WHITEPAPER

Defeating Advanced Persistent Threat Malware

Table of Contents

1. Malware is Everywhere

1.1. Attacks Can Come From Anywhere

Press headlines are filled by reports of malware attacks. Malware attacks, once the reserve of amateurs largely for amusement, are now launched by a number of entities. Today, a malware attack can literally come from anywhere in the world and can impact even the largest organization.

- Government "Cyberwar" teams: Governments are alleged to be attacking other governments' entities as well as private companies[1].
- Hacktivists: Hacker activists (called "hacktivists") are utilizing malware attacks as a form of protest against government, commercial, and even private web sites[2].
- Government censor organizations: Certain governments are allegedly using malware attacks as a form of censorship. For example, it is suspected that websites are selectively blocked to prevent social media from being used to organize protests and to coalesce public opinion against the government[3].
- Criminal Elements: Malware attacks upon banks and upon individuals are executed by criminal elements worldwide[4].
- Random Individuals: With the availability of low cost or even free 'roll your own' malware kits on the Web[5], almost anyone can plan and execute a malware attack.

> "Malware is profitable: malware is no longer just a fun game for script kiddies or a field of study for researchers. Today, it is a serious business and source of revenue for malicious actors and criminals all over the world. Malware, together with other cyber tools and techniques, provides a low cost, reusable method of conducting highly lucrative forms of cybercrime." [6]
>
> — Organisation for Economic Co-operation and Development (OECD)

[1] Winter, Michael, USA Today, "NBC: Iran reportedly behind cyber attacks on U.S. banks", 09/20/12.

[2] Dunn, John E., Computerworld, "Hacktivists DDoS UK, US and Swedish Government websites", 9/7/12.

[3] Wikipedia, "http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China".

[4] Wikipedia, "http://en.wikipedia.org/wiki/Botnet"

[5] Wikipedia, "http://en.wikipedia.org/wiki/Webattacker"

[6] OECD, OECD Guidelines for the Security of Information Systems and Networks, http://www.oecd.org/sti/interneteconomy/15582260.pdf, 2002.

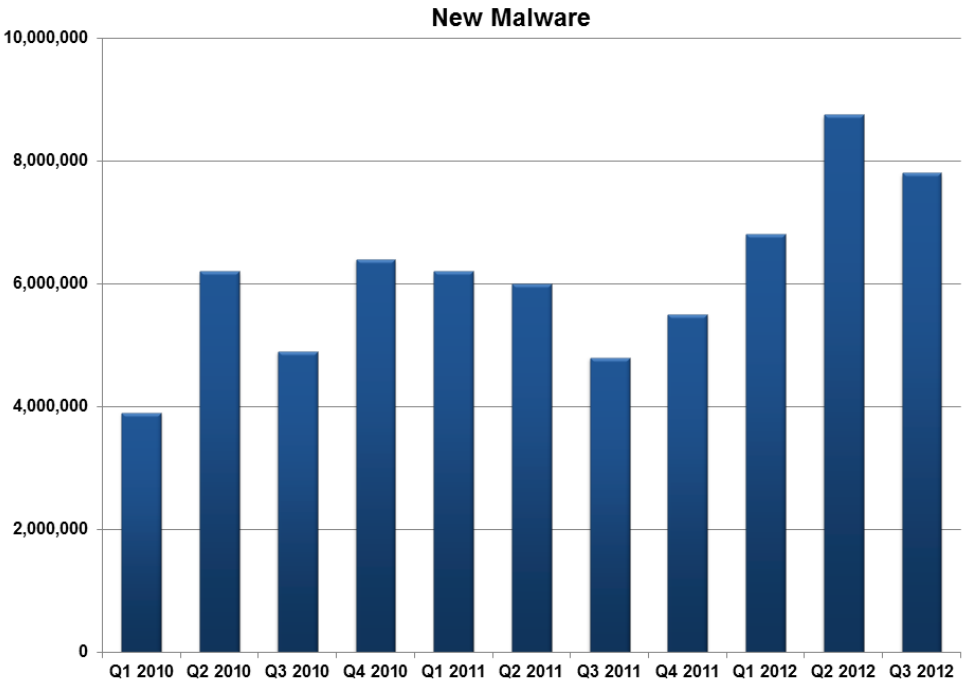
1.2. Malware Statistics are Startling

Statistics about malware attacks are truly startling due to the number of attacks, the number of successful attacks, and the time that it takes to discover malware.

