The First 15 Minutes

Critical Technical Considerations for Defending Enterprise Networks Against the Next Wave of Internet Threats

An Intrusion Prevention White Paper from ForeScout Technologies
Table of Contents

Executive Summary 3 & 4

Evolving Internet Threats: Fast and Furious 4 & 5

The First 15 Minutes: Why Conventional Defenses Aren’t Enough 5 – 8

How to Survive the First 15 Minutes Without Really Trying 8 – 10

ForeScout Technologies’ ActiveScout Intrusion Prevention Solution 10 – 12

About ForeScout Technologies 12
Executive Summary

“Know thy enemy,” declares the old adage. And IT security professionals have done just that. We track hacker exploits and document malicious code. We have built systems for alerting each other to new threats as they emerge. And we have instituted processes for quickly responding to those new threats with the requisite patches and fixes.

But there is one thing we know about our cyber enemies above everything else. They are infinitely creative. They never run out of new ways to attack our critical infrastructure. In fact, attackers have probably demonstrated more creativity in their development of new styles of attack than we have in developing new styles of defense. And therein lies the problem for security professionals.

This means our defenses are almost entirely based on knowledge of specific attack techniques. So, while we may be fully protected against known exploits, we are largely defenseless against unknown ones.

This is no longer a tenable situation. There are three primary reasons why corporate security managers must develop effective strategies for protecting their organizations against attackers – especially when those attackers employ unknown/undocumented exploits:

1. **Internet threats can now attack massive numbers of hosts in a very short period of time – aggressively proliferating before they can be documented and remedied.** Code Red and Nimda are just the beginning. Future attacks will be capable of inflicting damage on a global scale in less than an hour. By the time such threats become known and understood by the security community, most organizations will already be hit.

2. **The time between the recognition of a new threat and actual deployment of an effective fix creates an additional period of unacceptable vulnerability.** It’s one thing to find out about a threat. It’s another thing to deploy countermeasures across a complex network. Such deployments take time – leaving companies totally vulnerable while malicious activity is at its peak.

3. **Targeted and/or stealthy attacks don’t expose themselves to the security community at large and are therefore not addressed by conventional discover-and-fix processes.** New attacks typically come to light because of institutional observation or because they are launched in a scattershot fashion against large numbers of hosts. Truly malicious attackers specifically targeting your company won’t expose themselves or their techniques. So you can’t depend on the security community or your infosec vendors for a heads up or a preventive patch. These unknown attacks pose a grave threat to any company and require an effective defense.
Fortunately, now it is relatively easy to protect networks against unknown attacks. With ForeScout’s unique intrusion prevention technology, ActiveScout, such attacks can be detected and neutralized before they impact the network. This can be accomplished with minimal administrative overhead. Corporate security professionals can thus significantly reduce their companies’ exposure to risk – while incurring only minimal expenses or workloads.

**Evolving Internet Threats: Fast and Furious**

The scenario has become more and more familiar to IT managers of all sorts. News of the latest attack spreads like wildfire – but unfortunately not quite as fast as the attack itself. Everyone scrambles to see if they’re hit and to find out what to do next. In some cases, after hours of frenetic activity during which nothing else gets done, the enterprise seems to be effectively secured. For others, a breach is discovered – but early enough to at least minimize the damage. But for those who don’t move quite fast enough, or who have the misfortune of being an early target, things go very badly. They become statistics in the next day’s report about the first wave of destruction.

Code Red, Nimda, Spida, Slapper. The list waits for its next name. Everyone knows it’s only a matter of time.

What many people don’t fully comprehend is just how quickly the new generation of Internet threats can propagate and generate large-scale attacks. Worm authors have begun to employ a wide variety of clever techniques to ensure that their malicious code is capable of enlisting as many other hosts as possible into the attack with astonishing immediacy. These techniques are well outlined in a recent paper by Staniford, Paxson and Weaver presented at the USENIX Security Symposium entitled “*How to Own the Internet in Your Spare Time.*” They include:

**Localized scanning**
Here, a worm focuses more of its attention on hosts within the local IP address space. Because such hosts are more likely to be configured in a manner similar to the one already infected, they are also more likely to have the same vulnerability of being exploited by the worm.

