Google

Written Testimony of George Salem
Senior Product Manager, Google Inc.
Senate Permanent Subcommittee on Investigations hearing on
"Online Advertising and Hidden Hazards to Consumer Security and Data Privacy"
May 15, 2014

Chairman Levin, Ranking Member McCain, and Senators of the Subcommittee:

Thank you for the opportunity to testify today on Google's efforts to combat malware on the web. My name is George Salem and, as a Senior Product Manager on our Ads Policy team, I develop tools for and support our teams of engineers who fight abuse on our platforms. These teams work to identify bad sites and malware; specific divisions seek to find the root of the malware and combat malicious advertising, also known as "malvertising."

Ensuring our users' safety and security is one of Google's main objectives. One of the biggest threats consumers face on the web is malicious software, known as malware, that can seek to control computers or software programs. Malware allows malicious actors to make money off of innocent victims in various ways. Infected computers can be used to send email spam, support distributed denial-of-service attacks, or extract sensitive user information for means that include identity theft, which has now topped the list of consumer complaints reported to the Federal Trade Commission for thirteen years in a row. Protecting our users against such incursions on their data advances important security and privacy objectives.

Today, I wish to share three main messages:

First, we believe in providing our users the strongest protections against harmful or malicious content. We think about this problem broadly: beyond just malware, we seek to protect our users against any practice that negatively impacts their experience on the web.

Second, we have a two-pronged approach to fighting malware: prevent and disable. Through a combination of sophisticated algorithms and manual review, we prevent users from visiting bad sites and we proactively scan tens of millions of ads each day across multiple platforms and browsers, disabling any ads we find to have malware.

Third, the fight against malware is a team effort, and we collaborate closely with others in the internet community. The online ecosystem is complex and involves many players, particularly when it comes to advertising. Online platforms are in an ever-shifting battle against parties that benefit from malware and are constantly seeking new ways to avoid our detection and enforcement systems. For that reason, we actively contribute best practices, watch lists, and other resources with others to stay ahead of the game.

It's a complex problem, but we are tackling it head on through tools, user education, and community partnerships.

Protecting our users with the strongest protections against harmful or malicious content

Protecting the security of our users and their data is one of our main priorities at Google. Beyond malware, we work to protect our users against what we call 'badware' more generally. Badware encompasses any software that may not be strictly malicious or fraudulent but nonetheless results in an unwanted user experience. Badware may include "trick to click" ads and unwanted system preference downloads. Our business relies on users' trust and ease when using our services, and our goal is to protect against anything that may negatively impact a user's experience in using the web.

Some cybercriminals attempt to use online advertising to distribute malware, a practice known as malvertising. Possible vectors of attack include malicious code hidden within an ad creative (such as a .swf file), embedded on a webpage, or within software downloads. While most ads are safe and legitimate, some bad actors try to find ways to trick consumers by getting harmful and deceptive ads published on reputable sites, exploiting the fact that advertising space may be syndicated to parties who are not known to a web site owner.

Malvertising derails users' faith in the online ecosystem. Advertising has had a tremendous role in the evolution of the web, bringing more products, tools and information to consumers, often free of charge. It has allowed the web economy to flourish — Internet ad revenues surged to a landmark $20.1 billion in the last quarter and the advertising-supported Internet ecosystem employs a total of 5.1 million Americans. Bad ads are bad for everyone, including Google and our users.

Google has a long history of fighting malware, however it is distributed. Ten years ago, we launched a set of Software Principles to protect the broader web against unwanted programs. These principles are a broad, continually evolving set of guidelines around installation, disclosure, behavior and snooping. They state, for example, that applications should not trick our users into installing them; should make it clear when they are responsible for changes to users' experience;

