# Kelihos botnet, once crippled, now gaining strength

## Microsoft and Kaspersky Lab are now seeing the botnet it shutdown in September coming back to life

Jeremy Kirk (IDG News Service) | 02 February, 2012 02:04 | Comments | Like 9



A botnet that was crippled by Microsoft and Kaspersky Lab last September is spamming once again and experts have no recourse to stop it.

The Kelihos botnet only infected 45,000 or so computers but managed to send out nearly 4 billion spam messages a day, promoting, among other things, pornography, illegal pharmaceuticals and stock scams.

But it was temporarily corralled last September after researchers used various technical means to get the 45,000 or so infected computers to communicate with a "sinkhole," or a computer they controlled.

But the computers that comprised Kelihos were still infected with its code. Researchers knew that it would only be a matter of time before its controller used the botnet's complex infrastructure of proxy servers and communication nodes to regain control.

In fact, it happened shortly after the researchers intervened. Sinkholing the botnet was only a temporary solution.

"We could have issued an update to those machines to clean them up, but in several countries that would be illegal," said Ram Herkanaidu, security researcher and education manager for Kaspersky Lab.

**Related Coverage**

- Leaked EU memo highlights concerns over data retention law
- Anonymous releases recording between FBI, UK law enforcement
- FAQ about the VeriSign data breaches
- PHP 5.3.10 fixes critical remote code execution vulnerability
- Google won't delay new privacy policy despite EU concerns

**Related Whitepapers**

- Book 2 - The Practical Guide to Securing Assets
- HP Case Study: Streamlining archiving and data protection

Tags: security, Microsoft, kaspersky lab

Meddling with another person's computer could be considered a form of hacking, even with the best intentions of security researchers. Unfortunately, it appears that many of the machines infected with Kelihos are now controlled by the bad guys again.

There are also other new variants of Kelihos that are using updated forms of encryption to mask the communication with the botnet controllers, Herkanaidu said. Maria Garnaeva, a researcher with Kaspersky Lab, wrote that two different RSA keys are being used for encryption, which means it is possible two different groups are controlling Kelihos.

The resurrection of Kelihos comes as Microsoft last week amended a civil suit in the U.S. District Court for the Eastern District of Virginia to name a Russian man it believes is responsible for the botnet.

The man, Andrey N. Sabelnikov of St. Petersburg, freelanced for a software development company and formerly worked as a software engineer for a computer security software company.

After his name was widely published in media reports, Sabelnikov denied he was responsible and told the BBC, "I will prove my innocence."

Even if Sabelnikov is eventually criminally charged by U.S. prosecutors, Russia's constitution prohibits extradition of its own citizens.

Microsoft said it is working with Kaspersky on studying the latest Kelihos developments. The company remains committed to following its botnet cases and intends to hold those responsible accountable for their actions, said Richard Boscovich, senior attorney for Microsoft's Digital Crimes Unit, in a statement.

*Send news tips and comments to jeremy_kirk@idg.com*



**More about:** BBC, Creator, Kaspersky, Kaspersky Lab, Microsoft, RSA

**REFERENCES**

Kelihos/Hlux botnet returns with new techniques - Securelist

Microsoft Names Alleged Kelihos Botnet Creator : PCWorld Business Center

BBC News - Kelihos botnet suspect denies Microsoft accusations

## Post new comment

NAME

EMAIL ADDRESS

The content of this field is kept private and will not be shown publicly.

COMMENT

Users posting comments agree to the TechWorld comments policy.

Post Preview

Login or register to link comments to your user profile, or you may also post a comment without being logged in.

1. Google to auto probe Android Market for malware
2. Security Manager's Journal: Should physical security belong to us?
3. gTLD registrar VeriSign hacked in 2010
4. SaaS, APTs and asymmetric risk take spotlight at Security Threats 2012
5. Zuckerberg's Facebook: Hackers build, not break things

1. Google reveals Android malware 'Bouncer,' scans all apps
2. Lawsuit raises questions about email privacy at work
3. H-1B workers are better paid, more educated, study finds
4. Presidential candidates' mobile websites still works in progress
5. What are you saying: John Linton passing away, Dick Smith sell-off

1. Resources CIOs in Australia
2. A new era of IT transformation
3. Security breach
4. Supply chain management in Australia - Part 3
5. Big data - Part 2

1. APP OF TH
2. Data#3 for partnershi
3. NEWS RO from Garm SafeNet, a
4. CoSoSys recruitmer
5. PRODUCT latest from Quest, Pol Compuwa