The average volume of new malware threats is approximately 7.8 million per quarter for the first three quarters of 2012 alone, a rate of 1 new threat per second! During the same period, malware on mobile devices grew more than 10 fold, according to McAfee[7].

Further, malware attacks are extremely effective. A 2012 Verizon security study[8] illustrates that in 2011 alone there were:

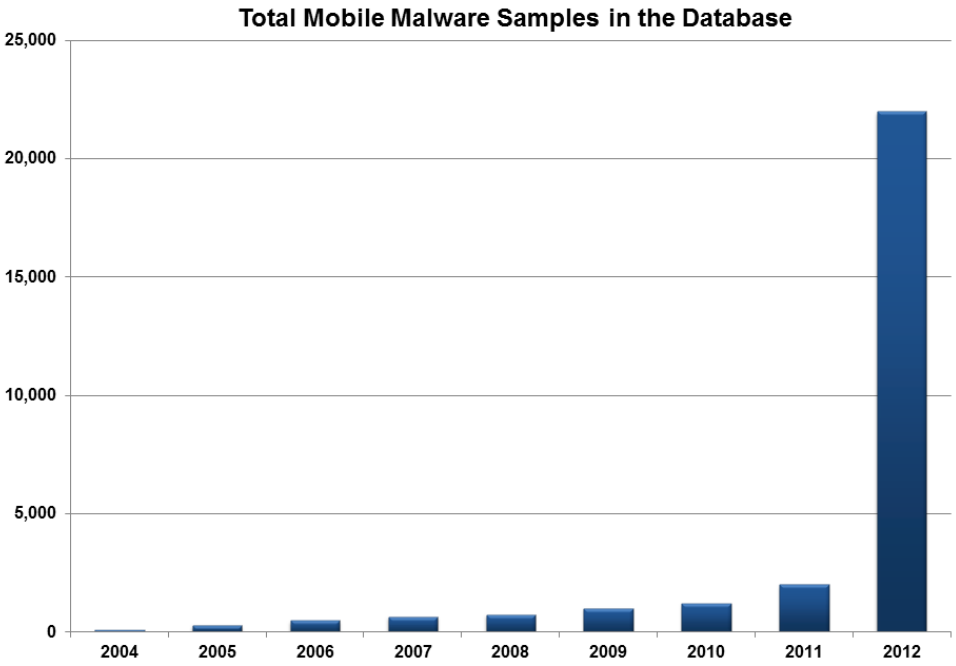
- Around 855 successful breaches of corporate or government entities that compromised around 174 million records.
- Of the successful breaches, 69% utilized Malware.



Source: McAfee, 2012.

[7] McAfee, "McAfee Threats Report: Third Quarter 2012", (http://www.mcafee.com/us/about/news/2012/q3/20120910-01.aspx?cid=110907)

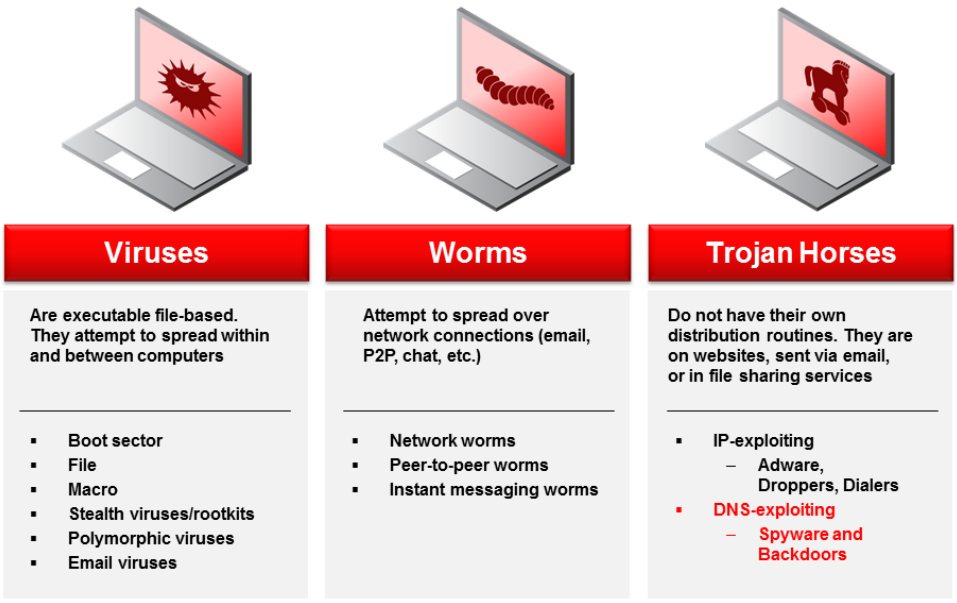
[8] Verizon, "Verizon Security Study 2012", (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, 2012)



