Defending Your Network in the Age of Botnets and Criminal Malware
Defending Your Network in the Age of Botnets and Criminal Malware

White Paper

The Botnet Problem 3

An Expensive Problem 3

Why Current Products Fail Against Botnets 4

Botnets and Criminal Hardware are Hard to Defeat 5

EdgeWave Solutions Mitigate Botnets 7

iPrism Web Security 7

The Botnet Index 8

EdgeWave Email Security Botnet Defense 8

EdgeWave Secure Content Management Solutions

EdgeWave™ develops and markets innovative Secure Content Management (SCM) solutions including iPrism Web Security and the ePrism Email Security Suite with next-generation solutions for Email Filtering, Continuity, Data Loss Protection, Encryption and Archive. EdgeWave innovative technologies deliver comprehensive protection with unrivalled ease of deployment and the lowest TCO on the market. The company’s award winning solutions can be delivered as hosted, on-premises, and hybrid services.
The Botnet Problem

Botnets are networks of compromised computers controlled by criminal third parties. They are different from Spam, Phishing and Viruses (“Spamware”) that current solutions address in three respects:

1. Botnets are usually controlled by organized criminal syndicates or state actors with a malicious purpose, as compared to individual or small groups of hackers engaging in pranks, on-line graffiti, or spam marketing. Botnets are formed from bots, autonomous applications created by cybercriminals for financial gain. The criminals form vast networks of these applications that can infect organizations and do massive damage before they are detected.

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. The bots that form botnets are very stealthy and can lurk deep inside your network for weeks or months. They remain inactive until they communicate with their command and control hosts (C & C hosts) outside your network to receive instructions. Once the bot reports “I am here waiting for instructions”, they begin to receive commands. They may be told to “replicate themselves” or to “infect other machines in the network”. They can also receive instructions such as “steal credit card numbers from your customer database”. By contrast, most spamware is acted on by the user, not through the control of a remote party, although bots are also sent via email.

3. Botnets are designed to steal your most valuable data, be it customer credit card numbers, your personnel data, or your engineering designs. Unlike these dangerous bot applications, the spamware we are used to seeing is primarily designed to get attention. While annoying, its main offense is to waste your time and slow down your machine. Botnets are a far more dangerous risk.

Pervasive Reach

Botnets are rapidly growing globally. Cisco's Q4 2010 Global Threat Report showed that global malware encounters grew by 139% in 2010. In sharp contrast, spam dropped dramatically from 375 billion pieces per month to 95 billion per month from January to December 2010.

In a survey 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%

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

- 20,000 cc accounts
- 97,200 student records
- 200,000 accounts

- 130 million cc accounts
- 114,000 e-mail addresses
- 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, but there can also be significant damage done to an organization’s brand reputation from public exposure and being forced to pay fines 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.
This was the case when hackers launched an attack on Sony PlayStation in April, 2011. Sony was forced to shut down their gaming network after personal accounts for more than 100 million customers were compromised. Just days later, hackers broke into Sony Pictures’ websites and walked off with personal information belonging to over a million customers. Sony has said these exploits were carried out by sophisticated criminals who carefully planned the attacks. The cost of these breaches have been estimated as high as $1 billion.

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 $750,000-31,000,000:

It’s important to note that the problems posed by criminal malware, such as botnets, are not solely confined to larger enterprise organizations. In fact, small to mid-size organizations can be even more vulnerable since they may lack the resources required to defend against these sophisticated, ever-changing threats.

Summary

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

1. The cybercriminals continually launch more sophisticated, attacks, overwhelming your defenses, and
2. The Internet provides an easy and ubiquitous conduit to more organizations and their data troves.

Why Current Products Fail Against Botnets – AV is Not Enough

Current products’ ineffectiveness against botnets is well documented. An analysis by NSS Labs shows that the chance of infecting a machine by standard web malware is 10%-45%, but 25%-97% by an active exploit such as a botnet. This implies a near-certainty that your network will be breached by a botnet.

The main reason for this is the poor (and worsening) detection rates of antivirus software—the workhorse of everyone’s information security. An analysis from August 2010 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. As time goes on, detection rates improve but the top rate achieved is still only 90%, with many topping out in the 30-50% range.
In summary: No anti-virus software will provide complete protection against malware and a zero-day attack has a greater than 50% chance of success. You must ask yourself if this is an acceptable risk to you.

