The Value of Early Warning Solutions
Contents

The Value of Early Warning Solutions ............................................................. 4
Threat lifecycle .............................................................................. 5
Components of an early warning solution .................................................. 6
Global data sources .......................................................................... 7
Human and automated analysis (people and technology) ......................... 9
Vulnerability analysis ........................................................................ 10
Malicious code analysis ..................................................................... 10
Threat analysis .................................................................................. 11
User access ....................................................................................... 13
Statistics ........................................................................................... 14
Analysis ............................................................................................. 14
Advanced reporting ........................................................................ 14
User administration .......................................................................... 14
Alerts ................................................................................................. 15
Security risks ...................................................................................... 16
Domain alerts ..................................................................................... 16
Timeliness and depth .......................................................................... 17
Case study: MS06-040: Microsoft® Windows® Server Service Remote Overflow Vulnerability 18
Conclusion .......................................................................................... 21
The Value of Early Warning Solutions

Among the many issues that security professionals face on a daily basis is the need to quickly gain awareness of the potential threats to their networks and systems and then prioritize those threats that could be most damaging to their environment.

Compounding this problem, security teams often do not have access to tools that can quickly provide them with information about these threats. By the time they receive the information, it might no longer be useful. Information that is stale does not provide an effective way to mitigate threats or provide awareness of the global threat landscape. What security teams really need is an early warning solution that allows them to manage threats and ensure business continuity.

Many types of intelligence are critical for delivering a global view of the threat landscape, including:

- **Data collection**—Data collection is an important building block, but having a large store of data does not make an early warning solution.

- **Technical and human analysis**—It is critical to take raw data and turn it into actionable intelligence that can be consumed by an analyst or administrator.

- **User access**—Security alerts and analysis must be easily accessible to security teams so that they can take necessary action to protect their IT assets.

A case study will illustrate why incorporating early warning solutions into the enterprise can provide better awareness of security threats, help maintain business continuity, and provide actionable information that makes IT staff more efficient and effective in their duties.

Being able to efficiently and effectively identify emerging threats in a constantly changing threat landscape provides the security team with the time to focus on the unique challenges of their own enterprise rather than on the need to gather security data and decipher its meaning. Symantec provides this kind of early warning solution through the Symantec DeepSight™ Early Warning Services by providing actionable intelligence covering the complete threat lifecycle, from the emergence of new vulnerabilities to the presence of active threats to remediation.
Threat lifecycle

To understand the value of an early warning solution, it is important to understand the threat lifecycle that exists today. There are a number of key milestones in the lifecycle, as shown in Figure 1.

It is also important to understand that not all threats include each of these milestones. In some cases, some milestones may occur concurrently or in a different sequence. It is important to note that, throughout this lifecycle, risks to networks and systems will increase and decrease, depending on the mitigation strategies, security policies, and awareness to the threat that the enterprise has in place.
Certain vulnerabilities have a greater chance of being exploited than others, and there are certain types of malicious code that will generate a greater threat to an enterprise than others. It is important to note that the time frame between when the exploit circulates on the Internet and when widespread patching occurs is when there is the most risk. Symantec DeepSight Early Warning Services can provide actionable information at every step of the threat lifecycle so that security teams are able to assess the level of risk that each vulnerability, malicious code, and threat poses to their enterprise. With this understanding of the threat lifecycle, it is important to learn more about the components that make up a successful early warning solution.

**Components of an early warning solution**

An early warning solution comprises four key areas (see Figure 2). These are:

- Global data sources
- Human analysis
- Automated analysis
- User access

Without these components, an early warning solution cannot provide the actionable information that enterprises require to assess the global threat landscape in a timely manner.
Global data sources

From an early warning perspective, security professionals and information technology (IT) staff need to be aware of the numerous vulnerabilities, malicious code, adware, and spyware that exist today, and they need to be alerted to new vulnerabilities and malicious code as they are identified. Additionally, security professionals need to be aware of emerging and actively propagating threats on the Internet.

The challenge an early warning solution provider faces is knowing what data should be collected. In response to this task of collection, Symantec developed the Symantec™ Global Intelligence Network. The Symantec Global Intelligence Network is a comprehensive collection of vendor-neutral security data sources and active global attack data that, when combined with expert research and analysis, provides an unmatched view of global threat activity.

