

Fwd: CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-03/0194.html>

From: Muhammad Faisal Rauf Danka (mfrd@attitudex.com)

Date: 03/13/03

Date: Thu, 13 Mar 2003 04:26:17 -0800 (PST)
From: Muhammad Faisal Rauf Danka <mfrd@attitudex.com>
To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

*** There is an attachment in this mail. ***

[ATTITUDEX.COM]
<http://www.attitudex.com/>

Select your own custom email address for FREE! Get you@yourchoice.com w/No Ads, 6MB, POP & more!
<http://www.everyone.net/selectmail?campaign=tag>

attached mail follows:

('binary' encoding is not supported, stored as-is)

Date: Tue, 11 Mar 2003 17:03:22 -0500
From: CERT Advisory <cert-advisory@cert.org>
To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares

Original release date: March 11, 2003

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- * Microsoft Windows 2000
- * Microsoft Windows XP

Overview

In recent weeks, the CERT/CC has observed an increase in the number of reports of systems running Windows 2000 and XP compromised due to poorly protected file shares.

I. Description

Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor, which are described in more detail below.

Background

Microsoft Windows uses the SMB protocol to share files and printer resources with other computers. In older versions of Windows (e.g., 95, 98, Me, and NT), SMB shares ran on NetBIOS over TCP/IP (NBT) on ports 137/tcp and udp, 138/udp, and 139/tcp. However, in later versions of Windows (e.g., 2000 and XP), it is possible to run SMB directly over TCP/IP on port 445/tcp.

Windows file shares with poorly chosen or Null passwords have been a recurring security risk for both corporate networks and home users for some time:

- * IN-2002-06: W32/Lioten Malicious Code
- * CA-2001-20: Continuing Threats to Home Users
- * IN-2000-02: Exploitation of Unprotected Windows Networking Shares
- * IN-2000-03: 911 Worm

It has often been the case that these poorly configured shares were exposed to the Internet. Intruders have been able to leverage poorly protected Windows shares by exploiting weak or Null passwords to access user-created and default administrative shares. This problem is exacerbated by another relevant trend: intruders specifically targeting Internet address ranges known to contain a high density of weakly protected systems. As described in CA-2001-20, the intruders'

efforts commonly focus on addresses known to be used by home broadband connections.

Recent developments

The CERT/CC has recently received a number of reports of exploitation of Null or weak Administrator passwords on systems running Windows 2000 or Windows XP. Thousands of systems have been compromised in this manner.

Although the tools involved in these reports vary, they exhibit a number of common traits, including

- * scanning for systems listening on 445/tcp (frequently within the same /16 network as the infected host)
- * exploiting Null or weak passwords to gain access to the Administrator account
- * opening backdoors for remote access
- * connecting back to Internet Relay Chat (IRC) servers to await additional commands from attackers
- * installing or supporting tools for use in distributed denial-of-service (DDoS) attacks

Some of the tools reported have self-propagating (i.e., worm) capabilities, while others are propagated via social engineering techniques similar to those described in IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging.

The network scanning associated with this activity is widespread but appears to be especially concentrated in address ranges commonly associated with home broadband users. Using these techniques, many attackers have built sizable networks of DDoS agents, each comprised of thousands of compromised systems.

W32/Deloder

The self-propagating W32/Deloder malicious code is an example of the intruder activity described above. It begins by scanning the /16 (i.e., addresses with the same first two high-order octets) of the infected host for systems listening on 445/tcp. When a connection is established, W32/Deloder attempts to compromise the Administrator account by using a list of pre-loaded passwords. Variants may include different or additional passwords, but reports to the CERT/CC indicate that the following have appeared thus far:

```
[NULL] 0 000000 00000000 007 1 110 111 111111 11111111 12
121212 123 123123 1234 12345 123456 1234567 12345678 123456789
1234qwer 123abc 123asd 123qwe 2002 2003 2600 54321 654321
88888888 Admin Internet Login Password a aaa abc abc123 abcd
admin admin123 administrator alpha asdf computer database
enable foobar god godblessyou home ihavenopass login love
mypass mypass123 mypc mypc123 oracle owner pass passwd password
```

```
pat patrick pc pw pw123 pwd qwer root secret server sex super
sybase temp temp123 test test123 win xp xxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx yxcv zxcv
```

On successful compromise of the Administrator account, W32/Deloder copies itself to the victim, placing multiple copies in various locations on the system. Additionally, it adds a registry key that will cause the automatic execution of dvlldr32.exe (one of the aforementioned copies). The victim will begin scanning for other systems to infect after it is restarted.

