

SOBIG.F - Ein Virus überflutet das Internet

Analyse von Marko Rogge // Brain-Pro Security :: 01.09.2003

Am 18.08.2003 kommen erste Anzeichen einer erneuten Internetepidemie in den Anti-Virenlabors auf, SOBIG.F ist auf dem besten Weg das Internet schnell zu verseuchen.

Noch ist das World Wide Web und die angeschlossenen User damit beschäftigt, die Computer, Netzwerke und Server vom MSBLASTER Wurm zu befreien, da taucht auch schon der nächste Wurm auf.

SOBIG.F ist jedoch nicht wie der MSBLASTER ein eher harmloser Computerwurm, sondern kommt mit einem destruktivem Inhalt und einer rasanten Ausbreitung.

Es ist davon auszugehen, dass tausende, gar weltweit Millionen E-Mails mit dem Wurm als Anhang über betroffene Systeme versendet wurden.

So wurden zum Beispiel in Unternehmen und öffentlichen Einrichtungen im fränkischen Raum ca. 40.000 E-Mails gezählt, die durch AV-Systeme als virenverseucht deklariert wurden und den Wurm SOBIG.F als Anhang hatten.

In einer Umfrage durch Brain-Pro Security vom 27.08.2003 an der ca. 60 Unternehmen teilnahmen, wurden die belastenden E-Mails ausgefiltert und ein größerer Schaden konnte abgewendet werden.

Problematisch stellte sich jedoch das enorme Trafficaufkommen dar, weil jede E-Mail die den Wurm als Inhalt hatte ca. 74-78 kb groß war.

Bei einer Masse von 40.000 E-Mails ergibt das eine stolze Summe von ca. 2.960.000 kb wenn man 74 kb zu Grunde legt.

Dies ist nur ein Rechenbeispiel aus dem Oberfränkischem Raum und deren Unternehmen.

In den Unternehmen die vom Befall des Wurms betroffen waren ist durch einen erfolgreichen und guten Virenschutz kein Schaden unmittelbar entstanden, jedoch kann man dennoch von einem wirtschaftlichen Schaden sprechen.

In Gesprächen mit einigen Vertretern von Firmen und deren IT-Beauftragten ist klar betont worden, dass durch das massive Auftreten des SOBIG.F Wurms Mehrleistungen an Arbeitszeit aufgebracht werden musste, um "Herr der Lage" über die betroffenen Netzwerke zu bleiben.

In einem Unternehmen mit ca. 50 Clients kann man davon ausgehen, dass ein Mehraufwand von ca. 800 Euro je Tag abgerechnet werden kann.

Zusätzlich ist ebenfalls finanziell der Schaden zu rechnen, der durch erhöhte Trafficrechnungen entstanden ist.

Wenn ein Unternehmen täglich 500 E-Mails mit dem Wurm SOBIG.F erhält, so macht das mindestens ein reines Mehraufkommen an Traffic von 37.000 kb was zusätzlich bezahlt werden muss.

Auf 5 Tage einer Arbeitswoche gerechnet ergibt das bei einem Unternehmen dieser Größe eine zusätzliche Trafficleistung von 1.850.000 kb.

Bei 60 Unternehmen und öffentlichen Einrichtungen im fränkischen Raum wäre das eine geschätzte Schadenssumme von ca. 48.000,- Euro je Tag.

Der übermäßige Traffic ist hierbei noch nicht berechnet worden.

Sind jedoch E-Mails Mime codiert, so würde sich der Schaden durch ein erhöhtes Trafficaufkommen nochmals erhöhen.

Viele E-Mails Clients bieten die so genannte Lesebeteiligung an und versenden diese natürlich auch im Falle des Wurms SOBIG.F.

Auch hierdurch wird das allgemeine Trafficaufkommen erhöht und belastet das Internet zusätzlich. Durch Verisign war zu erfahren, dass weltweit mehr als 100.000 root-Server mittels DNS-Lookup Tests eine Infektion aufzeigten durch die ein Wurm gesendet wurde.