Symantec leverages a variety of data sources:

- **BugTraq**—Through its acquisition of SecurityFocus in August 2002, Symantec maintains and moderates the BugTraq vulnerability mailing list. Symantec leverages the BugTraq mailing list, along with many other sources of vulnerability data, to collect and analyze new vulnerabilities that the security community identifies.
  
  Symantec maintains a database of over 20,000 vulnerabilities and is currently adding approximately 97 new vulnerabilities per week.

- **40,000 volunteer sensors**—Symantec collects log data from over 40,000 registered IDS and firewall systems in over 180 countries. This data is collected from all of the leading enterprise vendor applications, as well as home users. The data from these devices is anonymous, but it is tracked by industry, size of company, and country of origin. The data contribution is voluntary, and in return, Symantec provides access to Symantec DeepSight Analyzer, an online console with which participants can manage their event data that was submitted to the Symantec Global Intelligence Network.

- **500+ Managed Security Services customers**—The sensor data that Symantec gets from its 40,000 volunteers is enhanced with IDS and firewall data from Symantec’s Managed Security Services customers as well. Managed Security Services collects security log data from more than 6,200 security devices today, including data from 76 of the Fortune 500, many of the Global 2000, and government customers worldwide.

The Value of Early Warning Solutions
• **Attack Quarantine System**—Many security research organizations do not proactively capture malicious code, zero-day threats, and other exploits. The Symantec Attack Quarantine System identifies new threats by capturing them in a honeynet. Symantec analysts use this data to quickly identify new malicious code, new exploits, and botnet command and control servers. This data enables Symantec to provide deep analysis and actionable information to DeepSight users. Many instances of malicious code have been captured and analyzed that were not visible to other security organizations because of the complexity and ever-changing variants of malicious code. The honeynet is able to impersonate IP address space anywhere in the world and is configured to capture malicious activity from many different operating systems to ensure the best coverage in identifying potential threats.

• **120 million Symantec antivirus and Norton antivirus customers**—Symantec is the leader in the antivirus market space and is constantly updating its antivirus protection for its 120 million consumer and corporate antivirus technology users.

  Antivirus users can submit potential or unknown viruses to Symantec Security Response, the world’s leading Internet security research and support organization, using Symantec’s Digital Immune System and Scan and Deliver technology. Symantec currently receives over 200,000 malicious code submissions each month and provides analysis of malicious code on a 24x7 basis.

  These mechanisms provide Symantec Security Response with many new virus and worm samples. They are analyzed to provide DeepSight Early Warning Services users with information about new malicious code. This knowledge is also shared with Symantec products and provides updated protection through virus definitions, IDS signatures, and other security countermeasures.

• **30 percent of the world’s email traffic**—Leveraging two million decoy email boxes across many of the world’s Internet service providers, Symantec Brightmail™ servers monitor 30 percent of the world’s email traffic. By analyzing this vast store of email, Symantec can identify new attack vectors for cybercrime and fraud, such as new spam and phishing attempts, and provide detailed analysis of new types of phishing and fraud schemes to DeepSight Early Warning Services users.
These data collection points give Symantec many valuable vendor-neutral sources to assess security data and form it into actionable information that security professionals can use daily. While having many valuable sources of data is essential, an early warning solution must also be able to distill the data into actionable information.

**Human and automated analysis (people and technology)**

Collecting voluminous amounts of security data is a challenging undertaking. Symantec has responded to this challenge by leveraging the Symantec Global Intelligence Network. After data is collected, the next challenge an early warning solution faces is turning the data into something meaningful, to give priority and direction to its users and their organizations’ unique needs.

To convert data into actionable information, an early warning solution must be able to employ technology and personnel to create an overall security picture that can be used by an enterprise’s IT organization. The technology must be able to effectively and efficiently identify the key data points and correlate them so that new and potential threats are not missed. From a personnel perspective, a single team of analysts cannot do justice to all the data that must be examined to identify vulnerabilities, malicious code, spam, phishing, and other emerging threats. Threats can come at an organization from many different vectors. There are too many things to look for and not enough time for a single team of analysts to be experts in everything. Enterprises need to identify early warning solutions that can provide deep security knowledge and expertise so that vulnerabilities, malicious code, phishing, and other threats are identified quickly. Those solutions must also provide in-depth information to fully understand the issue.

