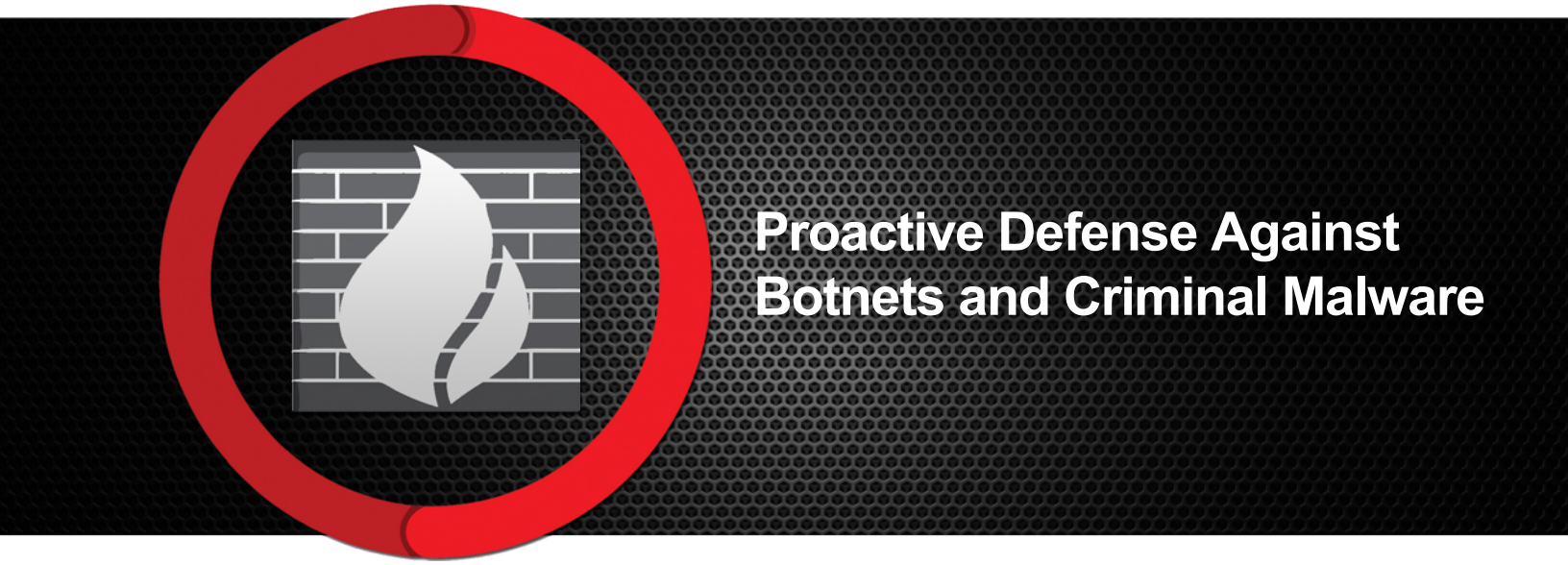
ThreatSTOP™



Proactive Defense Against Botnets and Criminal Malware

Core Elements

1) A comprehensive and accurate list of IP addresses to ensure users are blocking the right “bad” addresses (low false positives and negatives).

2) Real time updates, because the criminals are constantly changing the sources of their attacks.

Summary

Botnets created and spread by criminal malware are the biggest problem in information security today. They cause great financial and reputational damage to their victims and are not effectively prevented by the current crop of solutions. Research leveraged by ThreatSTOP is emerging as the method to address this growing problem and is becoming a required component of an effective layered defense against cybercriminals, just like anti-virus did starting 15 years ago.

An effective firewall setup requires two core elements:

1) A comprehensive and accurate list of IP addresses to ensure users are blocking the right “bad” addresses (low false positives and negatives).
2) Real time updates, because the criminals are constantly changing their attack sources.

ThreatSTOP not only has these two elements, but also has developed a unique, patented capability to distribute its threat list via DNS directly to users’ firewalls so they can automatically enforce traffic policy—both in bound and outbound—at the gateway.

Without this distribution capability, only the largest organizations with the financial resources to employ teams of dedicated security professionals can fine tune firewalls by “doing it themselves.” Our capability enables

Summary Continued

ThreatSTOP to provide a cost-effective service to everyone from small businesses to multinationals and government agencies of all levels. ThreatSTOP customers do not have to install new equipment or change their current network and security setup. Instead, ThreatSTOP can be deployed on most existing firewalls in under an hour.

