



Abuse of Trust

Preying upon those who trust.

The adage “trust is earned, not given” rings true; we have all seen examples of it. On the other hand, something that takes years to earn can be destroyed in seconds. Trust has never been a static model, and that has become even more apparent with the world’s population increasingly reliant on the Internet.

What is Abuse of Trust?

The exploitation of trust is discussed in depth in the **McAfee Labs Threats Report: November 2014**. In the online world, we assume that what we see is trustworthy, whether it's an app downloaded to a mobile device, a seemingly benign advertisement on a popular website, or an email from a company with whom we do business. Attackers prey upon the institution of trust in many ways, with exploiting unsuspecting victims the primary pursuit. Here are some of the attack types that are discussed in the report:

- **Malvertising:** When the innocuous advertisements on a company’s website are actually the source of the attack on unsuspecting consumers, consumers wonder if their trust is misplaced. **Malicious advertising networks like “Kyle and Stan”** deliver malware through “malvertisements” on websites such as amazon.com, youtube.com, and **major advertising networks such as Double-Click and Zedo**.
- **Signed malware:** An increasingly common tactic is for malware authors to acquire certificates from a Certificate Authority (CA) that either attempt to piggyback on the trust of established companies or pose as a legitimate company. Attackers exploit the inherent trust that we place in CAs. Recently a “malvertising” campaign delivered signed CryptoWall variants through the Zedo ad network, which **reportedly impacted users of Alexa top-ranked websites**. The digital signature issued to “Trend” was probably trying to pose as the security vendor Trend Micro, and is a perfect example of taking advantage of innocence by association.
- **Copycat applications:** Commercial brands spend a considerable amount of time and effort protecting their customers from counterfeit products that seek to capitalize on the brand’s established trust with consumers. With applications offering functions that extend past the digital world, it is no surprise that enterprising attackers have resorted to creating knockoff applications of legitimate, usually popular programs.

In this past quarter, McAfee observed scammers trying to distribute an application that appeared to be Flash Player 11 by Adobe. Judging from the Google Play Store’s download count and McAfee’s Mobile Security detection telemetry, the scammers achieved their goal in tricking users to downloading their poisoned knockoff.

Solution Brief

- **DLL "side loading":** Attackers know that if their malicious code can ride the coattails of a trusted application, then it has a greater chance of success. Malware has taken advantage of this factor for a number of years, using an attack technique known as DLL side loading. This technique involves executing a legitimate application that executes code from an external DLL. The attackers craft their payload to assume the role of the external DLL, thus causing the clean application to execute malicious code.

In the third quarter, McAfee Labs observed attacks on the Google Updater application. The new variant of the PlugX malware family assumes the role of the imported goopdate.dll, but the PlugX variant goes a step further to conceal its actions. The goopdate.dll module is nothing more than a middle man that reads the content of an encrypted data file, goopdate.dll.map, decrypts it into memory, and passes execution control to that malicious code.

- **Operating system and networking software:** There are many examples of attacks that abuse the trust within and between operating systems and networking software. Some attacks take advantage of the software that establishes secure connections across the Internet. Unsuspecting applications trust the connections passed to it by the operating system, which in turn trusts the networking software that purportedly established secure connections. Other attacks exploit vulnerabilities within operating systems or networking software. Often those attacks take advantage of open-source software incorporated into the operating system or networking software stack.

BERserk is a **recently announced** signature-forgery vulnerability that abuses OS and network software trust. BERserk enables malicious parties to perform "man in the middle" (MITM) attacks by allowing them to forge RSA signatures, and bypass the authentication to websites using SSL/TLS.

McAfee Solutions

McAfee security technology can help protect against attacks seeking to abuse the trust your company has in its day-to-day operations. Here are some of the products from McAfee that will enable your company to ensure that its trust model is not exploited by would-be attackers.

McAfee Application Control

Protecting your company and its legitimate applications from malicious code like BERserk is crucial.

McAfee Application Control lets your company control which applications are allowed to run in your environment through dynamic whitelisting and enforcement policies on both connected and disconnected endpoints.

