



Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave N.W.
Suite CC-5610 (Annex B)
Washington, DC 20580

Google would like to thank the Federal Trade Commission for organizing and hosting its recent *Fall Technology Series: Ransomware* event. The panels facilitated a substantive conversation about this important security issue and how consumers, businesses and industry can better address this challenge. We file this comment to provide additional information about ransomware, as well as about some tools provided by Google to help consumers and businesses avoid ransomware and related threats.

Characteristics & Evolution of Ransomware

As the FTC is aware, ransomware has become one of the most prominent threats that affects end-users of web and internet tech. Ransomware is a type of malware that holds consumer data for “ransom” by denying users access to their own computers, and then asks for a payment to regain access. Users may be tricked into installing malware that appears to be legitimate software, then, once their device has been infected, the demands for “ransom” often appear cloaked as some sort of fine, cleanup cost, or under another specious pretext. These payment demands often present a significant hardship to the affected consumers and businesses.

Although ransomware has received a lot of press and attention due to some recent high-profile cases, forcing infected users to pay a ransom is not a new technique for attackers. Locking-up a user’s data and requiring victims to pay their attackers with alternative currencies like Bitcoin are both novel twists on a base technique.

Experts have been aware of this approach for years: consumers get tricked or forced into making financial payments to attackers that have taken control of devices and data. For example, starting about a decade ago, consumers saw a rise in so-called “Fake-Antivirus” malware that falsely claims to have found malware infections on a user’s device, and continuously sends warnings and alerts (interfering with the user’s ability to operate the computer normally) until the user pays fees to remove the purported threats. The following screenshot is an example:

Ransomware has evolved over the years to take different forms, and recent variants exhibit increasingly aggressive behavior on user devices to elicit payment. Recently there has been a rise in ransomware that takes control of the device by fully encrypting a device's storage, denying the user access to her computer, mobile phone, or other device unless she pays a fee to obtain an unlock key.

Other forms of ransomware take over the user workspace (e.g., computer desktop or browser window) and ask the user to call a support number to get rid of the problem. Calling the number will often result in the installation of more malware, and users being charged a fee. In some cases, the computer has actually been infected, but in others the user is tricked into believing irreparable harm will come to their device unless they reach out for help to the "tech support" or "law enforcement" entity that is sending them warnings:



This computer contains pirated software and has been blocked by ICE-Homeland Security Investigations.



Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a \$250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)

As a first-time offender you are required by law to pay a fine of 500 USD
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities. You will be charged, fined, convicted for up to 5 years.
How to pay a fine? There are two ways to pay a fine:
1. You can pay the fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest vendor. Your computer will be unlocked after the payment is made.
2. (Offline Option) You can come to your local courthouse and pay the fine at the 'Cashiers' window.
A special restoration software will be sent to you by mail within a week after the payment is made.
To regain access now transfer BitCoins to the following address (click to copy):
1NdR8tEKRBoQ1oIyAPhpuks9Uct6XftEdW
After the payment is finalized enter Transfer ID below.

Amount: Transfer ID:
BTC 1.773

Note: All files on this computer have been encrypted with a strong symmetric algorithm and a 4096-bit key. Files will be inaccessible until the fine is paid. Attempt to remove this message will result in irreversible damage to your files, hardware and Windows installation. [View encrypted files](#)

[Payment](#) [BitCoin Information](#) [BitCoin Exchanges](#) [BitCoin ATMs](#) [Internet Browser](#) [Notepad](#)

Project Global 3 is a coordinated effort by U.S., Canadian, European, Australian, New Zealand and other law enforcement agencies across the globe targeting computers with pirated content and their operators.

Critical Error !

This Computer may have some System File Corrupted.
Contact Technical Department 1-888-671-██████

Enter a product key

Your product key should be in an email from whoever sold or distributed Windows to you, or on the box the Windows USB came in.

The product key looks similar to this:
PRODUCT KEY: X0000X-X0000X-X0000X-X0000X-X0000X

Product key

Dashes will be added automatically

Example Screen-locker.



Users are exposed to ransomware on their devices in different ways. Sometimes users will download malicious software that infects their device from the web. There are many examples where innocent-sounding software (e.g., utilities or screen savers) is made available for free, but malicious extras are bundled-in without the user's knowledge. Screen-lockers and fake security products are often delivered via so-called bundler networks that distribute unwanted software.

In other cases, users aren't downloading software on purpose; more egregious forms of ransomware (e.g., crypt-lockers) are distributed via exploits (where the ransomware is planted on the victim's device as part of an attack). These so-called "drive-by downloads" are particularly pernicious; the user may not realize they have downloaded ransomware. Sometimes drive-by downloads are made possible by taking aim at other aspects of the ecosystem—for example, by exploiting a browser or plugin vulnerability—and demonstrate how addressing the ransomware problem requires improving security habits at all levels. Other traditional channels of distributing malware are also being used by attackers. For instance, we have also noticed a recent trend of using spam emails, with the ransomware disguised as a link or attachment in the email.

Educating consumers and businesses about basic security best practices, as the FTC has done through its consumer education efforts, and encouraging all users to regularly install software updates with the latest security patches, will make them less vulnerable to these attacks.

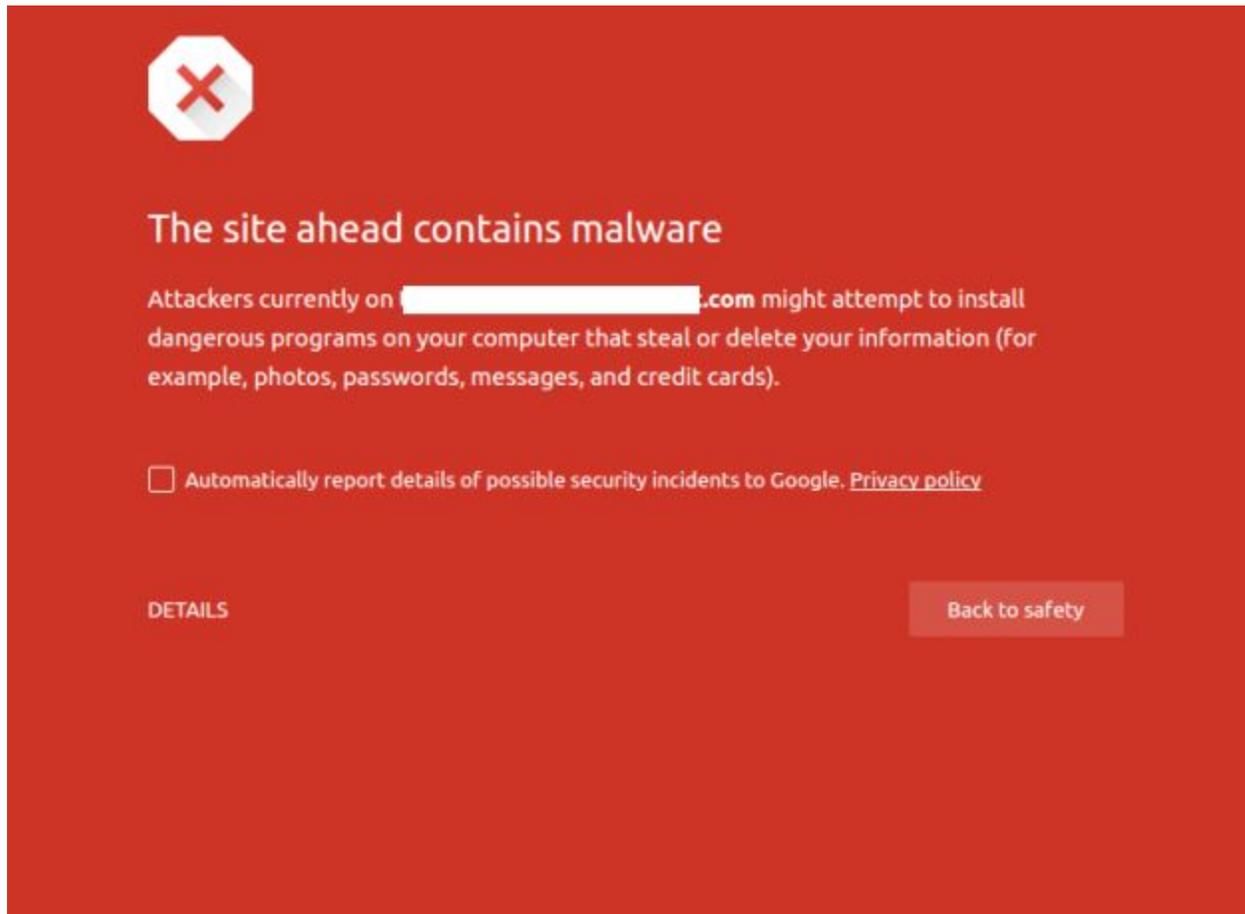
Google's Efforts to Protect Users from Ransomware

Over the years, Google has made significant investments to improve the security of the entire web ecosystem and to provide useful services that better protect users from various kinds of malware and phishing attacks. With Google Safe Browsing, we scan the web looking for malicious and deceptive pages that could harm users, and then we share what we find via warnings to end-users, alerts to potentially compromised website owners, and API services available to developers wanting to protect their users on the web. Our systems examine billions of URLs and uncover thousands of new unsafe sites every day. The results of our detection and analysis systems are built in to products across Google to inform and encourage users to avoid web-based threats.

Google designed Safe Browsing to also provide protection to people exposed to unsafe links and content who don't use Google products. We share Safe Browsing data for free via our publicly available API, which is why Firefox and Safari users also receive warnings whenever



they visit a web page that is known by us to distribute malware. Over a billion users and over two billion devices are protected by Safe Browsing from unsafe sites.



Example of Safe Browsing warning in Chrome.

Ransomware has become one of the highest-priority malware types that we are working to detect and combat. It poses a triple-threat to users: they can be financially defrauded, denied access to their own computers/data, and their personal data may be leaked to attackers seeking to cause additional harm. Google Safe Browsing has developed various capabilities to identify ransomware based on some of its unique features. By using Google's large-scale infrastructure to scan the web, in combination with our expertise in machine learning and software analysis techniques, we continually improve our capabilities identify web-based threats like ransomware. Our ongoing investment here allows us to identify new threats more quickly, and rapidly extend that protection to all our users and their devices.



Business users may also fall prey to ransomware attacks affecting employee devices or internal systems. We have also seen websites compromised by attackers that silently leave behind exploit kits (that are hidden from the legitimate webmaster and web developers), which then go on to exploit or infect visitors to the website. To assist webmasters and IT administrators, we provide proactive alerts when our systems detect that their websites may have been compromised and are now hosting malicious content. These alerts are available for free to website owners who register with Google's Search Console tool for webmasters, and are designed to help webmasters identify and resolve issues quickly.

Identifying threats and providing strong security is a constantly evolving challenge, and Google will continue investing in tools and resources that make the online ecosystem safer.

Conclusion

We would like to thank the FTC for holding this event and for its efforts to combat ransomware and educate consumers and businesses about strong data security. Making progress on this issue will require a commitment from all stakeholders to continue to improve security tools and raise awareness about data security best practices. There is still much work to be done to ensure that ordinary consumers and small businesses know how to keep their data secure, and the FTC's leadership on this issue is greatly appreciated.

Thank you for the opportunity to provide comments on this important subject.

Sincerely,

Moheeb Abu Rajab, Allison Miller, & Stephan Somogyi
Google Safe Browsing