The service provides a feedback loop for customers' log data to become part of its threat feeds to further enhance the coverage, timeliness, and accuracy of its Threat List and thereby better protect every member of the ThreatSTOP user network.

This whitepaper will discuss at a high level:

1) What is the botnet/criminal malware problem?
2) Why current products are not effective against botnets.
3) What is IP reputation?
4) How ThreatSTOP offers a unique solution.

The Botnet Problem

Botnets are networks of compromised computers controlled by criminal third parties. They are different from spam, phishing, and viruses that current solutions address in three respects:

1) Botnets are usually controlled by organized criminal syndicates or state actors with malicious purpose, as compared to individual or small groups of hackers engaging in pranks, on-line graffiti, or spam marketing.

2) Botnets are active exploits designed to get inside your network, often by social networking or piggybacking on devices brought in from outside, such as laptops, smartphones, and USB drives. They are generally very stealthy except for when they communicate with their command and control hosts (C&C hosts) outside your network. This can be as simple as to just report "I am ready!" or to receive commands such as "infect other machines in the network" or "steal the credit card numbers from the customer database." On the other hand, most spamware is acted upon by the user, not through the control of a remote party.

A Pervasive Problem

Botnets are rapidly growing globally. Cisco's Q4 2010 Global Threat Report showed a 139% increase in active malware in 2010. This is contrasted by spam dropping from 375 billion pieces per month, to 95 billion for the year.[1]

In a survey[2] of 130 large corporations by TrendMicro, they were found to have the following infestations:

Active malware	100%
Information stealing malware	56%
One or more IRC bots	72%
Network worm	42%

References

[1] **Q4 2010** *Global Threat Report*, **Cisco Corp.**

[2] **130 Global Threat Discovery Services trials through August 2009, TrendMicro.**

The Botnet Problem Continued

3) Botnets are designed to steal your most valuable data, be it customer credit card numbers, your personnel data, or your engineering designs. The spamware we are all (unfortunately) used to is primarily designed to get attention. While annoying, mostly it just wastes your time and slows down your machines.

Ramifications

Breaches reported in recent years have shown the magnitude of the issue. A small sample includes:

Western Union — 20,000 cc accounts

UNF University of North Florida — 97, 200 student records

Digital River — 200,000 accounts

Heartland Payment Systems (The Highest Standards | The Most Trusted Transactions) — 130 million cc accounts