- **Dynamic whitelisting:** Enable your organization to efficiently manage whitelisted applications by developing the whitelist automatically as systems are patched and updated. McAfee Application Control reduces your exposure to BERserk by not allowing applications to run that call the vulnerable RSA signature verification code.
- **File reputation:** Integration with McAfee Global Threat Intelligence allows McAfee Application Control to query real-time feeds of known good, bad, and unknown file types to help your company stay aware of vulnerabilities like BERserk.
- **Protection whether connected or disconnected:** Enforce controls on connected or disconnected servers, virtual machines, endpoints, and fixed devices such as point-of-sale terminals.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (GTI) is a comprehensive, real-time, cloud-based threat intelligence service that enables McAfee products to block cyberthreats across all vectors—file, web, message, and network. Proactively protect against abuse of trust with these features:

- **Certificate reputation:** Query real-time feeds of known good and bad certificates to protect your company against threats such as signed malware that can be delivered by malicious advertising networks.
- **File reputation:** Protect against copycat applications on the desktop, and stay aware of applications that may be vulnerable to attacks like BERserk. Query feeds of known good, bad, and unknown files in real time to stay protected.
- **Intelligence through vector correlation:** Collect and correlate data from and across all key threat vectors—file, web, email, and network—to detect blended threats such as advertising networks delivering signed malware, spear-phishing emails from apparently trusted sources, and drive-by downloads hosted on malicious websites or compromised “trusted” websites.
- **Security Connected:** Integrate with other McAfee security products to provide the broadest threat data, deepest data correlation, and most complete product integration available today to ensure protection against attacks that abuse trust.

McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in trusted URLs are just some of the attack methods used to take advantage of trust. **McAfee Web Gateway** will boost your company's protection against this type of threat.

- **Gateway Anti-Malware Engine:** Signature-less intent analysis filters out malicious content from web traffic in real time. Emulation and behavior analysis proactively protect against zero-day and targeted attacks. The Gateway Anti-Malware Engine inspects files and blocks them from being downloaded by users if the files are malicious. McAfee Web Gateway is No. 1 in the market for its ability to block malware downloads thanks to the unique inspection capability of this engine.
- **Integration with McAfee GTI:** Real-time McAfee GTI file reputation, web reputation, and web categorization feeds offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

McAfee SiteAdvisor Enterprise

Staying on top of the ever-changing threat landscape is challenging, especially when trying to protect online users against threats such as abuse of trust without imposing harsh policies that ruin the user experience.

- **Easily identify threats such as malicious websites posing as legitimate:** Featuring an intuitive color-coded rating system, **McAfee SiteAdvisor® Enterprise** gives an extra layer of protection at the desktop. McAfee SiteAdvisor Enterprise will deny connections to known malicious websites and inform users of the danger.
- **Enhanced security powered by McAfee GTI:** McAfee GTI provides real-time threat intelligence information to McAfee SiteAdvisor Enterprise so that the latter assesses websites based on the most current information.

McAfee Threat Intelligence Exchange

Abuse of trust comes in many forms; having an intelligence platform that can adapt over time to suit your environment's needs is vital. **McAfee Threat Intelligence Exchange (TIE)** significantly reduces exposure to attacks thanks to its visibility into threats such as malicious certificates discovered in your environment.

- **Certificate reputation:** Integration with McAfee GTI lets your company protect in real time against attacks that leverage signed malicious code by querying real-time feeds of known good and bad certificates. McAfee TIE can safeguard your endpoints against malicious certificates through centrally managed policies that can be deployed to protect both connected and disconnected endpoints.
- **Defeat DLL side loading, copycat apps, and other attacks:** Cutting-edge endpoint protection technology determines file-execution decisions with rule-based logic related to endpoint context (file, process, and environmental attributes) blended with collective threat intelligence.
- **Indicators of compromise:** Import known bad file hashes and known malicious certificates into McAfee TIE to immunize your environment against these known bad files through policy enforcement. If any of the indicators of compromise (IoCs) trigger in the environment, McAfee TIE can kill all processes and applications associated with the IoC.

McAfee VirusScan Mobile Security

- **Defeat copycat apps:** Backed by McAfee GTI, **McAfee VirusScan® Mobile Security** can defeat copycat malware-bearing applications in near real time. It can detect malware in less than 200 milliseconds without interrupting wireless operations or connectivity.

In addition to these Intel Security products, we recommend two additional classes of security technologies.

- **Email gateway security:** Most malware enters a system through an attachment to an email message, so a robust email gateway security product that scans all attachments for malware should be part of a good defense against this type of attack.
- **Vulnerability scanning and reporting:** Ongoing scanning of systems and networks for known vulnerabilities can reduce the likelihood that malware can exploit those vulnerabilities. Vulnerability reports can pinpoint the devices that should be upgraded.

Protecting your company against adversaries who seek to exploit this dynamic trust model can be a daunting task. McAfee security technology can enable your company to proactively protect itself against attacks that seek to abuse user trust.