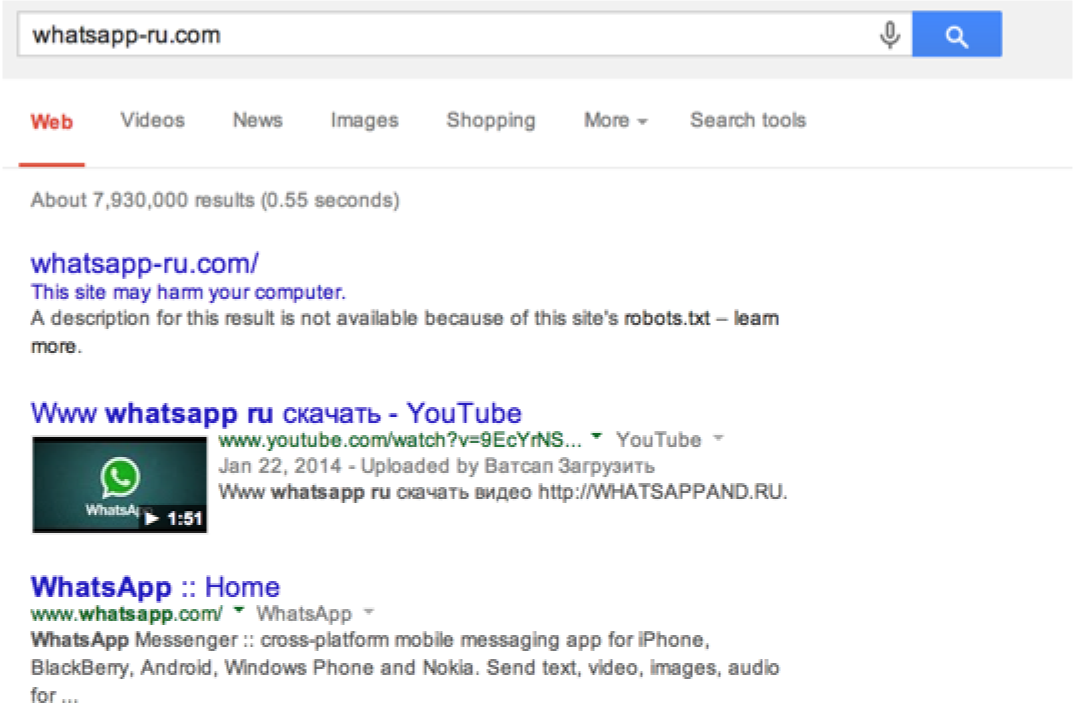
should clearly disclose when they collect or transmit users' personal information, including through an easy to find privacy policy; and should offer easy options for their disabling or removal, should a user desire it. We follow these guidelines with all the products we develop and distribute, and because we strongly believe they are good for the industry and users worldwide, we encourage our current and prospective business partners to adopt them as well.

Our two-pronged approach: Prevent & Disable

Malware and badware are a constantly evolving problem. Google has a two-pronged approach to protecting users from malware online: prevent and disable.

Prevent

One of the best ways to insulate users from the dangers of malware is by proactively preventing them from accessing infected sites altogether. To this end, we developed a tool called Safe Browsing to identify unsafe websites. Safe Browsing creates a continuously updated list of known phishing sites — sites that pretend to be legitimate while trying to trick users into typing in their username and password or sharing other private information — and malware sites. Any page a user visits, as well as all the resources on that page — including pictures and scripts — are checked against this list. Malicious sites we find are then clearly and conspicuously identified as dangerous in Google Search results.



whatsapp-ru.com

About 7,930,000 results (0.55 seconds)

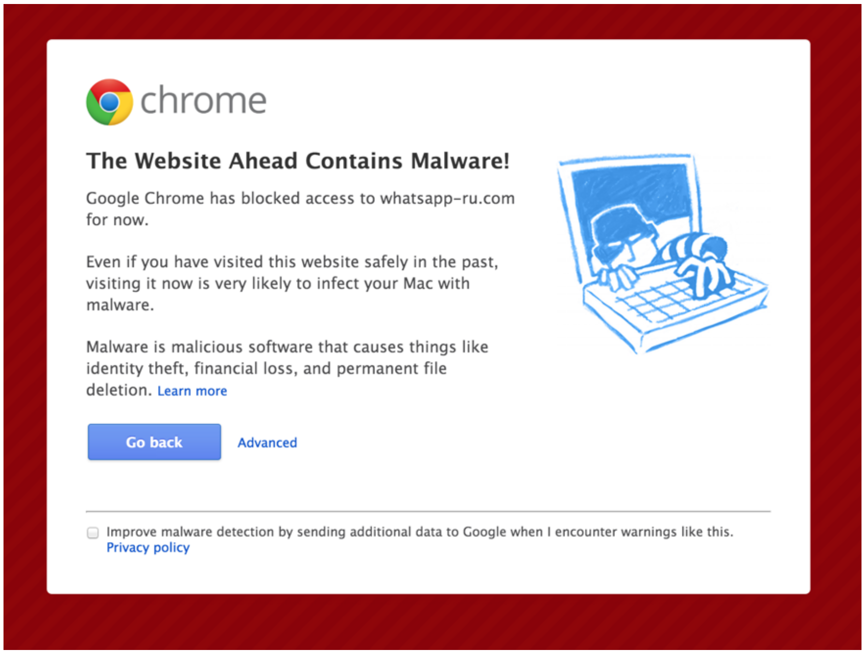
whatsapp-ru.com/
This site may harm your computer.
A description for this result is not available because of this site's robots.txt – learn more.