**Multi-vector propagation**
This involves using a variety of methods for spreading the worm. In the case of Nimda, these techniques included probing for a specific vulnerability in Microsoft IIS and scanning for backdoors left behind by other worms.

* View the complete paper “*How to Own the Internet in Your Spare Time*” at http://www.icir.org/vern/papers/cdc-usenix-sec02/

**Hit-list scanning**
Using this approach, the worm’s author performs a preliminary scan to create a target hit list of 10,000-50,000 potentially vulnerable hosts. When the worm successfully captures and controls its first few hosts, this list is then divided among them. In this way, a very large number of vulnerable hosts can be attacked with great speed.

**Permutation scanning**

This strategy allows multiple infected hosts to coordinate their search for other vulnerable hosts so that they don’t scan the same IP addresses. They thus work in tandem with each other to achieve extreme efficiency, enabling them to quickly scan millions of hosts for their requisite vulnerability.

**“Flash” worms**

In perhaps one of the most frightening—but realistic—scenarios presented by the paper’s authors, a hit list of all vulnerable hosts on the Internet would be propagated along with the worm itself. This list would be broken up as each successive generation of “child” worms was launched. According to the authors, while such a list would start at about 48MB (which takes about a second to travel over an OC-12 link), its size would quickly be reduced with each new layer of propagation. Based on their calculations, such an attack, launched on a high-speed connection, with a comprehensive list of all vulnerable hosts, could perform a global infection in less than thirty seconds.

The paper’s authors coin the term “Warhol worm” to describe a piece of malicious code capable of achieving global presence in 15 minutes or less. They also provide strong mathematical models to substantiate their conclusions.

While some readers may be skeptical about the authors’ more dramatic findings, no one can argue about the alarming rapidity with which each successive generation of worms has proliferated across the Internet. If the job of security managers is to expect the unexpected, then it is essential to develop a strategy for coping with the outbreak of threats that can spread across the Internet faster than a technician can read a security alert.

**The First 15 Minutes: Why Conventional Defenses Aren’t Enough**

The speed with which new, undocumented attacks can proliferate across the Internet presents a variety of problems for corporate information security managers. The consistent success that these attacks have achieved is indicative of the fact that current defense strategies are insufficient to thwart them.

This is not to say that existing security technologies serve no useful purpose. On the contrary, these technologies are essential for protecting organizations against the full range of potential threats that they face on a daily basis. And, to some extent, these security measures can also contribute to a successful defense against a new, unknown
form of attack. But, it is also clear that by themselves, they do not offer sufficient protection against worms.

The specific weaknesses of each of the legacy security solutions are as follows:

**Firewalls**
Firewalls are indispensable for preventing unauthorized users and/or malicious traffic from reaching your network. However, experience has shown that firewalls do have certain vulnerabilities. By their very nature, firewalls must allow various types of traffic in and out of the network. Once a firewall is configured to permit a specific service or traffic type, an attacker can then potentially exploit that permission to gain access to a vulnerable host. No permitted service is 100% secure. Time and again, hackers have shown that they can use even the most apparently innocuous permission to compromise the network. A properly configured firewall can make penetration extremely difficult for a skilled hacker and almost impossible for a mediocre one. But it cannot by itself guarantee the security of the network.

Of course, not every firewall is perfectly configured. So additional potential vulnerability arises not from the technology itself, but from the fact that human beings administer it. If policies are too permissive – or if errors are made in policy implementation – glaring gaps in network security can result. The purchase and installation of a firewall alone is thus no guarantee of network and systems security.

