- Mobile & wireless
- Network access control
- Networking
- Offbeat
- Open Source
- Operating systems
- Personal tech
- SaaS
- Science
- Security
- Server and data center
- Small business
- SOA
- Software
- Storage
- Tech & society
- Unified communications
- Virtualization
- Windows

new to ITworld?

learn what you can do

contribute

share a tip, submit a link, add something new

home » security » feature

Botnets: Reasons It's Getting Harder to Find and Fight Them

by Bill Brenner
4 comments | 8I like it!
Tags: authentication, botnet, conficker, data protection
More »
on this topic

- One bot-infected PC = 600,000 spam messages a day
- Microsoft global system aids worker rescue
- Gang of six' controls botnet of 1.9 million computers

April 20, 2009, 09:11 AM — CSO —

The perpetual proliferation of botnets is hardly surprising when one considers just how easy it is for the bad guys to hijack computers without tipping off the users.

Botnets have long used a variety of configurations, in part to disguise their control mechanisms -- see What a Botnet Looks Like. But as user-friendly but insecure applications continue to become available -- especially social networking programs used by the non-tech-savvy -- hackers have an ever growing number of security holes to choose from. They're also getting smarter about building resilient architectures, according to botnet

hunters who have monitored recent activity.

[See also: One bot-infected PC = 600,000 spam messages a day and Gang of six' controls botnet of 1.9 million computers]

Here are four reasons the botnet fight is getting harder, and what to do about it:

1. Operating below the radar
While much of the attention lately has been on botnet activity related to the Conficker worm (see Conficker Group: Worm 4.6 Million Strong), researchers say some of the largest botnets have largely escaped media attention. And that's how the bad guys like it.

Alex Lanstein, senior security researcher at FireEye Inc., a security vendor based in the San Francisco Bay area, said this is because their overlords don't want to make news and let people know their machines are infected. Cimbot, for example, is a piece of malware that has been used to create a botnet that now accounts for about 15 percent of the world's spam, he said.

Paul Royal, principal researcher at Atlanta-based security vendor Purewire Inc., has found several other examples of botnet herders operating below the radar. In one experiment he participated in, Project ZeroPack, he found that automated obfuscation techniques allow the bad guys to engage in such activities as server-side polymorphism. With malware morphing regularly, traditional antivirus vendors have more trouble keeping up with the right AV signatures. The Waledac botnet has used this method with much success.

Meanwhile, he said, hackers are moving away from the centralized command-and-control botnet structure in favor of a more peer-to-peer-based architecture. This is unfortunate because with the more centralized structure, security researchers at least have one large target to aim at. The P2P approach means more smaller targets that are tougher to aim at, he said.

"Conficker.C, Storm and Waledec have all moved from centralized architecture to peer-to-peer-based architecture," Royal said.

2. Malware can shield itself
Among the problems security researchers have encountered when trying to track and shut down botnets is that the newer worms used to build botnets are using strong cryptography to protect the command-and-control centers, said Paul Kocher, president and chief scientist at Cryptography Research.

"It used to be you could track how a botnet was getting its commands and send out fake commands to take it out," he said. "It's getting a lot

12next »
I like it!

Comments
4 comments Add a comment

- Mobile & wireless
- Network access control
- Networking
- Offbeat
- Open Source
- Operating systems
- Personal tech
- SaaS
- Science
- Security
- Server and data center
- Small business
- SOA
- Software
- Storage
- Tech & society
- Unified communications
- Virtualization
- Windows

new to ITworld?

learn what you can do

contribute

share a tip, submit a link, add something new

home » security » feature

Botnets: Reasons It's Getting Harder to Find and Fight Them

by Bill Brenner
4 comments | 8I like it!
Tags: authentication, botnet, conficker, data protection
More »
on this topic

- One bot-infected PC = 600,000 spam messages a day
- Microsoft global system aids worker rescue
- Gang of six' controls botnet of 1.9 million computers

harder to do that."

The newer botnets are also better at snuffing out a machine's security controls.

"We're also watching more sophisticated efforts among botnet-building worms to evade detection," Kocher said. "They're more polymorphic, changing from copy to copy. It makes it more difficult for an antivirus author to craft a signature to block it."

3. Popular apps are beyond IT's control

Researchers continue to find that the path of least resistance for bot herders is the variety of applications people use on company machines but outside the control of IT. They use these to pass a variety of sensitive data back and forth, including medical records, financial data and so on.

