Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« Government Employee Uses DHS Database to Track Ex-Girlfriend | Main | Remote-Controlled Toys and the TSA »

October 4, 2007

The Storm Worm

The Storm worm first appeared at the beginning of the year, hiding in e-mail attachments with the subject line: "230 dead as storm batters Europe." Those who opened the attachment became infected, their computers joining an ever-growing botnet.

Although it's most commonly called a worm, Storm is really more: a worm, a Trojan horse and a bot all rolled into one. It's also the most successful example we have of a new breed of worm, and I've seen estimates that between 1 million and 50 million computers have been infected worldwide.

Old style worms -- Sasser, Slammer, Nimda -- were written by hackers looking for fame. They spread as quickly as possible (Slammer infected 75,000 computers in 10 minutes) and garnered a lot of notice in the process. The onslaught made it easier for security experts to detect the attack, but required a quick response by antivirus companies, sysadmins and users hoping to contain it. Think of this type of worm as an infectious disease that shows immediate symptoms.

Worms like Storm are written by hackers looking for profit, and they're different. These worms spread more subtly, without making noise. Symptoms don't appear immediately, and an infected computer can sit dormant for a long time. If it were a disease, it would be more like syphilis, whose symptoms may be mild or disappear altogether, but which will eventually come back years later and eat your brain.

Storm represents the future of malware. Let's look at its behavior:

1. Storm is patient. A worm that attacks all the time is much easier to detect; a worm that attacks and then shuts off for a while hides much more easily.

2. Storm is designed like an ant colony, with separation of duties. Only a small fraction of infected hosts spread the worm. A much smaller fraction are C2: command-and-control servers. The rest stand by to receive orders. By only allowing a small number of hosts to propagate the virus and act as command-and-control servers, Storm is resilient against attack. Even if those hosts shut down, the network remains largely intact, and other hosts can take over those duties.

3. Storm doesn't cause any damage, or noticeable performance impact, to the hosts. Like a parasite, it needs its host to be intact and healthy for its own survival. This makes it harder to detect, because users and network administrators won't notice any abnormal behavior most of the time.

4. Rather than having all hosts communicate to a central server or set of servers, Storm uses a peer-to-peer network for C2. This makes the Storm botnet much harder to disable. The most common way to disable a botnet is to shut down the centralized control point. Storm doesn't have a centralized control point, and thus can't be shut down that way.

   This technique has other advantages, too. Companies that monitor net activity can detect traffic anomalies with a centralized C2 point, but distributed C2 doesn't show up as a spike. Communications are much harder to detect.

   One standard method of tracking root C2 servers is to put an infected host through a memory debugger and figure out where its orders are coming from. This won't work with Storm: An infected host may only know about a small fraction of infected hosts -- 25-30 at a time -- and those hosts are an unknown number of hops away from the primary C2 servers.

   And even if a C2 node is taken down, the system doesn't suffer. Like a hydra with many heads, Storm's C2 structure is distributed.

5. Not only are the C2 servers distributed, but they also hide behind a constantly changing DNS

5. Not only are the C2 servers distributed, but they also hide behind a constantly changing DNS technique called "fast flux." So even if a compromised host is isolated and debugged, and a C2 server identified through the cloud, by that time it may no longer be active.

6. Storm's payload -- the code it uses to spread -- morphs every 30 minutes or so, making typical AV (antivirus) and IDS techniques less effective.

7. Storm's delivery mechanism also changes regularly. Storm started out as PDF spam, then its programmers started using e-cards and YouTube invites -- anything to entice users to click on a phony link. Storm also started posting blog-comment spam, again trying to trick viewers into clicking infected links. While these sorts of things are pretty standard worm tactics, it does highlight how Storm is constantly shifting at all levels.

8. The Storm e-mail also changes all the time, leveraging social engineering techniques. There are always new subject lines and new enticing text: "A killer at 11, he's free at 21 and ...," "football tracking program" on NFL opening weekend, and major storm and hurricane warnings. Storm's programmers are very good at preying on human nature.

9. Last month, Storm began attacking anti-spam sites focused on identifying it -- spamhaus.org, 419eater and so on -- and the personal website of Joe Stewart, who published an analysis of Storm. I am reminded of a basic theory of war: Take out your enemy's reconnaissance. Or a basic theory of urban gangs and some governments: Make sure others know not to mess with you.

Not that we really have any idea how to mess with Storm. Storm has been around for almost a year, and the antivirus companies are pretty much powerless to do anything about it. Inoculating infected machines individually is simply not going to work, and I can't imagine forcing ISPs to quarantine infected hosts. A quarantine wouldn't work in any case: Storm's creators could easily design another worm -- and we know that users can't keep themselves from clicking on enticing attachments and links.

Redesigning the Microsoft Windows operating system would work, but that's ridiculous to even suggest. Creating a counterworm would make a great piece of fiction, but it's a really bad idea in real life. We simply don't know how to stop Storm, except to find the people controlling it and arrest them.

Unfortunately we have no idea who controls Storm, although there's some speculation that they're Russian. The programmers are obviously very skilled, and they're continuing to work on their creation.

Oddly enough, Storm isn't doing much, so far, except gathering strength. Aside from continuing to infect other Windows machines and attacking particular sites that are attacking it, Storm has only been implicated in some pump-and-dump stock scams. There are rumors that Storm is leased out to other criminal groups. Other than that, nothing.

Personally, I'm worried about what Storm's creators are planning for Phase II.

This essay originally appeared on Wired.com.

EDITED TO ADD (10/17): Storm is being partitioned, presumably so parts can be sold off. If that's true, we should expect more malicious activitity out of Storm in the future; anyone buying a botnet will want to use it.

Slashdot thread on Storm.

EDITEDT TO ADD (10/22): Here's research that suggests Storm is shinking.

EDITED T OADD (10/24): Another article about Storm striking back at security researchers.

Posted on October 4, 2007 at 6:00 AM • 115 Comments

To receive these entries once a month by e-mail, sign up for the Crypto-Gram Newsletter.

Comments

Phase II? That's something scary that I didn't think of...

Posted by: Anonymous at October 4, 2007 6:47 AM

Bruce,

It was funny how about a year ago when I made comment about "Guns for Hire" as a threat that was

It was funny how about a year ago when I made comment about "Guns for Hire" as a threat that was atleast 18 months old the prevailing sentiment was as a threat it was treated as being a bit of a "scare story".

http://www.schneier.com/blog/archives/2006/12/...

Ho Hum time move on...

Posted by: Clive Robinson at October 4, 2007 6:57 AM

Whatever platforms host Total Information Awareness, I think the end users are Windows machines, which would allow Storm not only to spy on the spies, but would give Storm the option of subverting the system and becoming its most important customer.

Posted by: Roy at October 4, 2007 7:11 AM

Why does evil have to be so awesome?

Posted by: jay at October 4, 2007 7:11 AM

Don't forget Storm's auto-dos on security researchers:

If you have a program following the URLs in a large spam feed, and visit a URL more than X times in Y seconds, Storm respnods with an ?automatic? DDoS attack.

Posted by: Nicholas Weaver at October 4, 2007 7:22 AM

> Unfortunately we have no idea who controls Storm ...

Almost sounds like a Government operation.

Oh, except for "The programmers are obviously very skilled."

:-]

Posted by: Conspiracy at October 4, 2007 8:27 AM

> Not that we really have any idea how to mess with Storm.

That's too bad - I would have expected a preeminent security guy such as yourself to have some ideas.

Posted by: Anonymous at October 4, 2007 8:28 AM

The controllers of Storm aren't necessarily "planning" anything for Phase II. They have a massively-distributed computer - eventually they'll think of new uses for it. Eventually one of those uses will be especially harmful.

It could be that they are planning to maintain its current low level of activity indefinitely, in order to keep it at its current level of "not worth doing much about". So "Phase II" might not happen unless/until it changes ownership.