W32/Deloder opens up backdoors on the victim system to allow attackers further access. It does this in two ways:

1. attempting to connect to one of a number of pre-configured IRC servers
2. installing a copy of VNC (Virtual Network Computing), an open-source remote display tool from AT&T, listening on 5800/tcp or 5900/tcp

Note: VNC in and of itself is not a malicious tool, and has many other legitimate uses.

During the course of infection by W32/Deloder, a number of files may be created on the system. Reports indicate that files matching the following descriptions have been found on compromised systems:

Filename
File Size (bytes)
Description

dvlldr32.exe
745,984
The self-propagating malicious code

inst.exe
684,562
This file installs the backdoor applications onto the victim host

psexec.exe
36,352
A copy of the Remote Process Launch application (not inherently malicious, but it is what allows the worm to replicate)

explorer.exe
212,992
A renamed copy of the VNC application

omnithread_rt.dll
57,344
VNC dependency file

VNCHooks.dll
32,768
VNC dependency file

rundll32.exe
29,336
The IRC-Pitchfork bot application

cygwin1.dll
944,968
IRC-Pitschfork dependency file

GT-bot and sdbot

Intruders frequently use IRC "bots" (automated software that accepts commands via IRC channels) to remotely control compromised systems. GT-bot and sdbot are two examples of intruder-developed IRC bots. Both support automated scanning and exploitation of inadequately protected Windows shares. These tools also offer intruders a variety of DDoS capabilities, including the ability to generate ICMP, UDP, or TCP traffic.

Tools like these are undergoing constant development in the intruder community and are frequently included as part of other tools. As a result, the names, sizes, and other characteristics of the files that might contain these tools vary widely. Furthermore, once installed, the tools are designed to hide themselves fairly well, so detection may be difficult.

The CERT/CC has received reports of sdbot networks as large as 7,000 systems, and GT-bot networks in excess of 140,000 systems.

W32/Slackor

The W32/Slackor worm is another example of a tool that targets file shares. On a compromised machine, the worm begins by scanning the /16 of the infected host for other systems listening on 445/tcp. When a system is discovered, W32/Slackor connects to the \$IPC share using a set of pre-programmed usernames and passwords, copies itself to the C:\sp directory, and runs its payload. The payload consists of the following files:

Filename
Description

slacke-worm.exe
The self-propagating malicious code

abc.bat
List of usernames/passwords

psexec.exe

A copy of the Remote Process Launch application (from sysinternals.com, used for replicating the worm)

main.exe

The bot application

W32/Slackor also contains an IRC bot. When this bot joins its IRC network, a remote intruder controlling the IRC channel can issue arbitrary commands on the compromised computer, including launching denial-of-service attacks.

Network footprint

Widespread scanning for 445/tcp indicates activity of this type.

Compromised hosts may also have unauthorized connections to IRC servers (typically on 6667/tcp, although ports may vary).

Additionally, the VNC package installed by W32/Deloder will typically listen on 5800/tcp or 5900/tcp. If a compromised system is used in a DDoS attack on another site, large volumes of IP traffic (ICMP, UDP, or TCP) may be detected emanating from the compromised system.

II. Impact

The presence of any of these tools on a system indicates that the Administrator password has likely been compromised, and the entire system is therefore suspect. With this level of access, intruders may

- * exercise remote control
- * expose confidential data
- * install other malicious software
- * change files
- * delete files
- * launch attacks against other sites

The scanning activities of these tools may generate high volumes of 445/tcp traffic. As a result, some Internet-connected hosts or networks with compromised hosts may experience performance issues (including denial-of-service conditions).

Sites targeted by the DDoS agents installed by this activity may experience unusually heavy traffic volumes or high packet rates, resulting in degradation of services or loss of connectivity altogether.

III. Solution

In addition to following the steps outlined in this section, the CERT/CC encourages home users to review the "Home Network Security" and "Home Computer Security" documents.

