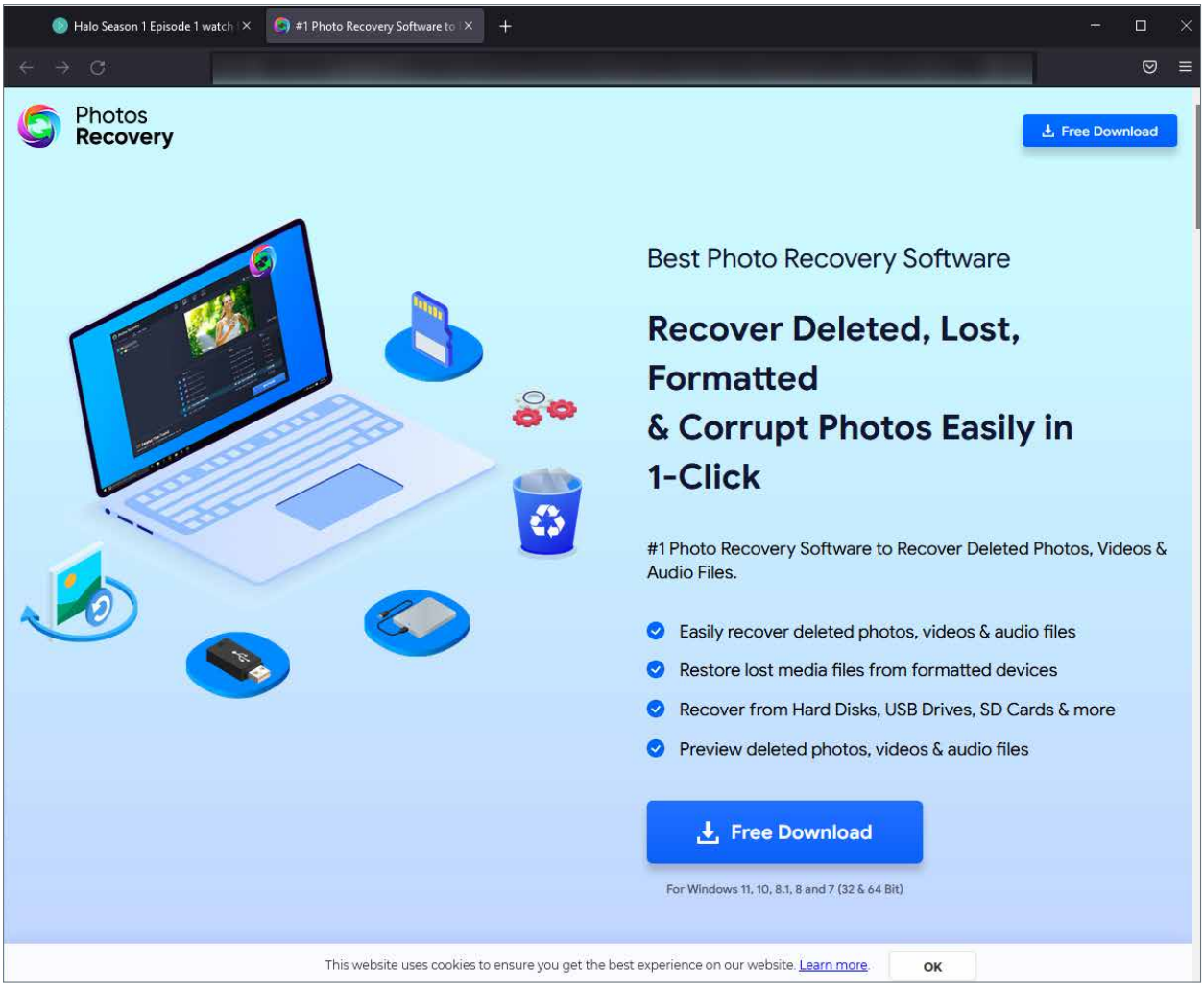


Image 6

Malvertising can also be presented as a wolf in sheep's clothing - i.e., appearing as a legitimate ad for an iconic television show. Misusing this brand enables illicit actors to create a perception that clicking on an ad is not dangerous.

Image 7. Pop-Under Ad for Game of Thrones Mobile Game

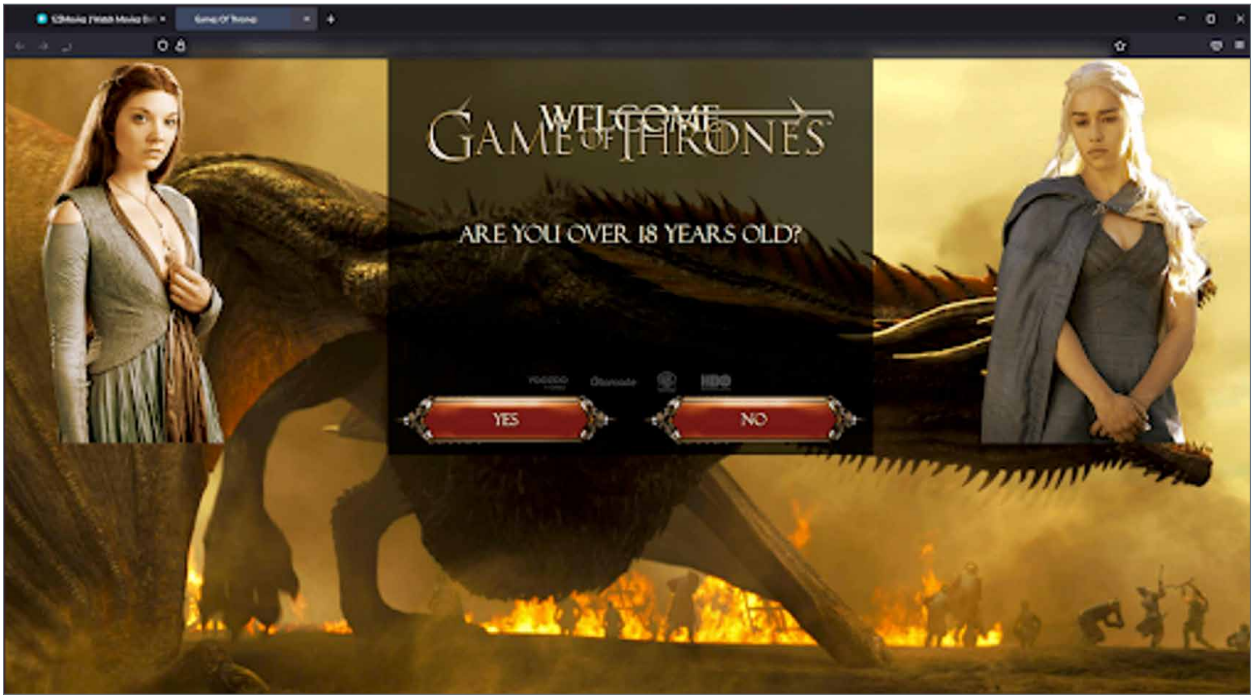


Image 7

It is understandable how visitors can be duped when a well-known or iconic image or brand appears that may ease their concerns over the risks. In previous research, Digital Citizens has shown how the appearance of well-known brands can lend unwarranted credibility to a piracy site.

While not all malware is equally dangerous, none is welcome. And many types wreak havoc on the personal and professional lives of those targeted, as the next section of the report illustrates.

After the Click: From Piracy to Ads to Ransomware

Ransomware is a devastating cyberattack that encrypts the files and data on a device. Once locked, criminals demand payment to make the files and data available. In the cases of businesses and government entities, criminals also threaten to leak sensitive information from the files if they are not paid.

Malvertising on piracy sites is one of the means by which an attack originates. In fact, investigators went from piracy to ads to being attacked by ransomware in just a few seconds and a few clicks.

It started with the promise to be able to watch free content on piracy sites such as mesfilms[.]pw (an alias for mesfilms[.]buzz) and kinomax[.]to.

Image 8. The Lure – Offers of Free Movies

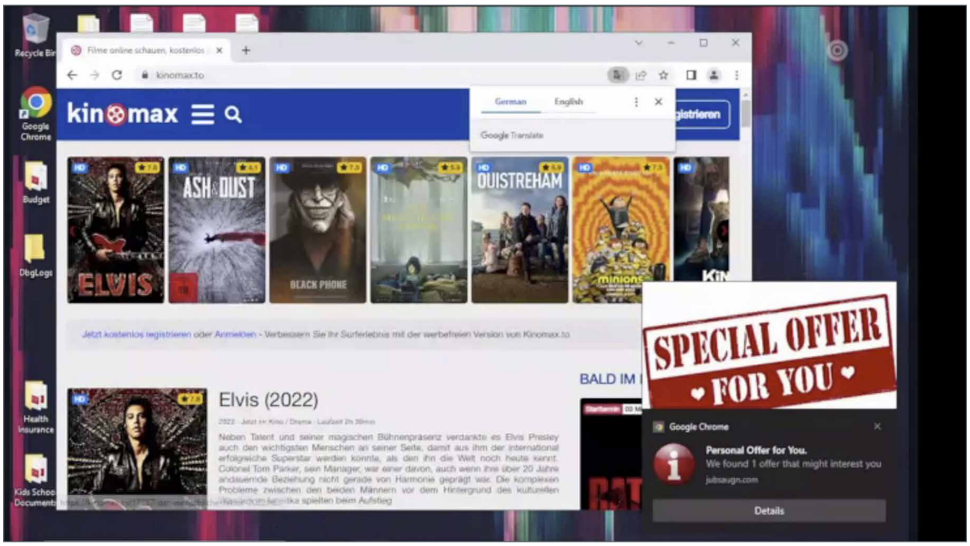


Image 8

When investigators clicked on a link to initiate the delivery of content on the piracy site, the link immediately opened new browser tabs or pop-up windows, prompting software or browser extension installations.

Ultimately, users are presented with a prompt for a download, copy button, and the password (1234) for an archive named "**file.rar**." But instead of triggering the download of their desired movie or television show, this link resolves to a publicly available file hosted on the Discord content delivery network (CDN), which automatically downloads when entered into the browser's URL bar. As this link is hosted through a known CDN, the source is considered trusted.

And the user is infected with ransomware.

