What is Kneber?

Kneber is a variant of **Zeus** (also known as Zbot and WSNPoem), a well-known builder application for creating password-stealing Trojans. Zeus-related Trojans have been around for at least three years, are highly dynamic, and often polymorphic, or designed to morph their own code to avoid detection.

The Zeus builder application includes a control panel based on the Web scripting language PHP and a Windows executable file to build the malware. The produced malware can steal data and credentials, capture HTTP and HTTPS traffic, capture screenshots, send its logs to a remote location, work as a proxy server, and decrypt encoded logs. Zeus users can take advantage of various options, such as exploit packages and an advanced command and control interface.

What are its attributes?

Zeus-related malware shares many traits with static-type worms, botnets, and other malware. It is stealth and carries a very light footprint. One common behavior associated with botnet installs is unexpected HTTP/HTTPS network traffic originating from infected hosts.

How does Kneber differ from other botnets? From Operation Aurora?

Kneber, or Zeus, is similar to other Trojan botnets in that it installs a back-door that enables information such as passwords to be logged and sent to a remote server. It is also capable of downloading files and updating its software.

Kneber, or Zeus, differs from Operation Aurora in that the latter was a highly sophisticated, targeted attack that leveraged zero-day exploits in Microsoft IE. The attackers in Operation Aurora were selective and narrow in the corporations and users they targeted and the information they stole. Zeus-related malware has been in the wild for more than three years and its variants have been used in more widespread attack of various kinds.

How can I protect myself?

McAfee anti-malware and Web security software can detect Zeus-related Trojans, including Kneber.

Consumers.

1. Make sure that you have the latest version of McAfee anti-malware and Web security software, including McAfee AntiVirus Plus, Internet Security, Total Protection, and SiteAdvisor.

Enterprises.

1. Ensure that your McAfee anti-malware software is up to date with the latest DAT file.
2. Run a full system scan on your system if yourDAT is earlier than 5890.
3. Enable Artemis – McAfee's real-time file reputation engine, which protects against known, new, and emerging threats – on your endpoint products. If you do not know how to do this, please visit the McAfee Corporate Knowledge Base to access a video tutorial.
4. Enable TrustedSource – McAfee's real-time Web reputation engine, which protects against malicious or suspicious Websites, IPs, domains, and senders – on your Web security products.

Am I protected with McAfee products?

McAfee releases updated virus definition files (DATs) as necessary to combat the latest Zeus variants. Protection against Zeus was released with the McAfee DAT file versions 5890 and later. McAfee Web Gateway products also protect customers from connecting to malicious Websites associated with Zeus-related malware.

Am I infected? What should I be looking for?

McAfee anti-malware and Web security software can detect Zeus-related malware including Kneber. If you don't have the latest DAT files (5890 or later) or still want to check, you should update to the latest DAT release and run a full system scan.

Closely monitor your client network traffic and firewall logs in order to track down infected hosts. Note that computers trying to connect to known malicious Websites or trying to connect to Websites at regular intervals are likely to be infected with this or another Trojan.

If I've been infected, what should I do?

Consumer:

- Make sure that you have the latest version of McAfee anti-malware and Web security software, including McAfee AntiVirus Plus, Internet Security, Total Protection, and SiteAdvisor.
- If your software is not up-to-date, you should update it and run a full system scan.

Enterprise:

- Ensure that your McAfee anti-malware software is up to date with the latest DAT file.
- Run a full system scan on your system if your DAT is earlier than 5890.
- Let our incident response team help you. If you fear you may have been compromised by this or other attacks, contact McAfee Foundstone.

What other resources can I leverage?

Researchers at McAfee Labs are delivering behavioral and content signatures, Web security, IPS, and IP security updates, product configuration suggestions, and advice on a continuous basis on the McAfee Labs blog.

Learn more specifics about Zeus-related and other malware at the McAfee Labs Threat Library.

McAfee Global Threat Intelligence, our comprehensive, "in-the-cloud" threat detection and protection capability, leverages sophisticated heuristic and reputation-based capabilities to deliver real-time protection against the latest threats. McAfee Global Threat Intelligence is continuously monitoring the Web for exploits and hot spots related to Operation Aurora and other threats. Learn more.