Www whatsapp ru скачать - YouTube
www.youtube.com/watch?v=9EcYrNS... YouTube
Jan 22, 2014 - Uploaded by Батсан Загрузить
Www whatsapp ru скачать видео http://WHATSAPPAND.RU.

WhatsApp :: Home
www.whatsapp.com/ WhatsApp
WhatsApp Messenger :: cross-platform mobile messaging app for iPhone, BlackBerry, Android, Windows Phone and Nokia. Send text, video, images, audio for ...

We were the first major search engine to provide this type of warning in search results in 2006, and over a billion people use Safe Browsing today. Every day, we examine billions of URLs, we discover more than 10,000 new dangerous websites, and we show clear and conspicuous warnings on up to 14 million Google search results and 300,000 malicious downloads.

We help tens of millions of people every week protect themselves from harm by making safe browsing the default setting to users of Google Chrome, Mozilla Firefox and Apple Safari browsers and when users attempt to navigate to a site that would steal their personal information or install software designed to take over their computers they get a warning. Whether a user navigates directly to a compromised site or is directed to it through other means, such as an advertisement, they will instead see an unambiguous interstitial — a page inserted before the user's intended destination site loads — alerting them to the presence of malicious content and advising them to click away from that site. We want to help protect all Internet users, not just those using Google services.



chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to whatsapp-ru.com for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

□ Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

We not only make Safe Browsing data and lists available for others to use for free, but we also provide an interface for others to plug in and review identified malware: our Safe Browsing API. An API is an application programming interface that details how certain software should work together. This API enables client applications to check website addresses against Google's constantly updated list of suspected phishing and malware sites, extending Safe Browsing protection to tens of millions of people every week.

We learned from our Safe Browsing data that most sites containing malicious code have been compromised by malware authors without the knowledge of the webmaster. Consequently, we encourage webmasters to sign up with Google's Webmaster Tools so they can receive notifications when we find security problems on their site. We send thousands of notifications to webmasters every day and provide them with resources to help them fix their issues. Once notified, most of them take action to clean up their sites within 30 days.

In addition, Safe Browsing Alerts for Network Administrators allow Autonomous System (AS) owners to receive early notifications for malicious content found on their networks. A single network or ISP can host hundreds or thousands of different websites. Although network administrators may not be responsible for running the websites themselves, they have an interest in the quality of the content being hosted on their networks. With this additional level of information, administrators can help make the Internet safer by working with webmasters to remove malicious content and fix security vulnerabilities.

Disable

While we work very hard to prevent users from coming into contact with malware on the web in general, we work just as hard to disable and keep malware out of our advertising products and services. We have always prohibited malware in our ads and we have strict suspension policies for partners that spread malware or badware. When an account is suspended, we stop running ads related to that account and we may also suspend any related accounts. We do allow advertisers to appeal a suspension if they fix the violations in the account and send us a report of the changes they have made. For those who we have found to repeatedly violate our policies or who have not resolved their violations, the account will be permanently suspended along with any new account setups the advertiser tries to create in the future.

In 2006, to fight the proliferation of malvertising, we built a dedicated system to scan our Ads platforms and disable any account that distributes malware or badware. Today, we proactively scan billions of ads for malware on all aspects of our advertising services, which includes search and display ads on multiple platforms and browsers. We subsequently re-scan the ads that pose greatest risk to our users to make sure malware has not been introduced into an advertisement after our initial vetting. It should be noted that the vast majority of ads served by Google are good, and most of the ads we disable are hosted by third parties.

Our internal systems have a proven track record in disabling malvertising. In 2013, we disabled more than 350 million bad ads, disapproved more than three million applications from joining our networks due to possible malware, blacklisted more than 200,000 publishers, banned over 270,000 advertisers, and disabled advertising from more than 400,000 websites hiding malware. In fact, we disabled 400,000 ads in the last 30 days for malware policy violations.

While we are very proactive in our efforts against malware, we are often silent to the public about our internal scanning technologies and other specific initiatives. Malware and badware are pushed by bad actors who are sophisticated and dynamic, constantly seeking ways to avoid detection and enforcement by internet platforms. Our goal is to stay one step ahead of malvertisers and not tip them off to our activities even as we share tips and best practices with our users and with the broader Internet community.