So, why are botnets and criminal malware so hard to beat?

There are two major factors:

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 constitute 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 even greater. Is Facebook a business application? For a defense contractor, most likely not; but for a retail chain, it can be an integral part of its marketing campaigns.

Signatures Approach is Broken

Basically all security products in the market today use some sort of signature approach, in which each attack signature is profiled and kept in a database so that a piece of traffic can be checked against it. By definition this is a reactive approach that requires ever more people and time to stay current with threats. But as the previous section shows, AV products are straining to catch up with active malware, leaving organizations that use them vulnerable to attacks. The combination of application-based attacks plus sheer volume threatens to bring the current signature approach to its knees.

The following chart from Symantec shows the problem. It had to write between 20,000-25,000 anti-virus signatures each day in 2010, up from 1,400 just 4 years ago. This approach just doesn’t scale.

Harrison concludes, correctly, that “we need a totally new approach”. That approach is IP reputation.
Defending Your Network in the Age of Botnets and Criminal Malware

What is IP Reputation?

IP reputation is profiling of IP addresses to determine whether they are “good or bad”. It enables network administrators to set a policy to allow or block communication to and from these addresses. In contrast to the current dominant approach, which tries to track the signature of each and every attack, IP reputation tracks who is doing the attacking. This approach works because Internet communications start and end with an IP address. Instead of trying to chase after each attack signature, which by definition is unknown beforehand, IP Reputation profiles the history of a known item—the address. While there are 4 billion total addresses today (under IPv4), there is a much smaller number of suspicious addresses which have a bad reputation and warrant tracking. iPrism access databases with over 25 million IP addresses. From that database, they extract a real-time block list of about 30,000 IP addresses and networks that are suspect and ones you want to block.

There are two requirements to have an effective IP reputation service: coverage and accuracy of the database, and the timeliness of updates.

Coverage and Accuracy

The need for comprehensive coverage of bad IP addresses is self-explanatory. More importantly, one needs 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 types of malware (botnets, phishing sites, spam etc.), criminal gangs (Russian Business Network), geography or some other aspect. There are overlaps in coverage between lists. Knowing which sources to use, how they interact with each other and their quality, are more important than the sheer number of sensors used. Since accuracy is of paramount importance (low false positives and negatives), the technology used to extract those addresses that pose a threat is critical.

Timely Updates

Timely updates are essential since the criminals rapidly change the IP addresses they use to do their work. Threat research indicates that 15%-20% of malware addresses change every day and around a third change in a week or less. Because the data changes so frequently the value of an IP Reputation system is greatly increased if it is updated many times a day.
EdgeWave Solutions Mitigate Botnet Threats

iPrism Web Security uses its unique botnet technology to provide exclusive outbound botnet defense that protects corporate data from the risks of these criminal malware attacks. EdgeWave also has the ePrism Email Security solution that adds another layer of protection by filtering messaging traffic to and from your network and blocking known “bad” IP addresses. These technologies, discussed below, result in higher accuracy and lower false-positive rates and offer the lowest TCO on the market. This multi-layered approach to mitigating botnet threats can help you maintain network uptime, achieve regulatory compliance and protect your bottom line.

iPrism Web Security Employs Exclusive Outbound Botnet Defense

iPrism leverages its exclusive botnet blocking data, which is automatically downloaded to your iPrism, to block criminal malware (botnets, Trojans, worms etc.). This defense protects your network by blocking bots from connecting with their command and control contacts outside your network. This avoids the expense, complexity and time you might spend deploying an additional appliance or software solution. Once you deploy your iPrism solution and enable botnet protection, it begins to block any bots from being activated, rendering them harmless.

iPrism Botnet Technology

Threat Feeds

iPrism aggregates feeds from leading malware monitors and other proprietary sources to get the extensive list of botnet threats available.

An example of the sources we use includes:
- DShield
- SRI
- ShadowServer
- AutoShun
- Cyber-TA
- PhishTank
- SpamHaus
- Abuse.ch
- Emerging Threats

Correlation Engine

We then filter the raw feeds to produce a predictive threat inventory by evaluating factors such as:
- dates an IP address is first and last seen in their database
- frequency of appearances
- how many sources have reported it

These algorithms are weighted for low false-positives. An address that appears in multiple reports from different sources is more likely to be added than one from the same source multiple times. Likewise, an address which has been on their list before is more likely to be added than one that appears for the first time. Finally they check to make sure that the address is not on a global whitelist of major Internet sites, and if it is, it will be removed. This is done because cybercriminals frequently seek to poison IP reputation services by spoofing the address of someone else and because the major sites are very active in removing malware on their servers and taking over the domains used by bot herders.

IP addresses, or rather the computers they represent, are also continually being remediated when problems are discovered. This is why an IP Reputation service must promptly remove addresses that are no longer a problem. Their algorithms are careful to ensure that our feeds actively prune addresses that are no longer active.

The total resultant threat inventory currently has approximately 30,000 entries (22,000 IP addresses plus 8,000 /24 subnets) split into a number of categories, and is updated every 15 minutes.

iPrism Blocks Outbound Botnet Attempts

Using the continuously updated botnet database, iPrism monitors and blocks bots from connecting back to the known malicious botnet hosts detected. iPrism blocks any attempt at an outbound connection, over any port, with no known false-positives. Using the botnet technology iPrism is able to inspect and enforce communication attempts over any network port on a per user and/or network-based policy per user and/or network-based policy.

To activate the botnet blocking feature, iPrism customers simply select the botnet check box. They can
also set email alerts to be generated when a block occurs. Any IP addresses detected will show up in iPrism reporting. Enforcement requires no manual rule or signature updates because iPrism pulls the botnet database as soon as it is updated.

Benefits of the iPrism with Exclusive Botnet Defense

• **“Call Homes” to Botnets Blocked**
  iPrism blocks bots that are in up to 97% of networks from calling home. Botnets need to communicate with their command and control hosts (C & C hosts) outside your network in order to carry out their mission. Once they succeed in connecting to those hosts, data leakage or compromise is near certain. The “call home” message typically looks, at first glance, like a legitimate web page request and may use standard SSL encryption that firewalls and other security devices can neither inspect nor block. Hence the cyber-criminals exploit what is essentially a huge hole in most firewalls. iPrism plugs these holes because it doesn’t inspect the content of the traffic, but rather the destination IP of the outbound traffic. Any attempted connection to an IP address on its threat list will be blocked, regardless of the protocol, application or content.

• **Prevent Zero Day Attacks**
  Because iPrism botnet technology does not depend on attack signatures, it can detect a new attack from an IP address much faster and thus better protect you 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 and often months, which is way too slow. In sharp contrast, once iPrism’s botnet defense detects and confirms that a new IP (either a brand new bad IP or more typically a dormant IP that’s been activated) is acting badly and warrants blocking, it will be sent to your iPrism at the next update cycle and any outbound connection will be blocked.

  This technology provides multi-layered protection because Criminals regularly reuse IP addresses for different attacks – indeed many bot herders rent their botnets out to other crooks for new attacks – so an address that appeared on the list last week as a C&C host may be a malware dropper this week and a spammer next week. With iPrism, once the address is blocked you are protected even if criminal hackers try to use it again.

• **Improve IT/Security Productivity Through Automation**
  iPrism botnet technology solves one of the biggest challenges to an effective IP Reputation service: how to update the list and get it to the device and people who 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. However, because iPrism leverages continuously updated lists automatically, administrators are relieved of 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, etc. IT staffs are able to free their resources to work on more high value projects.

EdgeWave Email Security Botnet Defense

Spam Botnet is a Serious Threat

Botnet Spam is a common way for this threat to proliferate. Often one wrong click in a spam message can release a botnet infection into your network. Botnet spam can also be used to secretly hijack your email account for use in a network of “bot” or “zombie” computers that sends out mass quantities of spam. The newest trend is for these botnets to send “Hit and Run” targeted email-based campaigns. Theses campaigns are sent out in short “bursts,” that last an hour “or less” and are gone before the last generation of detection systems can update their real-time blacklists (RBLs) or content filtering systems.