at&t — 114,000 e-mail addresses

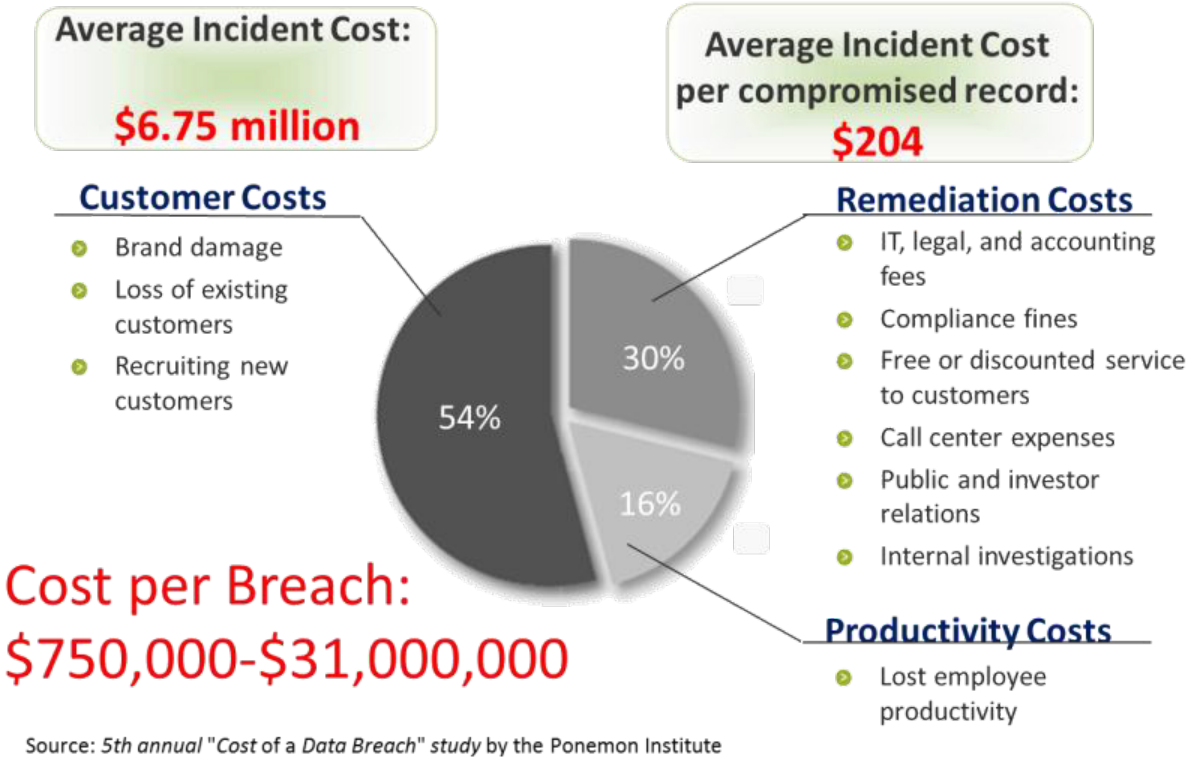
UCLA Bruins — 80,000 student records

An Expensive Problem

A breach by a botnet is an expensive problem to fix once discovered and the longer it remains undetected the worse it is likely to be. There is the obvious financial cost of remediation, as well as significant damage to a brand's reputation due to public exposure. Not to mention the fines incurred for failing data security compliance regulations. Careers of executives and IT/security personnel are often damaged, as well. In a few extreme cases, a breach can be serious enough to shut a business down.

In a well-known study by the Ponemon Institute, the average cost of a security breach for a large enterprise is almost $7 million, with a range of $75,000 - 31,000,000.[3]

[3] Fifth annual *Cost of a Data Breach* study, The Ponemon Institute.



Source: *5th annual "Cost of a Data Breach" study* by the Ponemon Institute

Section One Summary

Botnets and other criminal malware are a growing, pervasive and expensive problem for all organizations, large and small, private or government. This situation will only get worse since:

1) The cybercriminals continuously launched more, and more sophisticated attacks, overwhelming defenses.
2) The Internet provides a universal conduit to a growing number of organizations and their sensitive data.

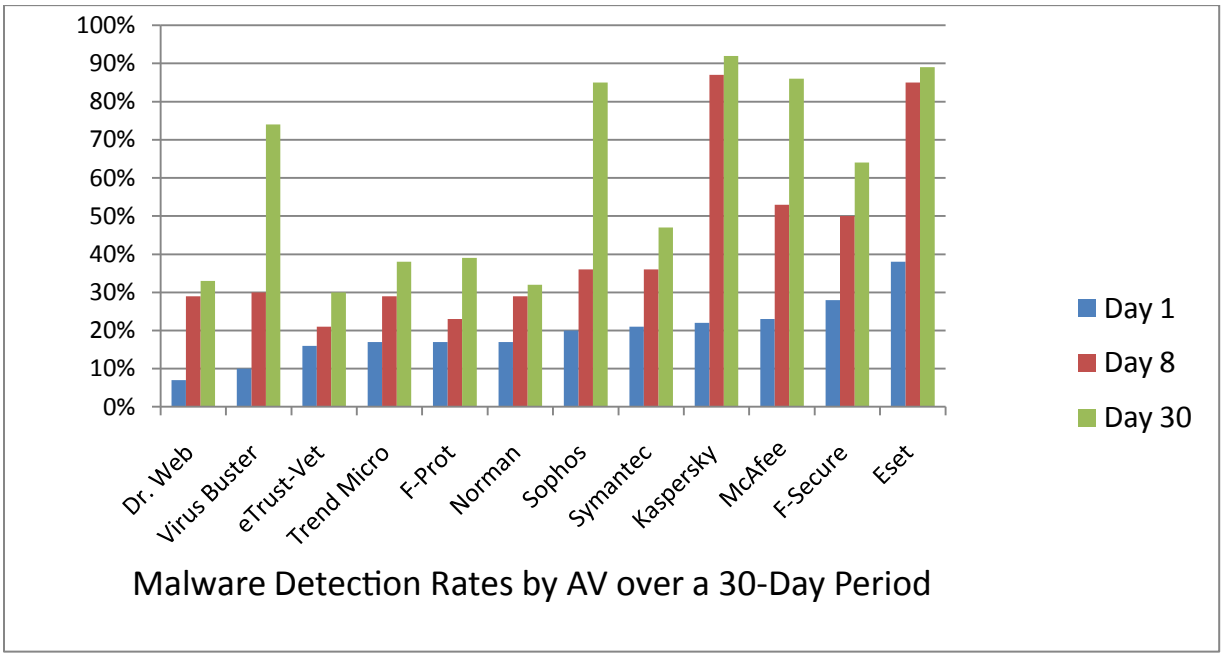
Why Current Products Fail Against Botnets