Another issue with firewalls involves the speed with which they can be configured. Even a superb firewall managed by an expert technician can be vulnerable to a new attack if the technician can’t modify the firewall appropriately before the attack hits. A new attack that is clever enough and that proliferates quickly enough can therefore defeat firewalls and their owners.

**Signature-based intrusion detection**
In order to gain another layer of protection against malicious intruders, many organizations have implemented signature-based Intrusion Detection Systems (IDS). These systems are designed to identify malicious traffic so that it can be shut down before network resources are compromised. Using a combination of protocol analysis and content monitoring techniques, these systems can detect various types of scans. Once the questionable activity is detected, the IDS can alert a technician and/or attempt to automatically block it.

Most IDSs use a signature-based approach to threat identification. The system’s developers build a set of threat profiles or signatures against which all network traffic is compared. If a series of packets matches any of the system’s signatures, it is flagged as suspicious and handled according to pre-defined policies.

It is worth noting that the signature-based approach generates a large number of false positives and requires quite a bit of ongoing maintenance. In addition, the signature must be 100% effective in its first iteration. If it is flawed in any way – a not-
unthinkable possibility considering how quickly it must be created and distributed – it will not effectively protect the network.

More significantly, however, the signature-based approach has four obvious shortcomings when it comes to protecting organizations against brand-new threats:

1. A rapidly proliferating attack will strike many potential victims before IDS vendors can create and distribute signature files to their clients.

2. Even after the new signature is created and distributed, organizations remain vulnerable until they have properly installed and configured it across all of their locations.

3. In many attacks, the signature is created some time after the original attack is launched. During this time, the new attack can morph quite rapidly into another attack that a signature may not cover.

4. In most cases, by the time a signature is triggered, the attack has already begun to do damage and/or enlist new hosts.

This last point is particularly important with rapidly proliferating threats. The new breed of Internet threats can enlist new hosts in a matter of seconds, vastly strengthening their power and – more likely than not – initiate attacks on any customer, supplier and other business partner they can easily reach.

**Anomaly-based intrusion detection**

Anomaly detection is an emerging approach to intrusion detection that attempts to overcome the problems associated with signature-based systems. Using anomaly-based detection, an organization’s network traffic patterns are “baselined,” so that any variation from that baseline can be flagged as suspicious. In theory, this eliminates the system’s dependency on pre-defined signatures – allowing it to respond effectively to new, unknown attacks.

However, there are two fundamental reasons that anomaly-based identification is not effective against new, rapidly proliferating threats. First, the nature of network baselining is problematic. In the past, network traffic patterns were reasonably consistent and predictable. Internal applications and services had knowable profiles and utilization patterns, and trends over time could be plotted with reasonable accuracy. With the advent of Internet-based services, however, this is no longer the case. If an article about your company’s Web site appears in the right magazine, traffic can spike overnight – and that’s a good thing. Internal users can also do all kinds of things that affect traffic patterns, such as mass-mailing a PowerPoint presentation to half the company. That may not be a good thing, but it isn’t a breach of security. Divergence from a baseline, that itself may be questionable, is therefore not a highly reliable indicator of an attack.
The second problem with anomaly-based detection is that it underestimates the brilliance of today’s hackers. Very dangerous worms can be very small in size and virtually impossible to distinguish from legitimate traffic. To detect these bits of malicious code in the midst of the millions of packets traversing today’s busy networks is like finding a needle in a haystack. To be more mathematically precise, it’s more like finding a needle in Nebraska. So, while anomaly detection can be very useful as part of a coordinated network defense, it is clearly very limited in its ability to help stop a well-designed attack in its tracks.

Alerts and events
One final note should be added regarding the whole notion of alerts and event notifications. While all of the technologies described above can be very effective at notifying security technicians about potentially problematic occurrences on the network, those notifications do not constitute sufficient protection against today’s fast-moving attacks. By the time a technician gets paged, sits down at a security console (or, if it’s the middle of the night, climbs out of bed and logs on to a security console from his or her home PC), and begins to take action, entire departments can be compromised and automated assaults on customer and supplier hosts can already be complete. Any system that depends on manual responses to secure the network is by definition impotent against the next generation of Internet threats.

