Botnet C&C Data Feeds

Primer on Botnet Attacks and Related Threats

Today, cyber attacks and infections often involve botnets and their infrastructure. Attacks perpetuated via botnets can be targeted against both regular internet users and specific organizations. Sophisticated techniques to escape detection (such as advanced cryptography and sandbox awareness) contribute towards the growing numbers of this type of attacks. The majority of botnet victims do not even know that they are infected and continue to operate normally, helping the botnet to persist and facilitating the criminals' access to valuable resources.

Botnet Facts

- First appearance in public: 2000
- Well-known botnets: Conficker, Zeus, Waledac, Mariposa, Kelihos, Rustock, etc.
- The number of endpoints and organizations infected and co-opted into botnets has increased drastically
- Main method of infection: drive-by downloads and emails
- Infection purposes: spam distribution, DDoS attacks, data and identity theft, large distributed resources of computing power, financial fraud, click fraud, etc.
- Botnet creators rent out the machines in the botnet to the highest bidder

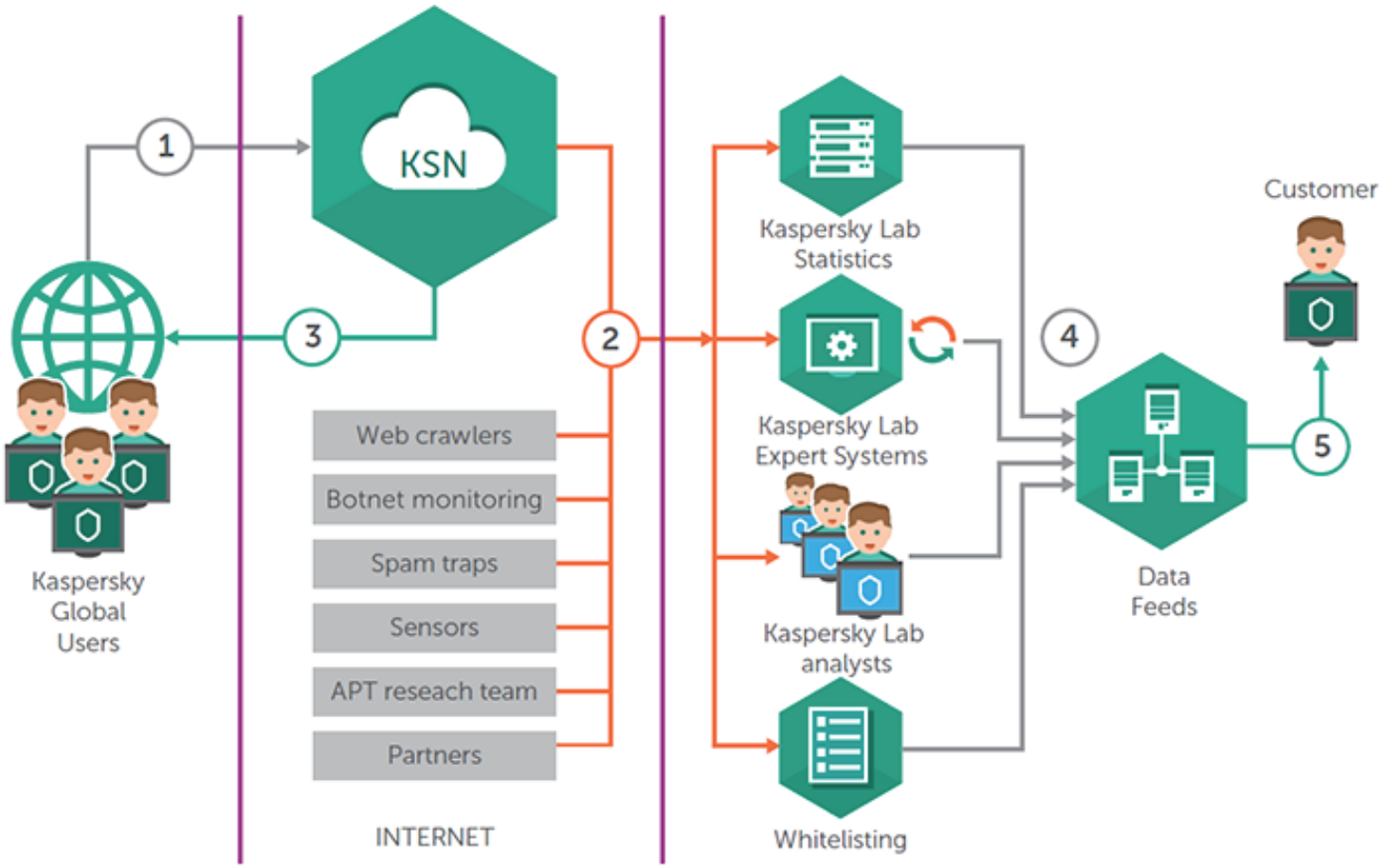
Kaspersky Botnet C&C Data Feeds

Kaspersky Botnet C&C Data Feeds are sets of URLs and hashes with actionable context (threat names, timestamps, geolocations, resolved IPs of infected web resources, associated malware hashes, and so on) covering desktop and mobile botnet servers and related malicious objects. Unlike traditional Botnet Feeds which provide raw information and unfiltered data, we provide accurate and timely intelligence based on real botnet activities in real time. Data feeds help detect connections to botnet servers (C&Cs) that are used by cybercriminals to control infected machines (bots).

Kaspersky Botnet C&C Data Feeds are well suited for both small network appliances and high-performance mission-critical gateways/servers as well as for content filtering/internet security vendors, ISPs and web-hosting companies. It is completely agnostic to software or hardware design and can be successfully implemented on proprietary (non-x86/*NIX) platforms.

Collection and Processing

Kaspersky Botnet C&C Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network and our own web crawlers, Botnet Monitoring service (a unique proprietary platform which monitors botnets and bots, their targets and activities 24/7/365), spam traps, research teams, and partners. Then the aggregated data are carefully inspected and refined in real time using multiple preprocessing techniques, such as statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling, etc.), validation by analysts, and whitelisting verification:



Kaspersky Botnet C&C Data Feeds contain thoroughly vetted threat indicator data sourced from the real world in real time.

Features

- Data Feeds littered with False Positives are valueless, so extensive tests and filters are applied before releasing feeds to ensure the delivery of 100% vetted data.
- Intelligence data are continuously collected from Kaspersky Security Network (a huge distributed network of over 100 million users worldwide) and updated in real time.