Security vendor Palo Alto Networks recently released its Spring 2009 Application Usage and Risk Report that reviewed enterprise application use and traffic from more than 60 large organizations across financial services, manufacturing, healthcare, government, retail and education. The assessments, conducted between August and December 2008, represented the behavior of nearly 900,000 users. Among the findings:

-
  - More than half (57 percent) of the 494 applications found can bypass security infrastructure -- hopping from port to port, using port 80 or port 443. Some examples of these applications include Microsoft SharePoint, Microsoft Groove and a host of software update services (Microsoft Update, Apple Update, Adobe Update), along with end-user applications such as Pandora and Yoics!
  - Proxies that are typically not endorsed by corporate IT (CGIProxy, PHProxy, Hopster) and remote desktop access applications (LogMeIn!, RDP, PCAnywhere) were found 81 percent and 95 percent of time, respectively. Encrypted tunnel applications such as SSH, TOR, GPass, Gbridge, and SwIPe were also found.
  - P2P was found 92 percent of the time, with BitTorrent and Gnutella as the most common of 21 variants found. Browser-based file sharing was found 76 percent of the time with YouSendit! And MediaFire among the most common of the 22 variants.

Collectively, the report said, enterprises spend more than $6 billion annually on firewall, IPS, proxy and URL filtering products. All of these products claim to perform some level of application control. The analysis showed that 100% of the organizations had firewalls and 87 percent also had one or more of these firewall helpers (a proxy, an IPS, URL filtering) -- yet they were unable to exercise control over the application traffic traversing the network.

As a result, malware pushers have a relatively easy time using these applications for foul play, including botnet building.

4. Social networking has widened the attack surface

Then there's the growing use of social networking programs like Facebook, Twitter and Myspace, which are easy for the non-tech savvy to use and also hard for enterprise IT shops to monitor.

At the ShmooCon security conference in Washington D.C. in February, for example, researchers Nathan Hamiel and Shawn Moyer guided attendees through attacks made easy because of the very nature of these sites, where users can upload and exchange pictures, text, music and other content with little effort. [See: Slapped in the Facebook: Social Networking Dangers Exposed]

Among the attacks targeting these programs, hackers use social networking tricks to dupe users into opening links that in turn drop malware onto the computer, effectively turning it into another zombie machine in a monster botnet.

User education still a key defense

Gunter Ollmann, vice president of research at Atlanta-based security vendor Damballa, Inc., said enterprise IT shops would do well to ramp up efforts to detect the lesser known malware being used to such devastating effect these days. In the last 2 years, he said, IT shops have deployed a broad range of detection and prevention technologies. Each layer of defense has gotten better at fending off certain attacks.

"The more common the threat, the better the protection," he said. "But the bad guys are very much aware of how these defenses work, so they're using more sophisticated, targeted social engineering attacks. Looking at the malware used, a high percentage is IDS and AV proxy aware."

Ollmann and others offer the same advice: Since attackers are so successful at using social engineering tricks --

luring users with fake headlines that play on current events and duping them into clicking on malicious links -- one of the best defenses remains user education.

Show the average user what they're up against every time they go online and they are less likely to be duped into downloading the bot-building code, experts say.

» posted by ITworld staff

CSO

« prev12
I like it!

- Email
- Print
- Share
  - Slashdot
  - Digg
  - Stumble
  - Reddit
  - Newsvine

Comments
4 comments Add a comment

How to combat Botnets - 5 letter word

LINUX
by Anonymous (not verified) on 4/22/09 at 7:28 am | reply

Linux isn't the answer...

I love it when people pout that Linux is the end all solution for malware. Wrrrong. IF Linux does become more popular- doubtful since M$ and Crapple knows how to market -They'll just target those machines. It's all about the market share.

Secondly, Botnets wouldn't exist for the most part if people didn't steal os's and not have them patched, as well as not have any security on them. Go on and pout some more about how Linux doesn't need patches... wrong they do and have been. Why you think there are updates for it? Hell even Ubuntu has a update service much like M$ does.
by Anonymous (not verified) on 4/22/09 at 9:35 am | reply

thin clients

99% of people use their computer for email and web. You don't need a full computer to do these tasks. Thin clients would solve a lot of problems. Small terminals that only do web, and you can't install software on without a firmware upgrade that you download from the manufacturer, and is digitally signed. Maybe even something like an Xbox360 with a mouse and keyboard. How many millions of those are in homes, yet there's no Xbox360 botnet... People need to give up this notion that they need "computers" when really they could everything they need with thin web terminals.
by PJ (not verified) on 4/22/09 at 10:03 am | reply
View all comments »

cartoon caption contest