Seculert
Advanced Threat Protection

BOTNET INTERCEPTION

A large percentage of today's advanced threats operate as a botnet – a network of malware-infected devices run by a series of Command and Control servers. They gradually spread throughout the users and endpoints in your organization until they can do significant damage. Remote employees and employees using personal mobile devices are a prime target for botnets because they are beyond the protection provided by enterprise security defenses.

Seculert Botnet interception analyzes botnet traffic to identify all infected users and endpoints – whether they are inside or outside of the corporate network. It takes minutes to set up - there is nothing to deploy or install and no need to direct network traffic to Seculert for analysis. As soon as you sign up for Seculert Botnet Interception, it detects malware infections that are already affecting your organization – and that your current security defenses have not detected.

Seculert is a comprehensive cloud-based solution for protecting organizations from advanced malware, APTs and zero-day attacks. Seculert combines several key detection and protection technologies – an Elastic Sandbox environment, Botnet Interception, and Traffic Log Analysis - in one simple solution that proactively identifies new threats as they emerge.

WHAT IS A BOTNET?

Like all advanced malware, botnets evolve. That is why it is essential to analyze them over a significant period of time. A typical botnet may undergo three stages:

- **Opportunistic:** Criminals attack the general population, usually for monetary gain. The risk is usually greater to the individual rather than to the organization.
- **Semi-opportunistic:** This category is programed to infect specific targets in a search for vulnerable entry points and key employees in a specific industry or country, and is often performed with the goal of selling the information onward.
- **Targeted:** Once vulnerable targets have been found, a targeted attack with well-defined goals may be launched by the original hacker or by a second criminal organization with more focused goals.

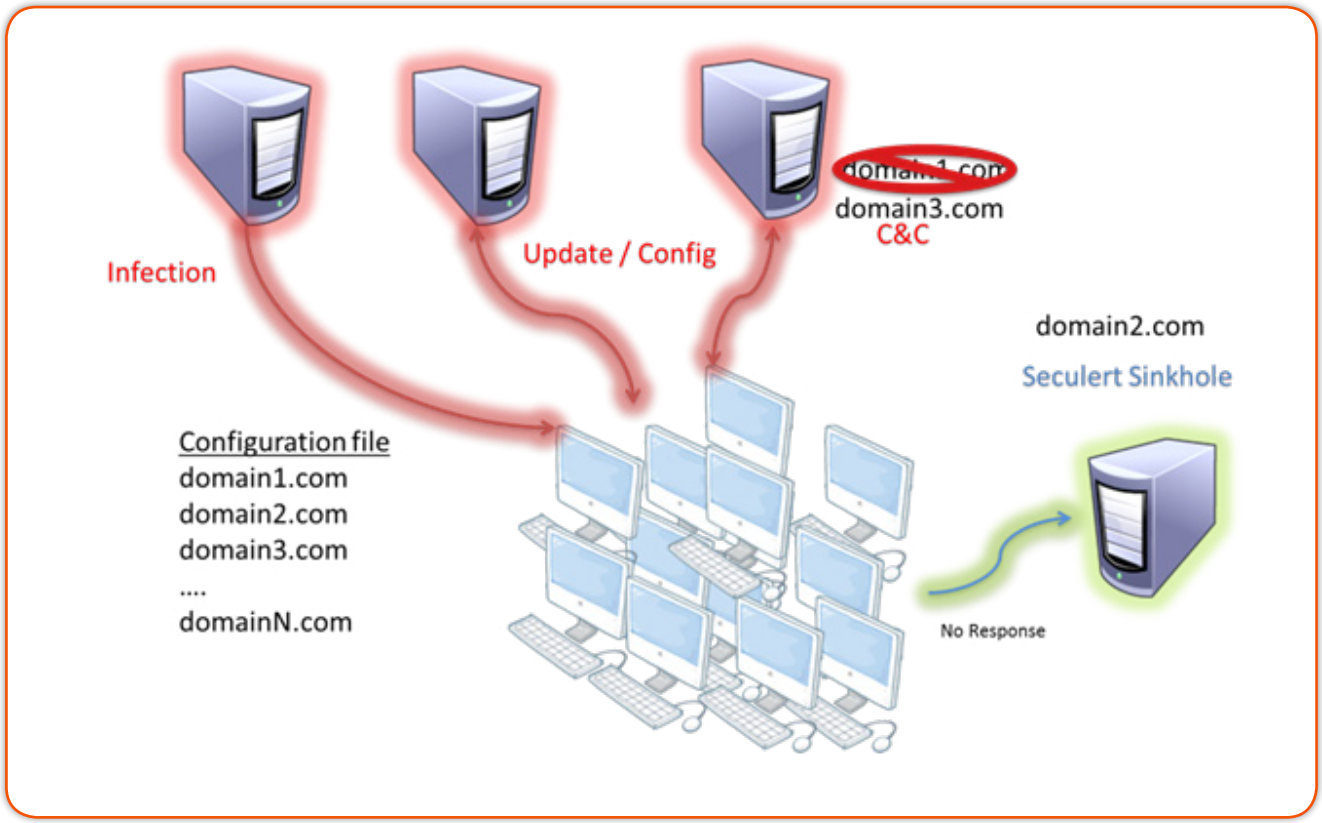
Seculert Botnet Interception is effective with all three types. It uses a number of recognized techniques, such as sinkholing and honeypots, along with proprietary, patent-pending methods that work together to collect information that no other method can deliver.

HOW IT WORKS

Standard botnet monitoring services provide a list of known Command and Control servers so you can block them. Seculert goes one step further and actually identifies the users and endpoints that are infected. As soon as we identify a botnet, we infect our own servers and join the network. We actually go "behind the enemy lines" to collect intelligence. Seculert Botnet Interception collects millions of global bot transmissions as they communicate with Command and Control servers (C&C) every day. Using a wide range of techniques, the Botnet Interception module silently intercepts the traffic, analyzes it and determines if our customers are infected.

Botnet interception uses known techniques, such as sinkholing and honeypots, along with proprietary technologies developed by Seculert to intercept and analyze botnet traffic.

EXAMPLE: HOW DOES SINKHOLING WORK?



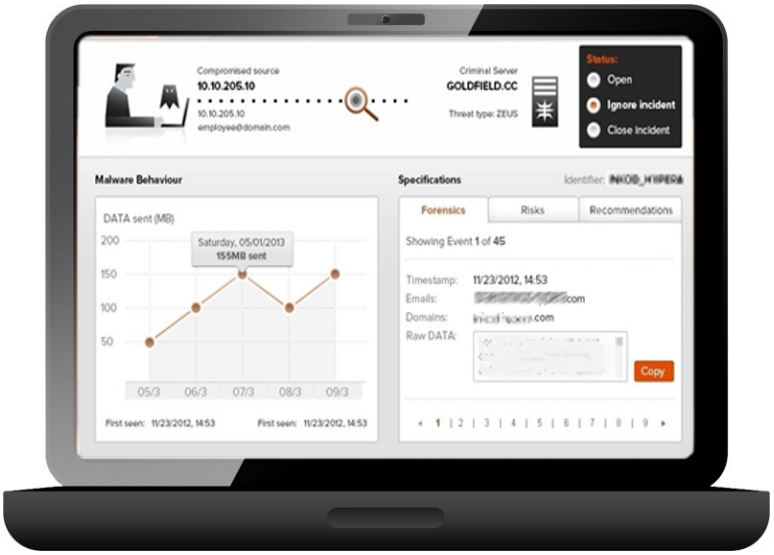
1. Suspicious code is allowed to run for an extended period of time in the Elastic Sandbox. The traffic generated by the malware is studied using Big Data analytics and proprietary machine learning technology. The platform understands the pattern of communication between the bot and its C&C servers.
2. One of a botnet's primary evasion tactics is to periodically change the address of the C&C server, so that you will not spot a lot of suspicious traffic going out to one address. Malware includes a configuration file that lists the servers to try to contact. Seculert understands the pattern and predicts the domains that the C&C is likely to use in the future.
3. Seculert identifies domains that are still available and registers them. The new domains are set up to direct all botnet traffic through Seculert's sinkhole server.
4. When the current C&C server domain is suspended or blocked by the ISP, the botnet will move on to the next C&C server on the list, which is actually registered to Seculert. It redirects the traffic to the sinkhole server, which automatically logs the communication and then immediately ends the session. It's important to note that the sinkhole server isn't actively perpetuating the botnet – it is only monitoring the traffic.
5. Seculert's Big Data analytics are again used to analyze the traffic from the sinkhole server and correlate customers' IP addresses, web interface domains and identities, in order to detect infected machines. In this way, it can identify users and endpoints up to the machine name, both inside and outside of your internal corporate network – including remote workers and BYOD.
6. Seculert immediately acts on the information, updating customer dashboards, sending email alerts, and through the API, informing proxies and firewalls of which users and devices to block. Through the API, seculert also provides full event information to SIEM systems for correlation and forensics.

