Solution Brief

# Stopping Backdoor Trojans

The Adwind remote administration tool (RAT) is a Java-based backdoor Trojan that targets various platforms supporting Java files. Adwind does not exploit any vulnerability. Most commonly, for an infection to occur, the user must execute the malware by double-clicking on the .jar file that typically arrives as an email attachment or open an infected Microsoft Word document. Infection begins if the user has the Java Runtime Environment installed. Once the malicious .jar file runs successfully on the target system, the malware silently installs itself and connects to a remote server through a preconfigured port to receive commands from the remote attacker and perform further malicious activities.

## A Brief History

Adwind evolved from the Frutas RAT. Frutas is a Java-based RAT, discovered in early 2013, that has been widely used in phishing email campaigns against prominent telecommunications, mining, government, and finance companies in Europe and Asia.

Since the beginning of Q1 2015, McAfee® Labs has seen a significant rise in .jar file submissions identified as Adwind.

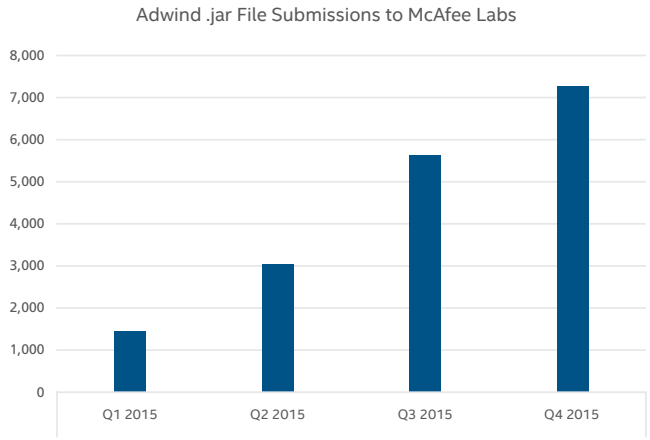


**Figure 1.** The number of Adwind .jar file submissions to McAfee Labs has grown to 7,295 in Q4 2015 from 1,388 in Q1 2015, a 426% increase.

intel Security

## Infection Chain

Adwind is typically propagated through spam campaigns that employ malware-laden email attachments, compromised web pages, and drive-by downloads. Its distribution mechanism has evolved. Earlier spam campaigns lasted days and weeks and used the same email subject or attachment name. This consistency helped security vendors quickly detect and mitigate Adwind. Now, spam campaigns are short lived, with frequently changing subjects and carefully crafted attachments, allowing Adwind to avoid detection.

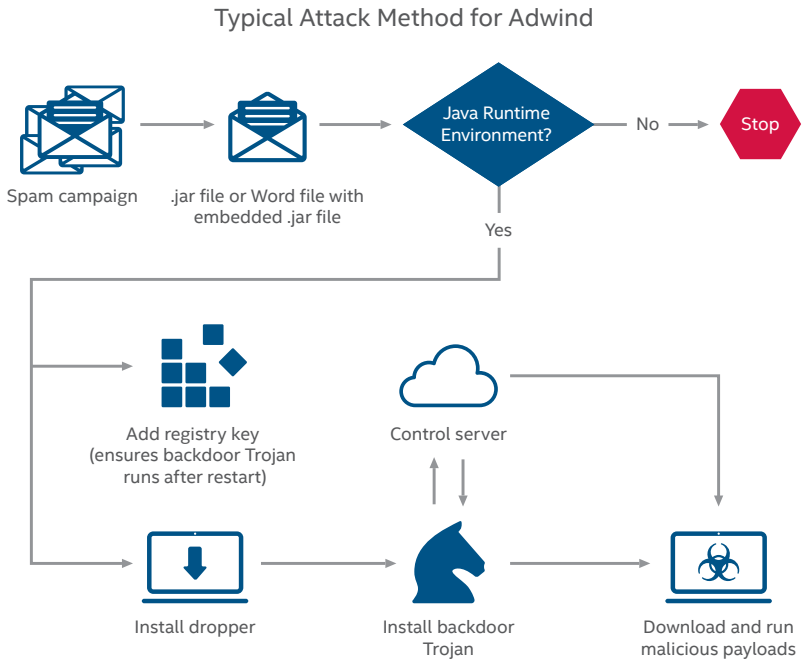


**Figure 2.** The Adwind infection chain.

After Adwind successfully infects a system, we have seen it log keystrokes, modify and delete files, download and execute further malware, take screenshots, access the system's camera, take control of the mouse and keyboard, update itself, and more.

