Global InfoTek Automated Malware Analysis System (GAMAS)

1. Background:

Malware and botnet activity in recent months and years has intensified across the Internet and other critical infrastructures, with recent events, such as the Target point of sales, Conficker, and Stuxnet, demonstrating the clear and present threat posed that is intelligent, adaptive, and effective at scale over increasingly shorter time periods.

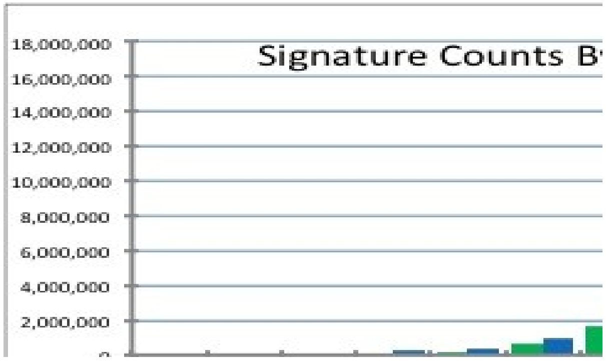
The technical problems are, wherever possible: to avoid allowing malware onto a platform (prevention); to protect systems from infection when malware is in the system's environment (protection); to detect malware that has been installed (detection); analyze malware's infection, propogation, destructive mechanisms, and to monitor and identify its source (analysis); and to remove malware once it has been installed and identify mechanisms to prevent future outbreaks (reaction/remediation).

GAMAS defense against malware to ensure secure and resilient networks include:

- <u>Prevent:</u> Prevent the production and propagation of malware
- <u>Protect:</u> Protect systems from infection when malware is in the system's environment
- <u>Detect:</u> Detect malware as it propagates on networks, detect malware infections on specific systems
- <u>Analyze:</u> Analyze malware's infection, propagation, and destructive mechanisms
- <u>React:</u> Remediate a malware infection and identify mechanisms to prevent future outbreaks

2. Why Is It Important

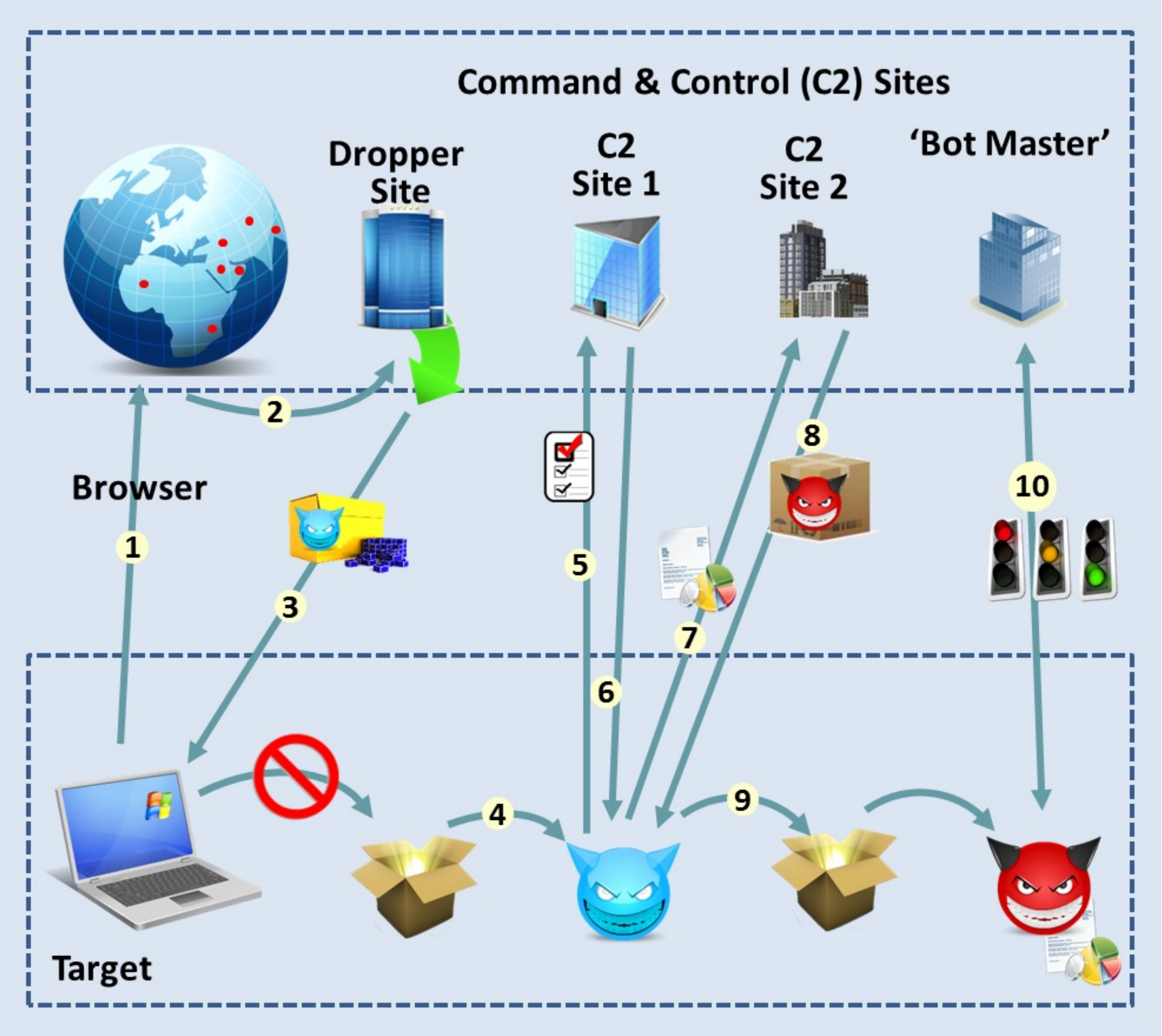
Malware and botnet activity has been increasing for many years across the Internet and other critical infrastructures. The number of unique samples is growing exponentially with the Anti-Virus (AV) vendors capitalizing on the sale and subscription to AV signatures[1]. Yet the protections have not been adequate. We need a game changing technology that does not rely on signatures!