Image 9. The Download – A File That Looks Fine, But is Actually Ransomware

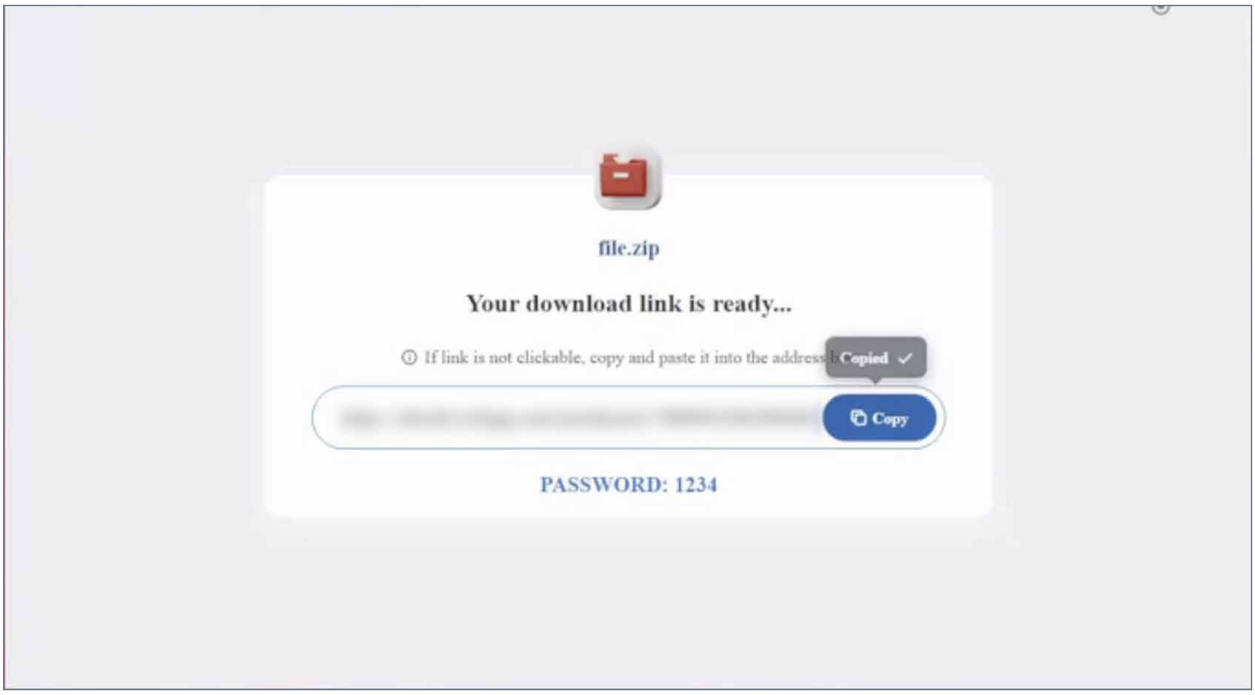


Image 9

Within seconds of being executed, the ransomware attack had notable effects on the investigator's device system. System and memory usage spiked.

The ransomware then restarted the system multiple times over the course of two minutes. When this process was completed, the user's files had been encrypted so they could not be accessed. Note that in the screenshot below the word document files have a ".hhwq" extension instead of the typical ".doc."

With that change, the attacker now had control of the data on the device.

Image 10. The Attacker in Command – The User Loses Control of Their Device

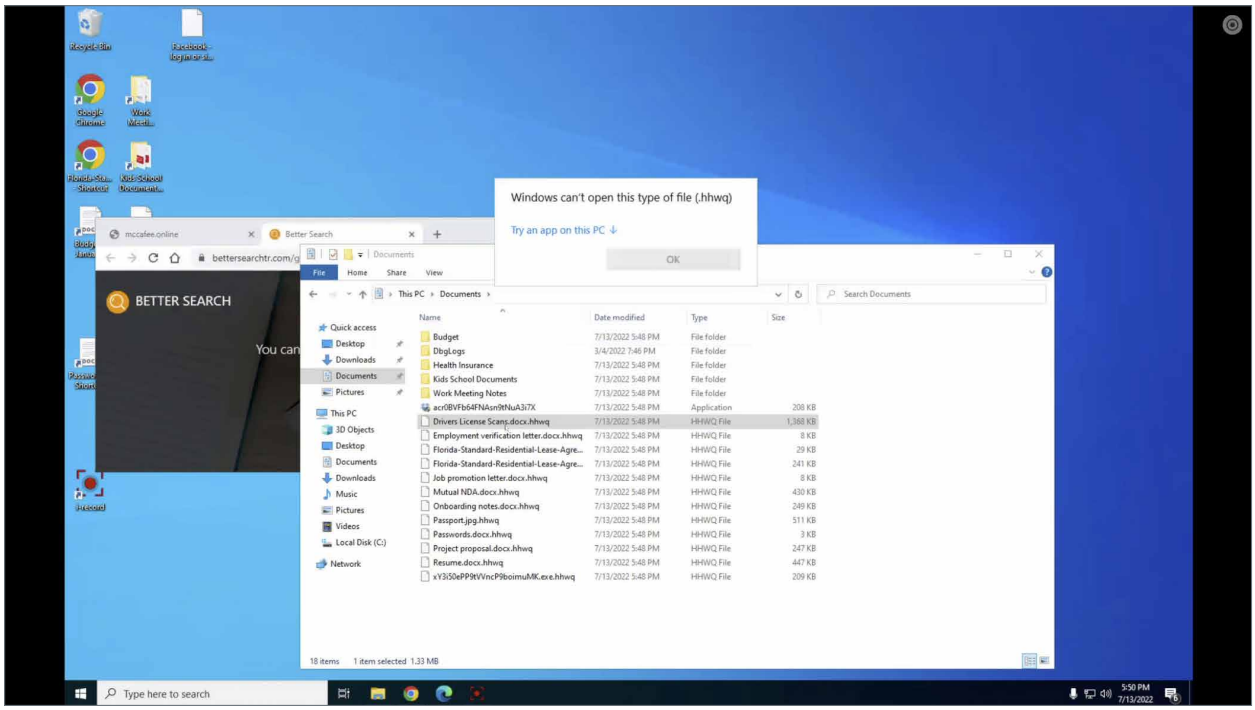


Image 10

Investigators were confronted with the demand: $980 to unlock the files. The extortionist offered to open up one file to prove their capability to do so and offered a 50 percent discount if payment is made in 72 hours (giving the victim incentive to pay and not involve the authorities).

It ended with a warning: "Please note you'll never restore your data without payment."

Image 11. The Demand – Your Dollars or Your Data

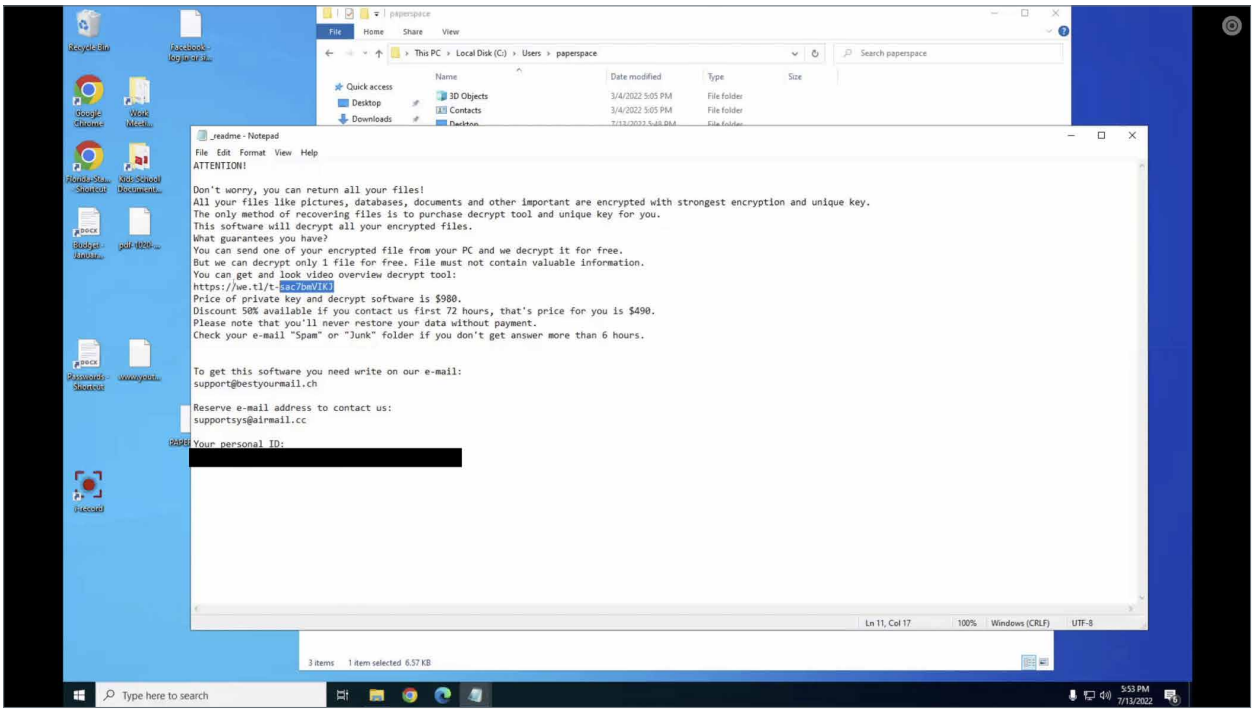


Image 11

To conduct this investigation, files were placed in a virtual machine in a "sandbox" lab environment utilized to observe the attack. The ransom was not paid.

The malware that spurred the attack was not isolated. Investigators found it on ads on multiple piracy sites. After the user clicked on any of the links on the page, a new tab would open that loaded a page with a link to download a file that surreptitiously would initiate a ransomware attack.

Ransomware attacks are devastating for Internet users, and unfortunately increasingly common. Nearly 1 in 5 Americans have faced an attack on their personal or work device. Most recover only about 65 percent of their data on average. The likelihood of attack increases at the business level, with 37 percent of companies having been confronted with a ransomware attack and thousands of healthcare companies, government organizations, and educational institutions forced to temporarily halt operations.

Ransom demands range from hundreds of dollars to a reported $40 million in one instance. Russia, China, Iran, and North Korea make up half of these incidents. As their primary target is the United States, it's a safe assumption that the motivations go beyond financial to geo-political with national security implications.Those concerns have some states reconsidering the protocols for dealing with an attack on government operations. Florida recently joined North Carolina as states that bar local government agencies from paying or acceding to ransomware demands.

Piracy & Ransomware – A Dangerous Combination

By Dr. Paul A. Watters

Ransomware has emerged as the most successful cybercrime vector of all time, accounting for 30% of attacks[3] and an estimated $20 billion in costs a year. The victims range from well-known corporations, small businesses, governmental entities, and individuals. The impact is broader than financial: consumers have endured food and gas shortages as a consequence and the global economy has suffered job losses and reduced profitability.