Allein der Mailserver von Brain-Pro Security registrierte täglich ca. 150 verseuchte E-Mails mit dem SOBIG.F Wurm und das Ende ist nach der Schadensroutine erst zum 10.09. des Jahres zu erwarten da er sich ab da nicht weiter verbreiten wird.

Zum Erscheinen dieses Artikels ist bereits ein deutlicher Rückgang zu verzeichnen jedoch kommer derzeit nach wie vor viele E-Mails mit dem Wurm SOBIG.F als Anhang.

In einem Gespräch mit Dirk Kollberg, Virus Research Engineer von McAfee (NAI) gegenüber Brain-Pro Security wurde die Problematik nochmals aufgegriffen und Dirk Kollberg war so freundlich,

einige Tipps mit auf den Weg zu geben:

"Die neuste Variante des W32/Sobig@MM Wurms hat in den letzten Wochen eine sehr starke Verbreitung gefunden.

Dieser Wurm nutzt keine Sicherheitslücken (Exploits) aus um sich zu verbreiten, sondern ist auf einen 'Doppelclick' von unbedachten Usern angewiesen.

Das hohe Datenvolumen, daß der Wurm durch das selbsttätige Versenden von infizierten EMail erzeugt, ist so hoch, daß viele Privatnutzer und Firmen sich vor große Probleme gestellt sehen die Datenflut zu verarbeiten.

Da der Wurm nicht nur EMail-Adressen aus dem Adressbuch eines infizierten Rechners nimmt, sondern auch nach EMail Adressen in diversen Dateien auf der lokalen Festplatte sucht, erhalten Nutzer die Ihre EMail Adresse auf Ihrer Webseite preisgeben oder sich z.B.

in Gästebücher eintragen besonders viele Exemplare des digitalen Schädlings.

Ein weiteres Problem bei diesem Wurm ist, daß er die Absender Adresse der infizierten EMail fälscht. Er wählt als Absender Adresse eine zufällige aus, die er auf dem infizierten System gefunden hat.

Anti-Virus Produkte oder Nutzer die den Absender der infizierten Mail informieren möchten, erreichen daher nie die Quelle der Mail, sondern senden die Antwortmail an die Adresse eines unbeteiligten, der sich dadurch eher verwirrt fühlt.

Anhand des SMTP Headers der EMail kann man erkennen, von welcher IP Adresse aus die EMail versendet worden ist. Jedoch ist dieses für Privatnutzer relativ aufwendig und rechtfertigt nicht den Nutzen.

Zum Schutz vor Viren, Würmern und Trojaner rate ich dringend dazu, ein aktuelles Anti-Virus Produkt auf dem Rechner zu installieren. Auch Personal Firewalls schützen in diesem Fall und verhindern, daß der Wurm sich in das Internet versenden kann.

Der beste Weg sich gegen EMail Würmer zu schützen ist jedoch, daß man seinen 'gesunden Menschenverstand' nutzt.

Erhält man EMail von Absendern die einem nicht bekannt sind oder verdächtige ausführbare Dateianhänge (z.B. *.SCR *.PIF *.SHS) sollte man die Mail ungelesen löschen, ggf bei dem Absender nachfragen - jedoch nicht durch einen Doppelclick die Kontrolle über den eigenen Rechner an eine fremdes Programm übergeben.

Dirk Kollberg

Virus Research Engineer

McAfee AVERT(tm) - A Network Associates Busines"

Technischer Hintergrund W32.SOBIG.F@MM:

Die Verbreitung ist wie bei den Vorgängern des SOBIG.F ausschliesslich per E-Mail möglich jedoch fälscht auch dieser Wurm die Absenderadressen, die er in .dbx .eml .hlp .htm .html .mht .wab .txt Dateien findet.

Die Gefahr dabei eine E-Mail zu öffnen ist dabei besonders groß, da der Absender eine bekannte Person sein kann.

Nur ein vorheriges betrachten des E-Mail Headers gibt Aufschluß über den Absender.

Der Betreff ist immer der gleiche und wandelt nur zwischen den folgenden:

Re: Details, Re: Approved, Re: Re: My details, Re: Thank you!, Re: That movie, Re: Wicked screensaver, Re: Your application, Thank you!, Your details.