As the previous section demonstrated, current products efforts to hamstring botnets are less than effective. While some vectors for attack are limited, cybercriminals are still able to gain control of internal networks through the firewall.

An analysis by NSS Labs shows that the chance of infecting a machine by standard web malware is 10-45%, but this increases to 25-97% by an active exploit such as a botnet. This implies a near-certainty that your network will be breached by a botnet.[4]

The main reason for this is the poor (and worsening) detection rates of anti-virus (AV) software—the engine of everyone's information security. An analysis from August 2010[5] showed that:

1) The initial detection rate of confirmed active malware by leading AV products ranges from a low of 7% to a high of 37%.
2) Over time, detection rates improve but the top rate achieved is still only 90%, with many topping out in the 30-50% range.



No anti-virus software will provide complete protection against malware and zero-day attacks have greater than 50% chances of success. Is this an acceptable risk to your company?

[4] *Consumer Anti-Malware Products: Group Test Report* Q3 2010, NSS Labs.
https://www.nsslabs.com/reports/consumer-anti-malware-products-group-test-report-edition-1

[5] Malware Detection Rates for Leading AV Solutions Cyveillance, August 2010

ThreatSTOP can provide corroborating evidence. All of our customers initially claim they have a full security suite including: AV, and/or IDPS which should take care of the malware problem, but as soon as ThreatSTOP is installed; virtually all find maleware-infected hosts inside their network.

Why are botnets and criminal malware so hard to beat?
The answer comes down to two reasons:

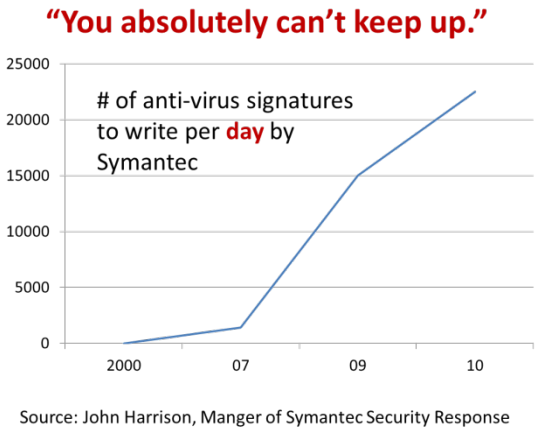
1) Application-based Attacks

The explosion of web applications has led to an explosion of application-based exploits. A recent survey showed that application-based attacks have become 35% of all network attacks. The reason is simple: there is an infinite combination of vulnerabilities that malware perpetrators can exploit. Any application can be a conduit for an exploit—PDF, YouTube, Skype, Facebook. The ever-blurring line between a business and non-business application makes the security challenge ever-greater. Is Facebook a business application? For a defense contractor, this isn't likely; for a retail chain it can be a necessary part of its marketing.

2) The Signatures Approach is Broken

Basically all security products in the market today examine attack signatures, build a profile of each and place it in a database to check pieces of traffic against. This is a reactive defense that relies on brute force, and requires ever increasing resources to maintain. As the previous section shows, AV products are straining to catch active malware, leaving organizations that use them on the defensive and vulnerable to attacks. The combination of application-based attacks and the pure numbers keep the signature approach on the ropes.

The following chart from Symantec shows the problem. It had to write between 20,000 - 25,000 anti-virus signatures each day in 2010. This was up from just 1,400 in 2007[6]. That, is a lot of over-caffinated programmers.