As an illicit business, ransomware is extraordinarily attractive to organized crime: costs of hosting "command and control" servers are low, risks of detection and attribution by law enforcement are low, and extraterritoriality means that there is virtually no risk of arrest or other legal consequences. Skilled IT personnel can procure and install ready-to-go "kits" on the dark web and use a range of techniques to infect devices. Payment by bitcoin means that funds transfers are virtually untraceable unless crime operators are sloppy or lazy[4].

Malicious actors are always looking for new means to entrap a victim – and they have found it through the simple act of an Internet user trying to watch a movie, TV show, or live event for free. In this report, investigators show direct evidence of how ads on piracy sites directly lead to ransomware.

By offering up free content as bait, a remote attacker, using several ingenious methods of cyber ingress, is able to commit a data breach, while at the same time encrypting data at the source, and holding businesses to ransom. As most businesses do not have effective disaster recovery and business continuity plans, often they are left with paying the ransom as the only option. However, this may not realize the benefits envisaged – according to the old adage that there is no honor among thieves, similarly, there is no guarantee that paying a ransom will result in either data being restored, or that sensitive data will not be further disclosed (or threatened to be disclosed) in the future. Revenue for the best gangs is estimated to be $5.2 billion over the past 3 years.[5] Home working during the pandemic has vastly increased the number of remote connections or desktops permitted, further fueling the opportunities for infiltration, and lateral movement within a network, driven by home user infections.

In terms of an effective cyber policy response, the key question is, how are businesses being infected by ransomware in the first place? A recent study by AVIA of consumers in five Asia-Pacific countries indicated that 31% believed that visiting piracy sites could result in malware infection. This self-report data was followed up with an empirical study showing that ransomware can be found on piracy sites and that a typical malware infection takes only 43 seconds from the piracy site being loaded.[6] Malware can be delivered through piracy sites using a number of vectors[7] – pop-up windows containing malicious links that are triggered when a user initiates an action, such as clicking on a magnet link; interstitial pop-ups, requiring a second click to download and install code; click-fraud malware, where a compromised browser simulated clicking on redirected ads that generate profits through illicit ad networks; browser notification hijacking that is used to then display malicious URLs; malicious browser extensions that can read personal data or insert malicious code; adware and ad hijacking; fully malicious application installation; and malicious banner ads.

In short, piracy sites are custom designed to be the most effective delivery mechanism for the initial attack on a consumer PC. Consumers – driven by the desire for a "free lunch" – are lured into using these illicit services, not realizing the risk that they are taking. Certainly, most would be unaware that the goal of these malicious actors is not the consumer's PC, but the business or work network to which it would routinely connect.

With an infected device that connects to an employer's network using a Virtual Private Network (VPN), remote attackers are able to move laterally within the behind, but behind border controls like the corporate firewall.[8] These activities give malicious actors an opportunity to infect as many systems as possible, which have the least possible protection, but the highest business value. Other security controls – such as Multi-Factor Authentication (MFA) or Zero Trust – have no capacity to defeat ransomware attacks launched through this vector.

From a technical perspective, companies can reduce the likelihood of a ransomware attack by (a) placing restrictions on piracy site access on corporate laptops and BYOD devices; (b) blocking advertising and pop-up windows through browser controls and third-party plugins; (c) training users to detect and avoid malicious sites; and (d) lobbying government to further regulate cryptocurrencies and other mechanisms used to "cash out", such as money mules.

Governments can reduce ransomware risk by improving regulatory site blocking, making it easier for courts to block access to known malicious sites. Governments can also invest in consumer awareness campaigns, making consumers more aware of their personal risk, as well as the impact that using piracy sites can have on their employers and family.

Finally, more radical approaches to ransomware prevention can be considered, such as using "nudges" at appropriate touchpoints to warn consumers when they are using sites and systems in a risky way. Research has shown that very significant reductions in cyber harm can be achieved by the appropriate use of messaging and chatbots at these touchpoints.[9] Further research is needed to determine how effective they can be regarding ransomware infection prevention.

Professor Paul A. Watters is an Honorary Professor in Criminology and Security Studies at Macquarie University, Adjunct Professor of Cybersecurity at La Trobe University, Strategic Cyber Security Consultant at Ionize, Academic Dean at Academies Australasia Polytechnic (ASX:AKG), and CEO of Cyberstronomy Pty Ltd, a Melbourne-based startup that develops Governance, Risk and Compliance software for small-medium enterprises. Professor Watters is a Fellow of the British Computer Society and Chartered IT Professional, a Senior Member of the IEEE, and a Member of the Australian Psychological Society. Professor Watters received his Ph.D. degree from Macquarie University, and read for an MPhil degree at the University of Cambridge.

---

[3] https://www.globenewswire.com/en/news-release/2021/12/23/2357418/0/en/Mimecast-The-Rise-of-Ransomware-During-the-COVID-19-Pandemic.html

[4] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[5] https://www.zawya.com/en/press-release/research-and-studies/cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000-rr9pfwf7

[6] https://avia.org/how-cyber-criminals-use-ads-to-compromise-devices-through-piracy-websites-and-apps/

[7] https://www.mcafee.com/enterprise/en-us/assets/light-point/white-papers/wp-most-serious-threat-to-business.pdf

[8] https://www.zscaler.com/blogs/product-insights/remote-access-vpns-have-ransomware-their-hands

[9] https://www.aic.gov.au/publications/tandi/tandi647

Beyond Ransomware: Scams, Theft, and Tracking

Ransomware may be the most drastic threat, but it is by no means the only malvertising-induced threat that users face. Even if the user downloads and installs merely annoying adware, it may still serve as a dangerous gateway that allows malicious actors to gain further access to a victim's device.

The majority of these malware executables are classified as "Potentially Unwanted Programs" (PuP) or "adware." Frequently, these programs are disguised as antivirus solutions or system tweak ("systweak") applications.

For example, a well-known variant of adware, "Reimage Repair," was served to investigators while visiting the piracy site 123moviesme[.] online. Its intent is to profit by deceiving and frightening users to purchase legitimate antivirus tools through an affiliate marketing program. When users sign up for the antivirus program through the link in the ad, the adware distributor gets a referral fee.

Clicks made while attempting to view the film *Ida Red* opened new tabs or browser windows.

Image 12. Adware from Pop-Up on Pirate Movie Part 1

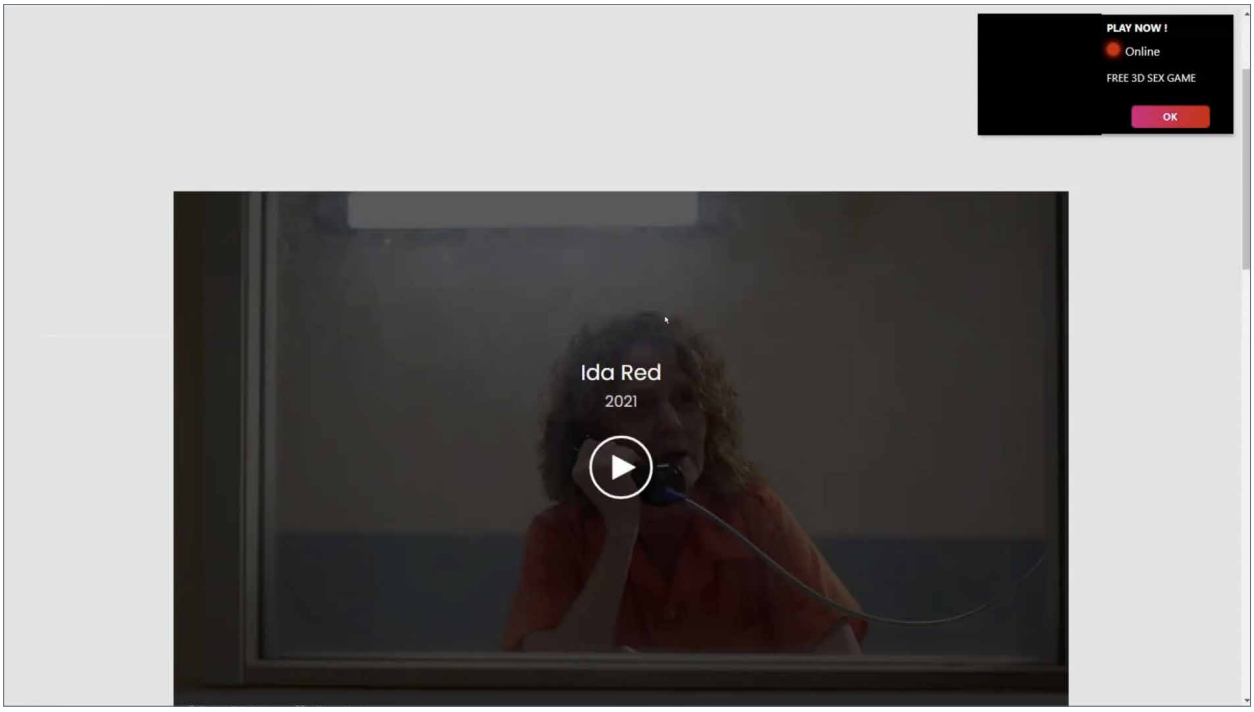


Image 12

A new tab opened, directing users to install a Chrome browser extension, "colors scale," in order to continue.

Image 13. Adware from Pop-Up on Pirate Movie Part 2

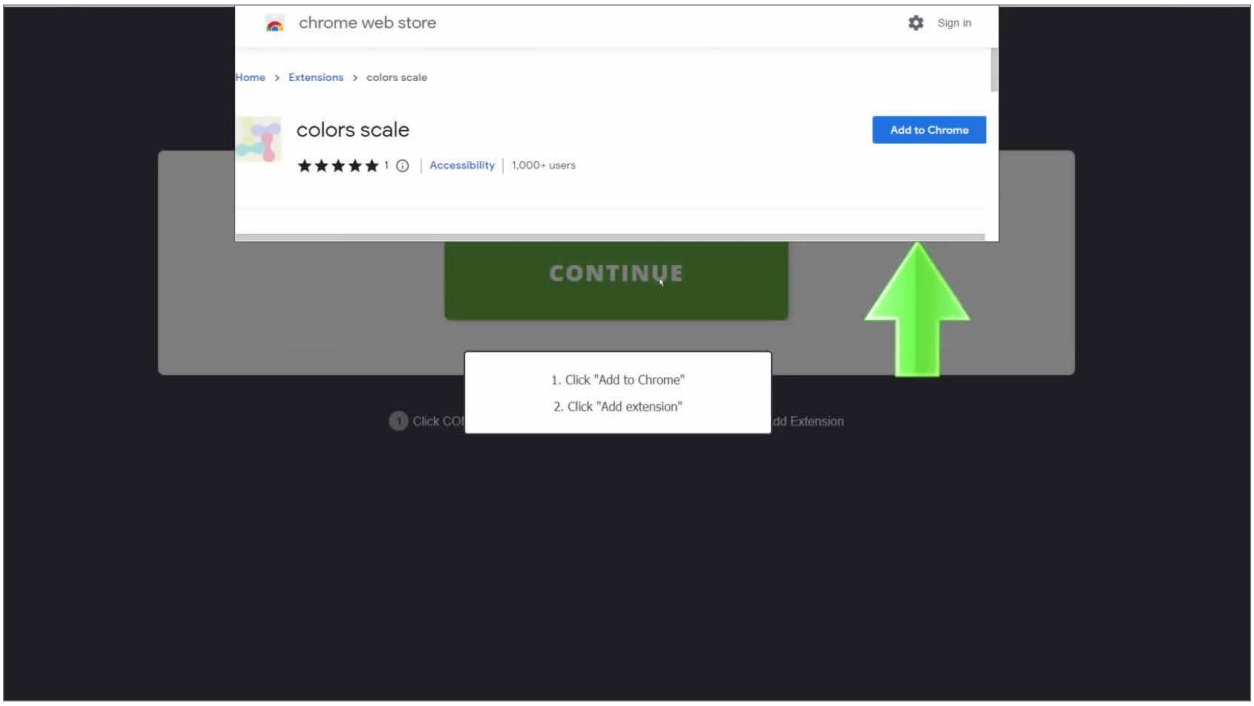


Image 13

The intention is apparently to deceive the user into believing installation of this extension is required for video playback. That led to a prompt to download a link for a PC repair tool. If a user bites at the bait, Reimage Repair adware (under the guise of DC Repair Tool) is installed on the device.

Image 14. Adware from Pop-Up on Pirate Movie Part 3

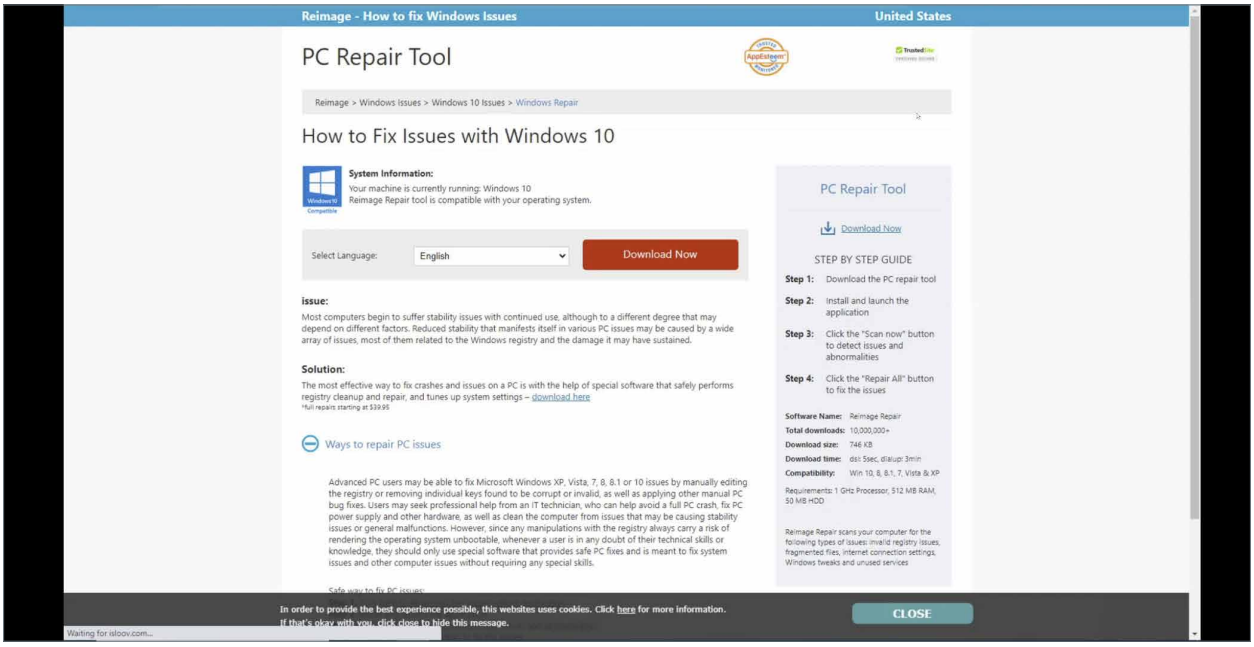


Image 14

Reimage is identified by VirusTotal[10] as an adware application. It presents the user with an "analysis" that includes fictional issues with the device. To "fix" them, users are directed to "Start Repair" through a paid Reimage subscription.

[1] On the website, VirusTotal is described as "as a free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content."

Image 15. Adware from Pop-Up on Pirate Movie Part 4

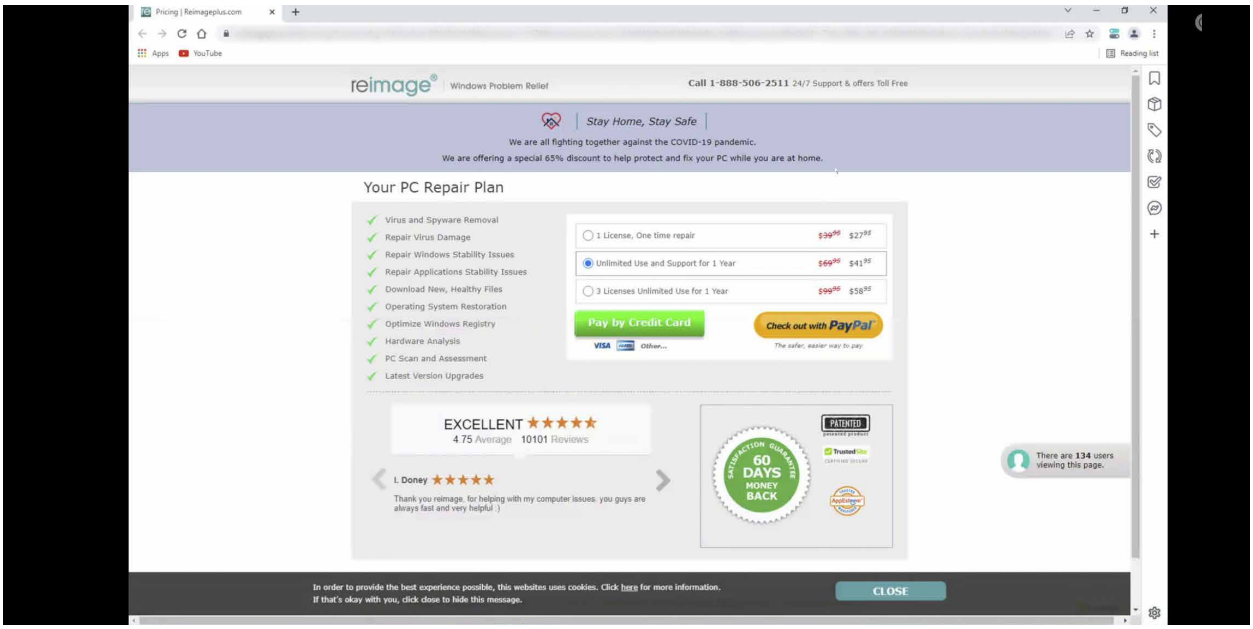


Image 15

These malicious actors use the fact that piracy sites may be perceived as risky as a means to sell anti-virus services, which may be an actual service or a tactic to get a user to download malware to a device. Recognizing that users of piracy sites might be concerned about protecting their privacy, or protecting themselves from malicious software on these sites, it appears that the purported ads delivered by these sites focus on services that can be used to conceal a user's identity and on the software of services designed to identify and mitigate malware (e.g., antiviral or anti-malware software ads). Thus, it appears that these pirate sites are aware of their reputation for delivering malware, and use that to push ads based on this reputation — effectively monetizing the very malware they perpetuate. For example, investigators found "ads" purported to be from privacy software providers such as McAfee, Norton, and TotalAV and VPNs such as ExpressVPN and NordVPN on multiple piracy sites.

It is important to underscore that these ads could well be fake or unauthorized. But their presence certainly could make users believe the claims made about cyber vulnerabilities on their devices. For example, on livesport24[.]net, investigators were presented with aggressive advertisements, as seen below. Of particular note are two "notifications" to the right of the window informing the user that their device has been infected. A notification on the right side of the page displaying the McAfee logo falsely claims the site has blocked 10 viruses.

Image 16. The "Cure" is Actually the Disease – A Security Ad that Serves Malware

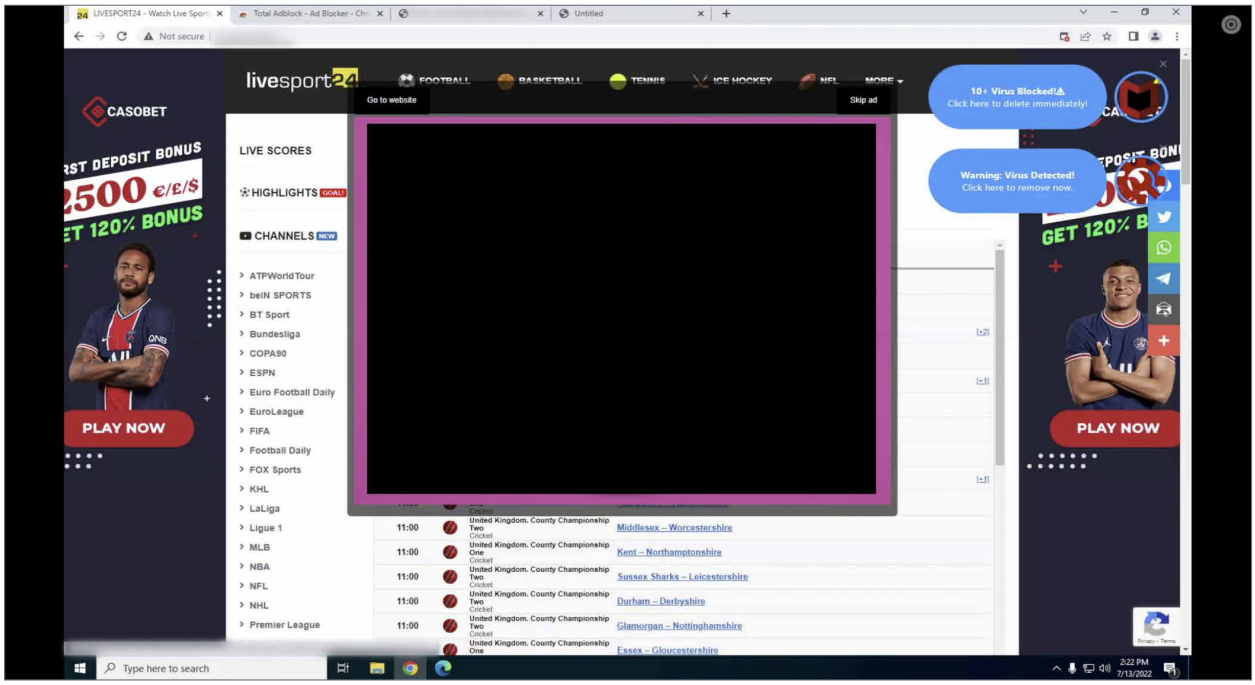


Image 16

Clicking on the "McAfee notifications" opens a new tab that displays a mirror of a purported McAfee antivirus dashboard, including "subscription information." A modal dialogue box is then opened within the same screen, informing the user that as a result of visiting an "illegal infected website," their "PC is at risk of being infected by viruses." If the user follows the prompts to conduct a scan of the device, they are informed multiple threats are "detected."