TWO MINUTE SETUP, IMMEDIATE RESULTS

Since it is a cloud-based service, Seculert Botnet Interception is entirely zero-touch for your organization: no need to change your security architecture, install software, deploy a new appliance, or redirect Internet traffic. You can set it up in seconds by simply defining a range of IP addresses or outward facing web domains (e.g. sslvpn.mycompanydomain.com or owa.mycompanydomain.com), and detection begins immediately.

After any attack is detected, the dashboard supplies you with a detailed incident report so that you can understand and mitigate your exposure and modify your security policies as needed.

Immediately see the users and devices infected – both inside and outside the corporate network



Incident Results within the Seculert Dashboard

You will see the compromised computer by IP, machine name, employees email, threat type, crime server, raw data of the transmission from the bot to the crime server plus the time and date of the transmission. We also group together all the relevant transmissions from the source to the crime server.

The raw data can sometimes include the confidential information that was leaked by the bot, e.g. credentials to access critical web services.

The malware behavior is displayed in a graph and shows the daily number of transmissions.

We also provide separate tabs for risks and recommendations.

REMOTE USERS AND BYOD

When it comes to advanced threats, remote employees pose one of the biggest risks to your organization. The steps you have taken to fortify your internal network simply will not detect or block infection from remote users including employees and partners working outside the office. Small offices and other “remote” sites pose a similar challenge. They are vulnerable to advanced malware and they regularly access your most crucial data assets, yet it is simply not cost-effective to implement pricey ATP appliances at each location.

Seculert is the only Advanced Threat Protection solution designed to protect remote users - no matter where they are located, and regardless of the computer, mobile device or operating system they use. Seculert’s unique Botnet Interception technology looks both inside and outside your internal network to identify every computer infected by known malware.

AUTOMATED PROTECTION API

To make the most of Botnet Interception, you can integrate it with your existing security infrastructure using the Seculert Protection API. The API features two simple interfaces for accessing and retrieving data:

- A web request that retrieves the complete list of crime servers and the time period they were observed to be active.
- A web request that retrieves all the incidents that were detected by Seculert for the specific organization, including the employees' internal and remote access, partners and customers.

The API can communicate directly with corporate firewalls and proxies to block traffic. To support complete forensics, threat detection data can also be sent to SIEM systems for correlation. Some additional examples of integration include:

- Updating Seculert's list of crime servers to the access list of the corporate web proxy or secure web gateway. This will ensure that the bot infected computers will not communicate with the crime servers.
- Using the API to upload the compromised computers into the firewall policies. This will help isolate infected computers and block them from accessing your data centers or internal assets until remediation.

SYNERGISTIC TECHNOLOGIES

Seculert's Botnet Interception is extremely powerful – but it is the combination of the Botnet Interception working together with all of Seculert's core technologies that provides the key to successful advanced Threat Protection. In addition to the Botnet Interception, Seculert features:

- **Elastic sandbox environment** to execute and study suspicious code for as long as necessary in order to profile it.
- **Automated traffic log file analysis** to identify unknown malware that is targeting your organization.
- **Protection API** to automatically stop identified threats through integration with perimeter defenses.
- **Big Data analytics** analyzes tens of thousands of malware profiles daily as well as petabytes of traffic logs in order to detect APTs.
- **Machine learning technology** identifies unknown malware based on an understanding of malware behavior in order to keep up with the volume and rate of change.
- **Intuitive dashboard** puts instant information about all advanced threats at your fingertips.
- **Full coverage of remote and mobile users** on all endpoints including BYOD - without installing a single appliance or endpoint solution.
- **Cost-effective cloud service** means no installation, instant results, and low total cost of ownership.

LICENSING

You can experience Botnet Interception completely for free; however, the fully detailed results will be limited. In addition the API and some of the reports are only available with the Premium version.
Please contact us for more details.

SECULERT
6 Efal Street, Petach Tikva, Israel
Tel: +972-3-9193366
Tel (US): +1-718-305-7067
Tel (UK): +44 (0) 203-468-1234
info@seculert.com

Seculert
Advanced Threat Protection