We work very hard to prevent malware in our system, but bad actors are very sophisticated and sometimes incidents of malvertising do occur. In 2010, a malware threat called JS:Prontexi was widely publicized. This was one of the first published accounts where an advertising malware threat occurred with no user interaction or clicks. What was not publicized was that Google had become aware of the issue and moved quickly before the reports made it to press. By that time, we were actively scrubbing existing and new ads, already disabling over 10,000 bad ads. The remaining few hundred malware distributing ads were found quickly thereafter.

Earlier this year, a rogue advertiser began serving malware infected ads to users in YouTube. Like many attacks, this began on a Friday afternoon. Days earlier, we had disabled the malware serving site with Safe Browsing. So users of browsers that subscribe to safe browsing - Chrome, Firefox, and Safari - were protected when the attack began. Bromium, the operation publishing the threat, worked with Google directly to identify the exact ads. Since this attack, our teams took the appropriate steps to resolve the issue and beefed up our dynamic tests to prevent such events from occurring again. These are a good examples where like-minded industry partners worked together, behind the scenes, to protect all of our users.

We work with industry and share best practices

The anti-malware teams at Google study malware distribution and work closely with the security community to identify malware on the web and share the information more broadly.

To further disseminate helpful information on how to protect users' security, last year we incorporated data on Safe Browsing into our Transparency Report. The site provides information on how many people see Safe Browsing warnings each week, where malicious sites are hosted around the world, how quickly websites become reinfected after their owners clean malware from their sites, and additional information. By providing details about the threats we detect and the warnings we show, we hope to shine some light on the state of web security and encourage safer web security practices.

We are a member of StopBadware.org, an anti-malware nonprofit organization run by the Berkman Center at Harvard Law School that offers resources for website owners, security experts and ordinary users. The site hosts the Search Badware Website Clearinghouse, a searchable database of badware URLs that is voluntarily submitted by StopBadware's partners, sponsors, and users. StopBadware uses the data to analyze and report trends in web-based infections, provide the public with research tools such as the Top 50 Networks list, and assist web hosting companies and other network providers with identifying badware sites on their networks.

We also own VirusTotal, a free web service that provides checks for viruses, worms, trojans and other kinds of malicious content. It uses 51 anti-virus products and scan engines to evaluate user-uploaded files or URLs, and it also offers a free public API. While the service helps identify malicious content, it may also be used as a means to spot false positives — innocuous resources detected as malicious by one or more scanners.

Furthermore, we created an email alias connecting vetted industry players and we use it to notify them directly of malware compromises and trends. Parties on the alias include the anti-malvertising teams from various ad-serving and tech companies. Additionally, we have industry contacts within companies that utilize Google ad products to provide direct feedback.

In 2009 we created Anti-Malvertising.com, a website that provides best practices and investigative resources for publishers and ad operations teams, as well as tips for users. The site includes a custom search engine to run quick background checks on advertisers: one can enter an advertiser's name, company name, or ad URL and access information to help determine whether said advertiser is trustworthy. Anti-Malvertising.com fits into our broader goal to help and encourage all members of the online advertising ecosystem to take an active role in malvertising prevention. It's one part of Google's commitment to educating our customers, improving the industry as a whole, and making the Internet a safer place for everyone.

More recently, we co-founded the Trust in Ads group with Facebook, Twitter and AOL to protect users from malicious online advertisements and deceptive practices. We kicked off this effort by identifying abusive practices in the tech support advertising space. Scam advertisers often present themselves as official representatives of companies of products for which users seek support. Under the disguise of paid assistance, these advertisers trick users into special downloads and installs that that may contain malicious software. Trust in Ads offers guidance on how to avoid these scams in the first in a series of trend reports on bad ads. The site also has a dedicated page at trustinads.org/report with information on how users can easily report any kind of suspicious ad on the group's founding companies' platforms.

Conclusion

The Internet is a driver of innovation, communication, and entrepreneurship, which underscores the importance of implementing policies and procedures that protect our users' data. We are committed to developing technology to protect users across the web, contributing research, and facilitating industry initiatives and conversations. We believe that if we all work together to identify threats and stamp them out, we can make the web a safer place for everyone. We look forward to working with this Subcommittee on additional ideas and initiatives to keep users safe online.

Thank you again for your time and consideration.