Im Anhang befindet sich dann eine Datei die NICHT ausgeführt werden sollte, da hier der Wurm dann aktiv wird: your_document.pif, document_all.pif, thank_you.pif, your_details.pif, details.pif, document_9446.pif, application.pif, wicked_scr.scr, movie0045.pif.

In der Registry benötigt der Wurm dann die nachfolgenden Einträge, um sich mit dem Betriebssystem zu starten und permanent aktiv zu werden:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

"TrayX" = C:\WINNT\WINPPR32.EXE /sinc

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

"TrayX" = C:\WINNT\WINPPR32.EXE /sinc .

Weiterhin ist der Wurm zu erkennen, wenn man folgende Dateien auf dem Computer finden kann: %systemroot%\WINPPR32.EXE sowie %systemroot%\WINSTT32.DAT.

Nach dem ausführen des Anhangs werden die beschriebenen Einträge in die Registry von Windows

eingetragen.

Durch eine eigene SMTP Engine ist der Wurm nicht auf Outlook angewiesen und kann sich selbst verschicken sofern ein Computer infiziert wurde.

Betroffen von diesem Wurm sind wie so oft Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT sowie Windows XP Systeme.

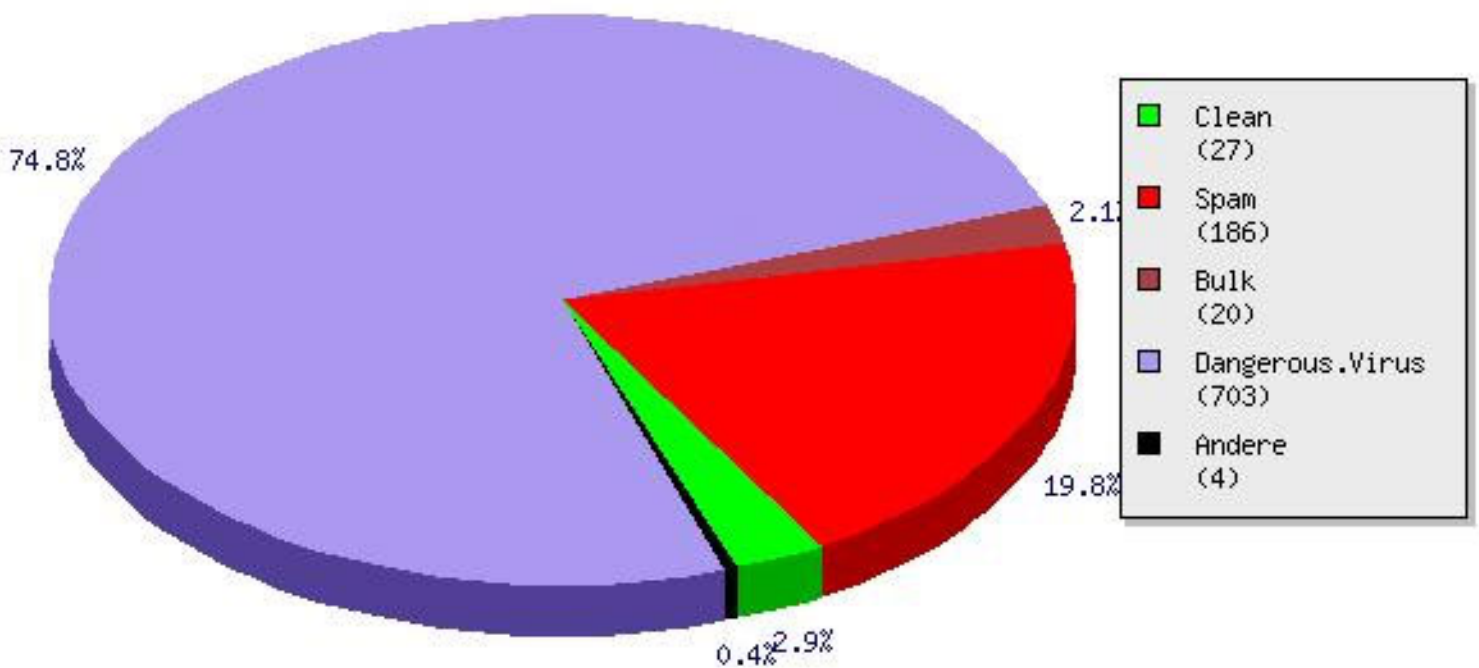
Absicht des SOBIG.F Wurm ist es, eine Verbindung über das NTP (Network Time Protocol) Protokoll auf Port 123/UDP herzustellen und im Wurm integrierte Master-Server zu connectieren.

