

# iS3 Research Process

*The Singularity Spider and Database was named in tribute to scientist and author Vernor Vinge. The term “singularity” had been used by mathematicians to describe a value that surpasses any limits, and by physicists to refer to the center of a black hole; a point of zero volume and infinite density.*

*In the early 1980s, Dr. Vinge posited that in the coming years, the ongoing exponential progress of technology would accelerate the evolution of intelligence, leading to the “singularity;” the era in which the distinction between machine and biological intelligence will blur, and our increasingly non-biological intelligence will become unimaginably more powerful than it is today.*

*iS3 Research is accelerating the pace of finding new Malware by using the mighty combination of human and machine intelligence. Machines are already superior to human intelligence in speed, logic and memory. These attributes, combined with pattern recognition, the hallmark of human intelligence, are enabling iS3 researchers to develop a predictive approach, detecting potential threats based on their behavior and content and targeting it.*

*iS3 Researchers developed the Singularity Spider to comb the Web in search of new Malware. Multiple bots run 24/7. Each one can investigate more than 900 sites per hour in an effort to become infected with Malware. Starting with a known malicious site, a bot investigates all links in that site, then all links in the tertiary sites, navigating a growing web of potentially malicious sites.*

## Identifying Malware

In addition to Web Crawling, iS3 identifies Malware (from malicious software) with Heuristics, and Scanning.

- **Heuristics: In the context of online security, heuristics refers to the ability to infer that a particular binary might be hostile based on typical sequences of operation within the object code. Optimally, Malware is identified as a potential threat by heuristics, before it does any damage. Researchers use a rules engine to evaluate software. Based upon behavior and content, certain sites or software applications are determined to be threats or potential threats, assigned a threat level according to iS3's severity scale and targeted.**

- **Scanning: iS3 uses three types of scans to identify Malware:**
  - An Application Scan is an image of a computer running a specific Microsoft-based operating system with known commercial software products installed and one new commercial application added. This application is assumed to be SAFE. These definitions are added to the Singularity database as SAFE.
  - A Malware Scan is an image of a computer running a specific Microsoft-based operating system with known commercial software products installed and one new application added. This application is assumed to be UNSAFE. These definitions are added to the Singularity database as UNSAFE.
  - A Customer Diagnostic Scan is an image of a user's computer with the latest version of STOPzilla installed. Using data called from Application and Malware scans, known SAFE applications are filtered out, and only UNKNOWN and UNSAFE applications are highlighted. Diagnostic Scans are performed by the subscriber, typically under the direction of a Customer Support Rep, when the subscriber is experiencing some anomaly usually attributable to Malware, and has contacted Customer Support. Diagnostic scanning is a free service to both subscribers and trial users of STOPzilla, iS3's anti-Spyware solution.

## The Targeting Process

Once Malware is identified, iS3 researchers target it. Researchers target Malware by finding attributes with which to identify a Watch Point and then associating an action to the Watch Point. As technology improves, the Singularity database is becoming "smarter", analyzing applications aggregately and assigning target actions to software determined to be malicious in nature. Please refer to Figure 1: The iS3 Research Process on page 4.

*There are three classes of Watch Points that can be targeted: Active Modules, Auto Runs and Hosts Files.*

- **Active Modules are any modules loaded in memory. They include processes, services, drivers, Winsock and WinLogon.**
- **Auto Runs are the locations from which Active Modules are spawned (instantiated). These are: run keys in registries, BHO registries, .DLL extensions, application extensions and the Start Directory.**
- **The Hosts file, stored in a PC's file system, is used to look up IP addresses. If the IP address is not found in the Hosts file, the computer will ask a DNS computer (domain name server) for the information. Malware programs that add entries to (infect) a machine's Hosts file are particularly virulent.**

## **Malicious files can be targeted by their attributes. Some attributes of a file include:**

- **Signature:** The unique alphanumeric identification string of the resource.
- **Filename:** The name used to identify the resource.
- **Path:** The route to the resource.
- **MD5 Signature:** The one-way hash function (algorithm) that generates a fixed string of numbers for encryption.

*Actions are the techniques used to “kill” the resource. There are six actions that can be applied to resources in order to kill them. Researchers apply the appropriate combination of the following actions to Malware:*

- **Extracting** is a two-step process of **Suppress** and **Extract**. If running, the software will delete the entry (**Suppress**) and then delete (**Extract**) the file.
- **Suppression** means that the software will stop a BHO or .DLL from being instantiated (run once) by removing the call to the .DLL file -which usually resides in the system registry- without actually deleting the file.
- **Restricton** pertains only to pop-ups. It means that the software will inject iS3 BHO code into the targeted process. It will detect pop-ups coming from a pre-defined executable and stop them.
- **Blanketing** applies to domains only. It means that the software will block or allow anything from a Web site.
- **Injecting** applies to the Hosts file only. The software will reconfigure the Hosts file to prevent users from going to particularly malicious sites.
- **Protecting** applies to Hosts Files. The software will remove malicious entries from the Hosts file.
- **Watching** applies to scanning a part of the system registry. Any changes made to the configured registry will trigger pre-defined actions by the software. To keep pace with the speed of new Malware proliferation, a watcher can be added dynamically via target update.

## **Anti-Phishing Definitions**

iS3 Research receives continual data on Phishing sites from the Anti-Phishing Working Group. Every thirty minutes, the newest definitions are sent to iS3 and incorporated into the next build of each iS3 product. In addition, subscribers can report “false negatives,” sites determined to be SAFE that are actually UNSAFE, and “false positives,” sites determined to be UNSAFE that are actually SAFE. These reports are analyzed by Research and added to the Public Blacklist and Public Whitelist, as appropriate. Report results are then conveyed to the Anti-Phishing Working Group.

## **The Singularity Database**

Through the synergy of Research, Customer Support and Development, iS3 has created an unparalleled repository of Malware applications, phishing definitions and knowledge known as the Singularity Database. The database also contains identifiers for all known SAFE software determined by scanning. This database is used to store all information gathered about known Malware and targets; the techniques used to kill it. Singularity is updated frequently, often daily, with the latest target definitions. The newest targets comprise the latest build of STOPzilla or other iS3 products. This version is pushed out to the iS3 server from which users can have it downloaded automatically or on demand, according to individual preferences.

***See diagram on next page.***

