Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Preventing Propagation of the NIMDA Worm with a Holistic Approach

The purpose of this paper is to discuss the main methods by which Nimda spreads, to share effective ways to prevent the spread of Nimda and to express that a holistic approach is needed to prevent the propagation and spread of recently developed worms. In the past, Virus propagation and spreading was dealt with by pure anti-virus products. Nimda introduced for the first time a complex, multi-pronged threat. In order to be prepared for future, and probably more destructive threats, an enterprise should deploy a holistic...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Preventing propagation of the NIMDA worm with a holistic approach

Version 1.2f

By David C. Petty

Introduction

Nimda is a worm that was discovered on September 18th 2001 and it was estimated that it infected 2.2 million Servers and PC's by September 21st. The cost for clean up from infection is estimated to be somewhere North of 530 million by Computer Economics [2]. The purpose of this paper is to discuss the main methods that Nimda spreads, to share effective ways to prevent the spread of Nimda and to express that a holistic approach is needed to prevent the propagation and spread of recently developed worms. In the past, Virus propagation and spreading was dealt with by pure anti-virus products. Nimda introduced for the first time widely, a complex, multi-pronged threat that needs to be dealt with via a holistic approach. It is an approach that will favor the security teams that can effectively integrate multiple tools to deal with the multiple vectors of infection.

Nimda is a worm that spreads itself without human intervention by several means. The most well known method is via scanning a network for unpatched Microsoft IIS webservers. After identifying the server, it will perform the Unicode Web Traversal Exploit to gain control of the server. The worm can also spread itself via email. It will take the email addresses from an infected machine and send out emails randomly. The recipient can infect their machine simply via a preview function or reading the email. This is accomplished by the worm via a MIME exploit. A third and fourth means occurs when users visit infected web servers and or click through a prompted download. Another method of propagation is through network shares that result in the creation of a backdoor. The final method is via a backdoor created by the Code Red II malware. This worm can use a lot of distinct methods to replicate itself.

Effective means for preventing infection by and spread of this worm include the securing of Gateways, Servers and Clients. This is accomplished most effectively with the use of Anti-virus tools on the gateway server and client levels. Micheal Erbschloe of Computer Economics said, "More than 90% of the time Nimda landed on a machine, the cleanup process was done through automated virus protection procedures." The application of Vulnerability assessment tools and Intrusion tools that are both network and host based also plays an important roll in identifying infected machines and preventing infection. A holistic approach will have all of the tools working together to solve the problem of infection.

The fact that this worm is one of the first of a new generation of worms that exploit various vulnerabilities without our intervention underscores and demonstrates the need for multiple tools to address these vulnerabilities. The next generation of this worm may include additional means of propagation and have more malicious payloads and side

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

effects. The effective deployment and application of manpower, policy and tools should prevent the spread of Nimda and Nimda-like malicious code.

Over the next few sections you will find description of how the worm propagates and simple steps to prevent infection with antivirus, intrusion detection, vulnerability assessment and firewalls. Each of these classes of products plays an important roll.

Means of Propagation and countermeasures

Random scanning for ISS Servers

Clients or servers that are infected will scan the network looking for unpatched IIS servers that can run on NT workstations as well as Servers. It will then run an exploit known as Unicode Web Traversal Exploit to get control of the Server. This Exploit has been known for almost a year now.

The following represents a timeline associated with this vulnerability that demonstrates that this individual vulnerability is almost a year old (This is from a paper by Steven Shields)[7]:
10/10/2000 Message posted to Packetstorm
10/11/2000 Vulnerability tested (unsuccessfully) by other forum users
10/14/2000(est) Message brought to the attention of Rain Forest Puppy
10/15-16/2000 Vulnerability brought to the attention of Microsoft
10/17/2000 Microsoft bulletin posted

"Web Server Folder Traversal vulnerability will allow users to gain access to a computer system running Microsoft IIS versions 4.0 and 5.0. Using a malformed Uniform Resource Locator (URL), an individual could gain access to folders and files that are located on the server's logical drive. Gaining this type of access could result in a multitude of possibilities. Specifically, this access could allow an individual to add, change or delete data, run code already on the server or upload and run new code to the server."

This is a vulnerability that has been well documented since October of 2000. As a side effect, the infected machines attempting to scan the network can sometimes create denial of service conditions.

This form of propagation can be prevented with several simple steps. Some are very practical and others are a bit extreme.

Apply the current patch to IIS servers, which is at http://www.microsoft.com/technet/security/bulletin/ms00-078.asp. This will close the vulnerability.

Run a host based vulnerability assessment product to ensure that the patches have been applied to all systems running IIS.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Run a similar product to ensure that IIS is not running on machines that do not need it.

Use a network based vulnerability scanner to search for additional machines running IIS in your enterprise. Once identified, these can be removed or patched as needed and appropriate.

When machines are identified as infected, they should be cut off from the network. This can be accomplished by use of a Network based intrusion detection product to look at the network traffic and identify infected machines. The logs will show the IP address of infected machines. These machines should then be removed from the network.

