INTELLIGENCE SERVICE: BOTNET THREAT TRACKING

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

Many network attacks are organized using botnets. These attacks can target casual internet users, but often these threats are aimed at the online customers of specific organizations and their online customers.

Kaspersky Lab's expert solution tracks the activity of botnets and provides rapid (within 20 minutes) notification of threats associated with the users of individual online payment and banking systems. You can use this information to advise and inform your customers, security services providers and local law enforcement agencies about current threats. Protect your organization's reputation and customers today with Kaspersky Lab's Botnet Threats Notification Service.

USE CASES / SERVICE BENEFITS

- **Proactive alerts** about threats coming from botnets that target your online users allow you to always remain one step ahead of the attack
- **Identifying a list of Botnet Command & Control server URLs** that are targeting your online users allows you to block them by sending requests to CERTs or Cyber Police
- **Improve your online banking / payment cabinets** by understanding the nature of attack
- **Train your online users** to recognize and avoid falling foul of the social engineering used in attacks

TAKE ACTION WITH REAL-TIME DELIVERABLES:

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

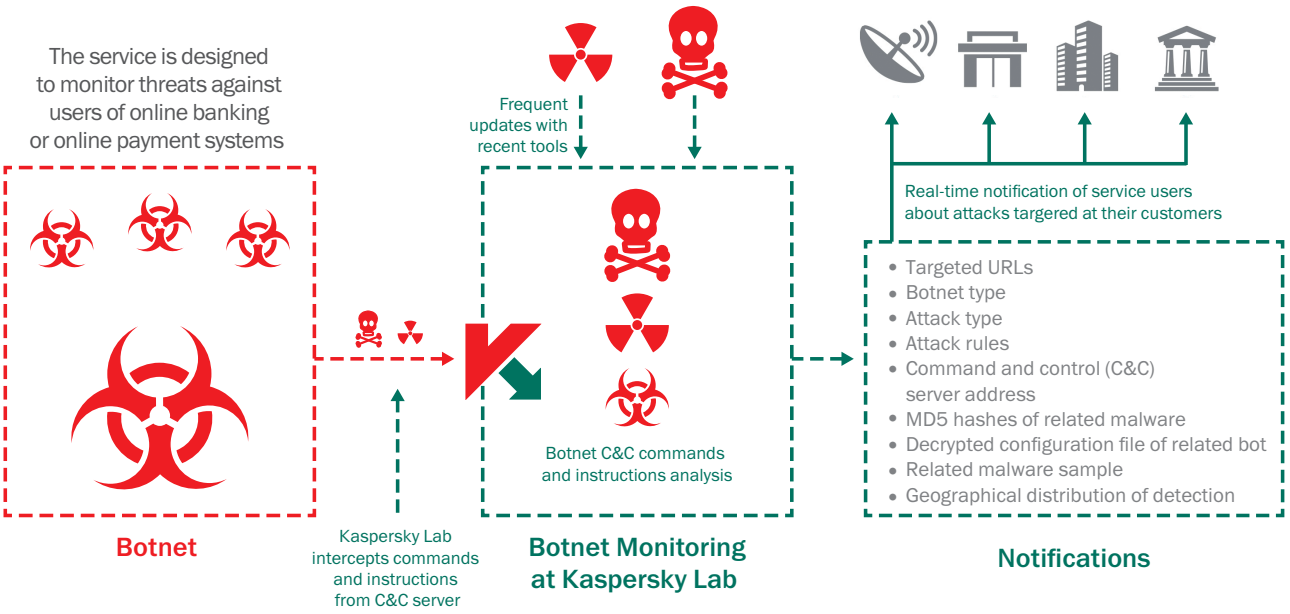
- **Targeted URL(s)** — Bot malware is designed to wait until the user accesses the URL(s) of the targeted organization and then starts the attack.
- **Botnet type** — Understand exactly what malware threat is being employed by the cybercriminal to jeopardize your customers' transactions. Examples include Zeus, SpyEye, and Citadel.
- **Attack type** — Identify what the cybercriminals are using the malware to do; for example, web data injection, screen wipes, video capture or forwarding to phishing URL.
- **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 to dismantle of the threat faster.
- **MD5 hashes of related malware** — Kaspersky provides the hash sum that is used for malware verification.
- **Decrypted configuration file of related bot** — identifying the full list of targeted URLs.
- **Related malware sample** — for further reversing and digital forensic analysis of the botnet attack.
- **Geographical distribution of detection (top 10 countries)** — Statistical data of related malware samples from around the world.

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

For more information on Kaspersky Intelligence Services, please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com.

KASPERSKY lab



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

SUBSCRIPTION LEVELS AND DELIVERABLES

	Premium	Notification in email or JSON format • Decrypted configuration file of related bot • Related malware sample (on demand) • Geographical distribution of detections for related malware samples	10 URLs monitored
Standard		Notification in email format • Target URL (identifying the URL(s) were the bot program is targeting users) • Botnet type (e.g., Zeus, SpyEye, Citadel, Kins, etc.) • Attack type • Attack rules, including: Web data injection; URL, screen, Video capture, etc. • C&C address • MD5 hashes of related malware	5 URLs monitored

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

For more information on Kaspersky Intelligence Services, please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com.

KASPERSKY lab