Symantec Security Response, in support of DeepSight Early Warning Services, provides this capability by generating the actionable information and content delivered through this service. The Security Response team is a global team that provides security intelligence for Symantec products and services. Security Response works with data collected from the Symantec Global Intelligence Network to identify vulnerabilities, malicious code, and threats from all over the world and provides analysis of this data in eight Security Response Labs around the world.

Symantec Security Response analysts focus on specific disciplines. Because they are specialists, they are able to provide the best level of analysis to Symantec DeepSight Early Warning Services users.
Vulnerability analysis
Symantec Security Response staffs a dedicated team of analysts that focuses solely on vulnerability analysis. These analysts are responsible for identifying new vulnerabilities and assessing the credibility, urgency, and severity of each vulnerability, as well as identifying exploits, mitigation strategies, and patches associated with the vulnerability. The vulnerability analysis team monitors over 150 different online resources, including the BugTraq mailing list, as well as many other public and private lists to identify new vulnerabilities.

When a specific vulnerability is identified, analysts will research and test the vulnerability in their lab to assess the impact of the vulnerability. They then provide a standardized action plan detailing the affected systems, key metrics, and technical descriptions of the vulnerability to Symantec's Vulnerability Database.

Analysts work with guidelines that clearly spell out the credibility, urgency, and severity rating for vulnerabilities. These guidelines ensure a clinical view of the vulnerability being observed rather than a subjective reaction to a specific vulnerability. The goal is to have a consistent approach to ratings no matter which analyst is looking at the vulnerability.

The content of the analysis is checked for quality assurance by another analyst on the team before the vulnerability is posted to the DeepSight Vulnerability Database and sent to DeepSight Early Warning Services users.

All vulnerabilities have a standardized output that is provided to DeepSight Early Warning Services users with all the relevant information pertaining to the vulnerability. Accuracy and depth are two key considerations in assessing an early warning solution, and Symantec DeepSight Early Warning Services deliver both.

Malicious code analysis
The analysis of malicious code is made possible by a combination of both technical and human analysis. The malicious code team focuses solely on the observation, reverse-engineering, and analysis of malicious code.

The malicious code analysis that this team provides includes assessing the risk and propagation mechanisms of the malicious code, as well as attack vectors, vulnerable software, and detailed analysis of the malicious code upon execution. The analysts also provide tools and instructions on the proper disinfection of malicious code on impacted systems. The malicious code analysts, like the vulnerability analysts, enter their findings into the Symantec Security Response Content Manager to ensure that all malicious code content is captured prior to release of the information.
Malicious code analysts will receive code submissions from both the Digital Immune System and Scan and Deliver mechanisms built into Symantec’s antivirus products, as well as submissions from Symantec’s Attack Quarantine System. This submission mechanism accounted for 18 percent of the malicious code samples not previously seen on the Internet between January and June of 2006.1 A final submission method is individual customers manually submitting samples to the malicious code team for analysis.

Threat analysis
Like the vulnerability and malicious code teams, the threat analysis team is a distinct team of analysts that are responsible for identifying new and emerging threats and reporting on them via DeepSight Early Warning Services.

The threat analysis team leverages the data from the Symantec Global Intelligence Network as its primary source of information. The team also leverages other internal Security Response resources as appropriate. Hundreds of external sources, including Web sites, IRC channels, and RSS feeds, are aggregated into a single console view for the analyst on duty to view and assess. The analyst on duty works with other analysts on the threat analysis team to develop detailed analyses of specific threats as well as providing longer-term research as needed.

The analyst on duty is responsible for assessing the threat and changing Symantec’s Threat Condition (ThreatCon), as appropriate. A ThreatCon number rating makes Symantec DeepSight users aware of the relative state of the Internet threat based on research that Symantec’s threat analysis team provides.