These tactics are often designed to scare users into buying a service or installing unwanted programs without the user's knowledge, revise computer settings, and enable browser pop-ups to appear that recommend fake updates or other software.

Illicit actors are also clever in their techniques to harm users. Earlier in the report, an ad offering *Photo Recovery Software* was shown. Here it is again below:

Image 17. Photo Recovery Software Advertisement… A Second Look

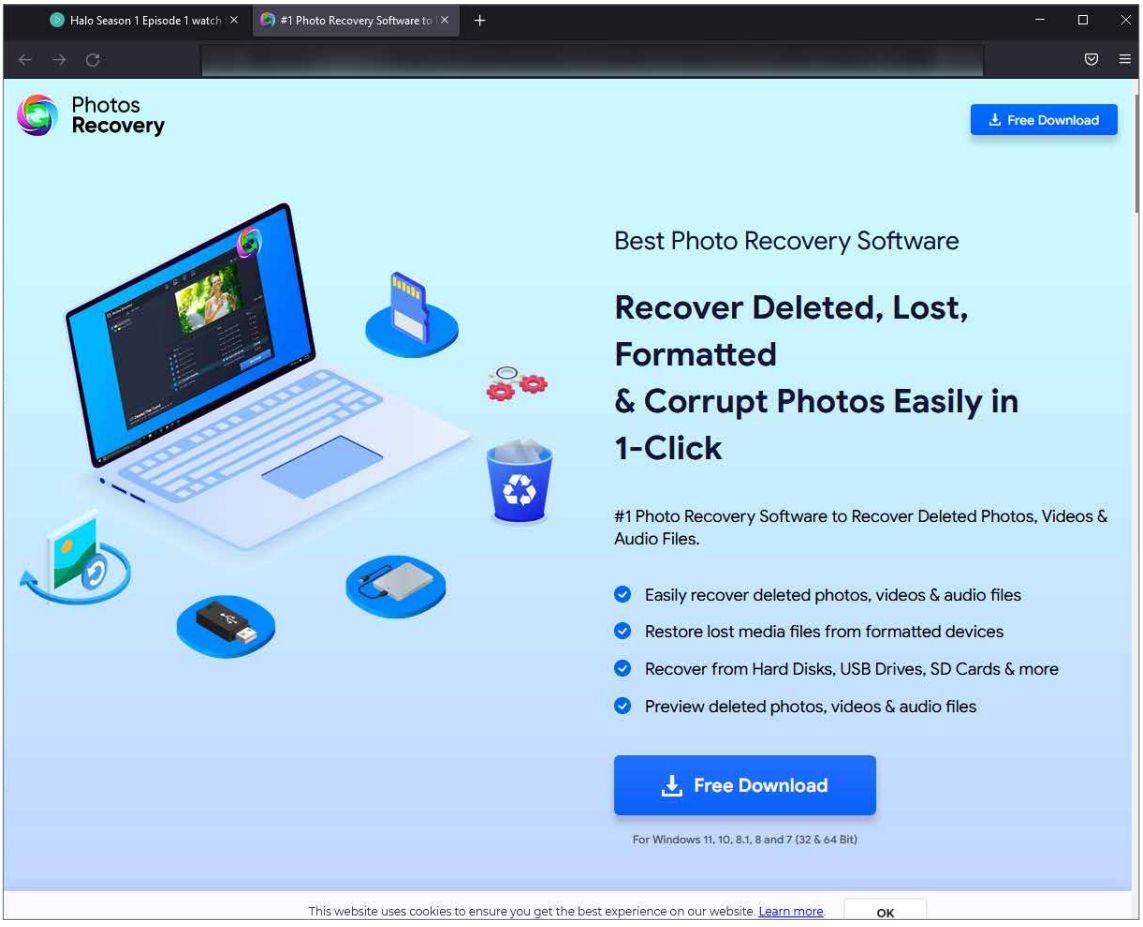


Image 17

An analysis of the ad reveals that it contains multiple threats:

Image 18 Malicious Adware – A Potential Threat to Consumers, Products, Networks, and National Security

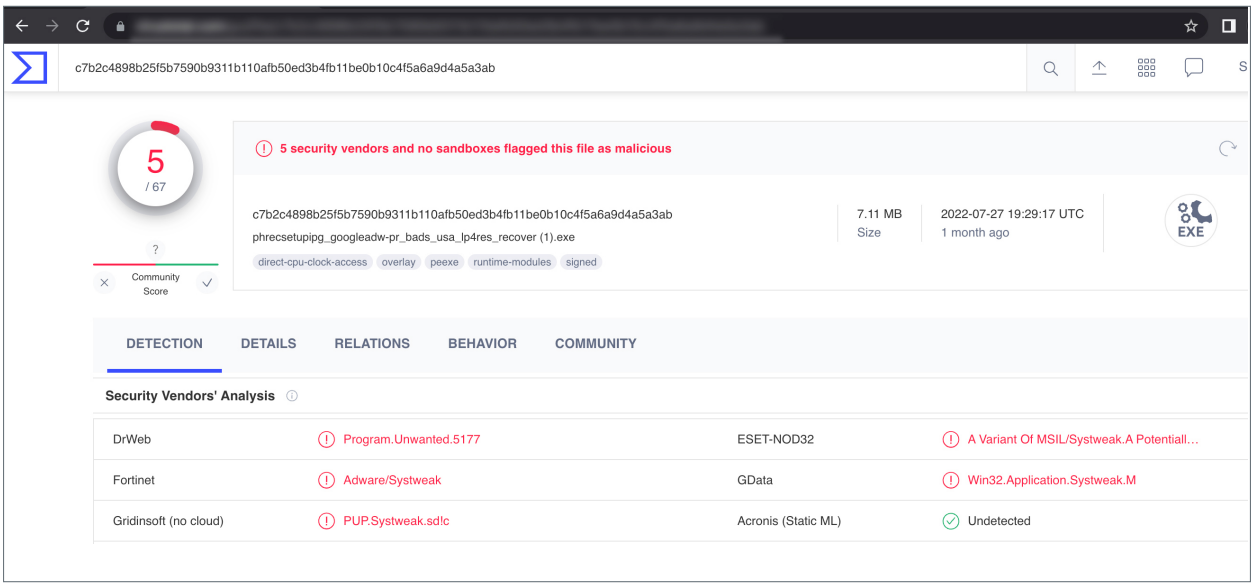


Image 18

This particular threat, Win32/Systweak, is highly risky because it can enable hackers to obtain access to a device's system configuration and registry. Through that, a hacker can steal banking information, download spyware to track a user's activities, or flag the device for a potential future ransomware attack. Interestingly, while this is an older malvertising technique, it still appears to be effective, and was found across multiple piracy sites.

The malicious activity discovered on piracy sites can cause substantial harm to consumers, products, networks, and to national security:

Data Thefts and Data Breaches. Malicious adware can lead to data breaches in two discrete ways. First, the adware itself can open a portal or access into a victim's device, allowing the malicious actor to directly access it and seize personal information, financial information, or other data on the device. This breach can enable the theft of a consumer's personally identifiable information. Second, the adware can make the device vulnerable to a theft of credentials — user IDs and passwords — which can then be used by the malicious actor to access the victim's email, bank, and social media accounts. This also makes the victim vulnerable to any type of "credential fraud" including identity theft, account takeovers, funds transfer, and business email compromise frauds.

Theft of Passwords of Account Access. In addition to theft of stored credentials, malicious adware can also deliver code that acts as a "keylogger" – capturing not only the victim's user IDs and account numbers, but transactional data, passwords, and the contents of text messages. This can also be used for account takeovers, funds transfers, impersonation frauds, or other fraud schemes.

Business Email Compromise Schemes. These are among the fastest-growing and most ubiquitous fraud schemes. While there are many variations, a threat actor obtains a victim's credentials and access to some account — such as an email account, or social media account. Using this account, the threat actor sends (or alters) a request for funds to a known vendor or supplier. The funds transfer request appears legitimate and uses the correct email address of the sender/recipient (because the account has been taken over). The wire transfer goes not to the intended customer/recipient but rather to an unknown bank account, often in Singapore or Hong Kong, and from there, through multiple banks until they reach the final destination. Often, the accounts of both funds sender and recipient are compromised, with wire transfer instructions subtly altered for otherwise legitimate transactions (such as purchasing a home). It is not clear which party here is liable for the funds transfer, and hundreds of millions of dollars have been stolen in this manner.

Botnet Trojans. Adware is a major facilitator of computer botnets. The adware acts as a vector for the installation of botnet malware, facilitating the creation of a command-and-control network, and allowing malicious actors to take control of user devices. Illicit actors then use compromised machines to facilitate a host of malicious activities, including distributed denial of service (DDOS) attacks.

Malvertising may also enable the tracking of a user's activity. While most websites, legitimate or ill-intentioned, try to track user activity, if users have strong security settings, they can thwart those efforts. But when it comes to piracy, malicious actors bank on visitors to piracy sites relaxing their security settings to gain access to the content they want to watch. In fact, many of the piracy sites actively encourage visitors to change their settings – for example telling them to allow pop-ups in order to view a video. A typical user may not realize that changing their settings opens them up to tracking and other threats.

Ad Intermediaries Straddling the Legitimate Ad & Malvertising Worlds

Over the last decade, the advertising industry has taken constructive steps to address the illicit side of its ecosystem. But now it faces a new challenge: ad intermediaries that appear to play in both the legitimate and malvertising worlds.

Cases in point: RichAds and PropellerAds, two well-known ad intermediaries.