Source: McAfee, 2012.

1.3. All Malware Is Not Alike

There are numerous families, classes, subclasses, and variants of malware. Many sources differ as to the categorization. Also, many types of malware exhibit characteristics of multiple families and classes and so can be described as 'hybrid'. To provide a reference point for this White Paper, Infoblox has created a classification system for Malware.



Source: Infoblox, 2013

Infoblox considers there to be three major families of malware as shown in the diagram – Viruses, Worms, and Trojan Horses. Of the Trojan Horses:

- One class – called IP-exploiting – typically uses Internet Protocol (IP) for communications.
- Another class – called DNS-exploiting – typically exploits Domain Name Services (DNS) for communications between the malware-infected device and the master controller of a network of infected devices (called a 'botnet').

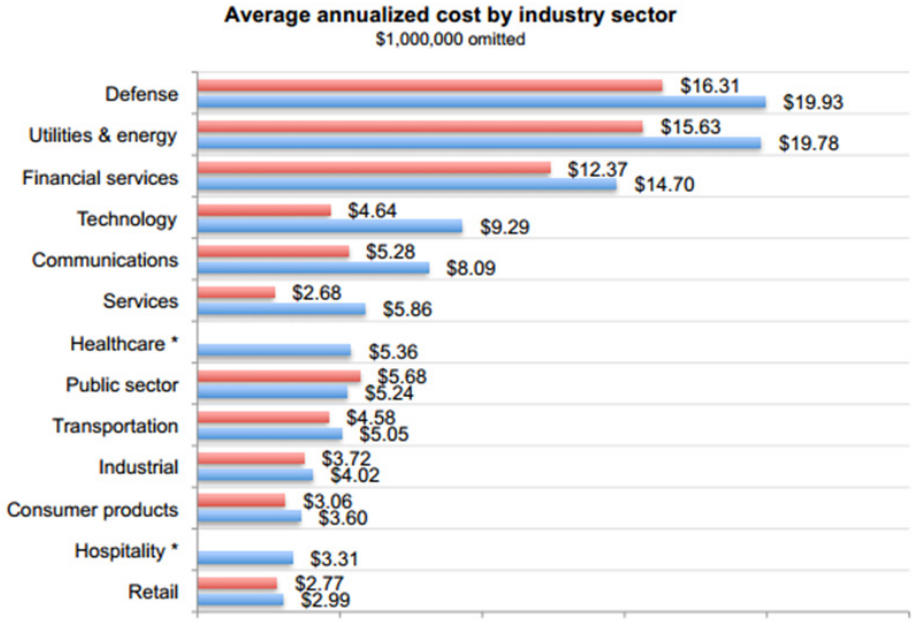
DNS-exploiting Malware typically is designed to remain undetected on servers and on personal devices over a long time period. Based on commands received from the master controller via 'backdoor' malware, infected devices will either capture data (via spyware malware) or execute actions – such as send SPAM emails or participate in a Distributed Denial of Service (DDoS) attack.

As this type of malware is very sophisticated and is designed to persist over time, a commonly-used description for this category is "Advanced Persistent Threat" or "APT Malware". This White Paper will use the term "APT Malware" for consistency across a variety of information sources.

1.4. APT Malware Breaches Are Expensive

A study by the Ponemon Breach Institute provides some estimated costs for malware[9]. In terms of total Malware cost per company, figures are:

- A 2011 median cost of $5.9 million dollars annually / average of $8.4 million annually across all companies and industries studied.
- While the study says that the figures may not be wholly trustworthy due to low sample size, the 2011 cost by industry is estimated to range from an average of almost $20 million / year for Defense down to $3 million / year for Retail.