The data collected from the Symantec Global Intelligence Network is then normalized, providing a standard method of analysis to identify trends in worm outbreaks and attack activity. Symantec DeepSight Early Warning Services uses the Symantec Key Predictors model to identify thresholds that exceed three standard deviations from the norm during worm outbreaks or widespread attacks.

The key predictors are the following:

• Number of targets seeing the attack by
  – Number of source systems originating the attack
  – Source IP count
  – New source IP count

---

• Number of source systems originating the attack by
  – Sensor count
  – Organization count
  – Anomalous sensor count
• Total number of attacks seen

It is important to note that even though technology identifies certain types of attack activity, a member of the threat analysis team will assess the validity of the activity and issue incident alerts to DeepSight subscribers as appropriate. This ensures that the information provided to DeepSight users is accurate and actionable. If a specific attack activity does not generate an alert, the activity is still noted and observed by the analyst. Depending on the metrics associated with the attack, information will still be posted to the DeepSight Early Warning Services portal for user reference.

Another key activity of the threat analysis team is to monitor the Attack Quarantine System for indications of breach. The analysts will investigate the infected host to identify where the exploit vector occurred on the system as well as which vulnerability was taken advantage of by the exploit. If the exploit is leveraging a vulnerability that has not been used before, the analysts will develop a Threat Alert to call attention to this specific threat.

The Threat Alert is an incredibly powerful tool that Symantec provides to DeepSight Early Warning Services users: It identifies attack vectors, exploits, and malicious code previously unseen elsewhere. It also provides the analysts with information that allows them to perform a deeper analysis of the specific exploit or malicious code. New malicious code that is found in the Attack Quarantine System is tested against antivirus scanners to determine if the malicious code has been previously identified. If it has not been previously identified, the new executable is submitted to the malicious code analysis team. In fact, between January and June of 2006, 18 percent of malicious code samples detected on the Attack Quarantine System had not been previously seen.\(^2\) As the threat landscape evolves, an early warning solution provider must be able to adjust to the threat. Symantec, through Security Response, is able to execute on this promise now.

By leveraging data from the Attack Quarantine System and sensors, Symantec is also able to compile and maintain lists of IP addresses that are associated with attacks on the Internet. Symantec analysts can also leverage similar lists from other Symantec Global Intelligence Network sources to quickly identify new and potential sources of malicious traffic or threats.

The threat analysis team also develops threat analysis reports in response to specific threats. Threat analysis reports provide more detail than a Threat Alert by including code reverse-engineering and packet captures. This kind of analysis is performed on new or unique kinds of threats. A couple of more recent examples include an eBay JavaScript Injection Phishing Attack and W32.Nugache.A@mm Peer-to-Peer Analysis. The threat analysis provides DeepSight users with depth of knowledge regarding new and different threats beyond what may be seen on a daily basis.

Research reports are another example of the in-depth technical knowledge that Symantec's threat analysis team possesses. Examples of these reports include examinations of the Windows Vista™ Kernel Mode Security, Mac OS® X Threat Landscape, and Online Fraud Communities and Tools. The research reports provide DeepSight users with in-depth information about unique attacks or other interesting developments and trends in information security that are pertinent to Symantec DeepSight users.

User access
The final key pieces of an early warning solution are a mechanism to deliver security intelligence to users and a portal to be able to research specific vulnerabilities, malicious code, and threats.

Symantec DeepSight Early Warning Services provide security intelligence delivered directly to the user as well as a secure portal that can be used to conduct security research.

The Symantec DeepSight Threat Management System portal is made up of five key functional areas:

- Statistics pertaining to Symantec's sensors
- Analysis—actionable reports based on analyst observations
- Advanced reporting based on sensor data
- User administration
- Alerts (Vulnerabilities, Malicious Code, Security Risks, Threat, and Domain Name)

Through this portal, users are able to view the current threat conditions and analysis by the threat analysis team. Additionally, users can view statistics from Symantec's sensors and define alerts that will deliver environment-specific vulnerability, malicious code, security risk, and domain information as they are identified. Users can also query the vulnerability, malicious code, and security risk databases to get historical information as well as query the sensor database to get trend reports about Internet threats.
Users of DeepSight Early Warning Services can choose specific delivery mechanisms to receive security intelligence. These include email, SMS, or voice. XML-formatted email and direct feeds are also available to integrate vulnerability and malicious code data into other enterprise systems.