According to the MessageLabs Intelligence 2010 Annual Security Report, an average of 88.2 percent of all spam originated from botnets last year. One botnet in particular, called Rustock, was solely responsible for 47.5 percent of all spam, cranking out an average of 44.1 billion spam emails per day over the course of the year. Though it’s easy to assume that these attacks are originating in Asia, Europe and Africa, the United States is the primary source of infection for the estimated 1.1 to 1.7 million computers acting as Rustock zombies.

While many people may consider spam more of an annoyance than a threat, computer infections originating from botnets are pervasive and serious. They can damage your business’s finances and reputation and cause legal troubles that can result in huge judgments against your company.
Defending Your Network in the Age of Botnets and Criminal Malware

EdgeWave Email Security Mitigates Inbound Botnet Threats

EdgeWave Email Security includes the Threat Defense Shield compromised of BotHunter, Spam Trigger, and Phish-Scam Filter all working simultaneously to immediately stop inbound threats to your email stream as they occur. Our Zero-Minute-Defense is a multi-layered approach to security that ensures the latest threats are persistently being stopped.

The Session Defense Shield incorporates real-time, session-level defenses against bot-based threats by employing a system that is automatic, adaptive and behaviorally-based. This defense is continually implemented in real-time and is not reliant on receiving updates from any centralized system or 3rd-party. EdgeWave's highly accurate technology is able to adapt its protection starting with temporary connection-level defenses operating in the 1 millisecond range to a 100 millisecond time scale. Next, there are greylisting responses for both DHA & DDoS protection that operate in the 100 millisecond to 30 second time scale. This transitions to more continuous blacklisting of source IP addresses that are known to be part of a Bot Network. EdgeWave's connection-level & session-level defenses are responsible for eliminating from 30% to 40% of the total SMTP sessions that are destined for your network. This conserves bandwidth, keeps mailboxes uncluttered, and because they are behaviorally based and key off the Botnets' known sending characteristics, virtually eliminates false-positives. The result is more efficiency and faster delivery of legitimate business-critical email.

Legacy Approaches are Too Slow

The EdgeWave Email Security approach greatly exceeds the performance of traditional message security defenses, which operate on time cycles that are too slow to stop the latest generation of zero-hour attacks. These legacy technologies operate reactively with update frequencies that allow threats to pass before an update can be made. And core filtering technologies for most current message security products rely on statistical analysis or scoring of message content probabilities. The issue with solutions leveraging such scoring processes is that such statistical analysis can be “gamed” to trigger blocking of valid messages, while allowing the most harmful messages through. It also requires constant adjustments to levels of aggressiveness and exemptions that only come after an event has happened.
Defending Your Network in the Age of Botnets and Criminal Malware

White Paper

EdgWave Email Security features Zombie Harvester Outbound Protection

Our email security solutions protect your outbound traffic by identifying computers that have been surreptitiously converted to a “zombie” or botnet clients. Many spammers use viruses, trojans, fake software downloads, and other tactics to create a network of infected client computers that are then used for sending out spam without the user’s knowledge. These zombies can result in your network being black-listed by other spam filters, preventing legitimate email sent by anyone on your network from reaching its intended recipient. EdgeWave managed email security appliances will block outbound spam and malicious email and then notify your network administrator so that any zombie computers can be identified and treated for the underlying infection.

Benefits of iPrism EdgeWave Email Security Botnet Defense

- **Zero-Minute Defense**
  EdgeWave Email Security’s Zero-Minute-Defense is also based on real-time knowledge that protects your inbound email with the same time-sensitive approach employed by iPrism botnet defense. Intelligence is gathered from a worldwide sensor network and this information is used to create new detection and protection rules, which are then sent out as updates on a continuous basis. This speed of rule execution allows the number of rules and the breadth of rules to effectively address the speed at which botnet creators try new attacks. This allows EdgeWave Email Security to block botnet spam at the perimeter before new bots can enter your network.

- **Both In-bound and Outbound Botnet Protection**
  While Zero-Minute defense is protecting your inbound email, EdgeWave Email Security is protecting your outbound traffic by identifying suspicious outbound addresses. This protects any of your computers from being converted to botnet clients.

- **Improve Network Performance and Reduce Bandwidth Utilization**
  By blocking botnet and other spam at the perimeter, EdgeWave Email Security greatly reduces the amount of mail your server needs to handle. Blocking spam assures security, reduces bandwidth use and de-clutters organization mailboxes.