12.158.102.205; 12.232.104.221; 24.197.143.132; 24.202.91.43; 24.206.75.137;
24.210.182.156; 24.33.66.38; 61.38.187.59; 63.250.82.87; 65.177.240.194; 65.92.186.145;
65.92.80.218; 65.93.81.59; 65.95.193.138; 66.131.207.81; 67.73.21.6; 67.9.241.67;
68.38.159.161; 68.50.208.96; 218.147.164.29.

Zu den nachfolgend aufgeführten NTP Servern versucht dann der SOBIG.F Kontakt aufzunehmen:
200.68.60.246; 62.119.40.98; 150.254.183.15; 132.181.12.13; 193.79.237.14; 131.188.3.222;
131.188.3.220; 193.5.216.14; 193.67.79.202; 133.100.11.8; 193.204.114.232; 138.96.64.10;
chronos.cru.fr; 212.242.86.186; 128.233.3.101; 142.3.100.2; 200.19.119.69; 137.92.140.80;
129.132.2.21.

Mittels einer Firewall kann in so einem Fall zusätzlich für Schutz gesorgt werden, in dem der Traffic nach außen dahingehend unterbunden wird.

Mailtypenverteilung gesamt (Mailanzahl)
(31.7.2003–31.8.2003) Stand: 31.8.2003 13:25:47



eXpurgate®.net

Grafik von www.eleven.de / Auszug aus dem Spam- & Virusfilter der das Aufkommen zeigt

Relevante Links & Verweise:

Hacking Intern (deutsch)

Kapitel 2 / Seite 101 ff; Virtuelle Hacker: Viren, Würmer und Trojaner

Rokop-Security Anti-Virus Test // Aktuell 08/03 (deutsch)

<http://www.rokop-security.de/main/article.php?sid=629&mode=thread&order=0>

McAfee Stinger Programm // Programm gegen die 20 Aktuellen Viren, kostenlos (englisch)
<http://vil.nai.com/vil/stinger/>

Removetool SOBIG.F von Sophos:
<http://www.sophos.com/misc/sobigsfx.exe>

Manuelles Entfernen: (englisch)
<http://www.sophos.com/support/disinfection/sobigf.html>

Informationen von TrendMicro: (engl. / deu.)
http://de.trendmicro-europe.com/enterprise/security_info/ve_detail.php?VName=WORM_SOBIG.F

NTP Distribution: (englisch)
<http://www.eecis.udel.edu/~mills/ntp/html/index.html>

MSBLASTER überflutet das Internet: (deutsch)
<http://www.brain-pro.de/risk.htm>

Computerviren - ständige Begleiter von E-Mails (deutsch)
<http://www.brain-pro.de/Seiten/virenkits/viren.html>

Linuxwürmer - eine neue Bedrohung (deutsch)
<http://www.brain-pro.de/wurm.html>

McAfee Sobig Definition: (englisch)
<http://de.mcafee.com/virusInfo/default.asp?id=helpCenter&hcName=sobig>

Trojaner-Info Seiten zu Computerviren: (deutsch)
<http://www.trojaner-info.de/viren/virentipps.shtml>

Respektvolle & Beste Grüße

Marko Rogge :: IT-Security Consultant unter Mitwirkung von MoMolly, Bernd Michler, Dirk Kollberg und Mixer // Danke

Brain-Pro Security Coburg

E-Mail: mr@brain-pro dot de

<http://www.brain-pro.de>

Tel.: +49 (0) 162-1964818

01.09.2003

Dieser Artikel:

<http://www.brain-pro.de/sobig.htm>