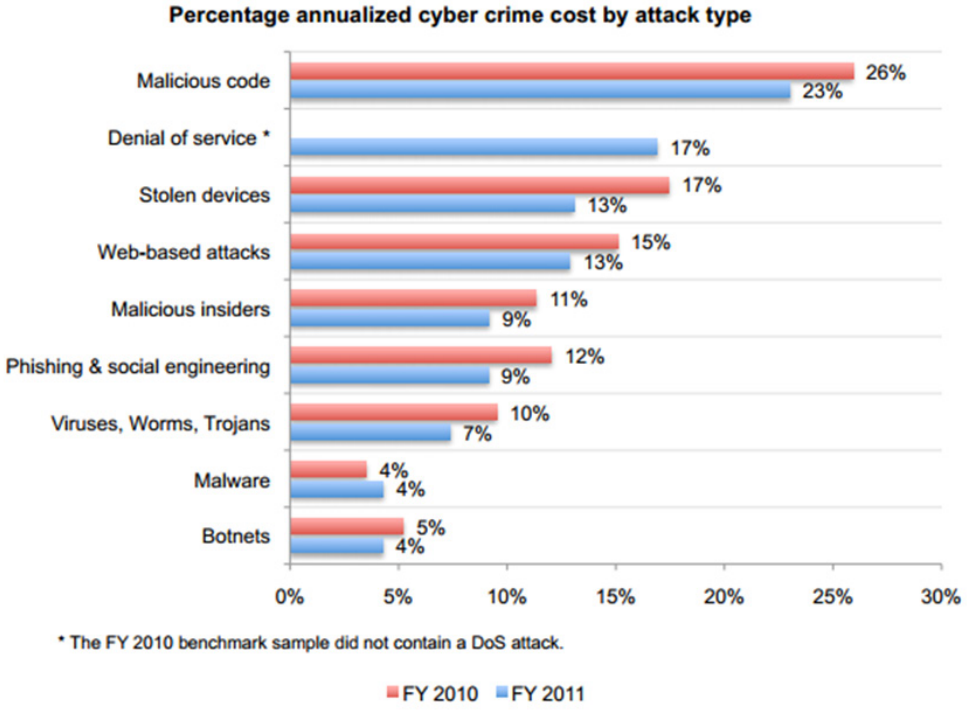


Source: Ponemon Institute, 2012.

APT Malware (categorized as “Malicious code” in the diagram below) is the most expensive kind of malware, accounting for approximately 23-26% of the total annual cost.

One factor in the expense of Malware is the length of time that it remains undetected, particularly by internal staffs. The Verizon study[10] calculated that:

- 54% of malware took months to discover
- 29% of malware took weeks to discover
- 92% of malware is detected by an external party.



Ponemon Institute, 2012

Netting out the figures above, it appears that most companies never detect malware at all much less in a timely manner.

[9] Ponemon Institute, “Second Annual Cost of Cyber Crime Study,” (http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf), August 2011.

[10] Verizon, “Verizon Security Study 2012”, (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, 2012).

2. APT Malware Requires a New Approach

2.1. APT Malware Exploits the DNS Protocol

For the Domain Name System (DNS) protocol to work properly, DNS communications must flow freely among all devices and applications. Further, since DNS is integral to the process of establishing and maintaining communications with a web server, applications such as chat, and mobile device applications, any delays in processing or potential decreases in availability could easily ripple into a much larger problem. As a result, DNS commands are typically not intercepted or inspected by existing security approaches.

By exploiting DNS, malware developers can sidestep existing security approaches:

- For example, since network firewalls typically blacklist at the IP address level, malware master controllers reportedly change their IP addresses hourly either by rotation on a list or by using techniques such as “Fast flux” to hide behind a variety of ever-changing proxy servers[11].
- Also, since web filter approaches typically work on the exact URL only, by changing URLs flexibly within a domain, malware circumvents web filter approaches.

DNS provides a powerful means for locating the botnet master controller and for transmitting instructions to infected devices. For example, DNS is used to locate the botnet master controller, even when it changes IP addresses and/or URLs frequently. Also, DNS is used to transmit instructions to the infected devices, via techniques typically called “DNS tunneling” or “DNS hijacking”[12].

2.2. DNS Security Gap

Many organizations believe in the concept of “layered security”. Wikipedia defines layered security as “For every category of threat, there should be an effective control deployed to mitigate the threat.”[13] (Security industry analysts also use the term “Defense in Depth” to describe this concept. [14]) In summary, each network layer typically has unique vulnerabilities that attackers strive to leverage. Further, different attacks can be directed at the same layer. So, on average, each network layer should have its own security mechanism that counters its unique vulnerabilities and protects against all relevant attacks.

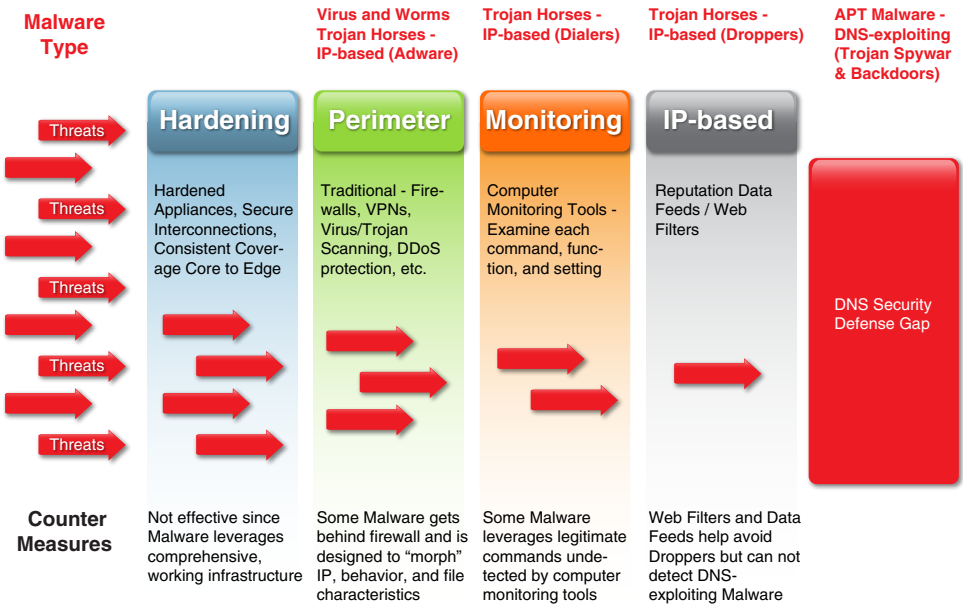
[11] Wikipedia, “http://en.wikipedia.org/wiki/Botnet”

[12] Wikipedia, “http://en.wikipedia.org/wiki/DNS_hijacking”

[13] Wikipedia, “http://en.wikipedia.org/wiki/Layered_security”

[14] Wikipedia, “http://en.wikipedia.org/wiki/Defense_in_depth_(computing)”

For example, the diagram to the right shows a variety of malware threats and the corresponding ways in which they are neutralized. For example, many Viruses and Worms are effectively addressed with antivirus scanning. Also, malware DDoS attacks can be neutralized within the DNS and/or overall networking architecture. Device monitoring packages can intercept questionable file downloads.



Layered Security To Combat Malware

However, APT malware that exploits DNS for communications cannot be effectively addressed by existing approaches:

- While this capability does not rely on DNS, APT malware defeats signature-based approaches built into anti-virus packages by techniques such as repacking[15].
- Web Filters typically act at the URL level since they are blocking specific content objects
- Firewalls typically act at the IP level since they are blocking specific servers
- Data Loss Prevention approaches typically would require numerous, overly intrusive sensor points in the network to enable 'sniffing' of all DNS traffic.

As existing approaches, while highly useful against certain types of malware, are not effective against APT Malware, a new defense must be designed and deployed.

[15] Caballero, Juan, et.al., Measuring Pay-per-Install: The Commoditization of Malware Distribution, USENIX White Paper, http://static.usenix.org/events/sec11/tech/full_papers/Caballero.pdf, August, 2011.

2.3. Solution to APT Malware: A DNS Firewall

Since the core communications protocol for APT Malware is DNS, an approach baked into DNS is worthy of exploration. In fact, the concept of an embedded malware security mechanism for DNS – called a "DNS Firewall" – was proposed in a recent Security Week article[16].