[1] http://www.triumfant.com/Signature_Counter.asp

3. GAMAS

Our Malware Runtime Analysis and Protection system will detect malware and bot infections on specific systems even when it is already present on the system; dynamically and stealthily analyze malware and bot code execution on the host (including infection, communication, propagation, and destructive mechanisms); and protect systems from further infections by that malware or bot via generation and deployment of detection/response mechanisms.



<u>Problem</u> -Malware is typically packed, obfuscated and encrypted to avoid detection. Analysis can *only* take place when the actual code is uncovered. State of the art approaches to malware analysis re-execute the malware in an instrumented environment (e.g., a virtual machine or a debugger) to gather the required information (interactions and code). This is a time consuming manual process. Furthermore, by detecting the instrumented environment and altering its behavior (e.g., not unpacking all code), malware can force the analyst do more manual work.

<u>GAMAS Approach</u> – GAMAS can prevent infections by only allowing known executables to run on a host or device. When this is not possible GAMAS captures all required information via real-time monitoring, making it unnecessary to rerun the malware. Using light weight instrumentation, it efficiently monitors possible malware as it executes to capture interactions with the operating system and follow detailed code execution. GAMAS traces exactly what code was executed and captures all unpacked code. It also captures a variety of internal program events (such as self-modifying code, unpacking, decryption, etc.) that are characteristic of malware. This low level detail is essential to understanding malware. It is also invisible to system call monitoring. Other more labor-intensive, offline techniques must be used. Using these attributes as clues, GAMAS performs advanced analytic to automatically determine anomalous behaviors that could trigger deeper inspection.

GAMAS monitoring is very low overhead. Instrumentation is used only on untrusted code or high risk applications like browsers. Trusted code is only monitored when GAMAS detects malicious activity elsewhere and turns on very lightweight mechanism (<1% overhead) to track critical activities (registry changes, file system changes, etc.).

GAMAS's automated analysis takes advantage of the unique information that it gathers during execution. It contains detectors for code commonly used by malware like unpackers, decrypters, stealth mechanisms, etc.

Applicability - The enterprise and government need to mitigate the effects of cyber-attacks on our critical infrastructures. These systems are under constant attack from new malware. Antivirus vendors (AV) estimate over 100,000 new variants a month. Prevention of attacks requires that malware be classified as such in near real time. The speed of this classification must be equal or greater than the rate of new threat generation or we will be fighting a losing battle. The Global InfoTek's GAMAS system delivers a game-changing capability to do this.