Source: John Harrison, Manger of Symantec Security Response

"We need a totally new approach."
-John Harrison, Manager of Symantec Security Response

[6] John Harrison, Manager of Symantec Security Response

How does ThreatSTOP's service work?

ThreatSTOP's service collects, investigates, and determines the nature of a DNS entry, and it's affiliated IP addresses. This allows network administrators to set a policy to allow or block communication to and from these groups. In contrast to the current dominant approach, which tried to track the signature of each and every attack, ThreatSTOP tracks where the attack is coming from. This approach works due to Internet communications relying on IP addresses. Instead of trying to chase down each attack signature, something that isn't known until the attack happens, ThreatSTOP's service keeps a log hostile servers. While there are four billion total addresses today (IPV4, still the dominant addressing scheme on the Internet), there is a much smaller number of addresses suspicious addresses with bad reputations that warrant tracking. In ThreatSTOP's case, we maintain a database of over 25 million IP addresses. From that, we provide a real-time block list of about 30,000 IP addresses and networks that we believe with high confidence are groups that you don't want to communicate.

Attack signatures and ThreatSTOP's service are not mutually exclusive. Neither alone will catch all of the Internet's hostiles. But used together, they form a cohesive defense against botnets and criminal malware.

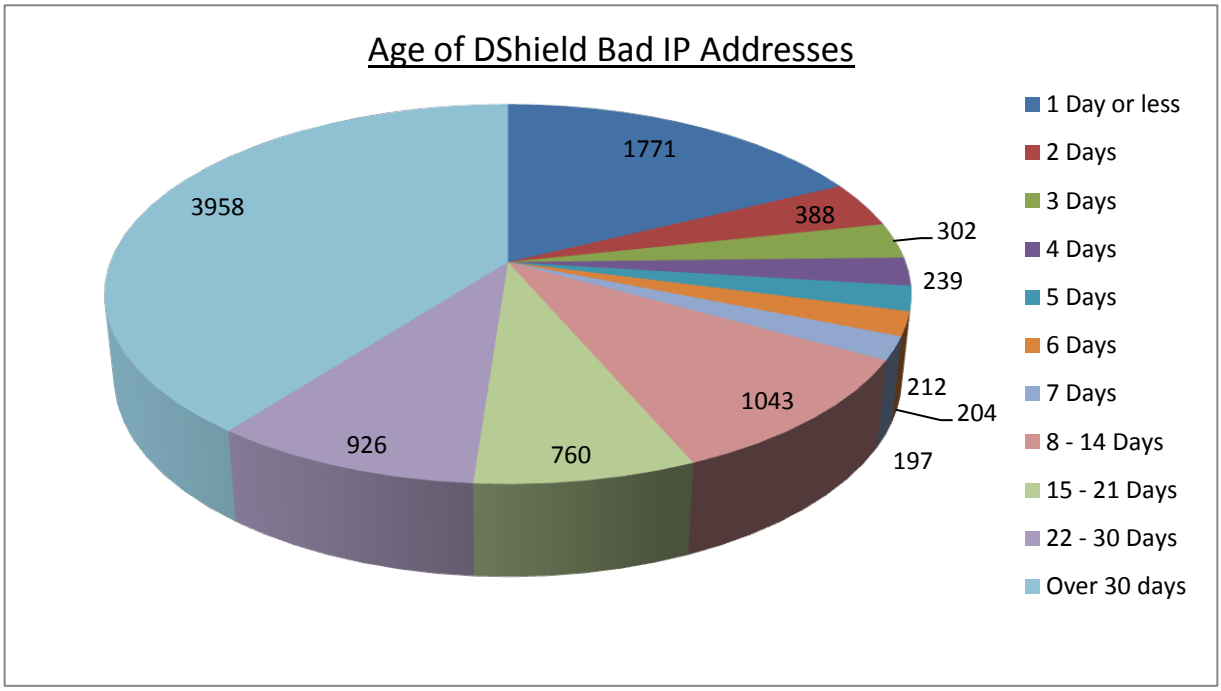
There are two requirements to have a service like ThreatSTOP's: coverage and accuracy of the database, and the timeliness of updates.

Coverage and Accuracy

The need for exhaustive coverage of bad actors is self-explanatory. More important is the need to evaluate the reputation and methods of the feed sources used to generate the list. There are many feed sources available; some are focused on specific types of malware (for example, botnets, phishing sites, or spam), while others focus on criminal gangs (like the Russian Business Network), or geography (Nigeria, for instance), or some other quality. There are overlaps in coverage between lists, and knowing which sources to use, how they interact, and their accuracy, are more important than the sheer number of sensors used. Since accuracy—that is low false positives and negatives—is of paramount importance, the back end engine used to reduce duplication, correlate, clean up, and then prioritize addresses and threats is critical. This is what ThreatSTOP specializes in doing.

Timely Updates

Timely updates are critical since the criminals rapidly change the source of their attacks. ThreatSTOP's research indicates that 15-20% of malware sources change daily, and roughly a third change in a week or less.[7]



Because the data changes so frequently, the value of systems like ThreatSTOP is greatly increased if it is updated multiple times per day.

This requires a reliable automated update method that will scale with your network. ThreatSTOP provides the only real-time service of this nature that meets all of these criteria.

[7] Age of Bad IP Addresses in DShield 10,000 List, February 11, 2011.

The Benefits of ThreatSTOP

Technology

1) Botnet "calls home" to Command and Control Blocked

Firewalls using ThreatSTOP block all traffic to and from all hostile sources on its threat list that are known perpetrators of botnet and criminal malware. However, the biggest benefit it delivers—and the biggest problem it solves—is the outbound "call home" problem. Botnets need to communicate with their command and control (C&C) hosts, which lie outside of your network. If they can make contact they can be made to exfiltrate data.

2) Prevent zero-day attacks

Because ThreatSTOP does not depend on attack signatures, it can detect a new attack from an IP address much faster, and offer better protection against zero-day attacks. The reason is that the signature approach requires a lengthy analysis, patch and signature development, update and patch process to mitigate against the latest attack. From discovery of a new attack, to an alert, to updating signatures, to writing a patch, to having the IT staff implement it may take days, weeks or even months. This is way too slow for the Internet's fluid environment. In sharp contrast, once ThreatSTOP detects and confirms that a new threat (either a brand new hostile, or one that's been dormant and is now re-activated) has appeared, it will be sent to your firewall at the next update cycle. This immediately protects your network from inbound and outbound attacks.

3) Improve Network Performance and Reduce Bandwidth Utilization

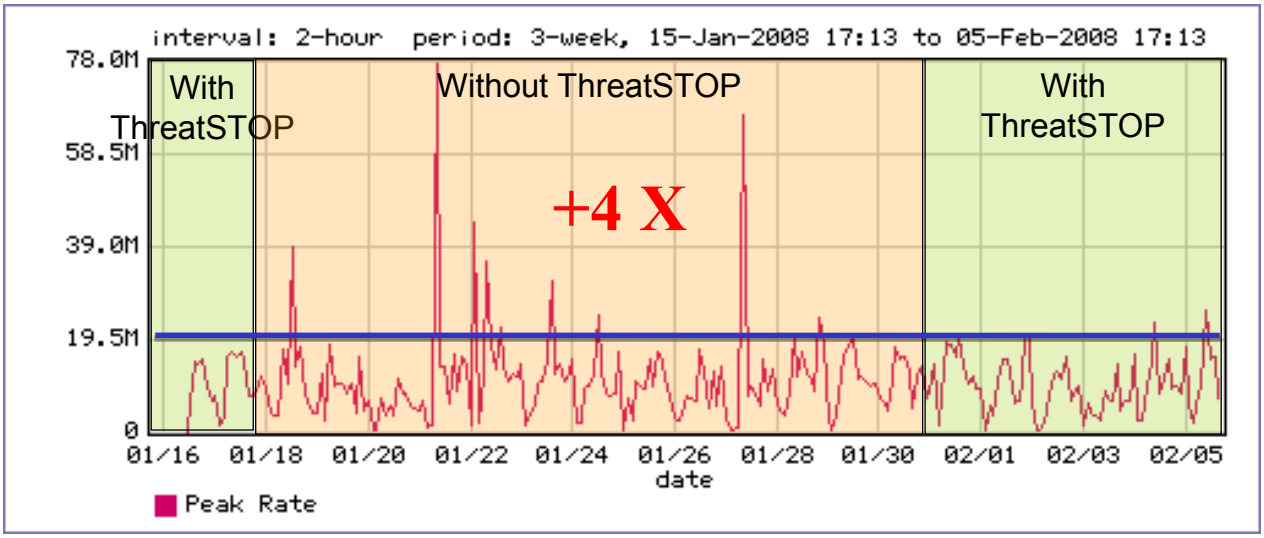
Due to the much simpler and more efficient way a firewall using ThreatSTOP filters bad traffic compared to the current approach of deep packet inspection, the load on network servers and security infrastructure is reduced, allowing for network bandwidth to be used more efficiently.

To understand this, you need to examine the difference between filtering by matching the first part of a packet for every connection versus the content which comes in packets received after the second packet in most connections.

For every incoming packet, a firewall using ThreatSTOP only looks at the source, for inbound traffic, and the destination for outbound traffic. This only requires 64 bytes to do. If an address is on the block list, it's rejected; if not, it's allowed through. Compare this to other security devices which use 800 - 4,000 bytes, and in almost all cases, at least three packets, to inspect the content of each message before determining whether to accept or deny access. The result: using ThreatSTOP requires less than 10% of the data deep packet inspection requires to reach a decision. Given that a meaningful amount of network traffic is junk (spam, bot recons, worms and other garbage), this efficiency advantage cascades

throughout the network and adds up to an average of 10-25% savings in capacity needed. This translates to savings in operational and capital costs for every ThreatSTOP user.

The following graph shows SMTP traffic to a 55,000-student community college. Their email system (without ThreatSTOP) experienced traffic spikes up to four times the baseline, which completely filled their 100 Mbps pipe and swamped the servers, resulting in denial of service. With ThreatSTOP turned on, traffic went back to a steady-state at a much more reasonable 19.5 Mbps.

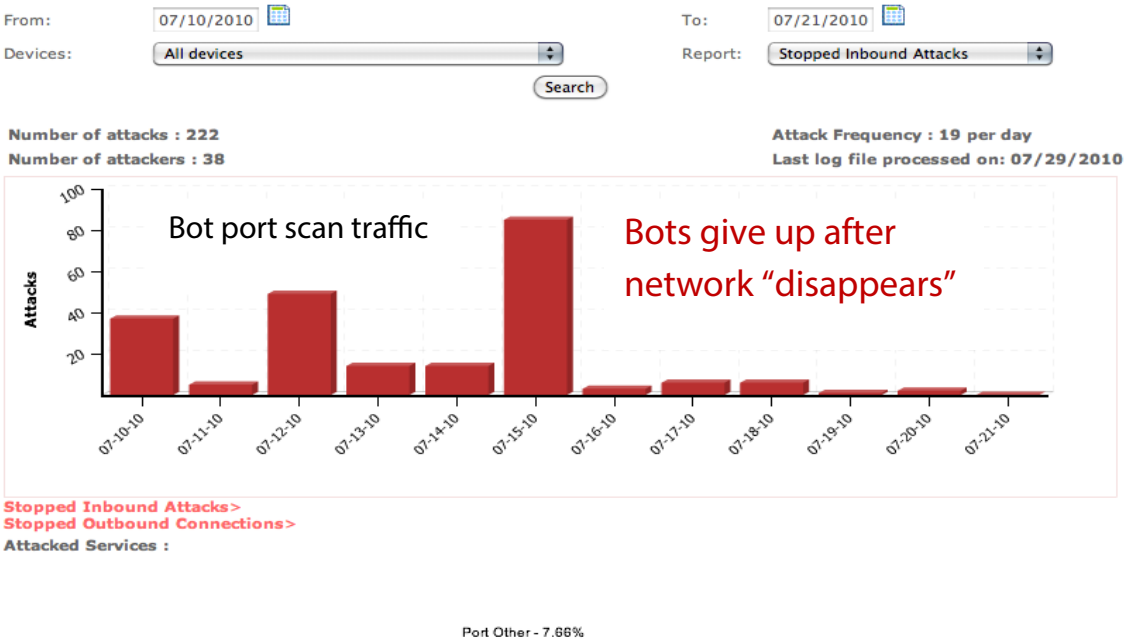


4) "Make Your Network Disappear," Reduce Spam and the Risk of Attack

When a firewall using ThreatSTOP sees an incoming packet from a bad IP address, it rejects it immediately. It doesn't even acknowledge the first SYN packet. This has the effect of telling the sender absolutely nothing. After a few tries, the attacker effectively sees a "black hole" where your network was, and they will move on to try their luck elsewhere.