RichAds is an advertising company that touts its ability to capture new quality leads from premium sources through its productive ads. The company is listed as being based in Cyprus, with many of its employees listing Belarusian universities as their alma maters on LinkedIn. It promises to deliver the best traffic and claims, on its LinkedIn page, that "We block any bot or other fraudulent traffic."

When it comes to deceptive ads designed to trick users, RichAds takes a lax, approach. Investigators created an ad, shown earlier in the report but placed here as well, obviously designed to trick users into believing that they have a virus. The ad includes a QR code that would take the user to a legitimate Microsoft support page to add to the deception that it was a legitimate virus alert.

Image 19. Malware Disguised as a Security Warning (revisited)

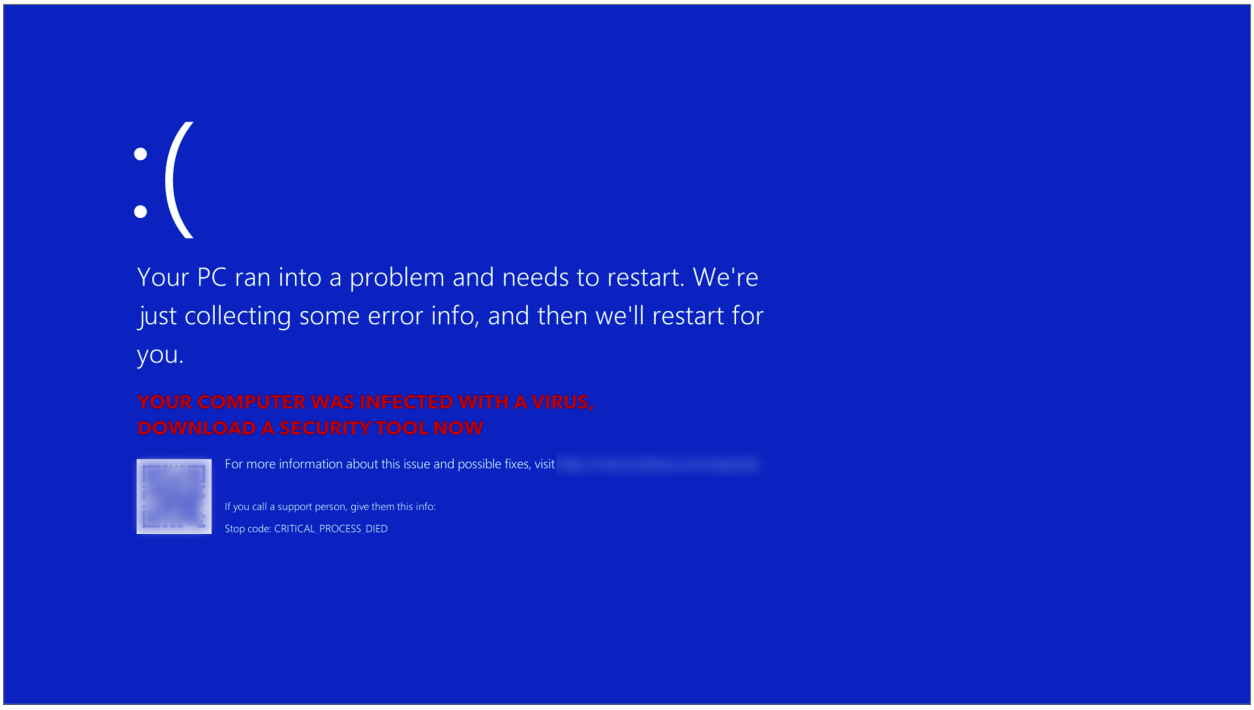


Image 19

The ad was submitted to RichAds by investigators operating undercover to test whether it would pass the company's approval process. The reply from the company's sales representative, translated from Russian to English, signaled full approval:

> *"Good afternoon! Thank you for the photo, I shared it with the moderation team, colleagues there said there would be no problems with campaign approval here."*

The image below is the actual LinkedIn exchange in Russian:

Image 20. "No problem" – Deceptive Ad Gets Approved

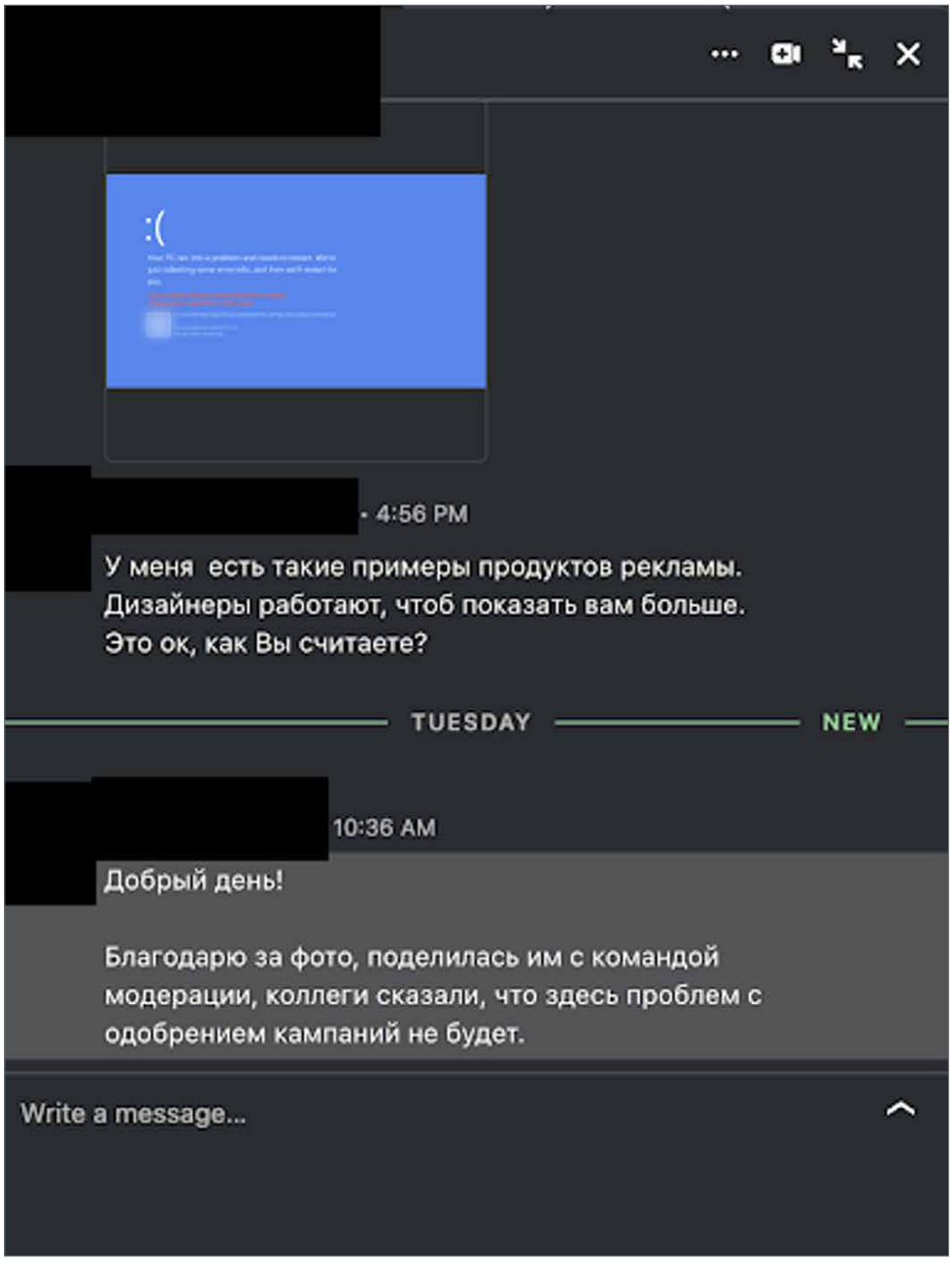


Image 20

Digging deeper into RichAds' practices provides clues as to why the company would approve such an ad - the company's website highlights a case study of a customer using similar deceptive tactics to market anti-virus services.

In the case study, RichAds highlights how the customer relied upon the company to generate and place ads that "warned" users that a virus was detected on their devices and they needed to update their antivirus software. Whether a user's computer was pristine or actually riddled with malware, targets of the ad would receive the same ominous warning that their device security was in jeopardy.

The case study highlights how the customer used a "calendar push" approach - a technique that, according to malware-guide.com, places event entries on a target's calendar that when clicked on redirects to malicious or unsafe online sources.

And RichAds did more than just place the ads, according to the case study: "All creatives were mainly produced by RichAds. In 2 months, there were 67 creatives total." Here is an image of the case study featured on RichAds' website:

Image 21. RichAd's Instructions to Users

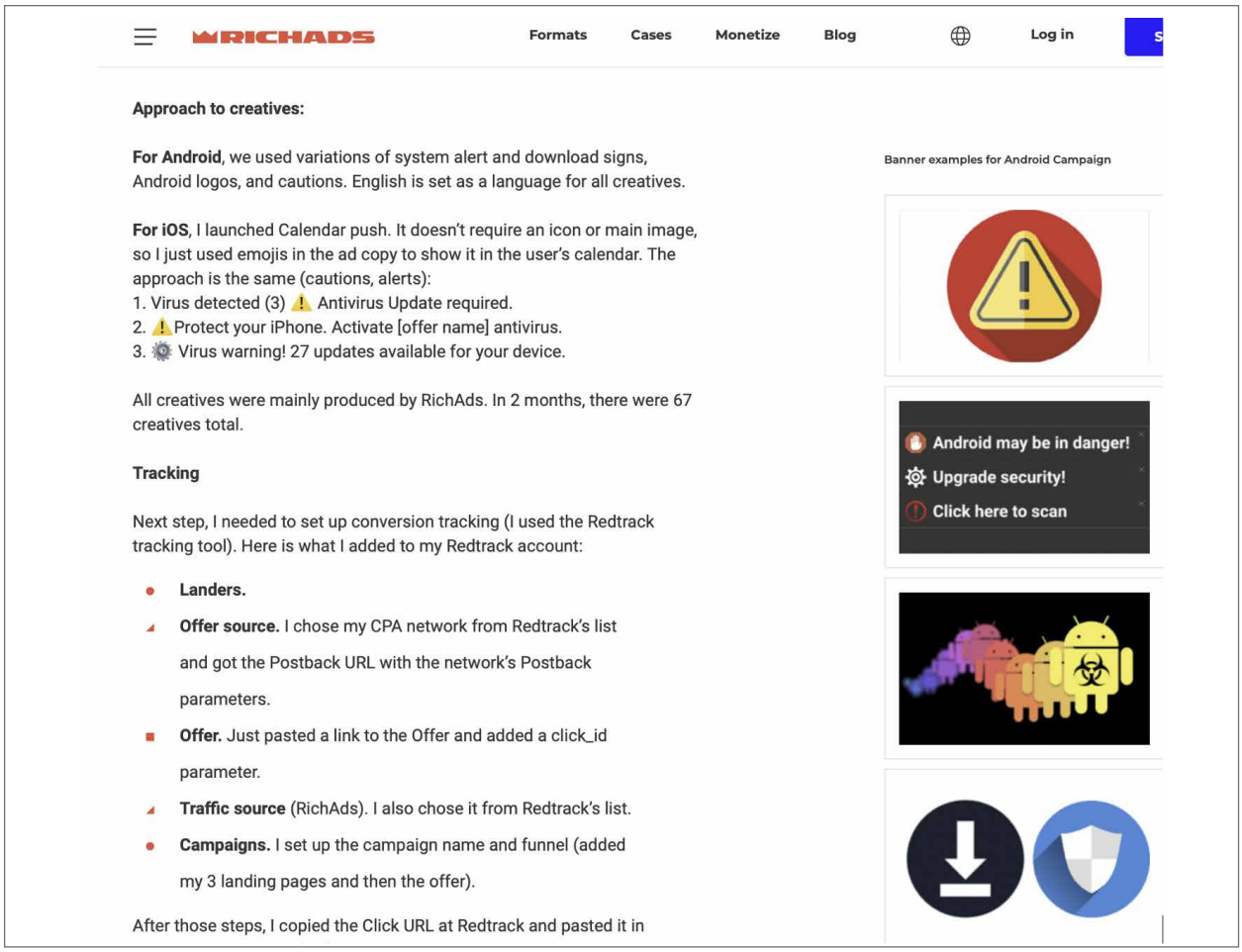


Image 21

What was the result? According to the case study, an ad spend of $8,360 led to 1.67 million clicks and 32,153 installs. The intent was to get targets to click and install by using fear tactics.

RichAds' willingness to facilitate deception went beyond this ad. When investigators asked about proposed ads for systweak and antivirus utilities (which are typically used for malvertising), the sales representative provided data on the best locations the company had found to serve those ads:

> *"In particular, the following geos showed excellent results for antiviruses: USA, FRA, CAN, BRA, MEX, DEU."*

Investigators also asked whether there were restrictions on potential malicious advertising content. RichAds didn't reject it, but simply said it wouldn't result in a high number of ad impressions:

> *"We work with various formats, there are no serious restrictions in this regard, but it is unlikely that such offers as auto-install, or landing pages with many pop-ups / too trigger pages that call for immediate action, false statements (on your phone detected 8 viruses) as well as content that blocks the screen and does not allow you to take further actions."*

It's worth noting that RichAds appears (or at least it did in 2021) to work with a company called AdSecure to combat malware. If so, it is striking that it does so while offering users the opportunity to place deceptive ads that are associated with adware and other forms of malware.

Like RichAds, PropellerAds is listed as being based in Cyprus, but LinkedIn profiles indicate a sizable contingent of its employees reside in Russia. It touts itself as uniting publishers and advertisers with a billion-plus monthly audience reach, 32,000 active advertisers, and 70,000 monthly campaigns.

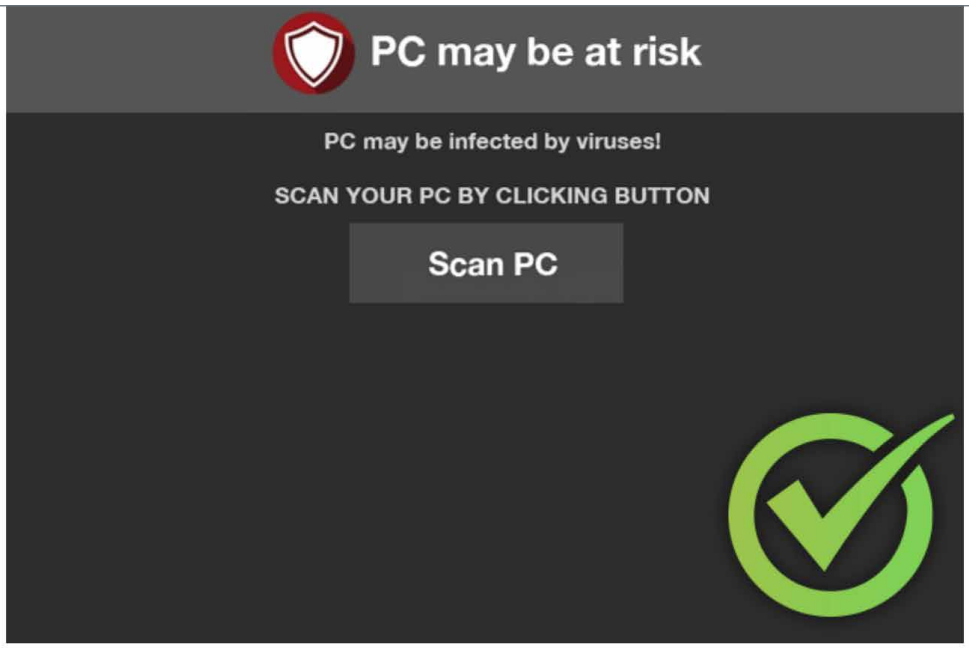
The company contends that it "does not knowingly or intentionally work with any advertiser or publisher that engages in any illegal or unlawful activities."

Yet, PropellerAds and its related domains (in-page-push.com and inpagepush.com) accounted for an estimated $31 million - or every 1 in 4 dollars - of the malvertising found on piracy websites.

PropellerAds also guides customers on what can only be described as a fine line of deception. The company's website includes guidelines on how far advertisers can go to trick users into clicking on an ad. For example, the company tells customers that they can use scare tactics in their advertising content: *"It is acceptable to use any information about possible viruses, potential threats, file damage, etc. on landing pages, which can frighten users."*

Here is an image from its website in a section it terms "Scary":

Image 22. Ad Intermediary Allows for Scare Tactics to Drive Clicks



However, please pay attention, that **it is forbidden to use logos of brands** on scary landings, such as Google, Google Chrome, Yandex, Apple, Safari, Adobe, Flash, Windows, Microsoft.

Image 22

The website also guides customers on "dos and don'ts." For example, PropellerAds says phrases such as "you won a gift card" are acceptable but not "you won an iPhone [or a] car." It also says "phishing" ads about receiving or winning substantial gifts are prohibited. At the same time, PropellerAds' focus appears to be the content on the initial landing page for the ad versus what happens after a user clicks on it. For example, the company's website says it prohibits content that contains malware, but the wording applies to landing pages. These landing pages frequently serve as the initial attempt to scare or lure users. Once a user takes the bait on the landing page, that is often where the malware trouble can start.

PropellerAds has previously pushed back on criticism it enables malvertising:

> *"Propeller Ads does not endorse, support, or encourage any malicious advertisement on its network. More to the point, Propeller Ads has a strict policy of forbidding advertisers from using the network to help advertise or distribute viruses, malware, or other unlawful or damaging content, and has implemented measures to limit this kind of content."*

Yet, the company has faced complaints for years about its role in enabling malvertising. SearchSecurity found that PropellerAds "played a significant role" in the early stages of a malvertising campaign that hijacked traffic from more than 10,000 infected WordPress sites and led to ransomware, banking Trojans, and botnets. And Ars Technica last year reported how PropellerAds was linked to a malvertising campaign to display malvertising on tens of millions of devices to lure users to purchase fake anti-virus services.

Advertising whose intent is to trick users is a serious issue for the ad industry. If companies that engage in these activities are considered part of the mainstream ecosystem - and currently they are - it calls into question how digital advertising can be trusted in the long term.

Digital Citizens reached out to PropellerAds and RichAds two days in advance of the report's release for comment. The full response from PropellerAds is posted on the Digital Citizens' website. Below are relevant excerpts:

"Propeller Ads profoundly supports any effort in identifying and combating piracy as also protecting the rights of legal owners. In fact, Propeller Ads is proud of its active efforts to prevent its network from being used for any fraudulent or illegal activity…The term 'Scary' is an online advertising industry term of art and is a common name describing a category of creatives used by antiviruses, cleaners and other utilities of such kind to protect the device of a user. It does not mean in any way that these creatives are used to mislead users or that such creatives are fraudulent."

To see the full statement from PropellerAds, go to: https://www.digitalcitizensalliance.org/issues/unholy-triangle-report.

Conclusion: Piracy Issues are Bigger than Content Theft

Piracy is the ideal environment to target Internet users. The sites provide enticing bait: free movies, TV shows, and live content, and an environment that encourages people to click where told. In short, visitors to piracy sites make malicious actors' jobs easy by voluntarily venturing into the killing fields.

The problem of piracy, ads and malvertising is multi-faceted, requiring a flexible and energetic response from law enforcement, consumer protection watchdogs, the legitimate advertising industry, and cybersecurity experts.

It starts with law enforcement.

Until the so-called piracy streaming loophole was closed in late 2020, those making millions of dollars streaming content faced minimal concern about consequences. A new law that made operating a commercial piracy streaming service a felony was a critical step; now it's important for the Justice Department to employ those tools. Indictments and convictions capture the attention of criminals, as do the seizure of domains that are used to profit off piracy.

In addition, Digital Citizens urges the Department of Justice and Federal Trade Commission to look into the connection between piracy and ransomware. In 2021, the DOJ launched StopRansomware.gov, a major initiative to combat attacks. The FTC has also warned Americans about the cyber risks of piracy.

As this report shows, malicious actors dangle free content as "bait" to lure users to be victimized. Therefore, it's vital that the DOJ targets malvertisers and piracy sites that are setting up users to be victimized by ransomware and other harmful software. In addition, the FTC should consider new efforts to alert consumers about the cyber security risks of piracy and the emergence of malvertising on these sites.

Among the biggest takeaways from this investigation is a reckoning for the legitimate advertising industry. It must make clear that ad intermediaries can't have it both ways – easily serving reputable advertisers and publishers while dabbling in the dark side of helping piracy operators to profit from ads and malicious actors to target and exploit Internet users.

With the revelation that malvertising on piracy sites is an estimated $121M annual business, legitimate players in the advertising ecosystem must decide who they want to do business with and who they will not. Anything less is enabling the illicit actors who are causing untold harm.

Consumers need a better understanding of how piracy is set up to bait them, how advertising on these sites often isn't what it appears to be, and the dangers that can come from just one catastrophic click. For that reason, Digital Citizens intends to ramp up its awareness campaigns at both the federal and state level.