Statistics
Statistics generated in the Symantec DeepSight Threat Management System are based on the sensor data collected from the Symantec Global Intelligence Network and are updated throughout the day based on event activity. These statistics encompass firewall, intrusion detection system (IDS), and antivirus data and contain metrics around IP addresses generating attacks, ports that are targeted, and demographic information about the victims.

Analysis
The analysis section of the portal provides users with a library from which to download and read pertinent security documents that the analysis teams create. These documents include periodic summary reports that are developed by the threat analysis team on daily, weekly, and monthly basis. These reports provide a snapshot of the threat environment for readers. Additional documents in this library include the threat analysis and alert documents and research reports that were discussed earlier. Vulnerability, malicious code, and security risk information is also available for reference within the analysis section of DeepSight Early Warning Services. A search engine is provided to perform historical research as necessary. Providing all these resources in a single location aids security analysts who need to research specific threats or vulnerabilities.

Advanced reporting
DeepSight Early Warning Services also contain a reporting module that allows users to generate ad hoc queries against the sensor data. These queries can provide attack trends or historical reporting of IP attacks as well as other reporting options. The reports can be scheduled to run and are generated in an easy-to-read PDF document.

User administration
User administration is another key piece of the DeepSight Early Warning Services portal. The administration module allows system administrators to add licenses and users, revoke access, and view allocations via the portal as well as reset passwords as needed. This gives an enterprise security staff maximum flexibility in providing DeepSight access to security and IT staff as required.
Alerts

Alerts are designed to notify a user when a specific set of conditions is met. These conditions include metrics pertaining to the vulnerability or malicious code as well as the technologies associated with the vulnerability or malicious code.

An often overlooked consideration by other early warning solutions is providing an administrator with information that is pertinent to the systems that are deployed within their enterprise. While many enterprises run Microsoft, Oracle, and Cisco products, there are many other products that security administrators need to be aware of as well. Operating systems should be observed, but so should databases, office applications, enterprise resource planning (ERP) packages, and many other types of software and hardware.

As more and more data becomes available via the Web, there are more vulnerabilities being identified in Web applications. In fact, between July and December of 2006, 69 percent of all vulnerabilities were associated with Web applications. Administrators must be able to have insight into vulnerabilities and malicious code on systems that might not have a large market share but are still running in their enterprise and accessing their data. Symantec is tracking vulnerabilities in over 20,000 technologies from 7,000 vendors; roughly 45,000 different versions of software are being observed. The breadth of software that Symantec monitors for vulnerabilities is unparalleled.

Being able to prioritize vulnerabilities, malicious code, and threats that require immediate action over some activity of lesser urgency can help a security manager to more effectively manage resources and deploy defenses to mitigate a threat rather than attempting to mitigate all threats, real or imagined. This focus can help an enterprise be more efficient in its use of limited information security resources. This can be a daunting task with 2,526 vulnerabilities between July and December, 2006, as well as 6,784 new Win32 viruses and worms identified in that same period.

Symantec DeepSight Early Warning Services enable each user to set alerting on specific technology and metric thresholds for vulnerabilities and malicious code. Users can receive all alerts or a subset of the alerts that carry the greatest urgency for their enterprise based upon their risk management strategy and threat posture.

To further enhance the DeepSight Early Warning Services, Symantec is the first vendor to introduce both security risk alerting and domain alerting to users.

---

1 Symantec Internet Security Threat Report, Volume XI, March 2007, see “Vulnerabilities” section.
Security risks
Adware and spyware pose additional sources of concern for the security staff, and Symantec is the first company to include alerting/reporting capabilities for these security risks into an early warning solution. Adware and spyware are delivered through DeepSight Early Warning Services by the same means as vulnerabilities and malicious code.