I wonder how many people currently have the keys to Storm.

Posted by: SteveJ at October 4, 2007 8:31 AM

As powerful as Storm is now, how much more powerful could it become?

Consider that adding PS3s pushed Folding@Home over a PetaFLOP...

Posted by: Anonymous at October 4, 2007 8:44 AM

Sorry the URL for Folding@Home story didn't come through, here's another try...

http://www.extremetech.com/article2/...

Posted by: Anonymous at October 4, 2007 8:46 AM

The question is what happens if storm comes out of control. If the "key" to storm leaks out. And comes i nthe hands of different groups. Maybe someone who sees his goal in purifying the net of every pedopornographic site? Someone who wil lcensor something?

What if someone ports storm for other platforms? imagine a Storm-"client" for mobile phones. Shared through bluetooth in a subway station of NYC. Or London. Or even just Milano? How many people would accept a shared file.. maybe named intrestingly (and we have seen that the guys behind storm are really skilled when it comes to social engineering). One out of hundert? That's enough to infect thousends if not millions of people during only one day.

just some random thoughs..

Posted by: ramsesoriginal at October 4, 2007 8:49 AM

Bruce,

Thank you very much for getting to the point of what's actually scary about Storm. There are anti-virus research blogs that focus on what filename it's using today, or the fact that it's distributing itself as a greeting card this week. You can almost feel the wind of the point flying right over their head.

Posted by: Wesley McGrew at October 4, 2007 8:58 AM

"Redesigning the Microsoft Windows operating system would work."

I disagree. Users are enticed to voluntarily click on the attachments and start the "payload." If we all switched to Linux or Mac today, then the worm would just be recompiled.

Sure, you could stop the worm if you changed the operating system to only run authenticated software (i.e., that is cryptographically signed), with the ability to blacklist software. (So that the OS vendor could disable software that the author registered under a false identity and that later turned out to be malicious.) But that would pretty much destroy freeware as well.

The key, in my opinion, is to follow the money. If Storm was implemented for profit, and the presumed ability to rent the botnet will be its downfall, using good old investigative work.

Posted by: FP at October 4, 2007 9:02 AM

I know this is said all the time, and I sound like a fan boy, but here is another reason to use Linux. Secure by design(you don't believe me, go look at the code and find a major vulnerability) as opposed to designed with all kinds of holes but you only know what they are once they have been used against you. Open source all the way.

Posted by: Nathan at October 4, 2007 9:15 AM

We have to at least try to stop the spread:

1) Microsoft has to allow pirates to get patches

2) ISPs disconnecting customers who are infected

3) ISPs have to stop home DSL lines from unlimited outgoing SMTP

Posted by: Another Anon at October 4, 2007 9:16 AM

@FP

Great idea and it would work in the US, or the EU, but if the controllers of storm are Russian, than traditional detective work may not be as effective unless it draws the ire of the Kremlin. Then watch out.

If Putin puts his mind to it they can be found. If he really puts his mind to it, they will never be found ... alive.

Posted by: Spider at October 4, 2007 9:18 AM

Q: How do you disperse a storm?

A: Make it rain.

Posted by: A. Poser at October 4, 2007 9:28 AM

">Storm began attacking anti-spam sites
> focused on identifying it and the
> personal website of Joe Stewart,
> who published an analysis of Storm.".....

Well, I guess we'll know what's happened if we cant read your blog for a few days Bruce.

Posted by: nzruss at October 4, 2007 9:30 AM

Windows, MacOS X, Linux and other *nixes
are vulernable to viruses, worms and trojans to some extent due to too much ambient authority.
Which is what. Well, it is best explained (imo) with an example. Solarite for instance only needs to be able to open a window to draw itself in and the highscore file. Yet it can open an tcp or udp socket, read all the users files, overwrite them, upload them, download new instructions.
So I point the curious to an answear: POLA (principle of least authority)

see also http://erights.org/

ps. forgive my poor spelling, english is only my second language.

Posted by: Any Mouse at October 4, 2007 9:35 AM

Ah the joys of using a Mac (or Linux). No worries about worms or viruses. Who's going to waste time writing a real-world exploit for platforms with a combined 10% market share?

(and before someone says "if everyone used Macs/Linux then they would have malware" all I can say is "if" you aunt had balls, she'd be your uncle)

Posted by: Mark at October 4, 2007 9:37 AM

@FP: "that would pretty much destroy freeware as well."

I don't agree. Supposed that under HypotheticalOS, X.509 is used to sign code from trusted roots installed on the machine. Distributors need either to:

1) Get an X.509 certificate from a suitable trusted root. Getting such a certificate should not be too difficult for any company or organisation. Provided that certificates are revocable, and are associated with a real person or organisation who can be identified if the certificate is used to sign malicious code, something like Storm which is morphing every 30 minutes becomes impractical, because if an AV firm fingers your malware, you lose the trusted certificate, not just the particular chunk of code they've identified.

Note that the scheme doesn't need to provide *trust*, it only needs to provide *audit*. We don't really care if one person gets hacked, provided that the malware doesn't become epidemic before the signing certificate is identified and revoked. So the certificates don't need to be any more expensive than, for example, SSL certs already are, because they only assert the identity of the author of the code, not any kind of trustworthiness. So there will still be malware, but it will be shorter-lived.

OR

2) You need the people you're distributing code to to be "power users" who can create their own self-signed X.509 certificate, add it to their OS's trusted store (the OS would of course have to be designed

to ensure that this cannot be done programmatically), and use it to sign the code you send them. That should be a complicated enough process that people won't be "clicking on" executable content in emails, but it doesn't prevent anyone from shooting himself in the foot, if that's what he really wants to do. Freedom prevails, but having shot yourself in the foot, at least the malware can't shoot all your friends in the foot too just by sending them "click this" emails.

I think that between them, these two cases cover the majority of free software: either it's distributed by a well-funded organisation (GNU, Mozilla, Sun, etc) or it's distributed to power-users. Everything else is software written by nobodies, for the average user. Most this is Flash games which can safely run in a tight enough sandbox that serious malware isn't possible.

If all this were done, then malware would, in order to propagate, have to exploit genuine flaws in HypotheticalOS and its applications. That's a much smaller attack surface than "anything the user clicks on".

Posted by: SteveJ at October 4, 2007 9:48 AM

So far, my firewall, antivirus, and antitrojan software is functioning and has caught all attempts of Storm Worm. Also, gmail always places these storm worm emails in spam designated folders.

I always forward these to both SpamCops and CastleCops within a couple of hours of receiving them.

Recent denial of service attacks against CastleCops have resulted in botmasters being placed on fair warning and one caught today.

Posted by: Anonymous at October 4, 2007 10:04 AM

If you were a medium-sized ISP and had fairly detailed records of your customers' message traffic, do you think it would be at all difficult to identify the customers infected by Storm?

Am I the only one hoping that NSA is already doing this?

Posted by: Peter Pearson at October 4, 2007 10:06 AM

I have a biological background, and the Storm Worm is interesting to me because it is similar to the techniques viruses use to constantly evade our attempts to eradicate them. I've been wondering when these guys would start implementing these principles.

1. Directed evolution in HIV selects for a reverse transcriptase that "works" but has a relatively high error rate. This means that some viral RNA will not be transcribed properly and will not form an infectious particle. The others that make it will eventually encode a modified reverse transcriptase that no longer binds inhibitor, and the virus will eventually rebound in the presence of antiviral drugs. The worm morphs to evade detection.

2. Paul Ewald has a hypothesis that states that the severity of an infection has a relationship with the method it uses to spread. Cholera can be as nasty as it wants in a village with a contaminated water supply if all of the villagers use it and it doesn't have to spread from person to person.
The flu would not spread as easily if it didn't have the 24 to 48 hour incubation period that allows the individual to spread the virus. It seems the programmers realized the same thing.