Piracy and malvertising are a toxic combination. Digital Citizens Alliance, White Bullet, and Unit 221B stand ready to share the findings of this investigation and work with responsible actors who share our goals of raising awareness about the risks of piracy and malware and thwarting those trying to harm Internet users.

Appendix A: Methodology – White Bullet

1. Selection of piracy sites

A total of 500 piracy sites were selected for ad monitoring and analysis by White Bullet as well as investigation by Unit 221b. These sites were chosen from the thousands of piracy sites in White Bullet's Intellectual Property Infringement Platform (IPIP™) to include the most popular piracy sites as well as sites with significant malvertising ad impressions. Specifically, sites were included if they were known to have advertising and met one of the following criteria:

a) The site was among the most popular piracy sites (those with highest ad impressions overall) with at least one malvertising ad impression in the three months prior to the selection process.

b) The site was one of those delivering high levels of malvertising in the three months prior to the selection process.

2. Collection/training ads

White Bullet's proprietary technology collected data on the ad profiles of the 2022 Malware Study Sites from 26 countries during April and May 2022:

1. Australia
2. Belgium
3. Brazil
4. Bulgaria
5. Canada
6. Czech Republic
7. Denmark
8. Estonia
9. France
10. Germany
11. Greece
12. Hungary
13. Ireland
14. Italy
15. Lithuania
16. Malta
17. Netherlands
18. Poland
19. Portugal
20. Romania
21. Russia
22. Slovakia
23. Spain
24. Sweden
25. United Kingdom
26. United States

White Bullet has developed its proprietary advertising monitoring system, which captures high-volume data about advertising placed on IP infringing sites (defined as infringing copyright or disseminating counterfeit goods) through which parties may monitor ad profile changes (the Ad Monitoring System).

The Ad Monitoring System:

- visits IP-infringing sites from local internet protocol addresses (IP addresses) to track locally served ads,
- captures images of ads in the context of the infringing web page,
- uses White Bullet's proprietary technology to identify brands and advertising sectors (e.g. malware, adult, financial, fashion, travel, technology), and
- identifies adtech intermediaries engaged in the placement of advertising (Ad Intermediaries), by analyzing data on all intermediaries involved in the process of targeting, placement and delivery of ads.

Each URL was visited daily from all countries tracked using one of the nine user profiles below. Each profile was rotated on a scheduled cycle to ensure all sites were visited equally.

- *Neutral (cookieless) profile*: for collection of non-targeted ads. This gave the monitoring exercise a neutral benchmark. It was also an important stand-alone category as many consumers of digital IP-infringing content use anonymization technology – such as VPNs and proxies – to protect their privacy and, therefore, do not visit IP-infringing sites with any attributable cookie profiles.
- *Female user profiles*: four profiles, each of which included multiple interest-based user profiles within this category.
- *Male user profiles*: four profiles, each of which included multiple interest-based user profiles within this category.

Over 100 specific interest sectors were used to develop profiles (including travel, weather, fashion, personal finance, etc.). Cookies also related to previous visits to IP-infringing content.

3. Revenue Calculation

Potential annual worldwide revenue is the potential estimated annual ad revenue that sites could generate worldwide based on actual advertising data collected by White Bullet's automated Ad Monitoring System and incorporating available pageview data and extrapolating to include full annual coverage for all countries.

White Bullet calculates estimates of the advertising revenue of piracy sites by combining multiple independent and proprietary data sources within a revenue calculation algorithm. This includes (i) data about actual ads captured by White Bullet during ad harvesting visits, (ii) pageview data for those sites indicating traffic volume drawn from independent third-party sources, and (iii) advertising valuation data based on a proprietary matrix calculated from industry advertising payment values combined with advertising bid values identified by White Bullet in the code behind captured ads.

To create the advertising valuation matrix, White Bullet applies multipliers to core base values for the three dominant payment models in digital advertising: Cost Per Mille (CPM), Cost Per Click (CPC), and Cost Per Action (CPA). White Bullet's methodology uses a different core base value for CPM, CPC or CPA advertising drawn from industry estimates from third-party sources, which depend on various data components, including market sector (e.g., health, finance, travel), ad format (e.g. display, pop up/under) and media type (e.g. image, video, rich media). Multipliers applied are dependent on the advertiser type (e.g., premium household brand, clickbait), ad dominance (e.g. density of ads on the webpage) and country where the ad is displayed (a multiplier is applied to each ad for that country based on average advertising spend by internet user for that country as a percentage of average advertising spend by internet user benchmarked against the US). For CPC and CPA advertising, core base values and related click-through rates depend on the market sector, and multipliers are applied to both core base values and click-through rates depending on the ad format, media type, as well as advertiser type, ad dominance and country, again drawn from industry estimates from third-party sources. Data points collected from ad harvesting visits by the Ad Monitoring System are cross-referenced with the advertising valuation matrix, after which extrapolation calculations are created using estimated third-party pageviews to those sites and the ratio of ads to visits by brand by country. Third-party data included in the above calculations are drawn from numerous sources, including Statista, eMarketer, Google AdSense, industry experts and ad exchange bid data.

Advertising values are heavily dependent on a range of factors and are therefore estimates based on extrapolating data using statistical correlations. White Bullet uses conservative base values and multipliers within the advertising revenue matrix and conservative pageview extrapolations, understanding that sites might command varying advertising rates with different demand side and advertiser buyers. The values in the advertising revenue calculation algorithm are periodically reviewed and updated as needed to reflect the digital marketplace.

Appendix B: Investigation Methodologies-Unit 221B

Pirate Site Review Methodology

Manual Review

Unit 221B manually reviewed each of the 500 target pirate sites to mimic organic user activity and experience.

Manual review environment:

- Windows 10 Virtual Machine (VM) sandboxes with native security features disabled.
- Mozilla Firefox browsers, also with all native security features disabled.
    - A snapshot of this low-security VM state was used for repeatable testing.

While auditing a pirate site, Unit 221B performed activities that were natural for an unsuspecting user.

- All notifications allowed, pop-ups enabled, and each available ad clicked.
- View at least one media file from each site, switching offered streaming servers where possible.
- If a site offered media or torrent downloads, Unit 221B downloaded at least one file to review for ride-along malware.
- Download malware for analysis.

Automated Testing

Unit 221B deployed automated scrapers to collect data from the surveyed sites and analyze connected sites and IP addresses. Scraper behavior:

Manual review environment:

- Scrape the front page of a pirate site.
- Automatically simulates clicks deeper into the site.
- Scrape content from linked third-party domains, including malvertising and malware providers.

URLs were then submitted to an array of Url Reputation services, which catalog and classify websites. Unit 221B analyzed the results from 13 Url Reputation sources to assign each pirate site and intermediary a risk score.

Scoring Algorithm

For score generation, target pirate sites and intermediaries were analyzed by VirusTotal and other URL reputation services for initial reporting data and metrics. Metrics unrelated to site maliciousness were disregarded. Weighted scores were compiled from initial values of this data, modified by described weighting criteria.

Pirates and Advertisers Methodology

In addition to the initial review of White Bullet's 500 pirate site list, Unit 221B conducted an investigation into the behind-the-scenes relationships between advertising networks, pirate sites, and hackers and malware distributors. Malware discovered in the first phase of the investigation, as well as new malware discovered on pirate sites, was executed within a secure environment to assess potential user risk. This methodology defines the criteria under which targets were selected, operational security measures employed by Unit 221B, and a summary of malware analysis procedures.

Approach

Using an undercover persona, Unit 221B submitted applications to malvertising networks, posing as a would-be malware distributor. Once applications were accepted, investigators reviewed site documentation including guides for conducting malvertising practices through the targeted distribution network. When possible, investigators communicated with staff at the target organization to obtain information including explicit policy rulings for items that might violate the site's stated content rules.

Ad Network Selection Criteria

Unit 221B selected advertising networks for investigation based on the following:

- Targets must be linked to multiple pirate sites present on the list provided to Unit 221B.
- Targets must have a strong advertising presence of their own (i.e. appear in public searches as sponsored content).
- Targets must be responsive to communications.

Operational Security Measures

To protect investigators and project security, Unit 221B established the following protocols:

- All project activities were conducted using Windows 10 virtual machines (VMs) stored in the cloud, with an established snapshot to easily restore machine state.
- VPNs were used to disguise network traffic.
- Investigators alternated between using Ukrainian-based and Russian-based location sources through these VPNs.
- Domains registered for use in advertising communications were created with anonymous information.
- Static content potentially served through these domains was hosted through Cloudflare.

Fake LinkedIn Profile

Unit 221B established a fake LinkedIn profile for communication with target advertising networks, subject to the following protocols:

- All communications between investigators and targets were recorded for transparency.
- No real personal identifying information was added to this fake account. Pictures used were created using open-source AI generation.
- Unit 221B's persona was fluent in both English and Russian.

Malware Analysis Methodology

Unit 221B subjected discovered malware to static and dynamic analysis under the following protocols:

- All project activities were conducted using Windows 10 virtual machines (VMs) stored in the cloud, with an established snapshot to easily restore machine state.
- Anonymous VPNs were deployed on these VMs with enabled kill switch functionality, preventing internet connection without first connecting to the VPN.
- VMs were loaded with fake PII to simulate the variety of data that may be affected during an attack.
- Screen recording software was run through the host machine to protect video data integrity.
- Malware samples were submitted to the VirusTotal engine for collaborative analysis from multiple security vendors.

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.

About White Bullet Solutions

Founded in 2013 by a leadership team of experienced Intellectual Property lawyers from the media and advertising industries, White Bullet offers companies piracy risk data and protection, brand safety solutions and full transparency on their advertising placement and digital supply chains.

White Bullet works collaboratively with brands, policy makers and the advertising industry to safeguard advertising spend and prevent ad placements from appearing on IP Infringing domains and apps. White Bullet is a certified brand safety anti-piracy solutions provider under the advertising industry regulator TAG and is a stakeholder to the EU Commission Memorandum of Understanding on Advertising and IPR.

White Bullet comprises IP experts and dedicated technical engineers who specialize in AI, big data models and predictive machine learning. The team includes highly skilled investigators and data analysts experienced in tackling the funding and distribution of pirated content. With offices in London, New York and Los Angeles, White Bullet advises policy makers and government bodies on regulatory and compliance programs globally.

About Unit221B

Unit 221B, LLC focuses on products and services designed for selected clients, primarily those seeking discreet advanced cyber requirements and operations. We are comprised of unique specialists in the fields of information security, cryptography, forensics, legal, investigations, law enforcement, and intelligence.

digitalcitizens alliance | whitebullet | UNIT 221B GUIDED BY INTEGRITY DISCREET BY DESIGN