Disable or secure file shares

Best practice dictates a policy of least privilege; if a given computer is not intended to be a server (i.e., share files with others), "File and Printer Sharing for Microsoft Networks" should be disabled.

For computers that export shares, ensure that user authentication is required and that each account has a well-chosen password. Furthermore, consider using a firewall to control which computer can access these shares.

By default, Windows NT, 2000, and XP create certain hidden and administrative shares. See the HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers for further guidelines on managing these shares.

Use strong passwords

The various tools described above exploit the use of weak or Null passwords in order to propagate, so using strong passwords can help keep them from infecting your systems.

Microsoft has posted a "Create Strong Passwords" checklist.

Run and maintain an anti-virus product

The malicious code being distributed in these attacks is under continuous development by intruders, but most anti-virus software vendors release frequently updated information, tools, or virus databases to help detect and recover from the malicious code involved in this activity. Therefore, it is important that users keep their anti-virus software up to date. The CERT/CC maintains a partial list of anti-virus vendors.

Many anti-virus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs of unknown origin

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Users of IRC, Instant Messaging (IM), and file-sharing services should be particularly wary of following links or running software sent to them by other users, as this is a commonly used method among intruders attempting to build networks of DDoS agents.

Deploy a firewall

The CERT/CC also recommends using a firewall product, such as a network appliance or a personal firewall software package. In some situations, these products may be able to alert users to the fact that

their machine has been compromised. Furthermore, they have the ability to block intruders from accessing backdoors over the network. However, no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

Ingress/egress filtering

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for internal systems to access SMB shares across the Internet.

In the case of the intruder activity described above, blocking connections to port 445/tcp from entering or leaving your network reduces the risk of external infected systems attacking hosts inside your network or vice-versa.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

Steps for Recovering from a UNIX or NT System Compromise

IV. References

1. Trends in Denial of Service Attack Technology:
http://www.cert.org/archive/pdf/DoS_trends.pdf
2. Managing the Threat of Denial-of-Service Attacks:
http://www.cert.org/archive/pdf/Managing_DoS.pdf
3. IN-2002-06: W32/Lioten Malicious Code:
http://www.cert.org/incident_notes/IN-2002-06.html
4. CA-2001-20: Continuing Threats to Home Users:
<http://www.cert.org/advisories/CA-2001-20.html>
5. IN-2000-02: Exploitation of Unprotected Windows Networking Shares:
http://www.cert.org/incident_notes/IN-2000-02.html
6. IN-2000-03: 911 Worm:
http://www.cert.org/incident_notes/IN-2000-03.html
7. IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging:
http://www.cert.org/incident_notes/IN-2002-03.html
8. VNC (Virtual Network Computing):
<http://www.uk.research.att.com/vnc/>
9. Home Network Security:
http://www.cert.org/tech_tips/home_networks.html
10. Home Computer Security:

<http://www.cert.org/homeusers/HomeComputerSecurity/>

11. HOW TO: Create and Delete Hidden or Administrative Shares on Client Computers:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q314984&sd=tech>

12. Checklist: Create Strong Passwords:

<http://www.microsoft.com/security/articles/password.asp>

13. Anti-virus vendors:

http://www.cert.org/other_sources/viruses.html#VI

14. Steps for Recovering from a UNIX or NT System Compromise:

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#36888]".

Feedback can be directed to the authors: Allen Householder and Roman Danyliw

This document is available from:

<http://www.cert.org/advisories/CA-2003-08.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center

Software Engineering Institute

Carnegie Mellon University

Pittsburgh PA 15213-3890

U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email.

Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

SecurityFocus Bugtraq: Fwd: CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

<http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2003 Carnegie Mellon University.

Revision History

March 11, 2003: Initial release

-----BEGIN PGP SIGNATURE-----

Version: PGP 6.5.8

```
iQCVAwUBPm5bd2jtSoHZUTs5AQGJkQQAskLQbGaPphIDbOdtvazUNJTUxroPQNyo
5Fw2RNeKkr3ECvmtuRRqDaDUyx1mziCDz8i655twWsY5k1Jexl+WICLIvfvf5jpA
bgJYskeEagBNAGlkvAZuI48tOtC/O3M01dTLzVmN083Tqn22ZXl/w5nHMVu4y81t
XqROPqun25M=
=hbFj
```

-----END PGP SIGNATURE-----