3. Viruses will sometimes integrate into the host's genome and stay dormant for years until some event triggers expression (HSV, chicken pox, and bacteriophages). The host has no way to detect this DNA, and it can even pass from generation to generation.

Neat stuff.

Posted by: jgk at October 4, 2007 10:10 AM

"I'm worried about what Storm's creators are planning for Phase II" Burn every Windows machine from the surface of the earth ?

Posted by: rjolly at October 4, 2007 10:13 AM

Nathan: Have a look...

"rPath Security Advisory: 2007-0206-1
Published: 2007-10-03
Products: rPath Linux 1
Rating: Severe
Exposure Level Classification:
Remote Deterministic Unauthorized openssl=/conary.rpath.com@rpl:devel//1/0.9.7f-10.10-1

rPath Security Advisory: 2007-0205-1
Published: 2007-10-03
Products: rPath Linux 1
Exposure Level Classification:
Local System User Deterministic Privilege Escalation Updated Versions:
xorg-x11=/conary.rpath.com@rpl:devel//1/6.8.2-30.11-1
xorg-x11-fonts=/conary.rpath.com@rpl:devel//1/6.8.2-30.11-1
xorg-x11-

rPath Security Advisory: 2007-0204-1
Published: 2007-10-03
Products: rPath Linux 1
Rating: Major
Exposure Level Classification:
Indirect User Deterministic Denial of Service Updated Versions:
qt-x11-
Package : linux-2.6
Vulnerability : several
CVE ID : CVE-2006-5755 CVE-2007-4133 CVE-2007-4573 CVE-2007-5093

Several local vulnerabilities have been discovered in the Linux kernel that may lead to a denial of service or the execution of arbitrary code. "

This is only two days worth. You are a fan-boy. Do your homework.

Posted by: pegr at October 4, 2007 10:27 AM

Worms etc have one more problem if Linux is the target. And thats diversity.

There are a lot of different Linux's out there with different configurations and different versions of different binary packages. It would be much more difficult to develop virus type code that would work on the majority of Linuxs boxes compared to windows.

this is why commercial vendors a reluctant to support "Linux" and instead support RE v X.XX.XX or whatever.

Posted by: greg at October 4, 2007 10:28 AM

The techniques used by this also mirror techniques used in terrorist cells to communicate without compromising security. It would be interesting to do a side by side.

Posted by: mark at October 4, 2007 10:30 AM

Pegr,

If you took three average grandmothers, gave one a Mac, one an Ubuntu Linux box, and the third a Windows PC, all running the latest operating systems set to their default settings, with a broadband net connection and turned them loose for a week of random surfing, emailing and so forth, would you take bets at the end of that week which box would have the most malware?

Posted by: Mark at October 4, 2007 10:38 AM

@jgk:

3. Viruses will sometimes integrate into the host's genome and stay dormant for years until some event

triggers expression (HSV, chicken pox, and bacteriophages). The host has no way to detect this DNA, and it can even pass from generation to generation.

It has happened a few times that computer viruses made it onto official software distributions. Recent example: http://news.google.com/news/url?sa=t&ct=us/...

Posted by: MathFox at October 4, 2007 10:41 AM

A better link to the same story: http://www.theregister.co.uk/2007/09/17/...

Posted by: MathFox at October 4, 2007 10:43 AM

This illustrates the problem with the the concept of anti-virus software today.

If the infection is NOT in the list that you have, it does NOT get flagged. Sony's rootkit is a great example of that.

Instead, take a hint from Tripwire and such. Microsoft should publish the md5 checksums, size, date, etc of their files and the STANDARD location of such.

#1. PREVENTION of infection by REDUCING the possible avenues of infection ... but when that fails (or you want to validate your system) ...

#2. VALIDATION of the files on your system. You boot with a LiveCD and check EVERYTHING on your hard drive. At the very least you should be able to validate the boot sector and OS files.

Yeah, that's going to get a little expensive ... but they sell re-writable CD's and DVD's.

And with Jigdo and such it is possible to keep your CD updated with the latest info.

Posted by: Brandioch Conner at October 4, 2007 11:05 AM

@ Peter Pearson: "Am I the only one hoping that NSA is already doing this?"

By "this" do you mean creating bot-net/trojan/viruses?

Me too. But then we dont know who is controlling the bot nets....

and yes... I am wearing a tinfoil hat. :-)

Posted by: Suomynona at October 4, 2007 11:07 AM

Between Postini and Frontbridge, Google and Microsoft are sitting on a rather large assortment of Storm.

Unfortunately for everyone, it's in Microsoft's interest to allow Windows machines of today to be compromised. This allows them to push their "Trusted Computing" agenda in which Microsoft holds all of the keys to all of the software and data which Microsoft decides to allow or disallow on your PC. When Microsoft can demonstrate that their Trusted Computing system successfully fends off Storm (and any successors), they win.

Posted by: derf at October 4, 2007 11:38 AM

Mac and Linux users: Since there is no way of scanning for, and no existing documentation of any viral or malware threats, how do you know your Mac isn't infected and rooted right now?

Posted by: hapbt at October 4, 2007 11:40 AM

@Brandioch Conner

OK, it's not Microsoft published but at http://www.nsrl.nist.gov/
you can find hashes for loads of software, Microsoft included. You just have to trust NIST!

Posted by: Bogwitch at October 4, 2007 11:48 AM

FP:

I beg to differ. While a system that would only run authenticated software could be a pain to use, operating systems could incorporate other mechanisms that would restrict the ability of malware to function and propagate. For instance, something resembling a mandatory access control system could deny permission to write to file systems and network connections to programs running in the context of a mail reader or web browser.

Posted by: Rennie at October 4, 2007 12:12 PM

@Bruce,

I don't know where to start with this. Some of the analysis is dead on, but other parts are really, really off.

First, Storm is NOT a worm, but a virus. It has no self propagating system. It uses humans to do that.

Second, Storm has been used for SPAM and other malware runs on a regular basis. This means that the herders are not just sitting by, it is ACTIVELY BEING USED.

Third, Storm is one of MANY other bots that exist (some even larger), and perform similar functions.

This is a multi-million dollar business for them, and they are doing it pretty well.

The solution is, as you put it, to go after the people running the bots. Just like we go after organized crime, oh wait, the word of the day is: Terrorists.

Posted by: David at October 4, 2007 12:23 PM

Rennie:

Core Force: http://force.coresecurity.com does this. That software, when configured properly, was able to block every exploit I've seen being pushed through the web.

Unfortunately, that solution is completely unsuitable for "regular users", as writing a policy that doesn't break anything major (or that doesn't restrict too little) is beyond the capability of most Windows users. As a matter of fact, but not surprisingly, that (very promising) package seems to have been discontinued.

Posted by: TNT at October 4, 2007 12:23 PM

David, Storm is most definitely NOT a virus, as it doesn't infect executables.

It has a semi-automated propagating system, since it uses email to spread. The user still needs to open the email and click on a link to go on a page that uses exploits, but that is the behavior of many malware pieces that are categorized as (Email) worms.

Posted by: TNT at October 4, 2007 12:27 PM

@Bogwitch
THANKS! I hadn't seen that one before.

It's a bit out of date. By about 4 months. But it does show that it CAN be done.

And, personally, I would consider it a basic requirement for any OS vendor to publish such information THE DAY THE BINARY IS RELEASED in a public site, in a downloadable format, with sufficient bandwidth to handle the demand.

Posted by: Brandioch Conner at October 4, 2007 12:34 PM

@Suomynona

... hopefully you're tinfoil hat is grounded or it won't do much good :)

Posted by: anonymous at October 4, 2007 12:48 PM

"payload -- the code it uses to spread"

No, "payload" is the load you are paying for. The payload is what you're doing all this work spreading to achieve. Think about it: the payload of a missile is the warhead, not the rockets.