The problem with many current solutions, such as DNSBL based spam filtering and web application firewalls, is that they must first allow a connection that they will later reject. This effectively lets the attacker know that there is a server available. When they reject suspicious traffic, they send an acknowledgment back to the sender, effectively a "go away", that not only confirms that your servers are there, but provides the reason for the rejection. This tells the attacker which system has "made" them, and allows them to adapt their methodology until they can compromise your network. By contrast, a ThreatSTOP user sees none of this brute forcing, because it has become invisible to the "recon" bot, and the botnet looks for easier targets.

As a result of this benefit, some ThreatSTOP customers have seen a 75% reduction in the amount of spam and virus traffic in their network, which further reduces network and server overhead. ThreatSTOP reduces the risk of attack by inviting fewer attacks in the first place when your network is invisible to attackers.



As a result of this benefit, some ThreatSTOP customers have seen a 75% reduction in the amount of spam and virus traffic in their network, which further reduces network and server overhead. ThreatSTOP reduces the risk of attack by inviting fewer attacks in the first place when your network is invisible to attackers.

5) Improve IT/Security Productivity Through Automation

ThreatSTOP solves one of the biggest challenges to an effective firewall deployment: how to update the lists and get it to the device and people whom need it? Without continuous updates or an automated method to distribute them, the service will not be effective, and may even result in denial of service, by blocking IP addresses that are no longer malicious. ThreatSTOP solved this problem through its patented distribution method via DNS. This relieves the tedious and inefficient need to manually update the lists, make sure they are properly correlated, deduped so there are no false positives, write scripts or code for specific devices to enforce them etc. Instead, IT admins and security professionals can spend their time doing higher-value work.

Business

1) Prevent Data Theft and Ensure Compliance

The most important job for ThreatSTOP is to stop the theft of your valuable data, be it customer credit card numbers, your customer list or employee data, or your intellectual property. ThreatSTOP accomplishes that by blocking traffic to and from your network and known “bad” actors with a very low false-positive rate. Since our default mode is to block the suspected traffic first, and provide you with log data to enable remediation of the breached machines, each failed attempt to breach is not a reportable event under the various compliance regimes. This is in contract with most other products which just alert you to suspected traffic. This is of course better than nothing, but by then the breach has already occurred and the whole incident response process, with its attendant costs and risks of legal action and lost reputation has to unfold.

2) Simple to Deploy, Low Total Cost of Ownership

ThreatSTOP has extremely low cost of ownership since it is implemented in the firewall natively or via a simple script that can be setup within an hour. There is no need to buy another piece of equipment or replace your existing firewall, and therefore none of the labor, time and expense of network reconfiguration, testing and certification, and employee training.

3) Lower Network Equipment Costs

By significantly reducing unwanted traffic and the resources needed to process it, ThreatSTOP not only improves network performance but also the need for new capacity to process the junk traffic. That can add up to hundreds of thousands of dollars a year.

Summary

Botnets are serious security problems that post a big challenge to existing security solutions, which were designed to counter the malware of the first 20 years on the Internet. The new crop of criminal malware is more malicious and more sophisticated than ever, and the dominant security approached today—deep packet inspection and signatures—have proven to be ineffective at dealing with them.

ThreatSTOP's techniques have been used by advanced security professionals in large enterprises and government agencies to combat this class of malware for several years. It has not been feasible for the wider market, until now. This is because there was no simple way to implement it using a universally compatible, automated distribution mechanism. Without a mechanism to ensure timely delivery of information, data cannot be acted on before its value expires.

ThreatSTOP has solved this with its patent-pending distribution mechanism that can be simply implemented on existing equipment. It does so by using a protocol that is universally available—DNS—and a very cost effective web based turnkey service, complete with reporting and analysis. As a result, the ThreatSTOP service should be a standard part of any organization's layered defense against criminal malware.

"You delayed my need to upgrade my email servers by 2.5 years. That's $200,000 a year we put in the classroom instead."

- Steve Gorham, CIO
Hillsborough Community College
Tampa, FL

www.threatstop.com
sales@threatstop.com
US: 760-542-1550

ThreatSTOP™