- Continuously updated feeds based on findings about botnets across the globe.
- Hundreds of thousands of masks to detect botnet C&Cs and related web resources.
- Huge coverage (tens of thousands of botnets and bots are tracked on a daily basis).
- Simple lightweight distribution formats (JSON, CSV, OpenIoC, STIX) via FTP, HTTPS, or ad-hoc delivery mechanisms support easy integration of feeds into security solutions.

Benefits

- Detect web resources to which bots transfer stolen data (dropzones that are controlled by the botnet's owner) and enhance your online users' protection (by not exposing their personal info/data or by protecting computational resources from hijacking) as well as your organization's brand reptation (by protecting business-critical confidential data from leaking).
- Detect web resources from which bots receive command-and-control instructions and proactively disrupt cyber-attacks from the corresponding botnets in real time.

- Block bad traffic from/to C&C nodes on the internet and learn about compromised machines within your organization/network.
- Filter source and destination addresses/URLs in your network traffic to take the proper risk prevention actions.
- Leverage intelligence to battle large global botnets without having to invest in complex threat analysis centers and have a global real-time view into malicious activities in botnets.
- Get the ability to report abuse to ISPs/MSSPs where botnets C&C are hosted, letting the providers eliminate the offending resources and impair or even completely block the botnet functionality.

Use Cases

- Reinforce your network protection solutions, including Firewalls, IPS/IDS, Security Proxy, secure DNS solutions with continuously updated Indicators of Compromise (IOCs) and actionable context to preemptively strengthen security measures and prevent data breaches.
- Develop or enhance anti-malware protection for peripheral network devices (such as routers, gateways, UTM appliances) and detect malicious objects by analyzing the network traffic.
- Expose active infections by checking for infected machines or nodes being used for illegitimate purposes within your security perimeter.
- Prevent loss and exfiltration of sensitive information that can be used in identity theft or brand abuse.
- Take down active C&Cs which issue the commands to attack specific clients and inform these clients about new attacks, risk level and actions to prevent similar attacks in the future.

Nothing suggests that the number of botnet attacks will ever decrease in the future. Leverage threat intelligence about botnets to stop criminals from targeting and exploiting your clients or business. Kaspersky Botnet C&C Data Feeds empower you to continuously update and harden your security conveniently and cost-effectively. Arm yourselves with unequalled intelligence about the immediate intent, capabilities and targets of the cybercriminal underworld, feeding directly and straightforwardly into your security solutions.

If you wish to know more, please fill in this contact form and indicate that you require more information about Kaspersky Anti-Botnet Feeds, and our representative will get in touch with you shortly.

KASPERSKY lab