Posted by: josh at October 4, 2007 1:03 PM

Estonia recently had a cyber attack on their systems. The internet for the most part is not government regulated, so we should get the government involved…..NOT! Business will love a lot of money, so naturally the Free market will take care of these threats and it might cost us a few bucks….the government would charge more in taxes. We should take a lesson from the Estonian government. I just saw a site about Estonia's Singing Revolution (http://singingrevolution.com).

Posted by: Tanvir at October 4, 2007 1:25 PM

@Nathan:

You are very naive to think that Linux is "secure by design". First of all, what is Linux? What flavor are you speaking of?

Every piece of software has vulnerabilities, because there were humans who wrote it. There are plenty of vulnerabilities targeting Linux (and applications for Linux). This is solely a market-share issue.

Posted by: Dan at October 4, 2007 1:27 PM

"'Not that we really have any idea how to mess with Storm.' That's too bad - I would have expected a preeminent security guy such as yourself to have some ideas."

Me, too.

And when I started researching Storm, I expected to be able to come up with some.

The problem is the distributed nature of the C2 system. We simply can't monitor enough of the net to get at it.

Posted by: Bruce Schneier at October 4, 2007 1:39 PM

"The key, in my opinion, is to follow the money. If Storm was implemented for profit, and the presumed ability to rent the botnet will be its downfall, using good old investigative work."

Agreed. If we're going to stop Storm, we have to go after its controllers. And we have to do that in the real world, not in cyberspace.

Posted by: Bruce Schneier at October 4, 2007 1:41 PM

There is a dark place that no one wishes to look. We avert our gaze if we happen to look in that direction. This dark place is the evil in men's minds; we all have it. It belongs to human nature so resistance is futile. Given this proclivity and the facts about Storm, I present this forum with a question: what real damage can the Storm network perform? If the answer is "none" then we have written a thousand words of naught. Otherwise, we can only wait for the Storm...

Posted by: Cmor Ivestiga at October 4, 2007 2:42 PM

"The key, in my opinion, is to follow the money. If Storm was implemented for profit, and the presumed ability to rent the botnet will be its downfall, using good old investigative work."

Sorry to spoil the fun but what if this is a hostile government program; I cannot help thinking that this is the sort of thing the Chinese army might try.

Whoever's doing it, I have a grudging admiration for their skill.

Posted by: Windows User at October 4, 2007 2:49 PM

Windows User, I really doubt it. It seems much more likely that there's organized crime behind this (and I do mean real world organized crime, not just cyberspace-related crime). Maybe supported by some politicians who guarantees them immunity.

Posted by: TNT at October 4, 2007 3:20 PM

> "So far, my firewall, antivirus, and antitrojan software is functioning and has caught all attempts of Storm Worm."

You mean, all the attempts that you know about. Hopefully that's all the attempts made to infect you so far, but you have to admit there's a non-zero possibility of an attack that hasn't been caught by your firewall, IDS, etc., and thus you wouldn't know about it, if that's how you're seeing whether you've been attacked. That's the tricky part about worms -- you tend to only be able to know you haven't been infected by known variants. It's very, very difficult to say with certainty, "I know I'm not infected by *anything*."

As a Mac user, although I'm pretty sure my system is clean, I can't even say that with certainty -- it's possible that there's some Mac worm out there that nobody's discovered yet. You just don't know, you can only be careful and look for strange behaviors. (A while ago there was an article about forensics on a rootkitted Linux box; the guy only noticed he'd been rooted because the "ls" command started behaving strangely.)

About the only good thing about Storm is that 'following the money' is something law enforcement is reasonably good at doing. I suspect they're probably better, and have more practice, doing that, than they do directly combating viruses and malware in the virtual world. Of course, if the malware is being propagated from a country that doesn't have any functional high-level law enforcement, or where that enforcement is easily subverted (bribed), then there's very little that can be done.

Posted by: Kadin2048 at October 4, 2007 3:39 PM

@hapbt: Offhand, Mac users at least have McAfee's Virex. A quick search reveals NAV, Sophos and Integos as solutions. Plus, it's fairly easy to keep a *nix system locked down, since you don't have to be an administrator to do every last task.

Posted by: tk. at October 4, 2007 3:56 PM

@TNT

"Windows User, I really doubt it. It seems much more likely that there's organized crime behind this ..."

Perhaps. The thing that spooks me about this is the implied discipline of the attackers. Apart from DoS attacks against security researchers, the thing just sits there and breeds. It could be a clever and patient criminal or it could be a weapon being assembled for more serious matters.

You're probably right but I'd have expected most criminals to have tried to use their new toy by now.

Posted by: Anonymous at October 4, 2007 4:08 PM

---

hapbt

Google for a application called Tripwire and be delighted and informed.

Posted by: LB at October 4, 2007 4:35 PM

I hate to disagree with such a revered crowd, but "following the money". doesn't sound like a good long-term solution. This is a beautiful piece of engineering, but most of it was foreseen years ago and much of it could be quite effective even without human maintainance and adjustment. How long will it be be before Storm, or something like it, apppears in the hands of script kiddies?

I'm not an expert, but I think we're looking at the future internet ecology. I think that we'll have to learn to live with the permanent presence of unkillable worms (I don't want to argue zoological terminology) that are so ubiquitous and nimble that trying to kill them one by one is a complete waste of time. Worms that mutate, worms that swap genes, worms that discover new vulnerabilities (like catchy subject lines and OS exploits) without human assistance. I can imagine three or four interesting ways things could play out from there, but not everyone likes science fiction as much as I do...

Posted by: Beta at October 4, 2007 5:07 PM

If I understand fast-flux correctly (based on the writeup here: http://www.kvaes.be/high-availability/... , there needs to be a master DNS record somewhere. Why isn't that record, or the nameserver it's on, a point of vulnerability? The storm software probably has a list of domain names, but it would have to be a fairly short list or the whole botnet would be disorganized while it tried to converge on the currently active DNS records. Bleadingthreats.net listed over 1000 IP addresses of compromised nameservers, but I would expect at some point each storm client has to do a series of SOA and A record queries against a rather small common set of domain names and then branch out from there. Am I missing something in botnet's architecture?

Posted by: False Data at October 4, 2007 6:34 PM

There's almost surely more than one of those out there. I fought something like this last Saturday and won (I hope). One characteristic one mind was that it "ate out" the guts of my anti-virus while leaving an apparently working shell.
Which economies would be hurt most by Storm mounting a coordinated one-time -attack?

Posted by: ForReal at October 4, 2007 6:43 PM

I can't conceive how this effects me. So what if the kernel has a "vulnerability"? Nothing gets installed on this gentoo box unless I give myself root privileges and use the command line.

Posted by: linux-fanboy at October 4, 2007 7:29 PM

Actually attacking Storm is possible, and A. Poser rather oddly got it right:
Q: How do you disperse a storm?
A: Make it rain.

The Storm authors are issuing commands, and a few C2 systems are known at any given time. This is enough information to begin making storm cost too much to use, eliminating it by attrition.

Now I'll freely admit that these are clearly grey hat techniques.

Start by compromising a known C2 with monitoring code, turning it into a honeypot, obviously it is best if this owner (and the future owners) know and agree to be a part of the investigation. When a command is received by the C2, observe where it comes from, these C2-prime systems are closer to C1 (Commander) than the current honeypot.

Repeat the process until the number of upstream C2-primes reduces giving a higher probability of a short trip. Of the consistently closer C2-primes pick a single candidate, the few storm members are compromised the harder the attack will be to locate.

Repeat the process with 2 C2-honeypots to get 3, 4, 5, 6, etc. With a small number of such systems a single root source will begin to emerge, that is C1. Once C1 has been caught continue monitoring the Storm network with the C2-honeypots to gather evidence of anyone else attempting to use the botnet.

This will not be a quick process, but as long as the C2-honeypot owners allow it, it is arguably a white hat process, and with the Storm network unusable without being caught it will die of attrition.