Domain alerts
Many malicious code payloads specifically call out company domains. These domain names might be spoofed email addresses or other elements within the malicious code to trick a user into accidentally spreading the malicious code. To provide better awareness to DeepSight Early Warning Services users, Symantec developed an alerting mechanism that allows a user to specify any domain name, and when it is referenced, the malicious code analysis will be sent, no matter what the rating is for that piece of malicious code. This is an important value to DeepSight Early Warning Services users. While subscribers can receive malicious code alerts based on a ratings threshold, the domain alert will always provide a copy of the malicious code when a domain name of interest appears. This generates a greater awareness of targeted malicious code than was previously available elsewhere. A sample alert email and a subset of the alert are shown in Figures 3 and 4.

---

**Subject:** Company Domain alert M3ID 0895 W32/Spbot.AWIC (RakZ)

This alert triggered due to the mention of the following domain names within the alert:

- symantec.com

**Location:**


**View public key as:**

http://alerts.symantec.com/gpgkey.aspx

---

Figure 3. Email alert
Figure 4. Domain alert

**Timeliness and depth**

When assessing the value of the information that is being received from an early warning solution, there are a couple of key points to keep in mind. The information needs to be delivered in a timely fashion but also must be in great enough depth so that the information is understandable and actionable. These are areas where Symantec DeepSight Early Warning Services are superior to any other product or service available.

The timeliness of information reaching a user is hugely important because of the shrinking window from the time a vulnerability is identified to the time an exploit for that vulnerability becomes available. Between July and December 2006, the average amount of time for an exploit to be developed against an application by an enterprise vendor was between 1–5 days.5

The depth of the information provided is also crucial in an early warning solution. Telling an administrator that there is a vulnerability without providing additional information is not helpful nor is it actionable. A full analysis of the vulnerability or malicious code is necessary to give an administrator an informed view of the issues and a path to remediation.

---

Symantec DeepSight Early Warning Services has been recognized in third-party testing for providing both timely and comprehensive alerts to its users. The depth of information includes affected platforms, exploits, workarounds, and a comprehensive set of links to vendor patches, to name a few.

**Case study: MS06-040: Microsoft® Windows® Server Service Remote Overflow Vulnerability**

The combination of the Symantec Global Intelligence Network of data sources, the automated and human analysis, and the user interface makes Symantec DeepSight Early Warning Services part of the solution in addressing compliance and threat management issues in any enterprise.

This case study is an example of leveraging information generated by Symantec DeepSight Early Warning Services to provide actionable information to assist in the mitigation of specific threats.

Microsoft released an advisory on August 8, 2006, regarding vulnerabilities in the Windows server service. This bulletin identified systems running Windows 2000 and above as being vulnerable, but the bulletin did not clearly define the possibility that older systems were also vulnerable. Microsoft also mentioned that there were active exploits in the wild for this vulnerability. Symantec DeepSight Early Warning Services alerts were released that same day based on this information.

The ThreatCon was at a Level Two (Elevated: Increased Alertness) when this threat was identified. Due to the successful exploitation of the vulnerability, a ThreatCon was issued to reinforce the heightened level of the threat.

In their Analyst Journal on August 8 the threat analysis team reported the release of Microsoft’s Security Bulletins. his alert was updated as the threat evolved to include:

- A technical description of the threat, including an explanation as to how a remote user could access the service and how Windows XP Service Pack 2 handled this differently than other versions of Windows

- Attack data demonstrating how a request could be made to bind to the server service interface

- MD5 Sums of the malicious code that exploits the vulnerability

- Information about available antivirus definitions for the malicious code

---

---

---
The Value of Early Warning Solutions

- DeepSight honeypot information about the attacks being observed, including payloads, IP addresses associated with the threat, and executables being downloaded from third-party Web sites
- Links to relevant patches
- Mitigation strategies at the network, host, and registry layers
- Links to third-party and Symantec Web sites for additional information

In addition to a Threat Alert, the threat analysis team posted reported information in the daily, weekly, and monthly reports concerning new threats that exploited this vulnerability. This information was initially posted to the Analyst Journal and was updated by the analysts as it was identified.