Unlike a traditional network firewall that protects from the physical layer going up to and optionally including the application layer, a DNS Firewall must absolutely include protection at the application layer as the quality of the actual DNS data must be protected. To put this need in terms used by network firewalls, there is a strong need for an "Application-level DNS Firewall."

> "… DNS firewalls likely would have prevented the success of more than 80 percent of these attacks."
>
> —Security Week

3. Design Considerations for a DNS Firewall

3.1. Security (including Malware) Related Standards Worldwide

The Organisation for Economic Co-operation and Development (OECD) is a group of 34 countries (including the United Kingdom, Israel, Japan, Korea, and U.S.) that together strive for economic growth. The 2002 OECD Guidelines for the Security of Information Systems and Networks provide a list of broad information security principles all of which are relevant and applicable to the fight against malware. The nine principles are Awareness, Responsibility, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, and Reassessment[17].

3.2. Malware-related Standards in the United States

The National Institute of Standards and Technology (NIST) is part of the U.S. Dept. of Commerce. A NIST publication, Guide to Malware Incident Prevention and Handling, provides specific and targeted recommendations for malware. Recommendations are summarized below[18].

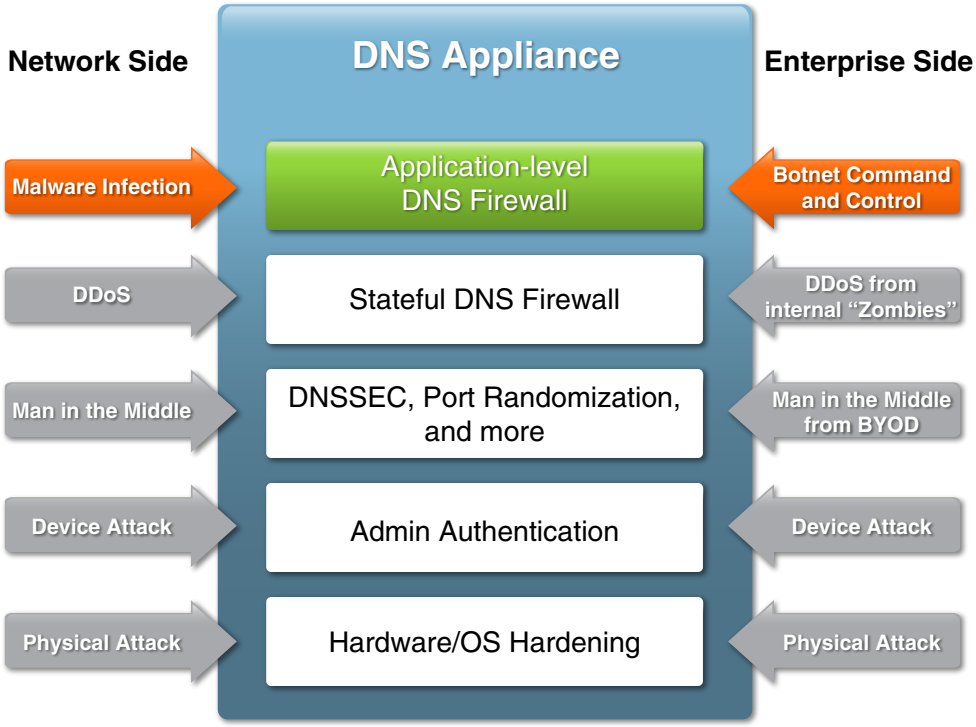
- Organizations should develop and implement an approach to malware incident prevention.
- Organizations should ensure that their policies support the prevention of malware incidents.
- Organizations should incorporate malware incident prevention and handling into their awareness programs.

[16] Rasmussen, Rod, Security Week blog, "Why DNS Firewalls Should Become the Next Hot Thing in Enterprise Security," (http://www.securityweek.com/why-dns-firewalls-should-become-next-hot-thing-enterprise-security, October 2011).

- Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.
- Organizations should have threat mitigation capabilities to assist in containing malware incidents.
- Organizations should have a robust incident response process capability that addresses malware incident handling.

3.3. Multi-tier DNS Security

A defense against APT Malware cannot be standalone since it must also resist attacks from hackers and from other types of malware. To illustrate all the defenses needed within the DNS layer, they are illustrated as tiers of attacks and corresponding defenses.



DNS Security must resist both external and internal attacks

[17] OECD, OECD Guidelines for the Security of Information Systems and Networks, http://www.oecd.org/sti/interneteconomy/15582260.pdf, 2002.

[18] National Institute of Standards and Technology, U.S. Dept. of Commerce, Guide to Malware Incident Prevention and Handling, http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf, November 2005.

A DNS Security approach must be built on top of a robust security foundation. Starting at the bottom of the figure to the left:

- A DNS appliance must be able to resist both internal and external physical attacks via hardening of the hardware and the operating system.
- Device attacks need to be repelled via advanced administrator authentication techniques (i.e. TACACS).
- Network attacks arising from hostile devices in the network and/or compromised Bring Your Own Devices (BYODs) can be overcome via a variety of techniques such as DNSSEC.
- DDoS attacks, including attempts to overload sessions, can be averted via DDoS techniques and the use of state to clarify which session creation requests are genuine. This is somewhat equivalent to the function of a 'stateful' network firewall and so is described as a "Stateful DNS Firewall" tier of defense.
- Moving to the top layer, Malware infection must be proactively prevented and Botnet command and control instructions, most likely from infected BYOD devices, must be disrupted. As these commands can be issued by applications, the functionality resembles to the function of a network application firewall. So, the functionality to combat APT Malware would be that of an "Application-level DNS Firewall" tier of defense.

4. Combatting APT Malware

4.1. An Approach Worth Investigating – Infoblox DNS Firewall

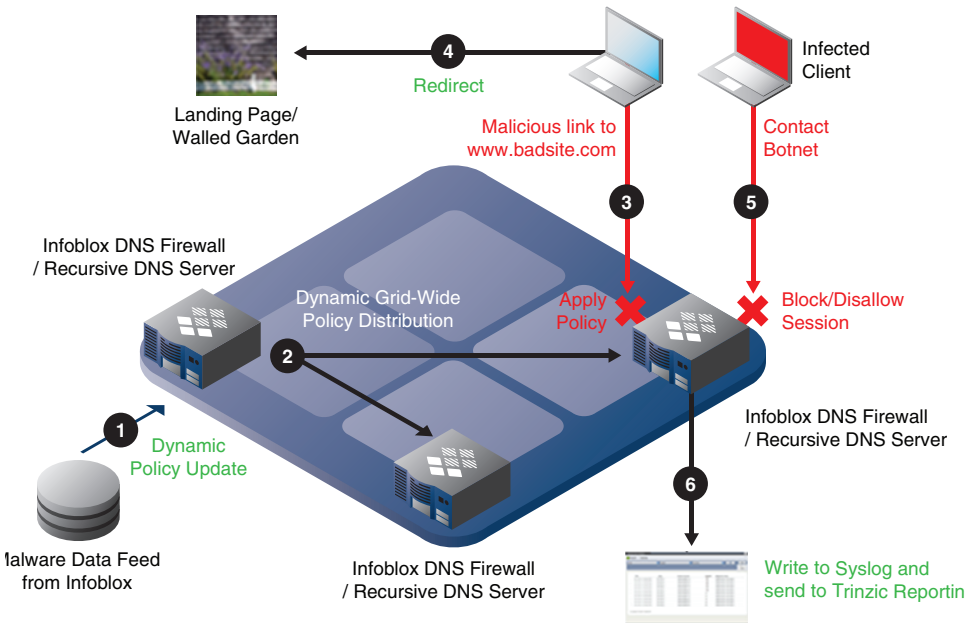
Infoblox created a DNS security solution – called the Infoblox DNS Firewall – based on its market-leading family of products – Trinzic DDI™. Infoblox believes that this approach is the industry's first true DNS security solution.

The Infoblox DNS Firewall solution is composed of:

- Product License: The functionality is pre-installed with the latest release of Infoblox's Trinzic DDI operating system and only needs a key for activation.
- Malware Data Feed from Infoblox (optional annual subscription): The product license will accept multiple data feeds. The customer has the option of subscribing to Infoblox's proprietary malware-specific reputational data feed.
- Infoblox Grid™: The solution requires an Infoblox Grid be installed as it leverages Grid functions such as automatic file updates, security, and more.