This works from the observation that every C2 is replacable except for C1. Once enough C2 systems are compromised the odds of being caught using a one-time C1 and being detected skyrocket (a C2-honeypot that receives a C2-connect followed by a C2-command has high probability of seeing a one-time C1). This makes the cost of using Storm simply too high, and a few high profile command terminations will make Storm very unprofitable indeed.

This is using the rain to disperse the storm.

Posted by: Joseph Ashwood at October 4, 2007 9:29 PM

I don't know what and how much Storm did until now.

A possibility for it, to do allmost nothing, could be a hacker or hacking group without contact to possible customers.

Not a great movie-plot, indeed.

Posted by: Stefan Wagner at October 4, 2007 10:45 PM

I've seen this 'not great movie' before...Swordfish. We need Hugh Jackman, a comically elaborate computer setup, thumping music, and some BS techno-babble akin to Hackers.

Posted by: Ricky at October 5, 2007 12:18 AM

With due respect to fanboys on all sides, after reading about this threat (and particularly with the similarities to biological viruses) I can't see how anyone would think that a monoculture or near-monoculture (such as we currently endure) is desirable. It seems obvious to me that if 90% of the desktop systems out there are running the same code (regardless of how inherently "secure" that code is deemed), a single flaw or successful attack vector can do a lot of damage.

Linux, at least, has the advantage of not being a monoculture within its own platform; two Linux boxes can have completely different sets of libraries/applications/utilities. Even when the selection of software is the same, some distros apply their own patches or compile options to the upstream code. But in spite of this advantage, a world full of Linux boxes would still have enough in common to be a problem.

I mean, does anyone think that having 3-5 platforms sharing roughly equal chunks of userdom wouldn't help this situation?

Posted by: Alan at October 5, 2007 12:45 AM

"Maybe this is a Singularist trying to bring the Singularity about sooner by building a compute cluster with enough power to invent an AI".

Kidding aside, that's a great writeup, Bruce.

Posted by: Pat Cahalan at October 5, 2007 1:05 AM

Windows XP/Vista actually has very good security; it is afterall used in most financial institutions and a large number of defense establishments.

The crux of the problem is that for consumer PCs all the security is turned off! Now there are several good logical reasons for this:
- Most home users will not have a windows "Domain" already set up and setting up a security Domain is way beyond the abilities of the average consumer.
- Ease of use, quick setup are major selling points for consuler PCs.

On Linux or Mac boxes (because of thier UNIX heritage) it is not possible to turn security off. So all Linuxes and Macs are running with some minimum level of security configured. This is probably the major reason that Linux has such a slow takeup as a consumer product much of the "Difficult to Install" griping is because you need to do some minimal security setup during installation.

Until MS can come up with a way of securiing thier OS out of the box these problems will continue. In my opinion the merginf of the business OS "Windows NT" and consuler OS "Windows 95" into the single "XP" product line is at the heart of the problem. Businesses require complex network based centrally adminiistered security, consumers require simple "works out of the box security" you just cannot downgrade the sophisticated enterprise level NT security model to a "Just Works" consumer product.

The creaky ancient Unix security model scales up (with great difficulty) to the enterprise level, and, also scales down to a single user (with some fiddling on install) -- so for the forseeable future you are safer on a Mac or Linux no matter what thier market share is.

Posted by: supersnail at October 5, 2007 2:23 AM

Re: everyone talking about Linux/MacOSX being more secure..

Remember back in the 70s / early 80s when the gay community was having sex all over the place with no protection? Nothing could possibly go wrong - sure maybe you had a small problem here or something, but a quick trip to the doctor and you're all fixed up. Never anything as life changing as having a kid or anything..

Well, we all know what happened. A culture built on the assumption they were safe (secure) by default without having to do anything all the sudden came crashing down. People died, and they died in horrible ways.

While I'm not suggesting a direct comparison between the Gay community and the Linux community (lets face it Linux users have NOT been persecuted - get over it kid, you're white, straight, and male), but the point is walking around with an attitude that nothing can happen to you because all the problems are straight people...errrr window's users is really naive.

Something will happen, and burying your head in the sand before hand isn't going to save you. Security is everyone's problem.

Posted by: RijilV at October 5, 2007 3:30 AM

There is an easy way to remove the Storm issue:

'format c:'

it is being treated like an epidemic that will kill millions of women & children. It is a stupid computer program on something than can be smashed with a hammer and thrown out for Waste Management to handle. Get a grip people. Back up your data and if you get a nasty you can't remove with software tools reformat and reload. If it because such as problem that most do this then the problem will go away in time.

Posted by: Johnny K at October 5, 2007 7:20 AM

Storm is not a 'worm'; it's a bot. It's delivered by one of several exploits. It has both centralized and P2P-type command-and-control, the latter using what appears to be an eDonkey-derived protocol, according to some reports. It has an auto-DoS feature which targets IP addresses which appear to be probing Stom-botted systems, and it also alerts the botmaster(s), who sometimes choose to launch larger/more sophsiticated manually-triggered DoS attacks. It contains a remote-update mechanism. It is in all probability owned and operated by the Russian Business Network.

Posted by: Roland Dobbins at October 5, 2007 7:52 AM

One of the recommended practices for all desktop users is to run with restricted rights. Is this not sufficient to block Storm installation and execution?

Posted by: Mike W at October 5, 2007 8:07 AM

"Security is everyone's problem." Agreed. But it is one's problem even more when one makes the most deployed desktop OS, which is the current vector of many nasty things, one should at least do his homework right and not have outstanding bugs unfixed for months.

That said, I'm not here to say that Linux+Mac=42 and are the answer to life, the universe and everything. Yet any unbiased, technically aware person has to agree that win* is less secure in multiple areas. I'm not preaching that linux is perfect, I just say it's more robust against those things.

But what I say even more is that some people should really get a brain and not open about any attached file. No amount of computing will ever compensate for uncleverness.

Back to the gay and aids parallel, what caused this is a major lack of both information and understanding at many levels as to what aids was and how it was transmitted. Today we have proper information on that, and you can be far more safe with simple measures (may it be condoms or tests+fidelity+trust, or both). Yet the information struggles to propagate, while the threat doesn't stop. Indeed the same parallel can be drawn: Linux is in no way a magic barrier to viruses, but a proper tool with a sane reasoning and use leads to a much better protection.

Posted by: Lloeki at October 5, 2007 8:34 AM

"There is an easy way to remove the Storm issue: 'format c:' "

As long as you can get almost everyone infected to issue that command at exactly the same time, then you've got a great solution. Unfortunately, that requires both an unrealistic level of coordination and identification of all (or a substantial majority of) infected machines. It doesn't do you any good to wipe your system if you get re-infected a short time later.

Posted by: Joey at October 5, 2007 10:10 AM

@Johnny K, just so you know there are a few viruses (this isn't one of the) that infect your boot sector so a format won't get them, best practie is to use somthing like DBAN to scrub the whole disk before reinstall, it will also properly destroy any sesitive data so that it cant be recovered if the comp gets in to somone elses hands..

Posted by: Prosthetic Head at October 5, 2007 10:19 AM

---

this is for all the linux fanboys out there

ebay jsut finished their threat assesmants for the storm botnoets..there findings, its nto the windows boxes thatare the biggest threat, its the rootkitted linux boxes used as bot net controllers. security through obscurity just dosn't work guys.