## How Intel Security helps protect against Adwind and other backdoor Trojans

Intel Security technology can help protect against backdoor Trojans such as Adwind. Here are some of the products that can help stop this type of attack.

### McAfee® Threat Intelligence Exchange

Having an intelligence platform that can adapt over time to suit an environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to backdoor Trojans, thanks to its visibility into immediate threats such as unknown files or applications being executed in the environment.

- **Comprehensive threat intelligence:** Easily tailor comprehensive threat intelligence from global threat intelligence data sources. These can be **McAfee Global Threat Intelligence** (McAfee GTI) or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.

- **Execution prevention and remediation:** McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to the product's powerful central management and policy enforcement capabilities.
- **Visibility:** McAfee Threat Intelligence Exchange can track all packed executable files and their initial execution in the environment, as well as all changes that occur thereafter. This visibility into an application's or process' actions, from installation to the present, enables faster response and remediation.
- **Indicators of compromise:** Import known bad file hashes, and immunize your environment against these known threats through policy enforcement. If any of the indicators trigger in the environment, McAfee Threat Intelligence Exchange can kill all processes and applications associated with the indicators of compromise.

**McAfee Advanced Threat Defense**

**McAfee Advanced Threat Defense** is a multilayered malware detection product that combines multiple inspection engines. The engines perform signature- and reputation-based inspection, real-time emulation, full static-code analysis, and dynamic sandboxing on suspicious objects to protect against malware that initially drops a binary on its target system.

- **Signature-based detection:** Detects viruses, worms, spyware, bots, Trojans, buffer overflows, and blended attacks. The comprehensive knowledgebase is created and maintained by McAfee Labs.
- **Reputation-based detection:** Looks up the reputation of files using McAfee GTI to detect newly emerging threats.
- **Real-time static analysis and emulation:** Provides real-time static analysis and emulation to quickly find backdoor Trojans and zero-day threats not identified with signature-based techniques or reputation.
- **Full static-code analysis:** Reverse engineers file code to assess all its attributes and instruction sets and fully analyzes the source code without execution. Comprehensive unpacking capabilities open all types of packed and compressed files to enable complete analysis and malware classification, allowing your company to understand the threat posed by specific malware.
- **Dynamic sandbox analysis:** For a file whose safety cannot be established through the preceding inspection engines, McAfee Advanced Threat Defense can execute the file code in a virtual runtime environment and observe the resulting behavior. Virtual environments can be configured to match host environments. McAfee Advanced Threat Defense supports custom operating system images of Microsoft Windows XP (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8 (32- and 64-bit), Windows Server 2003, Windows Server 2008 (64-bit), and Android.

**McAfee Network Security Platform**

**McAfee Network Security Platform** is a uniquely intelligent security product that discovers and blocks sophisticated threats in the network. Using advanced detection and emulation techniques, it moves beyond mere pattern matching to defend against stealthy attacks with extreme accuracy. Our open, integrated approach to security management streamlines security operations by combining real-time McAfee GTI feeds with rich contextual data about users, devices, and applications for fast, accurate response to network-borne attacks.

- **Signatureless defenses:** Advanced and unknown threats such as stealthy malware, advanced persistent threats (APTs), bots, and zero-day attacks often evade signature-based defenses. McAfee Network Security Platform has multiple advanced engines that do not require signatures to protect against these advanced and unknown threats. Signatureless detection analyzes web content, PDF files, Flash files, and JavaScript behavior in near real time using emulation.
- **Endpoint intelligence agent:** McAfee Network Security Platform provides real-time, per-flow endpoint traffic correlation. The agent combines behavioral analysis of network traffic flows with multiple sources of reputation intelligence. This technology leverages intelligence in the network and on every Windows host to reveal relationships between endpoint executables and network traffic flows, making it possible to identify malicious network connections and executables in real time. The agent incorporates detailed process context for attacks, blocks malicious communications, prevents the spread of advanced malware, and, finally, quarantines and remediates compromised host systems.

**McAfee Web Gateway**

Malvertising, drive-by-downloads, and malicious URLs embedded in phishing emails are some of the main attack methods used to deliver backdoor Trojans. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **Gateway anti-malware engine:** Signatureless 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.
- **Integration with McAfee GTI:** Real-time intelligence feeds with McAfee GTI file reputation, web reputation, and web categorizations offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites known to act as control servers.

In addition to these preceding Intel Security products, we recommend one additional class of security technology.

- **Email gateway security:** Most backdoor Trojans enter a system through an attachment to an email message, so a robust email gateway security product that scans all attachments for malware offers a good defense against this type of attack.



**McAfee. Part of Intel Security.**
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com