Defending Against APT Malware

Defending Against APT Malware with the Infoblox Trinzic DDI Product Family

One of the most critical tasks facing IT organizations today is protecting against sophisticated programs (often called Advanced Persistent Threat or APT malware) designed to remain undetected on desktops, pad devices, and smart phones over long periods of time while capturing and transmitting sensitive government, corporate, and private information to a master malware controller device. This class of malware also enables use of an entire network (called a botnet) of infected devices in launching Distributed Denial of Service (DDoS) attacks and in sending junk (SPAM) email.

Traditional anti-malware techniques cannot consistently counteract the malware threat. For example, this class of malware repacks frequently to defeat signature- based approaches such as antivirus programs. By exploiting the DNS protocol, this class of malware circumvents the protection of legacy IP firewalls, computer monitoring approaches, and web filters.

Government agencies and other organizations need a new approach that they can deploy as part of an enhanced “defense in depth” strategy. This new approach should address prevention of infections, their detection, and mitigation. It also should enable responses to new threats on a timescale comparable to or faster than the attackers. Further, it should not require expensive and disruptive changes to network infrastructure and end user systems.

One successful approach is the Infoblox DNS Firewall, an additional capability of the same Infoblox Trinzic DDI appliances that leading government agencies use today to provide DNS, DHCP, and related critical network services. Why build protection into the DNS layer? Because almost all activity on the network, including the actions of malware, relies on the Domain Name System to operate. Once malware infects a victim's system it uses DNS to locate botnet command and control systems and leverages the DNS protocol to transmit stolen information and to receive botnet commands. Botnet controllers also rely on DNS, rapidly changing the sites' IP addresses and URLs to obscure their network locations and evade traditional access controls.

The Infoblox DNS Firewall runs on Infoblox Trinzic DDI appliances acting as “recursive resolvers”, translating domain names to IP addresses and responding to other DNS queries. Leveraging existing DNS technology – the Response Policy Zone (RPZ) standards developed by ISC - the Infoblox DNS Firewall can block requests for designated domains or redirect them to an internal system. The Infoblox DNS Firewall can update the list of malicious domains in near real time using data sourced from one or more reputational feeds. Customers can subscribe to one or more options of the Infoblox Malware Data Feed (including an option designed for Government use) and/or commercial and internal feeds.

The Infoblox DNS Firewall can also block, drop, or redirect DNS requests from malware on already infected systems, thereby disrupting botnet operations and preventing already captured data from being transmitted. By deploying Infoblox Trinzic DDI appliances to resolve all end device DNS requests (as opposed to handling only requests passed on by Microsoft DNS servers and other systems) a customer can quickly and easily pinpoint the true source IP and MAC addresses of infected systems. With the assistance of Infoblox's NetMRI Switch Port Manager appliance they can even easily locate such systems within the overall network, down to the exact switch port interface.

The Infoblox DNS Firewall gives government agencies and other organizations a new and effective weapon in the ongoing fight against cyberattacks.
Infoblox Malware Data Feed, Government Option

Targeted to needs of Governmental Agencies and Suppliers, the data feed contains:

- Known botnet C&C domains/IPs and dropboxes as well as name servers that are known to be used solely by malicious entities.
- Resources used to sinkhole contact attempts by botnets that have been taken down by law enforcement and/or security researchers (e.g. conficker).
- The sites (IPs/domains/name servers) for known malware droppers and other places that can infect a computer. Includes entities on the “Do not Route Or Peer” (DROP) list.
- Known active phishing sites and other threats.
- IP subnets, the ccTLD domains and name servers for the countries on the OFAC Embargo and ITAR lists maintained by the US government.
- See [http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx](http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx) and [http://pmddtc.state.gov/regulations_laws/itar_official.html](http://pmddtc.state.gov/regulations_laws/itar_official.html)