Posted by: moonglum at October 5, 2007 10:38 AM

The point is that *nix provides a robust security fraimwork and privilage sepperation. While nothing can secure against user stupididty or programmer error the nix way of doing things means that there are very few flaws that can be exploited withought a suitabily privilaged user doing somthing to invite it.
The flaws in nixes are generaly found by developers and fixed, whereas the only windows flaws you find out about arte those that have already bitten somone...
I'm not a raving linux fanboy, its not perfict, but it is massivly more secure than windows when both are used properly

Posted by: Prosthetic Head at October 5, 2007 10:59 AM

The point is that *nix provides a robust security fraimwork and privilage sepperation. While nothing can secure against user stupididty or programmer error the nix way of doing things means that there are very few flaws that can be exploited withought a suitabily privilaged user doing somthing to invite it.
The flaws in nixes are generaly found by developers and fixed, whereas the only windows flaws you find out about arte those that have already bitten somone...
I'm not a raving linux fanboy, its not perfict, but it is massivly more secure than windows when both are used properly

Posted by: Prosthetic Head at October 5, 2007 10:59 AM

What about if there *is* no Phase II for Storm? It spreads. It infects machines. It stays quiet enough not to attract attention. Now, what if the goal is *only* to infect machines? A lot of those machines will be corporate and government machines with sensitive information on them, information that can be used or sold. If I were looking for maximum profit, I'd keep my worm quiet until it'd grown sufficiently, then start using it not to attack anyone/anything else but simply to let me see what interesting stuff was available and siphon it off.

There's always a market for corporate and other espionage, witness the McLaren/Ferrari FIA dust-up for example. How much would someone at Ford be willing to pay for complete plans for Chrysler's next model-year cars 6 months before they were announced? How much would Airbus be willing to offer for model year cars 6 months before they were announced? How much would Airbus be willing to offer for the inside scoop on the details of what Boeing was working on for their next aircraft?

How much would those same people be willing to pay to *change* that information, say to introduce problems that'd cripple their competitor's products at a critical time?

Posted by: Todd Knarr at October 5, 2007 11:58 AM

A few quick points.

1) What makes linux secure probably has as much to do with who runs it as qualities of the OS itself. Not many clueless grandmas who click on email links. Of course there is malware for linux but the problem isn't going to be as great simply because the sort of people who run linux are often the sort of people who like updating their box 3 times a week (or who run a server which they leave fairly locked down).

2) The nice thing about the analogy with biological viruses is that it means there won't be a disastorous stage 2. Both viruses and money driven malware programmers want to gain resources (reproduction/money). Brining attention to yourself or causing noticeable damage tends to interfere. If I was one of the guys behind Storm I would already be pretty worried that the NSA and CIA were trying to track me down (at least to know WHO controls all these computers) so I would try not to draw any more attention to myself then necessary. Just rent out the botnet to some low scale crime rings.

3) At this level of sophistication a honey pot solution will prove quite difficult. Sure you can trap some incoming connections but if they are smart enough these will propagate from a bunch of other random infected computers leaving the honeypot researchers no way to tell which direction moves them closer to the ultimate source. If they use cryptographically signed commands getting control of C2 servers won't even let you force uninstalls or anything.

Frankly the most efective solution here is probably good old fashioned police/intelligence work. Find the guys who built it and MAKE them send out uninfection commands. In the long term we should do something about getting these smart russian coders better jobs (like opening up immigration and letting them come here and code useful stuff).

5) If one was really clever one might be able to defeat the honeypot counter entierly. It would require some original crypto research but what you might be able to do is something like this.

Take some standard form of network data that computers receive that is highly variable to the point of being nearly random (maybe something like TTL headers or response times or some other common packet property). Now have each infected host amalgamate all this incoming data in a fashion that depends on some public key. That is the public key tells the worm some way to process the incoming statistical data. Done cleverly enough one might be able to create a system where anyone with knowledge of the public key and access to the statistical corpus could (with very high probability) recover a message being sent from some subset of the computers communicating with this infected host but without a corresponding private key it would be computationally infeasible to determine which of the contributors to the statistical corpus were participating in sending the message.

In other words you might be able to create a situation where every infected system gets it's orders from some set of DNS servers during lookups but it is infeasible to figure out which DNS hosts are participating in sending orders and which are not.

It's kinda the reverse of what a public/private key stenography system would be (where anyone with the public key could hide a message in random looking data but determining a message was hidden would be computationally infeasible without the private key).

Posted by: Truepath at October 5, 2007 12:09 PM

Damn't stupid spelling I meant steganography in that last part not stenography.

Posted by: Truepath at October 5, 2007 12:11 PM

---

if storm uses edonkey/overnet p2p protocol - well, it can be easily identified and blocked by any ids/ips system. yes, it will also eliminate the edonkey itself. not that anyone actually cares.

why does anybody want to allow incoming tcp to desktops on high ports anyway?

Posted by: asdf at October 5, 2007 2:03 PM

Umm.... from a botnet point of view I'm not sure running Linux is as secure as you may think.

Although you can't install applications in system locations, you probably don't need to - the software can live in a users local dir (simply hidden with a leading '.' or innocently named), login scripts can restart it in the users context when they next log in after system reboots (or via cron/at?), and it can run as innocuously named processes (changing to avoid detection). Opening ports to listen and attack isn't a problem at all.

Linux isn't a huge portion of the systems out there, but x86 linux systems are common enough to be worthwhile, especially as linux systems are, on average, attached to fatter/more attractive pipes than your average windows dialup machine..

Sure, it's a lot easier to clean out than a windows version as there are less places for it to hide with only linux user privileges, but that doesn't make you safe.

Posted by: Darren at October 5, 2007 9:16 PM

Linux users are less vulnerable for a number of reasons. I believe the most important reason is security updates. Updates come out more frequently from Linux vendors and Linux users install security updates more frequently than Windows users. A high percentage of Windows boxes are pirated and not even allowed to install many security updates.

---

For PhaseII my guess is they will choose a political reason to launch some large scale attack. According to statements by Russian foreign minister Lavrov the most probable upcoming political conflict seems to be Kosovo. So my guess (speculation) is that PhaseII might be synchronized with a future Russian engagement in the Kosovo-conflict.

Posted by: Alex at October 6, 2007 3:13 PM

The research group I was interning with this summer did some work on disassembling and analyzing storm. (I wrote some visualization / graphing tools.) There was a palpable feeling that this guy was different. I haven't kept up with what's been going on since then. Thanks for posting.

Posted by: randomwalker at October 6, 2007 5:08 PM

As far as that AIDS analogy... remember that a major reason the epidemic got as bad as it did was because the government(s) couldn't be bothered to push research on a disease that only affected "undesirables" like gays, drug users, and Africans. Of course, it turned out that (1) more people were in those groups than most folks realized, and (2) AIDS didn't *stay* confined to those groups...

Posted by: David Harmon at October 6, 2007 9:29 PM

@David Harmon

Another reason is because of the long incubation time, frequently years without any symptoms at all.

There was also no test for a long time, either, even after the HIV connection was made. Basically the only way to tell if you were infected was to die from it.

Posted by: Anonymous at October 7, 2007 12:16 AM

For all the people saying "X is more secure than Y", remember the way Storm spreads: social engineering. It doesn't matter how good your computer security is if the bozo at the keyboard is opening every email and clicking on it and agreeing to anything it tries.

It may be hard to believe people can be that ignorant or apathetic, but while you're arguing about whose security is better, or whether it's a bot, worm, virus, or dessert topping, Storm is quietly spreading to the 99% of users who neither know nor care.

You are coming to a sad realization: allow or deny?

Posted by: Anonymous at October 7, 2007 12:26 AM

There is one solution to a lot of the problems presented by storm and other "infective" agents.

Simply stop using a system where an infective agent can get in even if the user invites it in.

As a simple solution how about using a system where the OS and otehr required programs are stored on imutable memory (say a DVD for arguments sake). The user files are stored on appropriate mutable memory and scanned by the OS as part of write/modifiy/read. For 90-95% of computer users this would be sufficient as they do not produce exacutable code as part of their work based activities

If you think this sounds a lot like a Knoppix based system with a thumb drive, as a solution it would be a step in the right direction. However you would still need the corectly implemented scanning part both for the mutable storage and memory used to run the OS.

Posted by: Clive Robinson at October 7, 2007 9:01 AM

Following Gutmann's post on this I wondered what would be the capability if a botnet this large seeded a distributed service client to it's zombies and started cracking - I don't know enough about encryption to know what schemes this would bring in to doubt, but it would certainly give the authors an incentive to keep relatively "quiet". I'm waiting for phase II too.

Posted by: rdsc at October 7, 2007 9:30 AM

To bulid on what Alex said above:

updates are very important to preventing system compromise. Arguably, windows and linux are on par with eachother. However, linux has a far superior application update infrastructure compared to windows, and that should make all the difference. That, and far fewer people are forced to "run as admin".

Posted by: nordsieck at October 7, 2007 12:43 PM

Anonymous, Storm doesn't spread with social engineering.

If user clicks on the link on a machine that's not vulnerable to the browser exploits that Storm uses, he's not going to get infected anyway. To say Storm relies on social engineering to spread is simply false.

Posted by: TNT at October 7, 2007 6:15 PM

@TNT

To pretend storm DOESN'T rely on social engineering is equally false.

Posted by: Anonymous at October 7, 2007 8:39 PM

You know what? The Storm virus reminds me of this little game where player takes the role of a "strong" AI, and takes over various PCs and servers worldwide to harness their computational power http://www.emhsoft.com/singularity/

Posted by: passer-by at October 8, 2007 3:24 AM

Anonymous, the amount of people who get infected because they manually download and execute the file is vastly inferior to the amount of people who get infected through the exploits. If people were infected just by social engineering, Storm would be a much lesser problem.

Posted by: TNT at October 8, 2007 9:28 AM

Ouch.

Quite a long flamebait about Windows/Linux/Mac security by people who apparently don't have a clue

Quite a long flamebait about Windows/Linux/Mac-security by people who appearently don't have a clue about what security really is (exception: Any Mouse).

My suggestion: go on with your lives without calling acl-systems secure until you've read about and understood capability based security.

That is security by design.

4 days ago here was a wise guy, but he was ignored... weird

Posted by: borgåbo at October 8, 2007 4:06 PM

BLAH, we went from chatting about storm to ALWAYS "this is more secure, that is more secure, heres why, heres why not" I wish we could just concentrate on STORM instead of itching at eachother about the pros and cons of a system. You know, if we actually spent the time we do bickering about who's more secure, we MIGHT be able to defeat storm, or produce more and better security products to protects of from threats like storm. (This isn't going to happen considering the time people tend to WASTE for their bickering comments.)

Posted by: Stop Fighting at October 8, 2007 6:52 PM

Bruce,
Very, very important and scary information. As much as we IT professionals repeat the credo, "Treat every email as if it contains a virus," it is through articles like yours that the message is best delivered. It allows us to point our user community to an external source that not only reinforces what we've been telling them, but makes it abundantly clear that we are neither kidding nor being overly cautious. By the way--the parallels to current global terrorism are obvious. Let's hope the two are not as closely related as I fear they are. - Roy

Posted by: Roy Atkinson at October 8, 2007 7:09 PM

How do I get a copy?

I need to infect one of my OWN computers - so I can test removal techniques. How do I get a copy of the Storm Worm? Sadly, none of my customers have gotten it, so its not like I can just "take a copy" from their computer.

Heck - let me make it easier for you: Here is my email address: j1076366@hotmail.com please put STORM WORM in the subject line - so that my filters will pick it up - and that my anti virus programs will not filter it out!

Thank you,

Posted by: computer virus removal at October 9, 2007 4:07 AM

Reconstructer has a paper (PDF) available in the downloadable ZIP file titled "Peacomm.C - Cracking the nutshell.zip" with disassembly of the Storm Worm code.

http://www.reconstructer.org/papers.html

Note that there is a 2nd ZIP within the first with *infected binaries*. The 2nd ZIP is password-protected, so you cannot simply drag the infected files out. Not that I'd want to do that, but I did not find the password on the site or in the ZIP to do so.

The paper covers the various encryption, packing, phony file headers, rootkitting, VM-detection, firewall-poking, anti-debug tool defeating, SFC (system file checking) bypassing, explorer.exe hooking techniques employed by Peacomm (aka Storm Worm or NuWar or other names).

One can safely extract the analysis PDF (same name as the ZIP) without messing with the 2nd ZIP. PDF is 22 pages.

Posted by: Al at October 9, 2007 4:33 PM

For a list of Windows sites infected with Storm, see www.spamtrackers.eu/downloads/botnets. You can see what spamming brands and phishing operations are running on the Storm botnet. Where owners of those brands are identified, you can check that out at www.spamtrackers.eu/wiki. Leo Kuvayev is the hottest contender.

And for the Linux lovers, there is a list of infected machines used by Alex Polyakov at www.parmalert.zoomshare.com. together with the spam brands using them.

For a list of C&C nodes for Storm, you can find those posted in the honeypot project's site.

There is one and only one antidote to the Storm plague. The arrest and incarceration of the Russian/Ukrainian gang who devised and maintain it, together with their affiliates who are benefiting from it.

Posted by: Botnet Tracker at October 9, 2007 7:21 PM

(Minor corrections to previous posting)

For a list of Windows sites infected with Storm, see http://www.spamtrackers.eu/downloads/botnets

You can see what spamming brands and phishing operations are running on the Storm botnet.
Where owners of those brands are identified, you can check that out at
http://www.spamtrackers.eu/wiki
or just follow the links for each brand. Leo Kuvayev
(http://www.spamtrackers.eu/wiki/index.php?...) is the most likely perpetrator.

And for the Linux lovers, there is a list of infected machines used by Alex Polyakov
(http://www.spamtrackers.eu/wiki/index.php?...) at http://www.pharmalert.zoomshare.com together with the spam brands using them.

For a list of C&C nodes for Storm, you can find those posted in the honeypot project's site.

There is one and only one antidote to the Storm plague. The arrest and incarceration of the Russian/Ukrainian gang who devised and maintain it, together with their affiliates who are benefiting from it.

Posted by: Botnet Tracker at October 9, 2007 7:32 PM

Bruce, I'd like to thank you for addressing this. You mentioned how the creators are using subject lines that are very enticing to people reading the email. I think part of the education of infections should involve the concept of social engineering, and as more people become aware of what it is, maybe less will fall victim to infections.

Posted by: identity theft at October 9, 2007 9:04 PM

Cyber Threat Analysis has a technical report on Storm available here as a PDF download:
http://www.cyber-ta.org/pubs/StormWorm/

Found via SANS:
http://isc.sans.org/diary.html?storyid=3481

Posted by: Al at October 11, 2007 7:57 PM

@al: password for the malware files at reconstructer is: infected

Posted by: jumbo at October 12, 2007 2:10 PM

We can't fix the root cause, because users can always be duped into running untrusted executables. We can't detect and block it, because
the creators will adapt the code. We can't block its behavior on a system-wide basis, because what it does is entirely valid for a single host.

But there are other options!

For example, let's say that Microsoft hid Storm detection in the Windows kernel, and pushed it out as a critical update. It detects the worm -- using signatures, filenames, rootkit detection, etc, the same stuff an antivirus program can do

But it doesn't actually do anything about it. Windows doesn't clean the infection, it doesn't block the worm, and the creators never know that
they're being watched.

But when the huge botnet starts attacking the root DNS servers and the Internet starts to suffer, Microsoft flips a magic switch, a special code is pushed out to the normal Windows update site that every computer checks periodically, and every infected computer suddenly deletes the worm. Internet saved.

Stupid, yes, but the point is... when trying to come up with a solution, be creative! It's a new and interesting problem and the real solution will definitely be unique.

Posted by: Jim at October 15, 2007 1:10 AM

I wonder if it truly would be unethical to design a "counterbot". Counterbot? You know, use the same technology, viz. distributed command and control, polymorphism, the works.

After all, people generally recognize that viewing ads is just something you learn to live with if you're going to spend time on the net. (Some people have ad eliminating software, but I don't mind letting vendors try to earn a buck from me. Nothing says I have to click on anything. And I can block the most pernicious ones, eg. pop-ups.)