At the same time, the plethora of non-meaningful alerts generated by these systems will ultimately drain IT productivity and dull responsiveness to real emergencies when they do occur. The human resources that organizations can throw at the problem of network security are limited. To waste those limited resources on false positives is both foolish and dangerous.

Clearly, security managers need a better solution for defending their organizations against Internet threats that continue to get faster and stealthier. Fortunately, such a solution is now available.

How to Survive the First 15 Minutes Without Really Trying

New Internet threats proliferate too quickly for conventional defenses such as firewalls and intrusion detection to be 100% effective. And they can do their damage before technical staff can take effective action against them. So how can the network protect itself from those first 15 minutes of the next major Internet attack?

Three essential principles can help provide the answer. These principles form the foundation of a defensive strategy that has been proven capable of fending off unknown threats regardless of how rapidly they proliferate or how potentially devastating their impact may be. They are:
1) **Use pre-attack scanning/reconnaissance activity to detect potential attacks, rather than waiting for the attack itself**

Authors of malicious code are exceedingly creative and clever. The new worms and attack exploits that they dream up will always defy the security community’s attempts to predict them. Any defensive strategy that requires the defender to have a good understanding of the exploit itself either before or soon after the attack is mounted is doomed to failure – because attacks can start doing damage before such reactive defenses can protect the network.

However, authors of malicious code are entirely unoriginal when it comes to performing the scanning/reconnaissance that precedes their attacks. There are, after all, only a limited number of ways to scan a network if you’re trying to discover a particular type of vulnerability: a port scan, a NetBIOS probe, SMTP-based interrogations, etc. While not all scans lead to attacks, almost all attacks are preceded by some type of scan. This means that by responding effectively to pre-attack reconnaissance, the need to recognize the specific nature of any subsequent attack can be eliminated.

This is an essential requirement for successful defense against unknown attacks. Once an unknown attack is launched against a network, it is too late to start gathering information about it. Countermeasures against such attacks must begin at the scanning/reconnaissance stage.

2) **Immediately – and, if possible, automatically – halt any and all traffic coming from a host that previously executed a potentially malicious scan**

There is no reason to examine or evaluate such traffic to figure out whether or not it is malicious. Legitimate hosts do not scan networks before accessing them. They are granted permissions and provided with services through normal administration of access, authorization, and authentication processes. So any host that bases its access attempts on information previously gleaned via reconnaissance can be assumed to be malicious.

It is also imperative with today’s fast-moving attacks to block such traffic with absolute immediacy. To wait for a technician to respond to an alert and/or look over a set of log files is to court disaster. Next-generation infosec defenses must be capable of automatically, immediately and effectively preventing malicious traffic from touching critical network resources. Conventional alert-and-respond strategies are too slow and unreliable for effective protection against next-generation threats.

3) **Integrate traffic prohibition policies across all network access locations – and potentially to other business partners and the Internet community as a whole**

The network infrastructure that security managers are charged with protecting is often broadly dispersed, with multiple connections to the Internet. So when one site is
scanned and attacked, managers must take advantage of that event to protect every other site on the network – even if those sites haven’t been scanned or attacked yet. In this manner, the entire enterprise can be “vaccinated” against any impending threat.

By the same token, it is evident that business partners must start to take action to help protect each other from these rapidly proliferating attacks. From a technical perspective, this makes sense because worms and other code take advantage of the connections between networks to accelerate their proliferation. From a business perspective, this makes sense because every company has a stake in the financial health of its customers and suppliers. There is also a social element to such mutual protection, especially in light of the federal initiatives that now enlist the private sector in the fight against cyber-crime and cyber-terrorism.