Nimda can also spread via email.
Nimda contains its own SMTP engine and propagates in a manner similar to the W32.Magistr.Worm. (http://securityresponse.symantec.com/avcenter/venc/data/w32.magistr.24876@mm.html) This worm propagates via email using SMTP commands by sending copies of itself to all addresses listed in an infected user's address book (It can get email addresses from any MAPI compliant email programs, mailboxes and HTML files). The Virus will randomly place these addresses in the send and from locations. The result is that it is more difficult to determine where the mail comes from and the body is generally blank[6]. When the worm (email) arrives, it uses a MIME exploit (Currently 25 different MIME vulnerabilities are listed at http://www.cve.mitre.org). This allows the Virus to be executed just by reading or previewing the email.

This vulnerability is best addressed by applying the patch for the vulnerability used. It is at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp

This form of propagation should also be addressed through the use of an anti-virus product at the Gateway, email server and client levels. The e-mails have various formats. This is a case where scanning email at the Gateway both inbound and outbound can really slow the spread.

Host and network based vulnerability scanners can help to determine infection.

Some of the more recent anti-virus product releases include outbreak management to identify mass sending of email. This may be of little value due to Nimda having it's own SMTP engine.

Internet browsing.
Clients that visit compromised or infected web servers will be prompted to download an email file (*.eml). This will have an attachment on it entitled readme.eml. This attachment contains the worm. It is also understood that simply browsing infected web servers can result in infection in certain situations.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

This third vulnerability is accomplished via a well-documented MIME exploit.[1]

This form of propagation is best addressed by updating to the newer IE release 6.0. or applying the patch available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp to 5.01 and 5.5 IE browsers.

Client, Server and Gateway level anti-virus can also help to prevent this method of infection. The Gateway AV product scans the HTTP traffic and the Malware is detected and hopefully rejected. This assumes that the signatures or DAT's are up-to-date on the machine in question.

Nimda will also attack the hard disks that have enabled file sharing over the network.

It will copy itself to open drives, folders and file shares. While doing this it will create a guest account with Administrator privileges on the machine directly infected.

This is best addressed via preventing the infections in the first place. This can best be accomplished by following the steps outlined above.

If a machine is identified as infected it should be isolated. This will prevent propagation via file sharing over the network. To discover wether a machine is infected, use an intrusion detection product to look at the network traffic and identify infected machines. The logs will show the IP address of infected machines. It can also be found with anti-virus tools. Some of the fix tools for infections include scanners.

Limiting or controlling open shares will also help with this.

The worm can also use a back door created by Code Red II to spread.
Symantec describes this back door at http://securityresponse.symantec.com/avcenter/venc/data/codered.ii.html

It allows the attacker to run scripts on the web server to get root access. Nimda automated this attack and uses it to gain access.

Countermeasures for this mode of transmission include:

Apply the patch available at http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Clean up and isolate infected machines in a timely manner.

Ensure all signatures are up-to-date and used.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Nimda virus took a lot of IT departments by surprise as a result of the many means of transmission. Erbschloe , who is the author of “Information Warfare: How To Survive Cyber Attacks”, said “Some people are calling Nimda another wake-up call, but if Nimda had a destructive payload it would have been a messenger sent by Satan," Erbschloe added "This would have easily cost well over $3 billion in cleanup costs and another $3 billion in lost productivity if there was a killer payload and if there were no automated processes in place to eradicate the bug." Currently, October 31,2001, a new version of Nimda has been infecting machines and demonstrating that these worms do get modified and reappear. To reference this go to (http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.e@mm.html). This new modification includes some new “bug fixes” and modifications to the names of files that are attached to emails and dropped.

The steps above give some straightforward means of preventing propagation of the worm. Due to the multi pronged attack perpetrated by Nimda, and it’s close relatives, it is necessary to evaluate the countermeasures applied and available in order to prevent future losses. It is estimated that Nimda and other similar worms have cost companies in excess of a billion dollars since September 18th. There is a real threat that future malware will use additional means of propagating and carry a more destructive payload. In order to be prepared an enterprise should deploy a holistic approach using traditional anti-virus products at the client server and gateway levels as well as firewalls, vulnerability assessment and intrusion detection tools. The defense needs to be mapped out holistically with combating malicious code as one of the key goals. This has focused on the tools that help with this vulnerability. However, when it is all said and done, it is the trained and knowledgeable teams that really need to be nurtured and acknowledged. Without the experience and knowledge to apply best practices they will never be deployed.

Sources:

1. URL: http://www.cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mime
   Mitre “common vulnerabilities and exposures”

2. URL: http://www.computereconomics.com
   Computer Economics “Nimda Battle Shows Progress in the War Against Malicious Code”

3. Symantec "Responding to the Nimda worm:Recommendations for addressing blended
   threats” 3 Oct 2001.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

URL: http://www.symantec.com/avcenter/venc/data/qaz.trojan.html (5 Jan 2001)

4. URL: http://www.cert.org/advisories/CA-2001-26.html
   Carnagie Mellon Software engineering institute "CERT® Advisory CA-2001-26 Nimda Worm"

5. URL:
   http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html
   Symantec" W32.Nimda.A@mm"

6. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=99209&
   McAfee W32/Nimda.a@mm

7. Shields, Steven. ""Web Server Folder Traversal" vulnerability (MS00-078)" 13 Feb 2001. URL: http://www.sans.org/infosecFAQ/threats/traversal.htm (3 Oct 2001)

8. URL:
   http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp
   Microsoft "Microsoft Security Bulletin (MS01-020)"

© SANS Institute 2001, Author retains full rights

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced