

OPERATION AURORA



McAfee Offers Guidance as China-Linked Google Cyberattack Continues to Unfold

McAfee, Inc., has recently released guidance to help organizations determine if they were targeted in the same sophisticated cyberattack that hit a growing list of companies, including Google. The high profile cyberattack, linked to China by Google, targeted valuable intellectual property.

"This is the largest and most sophisticated cyberattack we have seen in years targeted at specific corporations," said McAfee Worldwide Chief Technology Officer George Kurtz. "It is a watershed moment in cybersecurity because of the targeted and coordinated nature of the attack. As a result, the world has changed; organizations globally will have to change their threat models to account for this new class of highly sophisticated attack that goes after high value intellectual property."

"Today's cyberattacks are so sophisticated that they do great damage without leaving a trace," according to McAfee Worldwide Chief Technology Officer George Kurtz. "Which leads to a major problem that seems to be a common theme: there is no body to be found. And without that body—the data—the CEO and CIO won't necessarily believe there's an urgent issue because in the past, all serious security threats came with a very obvious body included at no extra charge."

"While a sophisticated attacker will leverage insidious malware, don't expect them to drive a truck through your network and leave a calling card on the way out," Kurtz continues. "Instead, expect low and slow movements of data that 'blend' into the massive amount of traffic flow that happens on a daily basis on your network."

As part of the fallout of the attack, Windows users currently face a real and present danger due to the public disclosure of a serious vulnerability in Internet Explorer. McAfee was the first to discover and announce that an Internet Explorer vulnerability was a key vector in the attack on Google and others. Unfortunately, the risk has been compounded because the attack code that exploits this Internet Explorer vulnerability has now been posted in the public domain, increasing the possibility of widespread attacks. McAfee technologies provide protection against current threats related to the attack on Google and others.

How to know if your organization was compromised

Over 30 organizations have reportedly been targeted by the same attack that hit Google and the list of victims continues to grow. McAfee calls the cyberheist "Operation Aurora" and today provided detailed guidance to help organizations determine if they were impacted by the attack, which occurred over the December holidays and into early January.

McAfee's guidance involves three steps:

1. If you are a McAfee customer, verify that you are using the latest threat definition files and perform a full scan on all machines within your enterprise.
2. Inspect network traffic history for communication with external systems associated with the attack.
3. Examine computers for specific files or file attributes related to the attack.

Detailed guidance is available on the McAfee Web site at www.mcafee.com/operationaurora.

How to protect against the Internet Explorer vulnerability

McAfee products protect against attacks that may use the now publicly available exploit to attempt to attack Internet Explorer users and the malware used in the attack on Google and others:

- McAfee consumer and enterprise PC security products provide protection against the malicious computer programs used to target Google and others through the threat definition files released on January 11 and through the McAfee real-time, cloud-based Global Threat Intelligence. Current customers should ensure the latest definition files are installed and that cloud detection is enabled. McAfee consumer security products are available online.
- McAfee® Network Security Platform detects attacks that use the Internet Explorer zero-day exploit through the threat definition files released on January 15. Users of the McAfee Network Security Platform should ensure the latest definition files are installed.
- McAfee Web Gateway and McAfee Firewall Enterprise provide powerful Web security technology to filter malicious traffic on the network. Users of either of these McAfee products should ensure that outbound Web security capabilities are enabled and malware scanning within the firewall is based on the latest signatures and associated rules.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com

Use Advanced McAfee Technology To Detect Future Attacks

The attack on Google and others marks a new, high-risk era in the world of cybercrime where these advanced persistent threats are no longer targeted at just governments, but are also targeted at organizations in many different sectors. McAfee is making available free trials of its advanced protection technologies to help companies shield themselves against sophisticated attacks such as the recent attack on Google and others.

Organizations can evaluate the following McAfee technologies at no cost:

- McAfee Network Threat Response, a network security appliance that automatically analyzes threats attempting to spread on a network. McAfee Network Threat Response would have allowed victims to detect the attack that hit Google and others.
- McAfee Application Control, a whitelisting application that prevents zero-day attacks past and future and ensures only trusted applications run on servers and PCs. It reduces risks from unauthorized software, boosts endpoint control, extends the viability of fixed-function systems without impacting performance, and lowers operating costs.

Also, McAfee Foundstone® has consultants who are available for forensic investigations. Complete the [911 Contact Form](#) on the Foundstone Web site for help.

McAfee will continue to provide updates on the attack that hit Google and other cyberattacks on its Web site and [blog](#).