So, why not teach people to expect PC-scanning, counterbot-installing securityware as the price of visiting major sites (e.g. google, msn, etc.)? Especially when it's in their own interests, in the long run.

Perhaps the only thing about the scheme that would bother me (on a first pass, anyway) is the disclosure aspect. Do we need to provide a splash-screen with EULA, etc? If so, (justly) paranoid people may refuse it. And no one wants to mandate something like this for their services, because they lose market share to their competitors that don't require it.

But suppose there were some kind of cooperative, industry-wide initiative -- the kind of cooperation that we see in WBEM, various net protocols, etc.? If the "counterbots" were developed by industry for consumers, they could be adopted more-or-less at once by multiple competing organizations.

Hmmm... As I think about it, there's also the issue of "who's in charge". Maybe set up a foundation to pay for a few "command and control" types, under the auspices of the umbrella organization.

Just thinking out loud...

Posted by: coyoteworks at October 17, 2007 8:44 AM

You silly humans understand so little.

Posted by: Storm at October 17, 2007 9:15 AM

More on the "counterbot" idea. I can't seem to be able to drop it, now that it's in my head. So, here's more. But first a few quick intro thoughts...

Think about it. Do you really believe that the "bad guys" are that much smarter than the "good guys"? What are the chances, statistically speaking? In truth, the chances are essentially zero that the very smartest .01% of the world's population are *all* making botnets. So, assume that the good guys are just as well equipped intellectually.

Why are the good guys continuing to get trounced, then? Think about chess. If you take the defensive, only responding to the aggressor's moves, you'll almost always lose, even to an inferior opponent. You have to take the offense to the other side -- you have to attack.

Quite simply, the bad guys are winning because they know all the cards in our hands. They have servers equipped with all the software that we use to detect their shenanigans, and they test their new stuff against it. Of course they're always going to stay a step ahead!

But now take a quick look at wikipedia's entry on the "t-cell" (http://en.wikipedia.org/wiki/T-cell). The immune system is amazingly complex, with an almost bewildering variety of specialized cells, each contributing to a larger whole.

Suppose that someone really smart wrote a program that could copy itself around the net, while transmogrifying itself so that the bad guys would never have a good copy on hand. Suppose, furthermore, that the "payload" did something like this: (1) hide myself (2) monitor for strange behavior (heuristics based, not signature based) (3) check to see if anti-malware is installed (4) if strange behavior detected, send out for help.

The cry for help is detected by a server that consequently sends the "mega-payload". This payload does something like this: (1) quarantine the files detected by the "detector" program (2) send an alert to the end user alerting them to the problem (3) if no anti-malware installed (see above), then send a message to the end user (4) delete itself (but not the detector), so as to avoid detection by future malware.

Some possible objections:
(1) invasion of privacy
(2) incompatibility -- the thing breaks other software
(3) who's in charge?
(4) antivirus products will destroy the "immunityware"

Replies:
(1) See my previous comment
(2) If the storm botnet can hide itself well enough never to be detected, then it must not be conflicting with much software. Ergo we can do the same. Nothing is perfect, but this would be a small price to pay.
(3) Easy -- no one. You get some smart people who distribute newer, better versions of the immunityware, but they don't even have to control it. Just let it go. (But maybe a certain percentage of the detectors could have a "suicide" code...?)
(4) Not if it's as good as the "storm" botnet. Or, if the antimalware does get the immunityware, then it can also get the storm botnet.

Don't you think that there would be lots of willing people who would love to host spores in a tor-like network, knowing that their computer was spitting out botnet-busting "t-cells"? I, for one, would get a kick out of it.

So much for tonight. It's late.

Posted by: coyoteworks at October 20, 2007 12:52 AM

Another go at the "counterbot" idea.

The counterbot-net could be built to have all the advantages of the bot-net, including polymorphism, delayed activity, decentralization. For example, you could use a "nearest neighbor" technology. Suppose that I'm in regular, very-low-bit-rate contact with my nearest neighbors. If one of them dies, I commit suicide. This effectively cuts off the possibility that anyone can use me to get through the rest of the network to any command-and-control centers.

More than that, the counterbot-net would have several huge advantages over the bot-net. First, unlike Storm, people would want it. "That thing will protect my computer...?! Where can I get infected...!" Instead of trying to protect against it, people would seek it out.

Second, the bots in the counterbot could be leaner than their evil twins, because they would have no need of a criminal payload. They would be there only to detect the evil twins. They not need to collect SSNs, be able to send out spam, or whatever.

It would be crucial that no one group controlled all counterbots, or else privacy issues or issues of control would undermine the project. Therefore, the government would need to declare amnesty for people engaged in this kind of work, so long as they were willing to be supervised and regulated by the government. Also, third-party watch-dog groups should be given access to any command-and-control records.

Posted by: coyoteworks at October 22, 2007 8:17 AM

Update:
http://www.eweek.com/article2/

http://www.eweek.com/article2/...

"Storm Worm Botnet Lobotomizing Anti-Virus Programs"

The latest version of the Storm Worm code appears to be able to say to the anti-virus programs "These aren't the droids you're looking for" - it doesn't disable the AV program; it merely tells the AV program that all is OK. "All clear" (Time Machine, 1963).

Posted by: Al at October 24, 2007 9:35 PM

Please, PLEASE use a dictionary. How can you be considered intelligent and/or knowledgable if you can't spell or puncuate or use caps where necessary?

Posted by: esplendido at October 29, 2007 7:59 AM

Yes/ spelling is important] but puncuation is hard@

On a more serious note, I have not yet been convinced that this is much more than a live pilot project. I suspect that what has been, is being and will be learned by the authors is more valuable than any "rentals" they might have collected so far.

Posted by: tomliotta at October 29, 2007 11:14 PM

Storm is back now using a Christmas theme, it's pretty funny (I can't believe that people still fall for this stuff---I guess sometimes they think that they will actually get something out of it?), anyway it is using a slurry of webhosts that serve up the website [don't ever go to this site unless you have some sort of virtual machine] merrychristmasdude dot com with attractive women and the promise that once you install their software your wildest fantasies will come true, just scanning the file makes it VERY clear that it is "bad" deep in the file you see the plaintext: enable netsh firewall set allowedprogram "disnisaSoftware\Microsoft\Windows\CurrentVersion\Run disnisa.exe\disnisa.exe Anyway, Merry Christmas indeed

Posted by: Skizzy at December 24, 2007 12:29 AM

The whole idea of making it attractive for people to install a "counterbot" can be used by the bots themselves, in an attack on the meme that "viruses are bad".

From creating novelty services such as message boards with kudos points for promoting the bot, anonymising proxies and the ability for people to see things on each others computers, perhaps backed up with a more substantial threat such as encrypting the users files and granting access only to those who have the bot installed, this could be a very intriguing idea.

Posted by: Eddy at January 4, 2008 9:00 PM

I like how you've all listed interesting ideas, paths forward, and security vulnerabilities for Storm to look at and use. Well done.

Posted by: Nick at July 16, 2008 10:55 PM

---

something very latest about storm

http://blog.fireeye.com/research/2008/10/...

Posted by: allen at October 20, 2008 8:21 AM

You silly people, you have my software all confused. Certainly you aren't THAT stupid. You Americans should know more.

Posted by: Storm at December 9, 2008 7:51 PM

It doesn't look rational to attack it head on like that. Seems going for the soliciting vendors, or having an audit your network day seems more realistic- as strange and trivial as that may seem.

It's also scary that email->human intervention is still so effective decades later.

Posted by: Totholial at January 8, 2009 10:56 AM

Subscribe to comments on this entry

Post a comment

Name:

Email Address:

E-mail is optional and will not be displayed on the site.

URL:

Remember Me? Yes No

Comments:

Preview **Post**

Powered by Movable Type. Photo at top by Geoffrey Stone.

Schneier.com is a personal website. Opinions expressed are not necessarily those of BT.