The vulnerability analysis team subsequently identified additional information regarding this vulnerability and sent updates to users. These updates included:
- A proof-of-concept exploit becoming available
- A metasploit exploit module that was created and later ported to C code
- A free vulnerability scanner from a security vendor being made available
- Information regarding malware exploiting the vulnerability in the wild
- Validation that a worm exploiting this vulnerability
- Additional exploit code from other sources being available
- Information regarding a new botnet

Starting August 10 the Analyst Watch section of the portal provided some additional statistics regarding the threat around the MS06-040 vulnerability. The Analyst Watch charted activity from IDS and firewall sensors on TCP ports 139 and 445 as well as information about the threat, mitigation strategies, and links to the vulnerability and threat alert. The graphs and information were updated through October 6 as the threat evolved and new variants were identified.

The malicious code analysis team received their first sample of what became known as W32.Wargbot on August 12. They analyzed the malicious code and identified that it was leveraging the MS06-040 vulnerability to propagate. The analysts identified two variants and documented the characteristics of the malicious code. This piece of malware was a bot that
opened up an IRC command and control channel and, in some cases, downloaded a Trojan
of a backdoor called Backdoor.Ranky.X. This information was sent to Symantec DeepSight
Early Warning Services users. Shortly thereafter, additional pieces of malware were identified
attempting to use this exploit. As of January 2007, in fact, Symantec DeepSight Early Warning
Services has documented 73 different pieces of malicious code that exploit the Microsoft
Windows Server Service Remote Overflow Vulnerability (MS06-040).

On August 22, the ThreatCon was decreased to Level One (Low: Basic Network Posture)
when patches and mitigation strategies had been identified and made available for two weeks.

On August 31, the ThreatCon was escalated back to Level Two because of an increase in
malicious activity on Port 139, one of the ports where Symantec’s honeypots observed attacks
exploiting the MS06-040 vulnerability. Additionally, there were reports of successful compromise
of Windows NT® 4.0 devices. Microsoft did not issue patches for Windows NT 4.0, creating a
significant risk for users of this platform.

A final ThreatCon was issued on September 1 regarding threats targeting the MS06-040
vulnerability based on the threat analysis team’s confirmation that Windows NT 4.0 devices
can be compromised. The ThreatCon also provided recommendations for mitigating the threat.
Alerts regarding the ThreatCon and the evolution of the threat were sent to users of Symantec
DeepSight Early Warning Services.

In September 2006 the threat analysis team also completed a comprehensive analysis of
the MS06-040 vulnerability that included:

• A timeline of the malware and threats
• Attack data statistics based on Symantec sensor data
• Packet captures from the DeepSight honeynet of systems being compromised
• Mitigation strategies

In the case of the MS06-040 vulnerability, it did not evolve into a global, widespread threat.
However, many different variants of malicious code were and still are being created to exploit this
vulnerability. Users of the Symantec DeepSight Early Warning Services have been able to track
the threat across its entire lifecycle from the identification of the vulnerability forward. This
actionable information has given users the information they need to make informed decisions
regarding the threat in a timely manner and updated them as new information is identified.
Conclusion

Symantec DeepSight Early Warning Services are able to provide early warning threat capability by leveraging the Symantec Global Intelligence Network of 40,000 registered volunteer sensors that send firewall and network intrusion detection system data to Symantec, providing an excellent picture of threat data traversing the Internet. This view is enhanced by input from the 500 Managed Security Services customers, submissions from Symantec antivirus customers, and data from Symantec's unique Attack Quarantine System. A team of threat analysts is responsible for analyzing the data from these disparate data sources, and performing their own research on the Web to identify new threats that are appearing across the Internet. Additionally, Symantec's teams of vulnerability and malicious code analysts provide actionable information, mitigation steps, and workarounds for vulnerabilities and malicious code as they are identified. This research, analysis, and response capability is occurring 24x7.

The output of this effort is Symantec DeepSight Early Warning Services. Symantec DeepSight Early Warning Services provide knowledge about vulnerabilities, malicious code, security risks, and threats to users as they occur and allow users to make informed judgments on how to mitigate vulnerabilities and threats. While some companies may claim the ability to identify vulnerabilities and malicious code, Symantec DeepSight Early Warning Services provide early warning information to users based upon current Internet activity. This combination of current activity and expert analysis around threats and vulnerabilities is unmatched.

The Value of Early Warning Solutions
About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com