These three principles – capitalizing on pre-attack scanning, automatically and immediately prohibiting malicious scan-related traffic from communicating with your network, and integrating scan-driven flags across and potentially beyond the network – can be applied to successfully defend any organization against new attacks, even if those attacks have not yet been documented by the security community or remedied by the IT vendor community. Only by implementing such automated, scan-driven defenses can infosec managers keep their companies safe during the first 15 minutes of the next major Internet attack.

One additional point should be made about attacks that are targeted at a specific organization or organizations, rather than at every possible vulnerable host on the Internet. These attacks present a similar problem of “unknown-ness” to security managers, since the exploits that such a focused attacker uses are likely to escape the attention of the security community at large. Techniques that are effective for fending off an unknown attack are therefore equally applicable to defense against a highly focused/targeted attack.

**ForeScout Technologies’ ActiveScout Intrusion Prevention Solution**

In response to the security challenge posed by threats that proliferate faster than conventional defense mechanisms can respond, ForeScout Technologies has developed ActiveScout – a unique scan-based solution that stops attacks regardless of their form, or speed, and most importantly, regardless of whether or not they are known to the security community.

ActiveScout uses a unique three-phase process to achieve this:

**Phase 1: Receptor**
ActiveScout sits outside the firewall, continually monitoring network traffic and looking for any signs of network reconnaissance. This monitoring can be done with a very high level of sensitivity, since ActiveScout does not send alerts about the
reconnaissance it discovers to security managers. In other words, because it doesn’t generate false alarms, ActiveScout can be configured to detect even very slow and/or unknown reconnaissance activity.

Phase 2: Deceptor
When ActiveScout detects reconnaissance activity, it automatically identifies the type of reconnaissance being used by the attacker. ActiveScout then responds to the reconnaissance attempt with information similar to that which is being sought – but which is purposely counterfeit. ActiveScout’s *deceptor* data specifically mimics the resources targeted by the potential attacker’s reconnaissance – such as an IP service or a NetBIOS resource. The attacker thus views this deceptor data as valid, and will make use of it in any subsequent attack.

Phase 3: Interceptor
If and when an attack is then launched, ActiveScout can immediately identify it. Rather than depending on an attack signature, ActiveScout simply recognizes its own *deceptor* tag. In other words, ActiveScout has planted a *mark* by which it can detect and intercept traffic coming from a source that previously performed suspicious reconnaissance. At this point, ActiveScout deflects the attack from the network, alerts the security team, and can even block all traffic from the offending IP address. Every location on the network is thus fully and pro-actively protected from even the most insidious type of attack.

The attack can occur days or weeks after the reconnaissance. The attack may also come from a totally different IP address than the reconnaissance. ActiveScout’s effectiveness is unaffected by time delays or the use of a *moving source*. As long as attackers performed a scan beforehand – which they invariably do – ActiveScout will protect every site on the network.

ActiveScout’s unique approach to network security delivers several key benefits, including:

**Instantaneous defense of any rapidly proliferating unknown attack – as well as against known exploits**
No previous knowledge of the specific attack technique is required – only the occurrence of a preparatory reconnaissance activity. ActiveScout is therefore able to stop attacks even if they have yet to be addressed by the security community.

**Unrivaled protection against business disruption**
ActiveScout’s uniquely pro-active approach intercepts and neutralizes attacks before they can even reach the firewall, thus delivering maximum protection of critical assets.

**Absolute elimination of false alarms**
ActiveScout’s precise identification of attacks, ensures no irrelevant events and/or anomalies are created, so it does not drain your security team’s time and energy.
**Reduced workloads**
ActiveScout doesn’t require continual signature updates, extensive tuning or other manual administration. Plus, it neutralizes attacks automatically. No other security technology offers more protection for less work.

**About ForeScout Technologies**
ForeScout Technologies delivers automated Intrusion Prevention solutions that precisely identify and selectively block *both known and unknown* attacks. Based on patented ActiveResponse technology, the ActiveScout solution ensures zero false alarms and zero time to prevention at a minimal cost.

For more information on ForeScout Technologies, visit [www.forescout.com](http://www.forescout.com).