4.2. How the Solution Works

As shown in the figure to the right, the solution works as follows:



Operation of the Infoblox DNS Firewall

1 When the Infoblox experts detect a new malware, the Infoblox Malware Data Feed immediately sends an update to our customers.

2 Either directly or by leveraging the Infoblox Grid™, the updated data is sent to all Infoblox Recursive DNS Servers in near real time.

3 If an end user clicks on a malicious link or attempts to go to a known malware website, the attempt will be blocked at the DNS level.

4 The session can be redirected to a landing page / walled garden site defined by the company administrator.

5 For clients that are infected already, very typically user-owned devices, the infected client will attempt to use DNS commands to communicate with the botnet master controller. The Infoblox DNS Firewall will not execute these commands, effectively crippling the botnet.

6 All activities are written to industry-standard Syslog format so that the IT team can either investigate the source of the malware links or cleanse the infected client. Data is also fed to the Trinzic Reporting product for analysis and reporting.

4.3. Meeting Malware-related Security Standards

In addition to the OECD standards, the Infoblox solution fully meets the NIST standards as summarized in the table below:

NIST Standard	Infoblox DNS Firewall
• Organizations should develop and implement an approach to malware incident prevention.	• Provides an end to end approach that proactively prevents infection as well as execution of Malware, therefore minimizing or eliminating malware incidents.
• Organizations should ensure that their policies support the prevention of malware incidents.	• Malware policies are automatically updated via the Infoblox Malware Data Feed. Policies can also be set or modified by the security administrator.
• Organizations should incorporate malware incident prevention and handling into their awareness programs.	• The “Landing Page / Walled Garden” functionality is tailor-made for incorporation into awareness programs.
• Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.	• Vulnerability mitigation is built-in via both redirection of infected clients and disruption of botnet communications.
• Organizations should have threat mitigation capabilities to assist in containing malware incidents.	• Since botnet communications and sessions are disrupted, Malware is contained.
• Organizations should have a robust incident response process capability that addresses malware incident handling.	• All malware activities are logged. With the use of the Infoblox Reporting Server, malware reports can also be exported into IT task lists for malware incident handling such as cleanup of infected devices.

4.4. Meeting Multi-tier Security Requirements

As the Infoblox DNS Firewall leverages the security architecture of both the Infoblox Grid™ and Infoblox appliances, the multi-tier security requirements detailed in the previous section are all provided. Most importantly, since the actual DNS commands issued by all applications and devices are monitored, the product provides the protection of an Application-level DNS Firewall.

4.5. Why the Solution is Unique

The Infoblox DNS Firewall provides differentiating capabilities to Security and Networking organizations in terms of being Proactive, Timely, and Tunable.

4.5.1. Proactive

The Infoblox DNS Firewall stops clients from becoming infected by going to a malware website or clicking on a malicious link. Further, 'hijacked' DNS Command and Control requests are not executed to prevent the botnet from operating. Lastly, all malware activities are logged and reported to pinpoint infected clients and attacks.

4.5.2. Timely

The Infoblox DNS Firewall leverages comprehensive, accurate, and current malware data to detect and resolve malware weeks to months faster than in-house efforts. The robust data provided by Infoblox is comprehensive in terms of including all known attacks and very accurate in terms of a very low false positive rate. Automated distribution maximizes response timeliness from Infoblox throughout the customer's Grid in near real-time.

4.5.3. Tunable

The solution is tunable to ensure that all threats can be countered in the customer's unique environment. The solution allows the definition of hierarchical DNS, NXDOMAIN Redirection, and Malware policies that maximize flexibility. The administrator has full control over which policies are enforced by each recursive DNS server. The Infoblox Malware Data Feed includes several options that enable the precise matching of data, including geography, to the threats encountered. In addition, the Infoblox Data Feed can also be combined with multiple internal and external reputational data feeds.

4.6. Learning More

To learn more, please point your browser to www.infoblox.com/dnsfirewall or contact sales@infoblox.com.

CORPORATE HEADQUARTERS:

+1.408.625.4200

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32 (0)22 590 430

info-emea@infoblox.com

APAC HEADQUARTERS:

+(852) 3793-3428

sales-apac@infoblox.com