▶ INTELLIGENCE SERVICES: BOTNET THREAT TRACKING

Expert monitoring and notification services to identify botnets threatening your reputation and customers

Many network attacks are organized using botnets. Such attacks might target casual Internet users, but often these threats are aimed at specific organizations and their online customers.

Kaspersky Lab's expert solution tracks the activity of botnets and provides real-time notifications of threats associated with specific enterprise brands. You can use this information to advise and inform your customers, security services providers and law enforcement about current threats. Protect your organization's reputation and customers today with Kaspersky Lab's Botnet Threats Notification Service.

TAKE ACTION WITH REAL-TIME DELIVERABLES:

The service provides a subscription to personalized email or JSON format notifications containing intelligence about matching brand names by tracking keywords in the botnets monitored by Kaspersky Lab. Notifications include:

Targeted URL of the botnet — Bot malware is designed to wait until the user accesses the URL(s) of the targeted organization and then starts the attack rule.

Botnet type — Understand exactly what malware threat is being employed by the cybercriminal to affect your customers. Examples include Zeus, SpyEye, and Citadel.

Attack type — Identify what the cybercriminals are using the malware to do; for example, web data injection, keylogging, screen wipes or video capture.

Attack rules — Know what different rules of web code injection are being used such as HTML requests (GET / POST), data of web page before injection, data of web page after injection.

Command and Control (C&C) server address — Enables you to notify the Internet service provider of the offending server for faster dismantling of the threat.

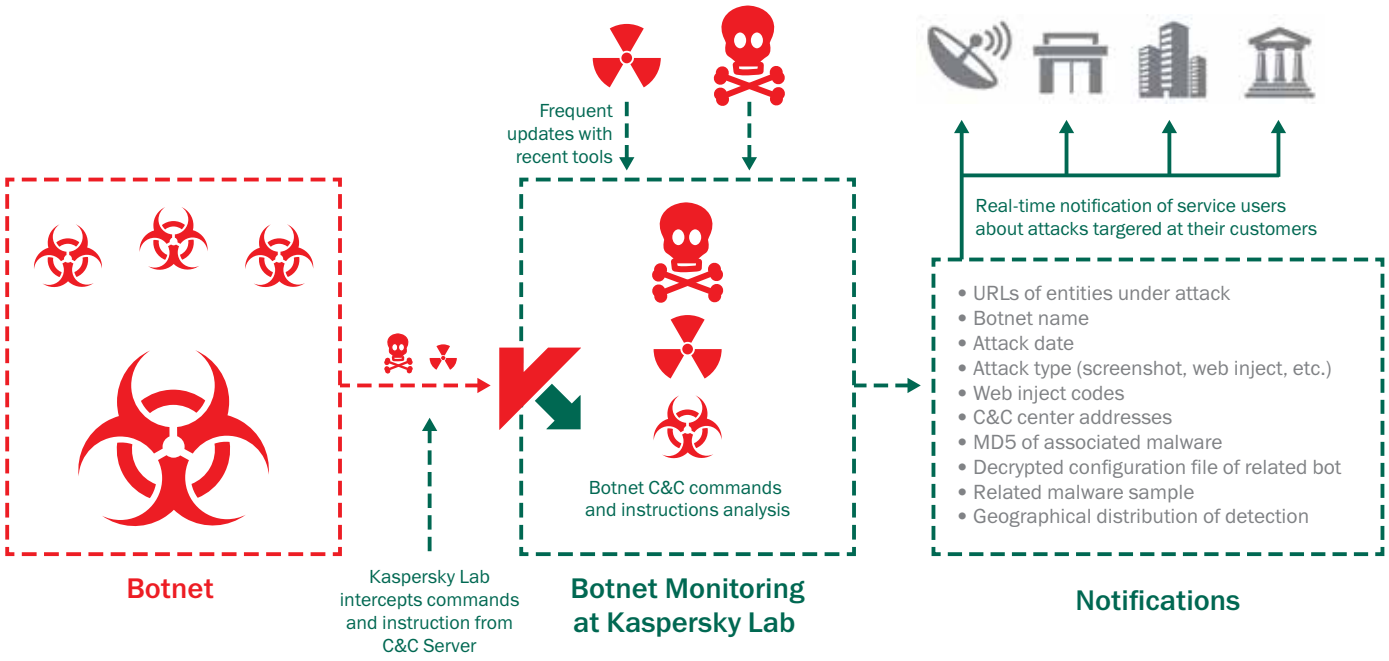
MD5 hashes of related malware — Kaspersky provides the hash sum, which is used for malware verification.

PREMIUM SUBSCRIPTIONS ALSO INCLUDE:

Decrypted configuration file of related bot — identifying the full list of targeted brands.

Related malware sample — for further reversing and cyber forensic analysis of the botnet attack.

Geographical distribution of detection — Statistical data of related malware samples from around the world.



Kaspersky Lab's solution is available in either Standard or Premium for a variety of service terms and monitored brands. Consult with Kaspersky Lab or your reseller partner to determine which is right for your enterprise.

SUBSCRIPTION LEVELS AND DELIVERABLES

Premium	Standard	• Target URL (The URL the bot program is targeting its users. • Botnet type (e.g., Zeus, SpyEye, Citadel, etc.) • Attack type • Attack rules, this includes: Web data injection, Key logging, Screen, Video capture, etc. • C&C address • MD5 hashes of related malware
		• Decrypted configuration file of related bot • Related malware configuration sample (on demand) • Geographical distribution of detection for related malware samples

For more information on Botnet Threats Notification or other Kaspersky services, please contact us via intelligence@kaspersky.com today!

WHY KASPERSKY LAB?

- Founded and led by the world's foremost security expert, Eugene Kaspersky
- Partnerships with global law enforcement agencies such as Interpol and CERTS
- Cloud-based tools monitoring millions of cyberthreats across the globe in real time
- Global teams analyzing and understanding Internet threats of all kinds
- World's largest independent security software company — focused on threat intelligence and technology leadership
- Undisputed leader in more independent malware detection tests than any other vendor
- Identified as a Leader by Gartner, Forrester and IDC

TO LEARN MORE VISIT: **WWW.KASPERSKY.COM**