

The threat of the spam economy

Is your organization sending out spam? Are you sure? Are you certain that no one on your network has a hijacked system that is being surreptitiously used to send spam from your domain?

Data gathered by Sophos labs shows that 30% of spam originates from hijacked systems today, primarily but not exclusively on consumer broadband networks. Our spam honeypots receive millions of messages from tens of thousands of new and unique domains every day. There aren't tens of thousands of spammers and we know the organizations that own most of those domains aren't spammers and yet the spam is originating from those domains. How can this be?

Spammers can only be delivering messages from thousands of domains if they have access to a continuously replenished network of servers. This network is provided by virus writers and hackers who exploit network and system weaknesses to gain control of legitimate systems such as yours. The new demand for hijacked systems changes the rules for virus writers, spammers and for those that defend against them.

This article details how new economic incentives are changing the targets and the tactics used by virus writers, the threat to organizations caused by the spam/virus convergence, and the spam and virus protection required to combat the threat.

The spam economy

The spammer's goal is simple: make money by selling to (or defrauding) email users. But as more and more organizations deploy spam-filtering solutions, accomplishing this goal has become increasingly difficult and resource intensive. Spammers now require increasing levels of specialization and innovation to deliver spam messages.

Driven by the incentive of making money through unsolicited email, spamming operations have evolved from individual efforts, to large spammer communities, to an entire underground economy powered by spammers, virus writers and hackers.

The spammer's demand for hijacked access to legitimate systems to act as spam servers and hide their operations is one of the drivers behind the convergence of the spam and virus threats. Organizations now face the threat of continuous attacks involving a high level of cooperation and coordination between these formerly distinct groups.

The spam/virus/hacker connection

Spammers, virus writers and hackers used to be unique communities with unique motivations, but they are now unified by the singular goal of driving revenue through spam.

Each group contributes to the threat. Spammers pay the virus writers and hackers to provide a constant supply of servers to hide their identity and generate huge volumes of mail. As spam operations are detected and blocked by the filters, the supply of servers must be constantly replenished. The hackers and virus writers accomplish this through frequent attacks on networked systems and infrastructure.

- Hackers break into mail servers and other exposed systems to hijack them for use by spammers as relays and proxies
- Virus writers infect large numbers of machines with worms, Trojans, spyware and other types of malicious code that enable the virus writers to assume control of the machine and surreptitiously host spammer activities. MiMail, Sysbug and other recent virus attacks have all had machine-hijacking features

Together, these hacked and hijacked systems provide a massive network of servers, which are then rented by virus groups to the spammers and used to:

- Send spam messages
- Act as proxies and relays to hide message routing
- Steal the identity of the original owners and use these legitimate credentials to bypass black and whitelists
- Conduct Denial of Service attacks to shut down DNS blacklists
- Conduct Directory Harvesting Attacks against legitimate email systems
- Provide temporary spam website hosting

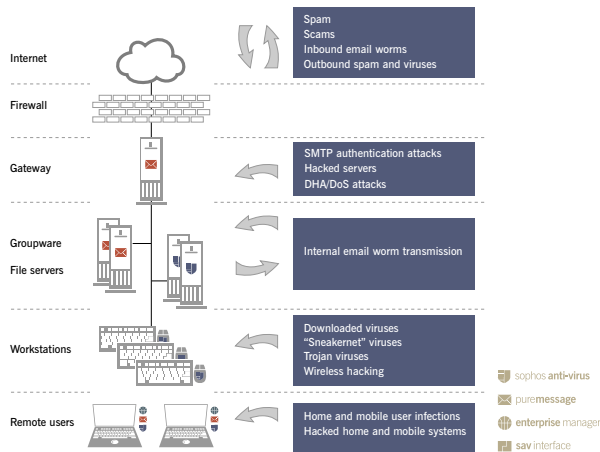
This convergence of spam and virus interests is particularly dangerous as it changes the motivation for virus writing from vandalism driven by ego to system theft with profit motive. Now that spammers are paying for access to hijacked servers organizations can expect viruses with hijacking features to be increasingly stealthy as their creators look for new ways to secretly take and maintain control of systems.

Virus protection stops the bulk of these attacks, but virus writers rely on a small percentage of machines remaining infected even after the attack is addressed. These machines act as "zombies," waking up and operating at the virus writers' command, and continuing to provide services to spammers until the zombie is removed by the legitimate owner or it is detected and blocked by the anti-spam systems, potentially impacting all email originating from the zombie's host network.

To prevent infiltration of zombies, organizations must have effective user education and virus protection systems at all levels of their organization: gateway, workgroup, server and desktop. Desktop protection must also be extended to remote users to prevent the download of zombies from home systems.

The threat to business

In addition to the spam/virus/hacker connections, the underground economy involves the market for other tools for spammers, including "ratware" (software that sends spam) and services providing lists of email addresses to target. The whole underground economy extends the concerns about spam and scams to include not only productivity, morale, and email resource consumption, but also a variety of security risks at every level in an organization's infrastructure. These risks must be defended against to avoid system downtime, system hijacking and damage to reputation.



As a result of spammer activity, organizations must contend with:

- Increasingly coordinated, round-the-clock virus, hacker and spam attacks, with faster exploitation of identified system vulnerabilities
- Growing volumes of spam
- Increasingly sophisticated and varied spam attacks involving changing, international spam sources
- More frequent attacks from viruses, worms and Trojans as the virus writers adopt spam delivery techniques
- Increased attempts to hijack servers for their sender authentication and other purposes
- Increased prevalence of Denial of Service attacks designed to overwhelm and bypass filters
- Higher incidence of directory harvest attacks to grow mailing lists

Converging threat, converging protection

For enterprises, protecting their users and systems against this converging threat presents a challenge because:

- A mixed set of single purpose security solutions deployed at various locations, require compromises in system design and message routing to meet competing system needs
- Security functions such as network, email and anti-virus protection may not be integrated resulting in different, overlapping or even contradictory policies
- Expertise and resources may be insufficient to keep pace with the sophistication of today's spam, virus and other attacks
- User education, communication policies, patch management processes and systems that deal with occasional threats and outbreaks need to evolve to address the current environment of continuous attacks

- Protections built to protect against external attack may be unprepared to detect and isolate compromised internal systems

To minimize their risk, organizations need consolidated protection against spam, viruses and other malicious activity. This protection should take a multi-faceted approach involving user education, technology, policy and process changes. Recommended protection initiatives include:

- Ensure administrators have a common view of messaging threats by deploying an integrated messaging security solution that includes anti-spam, anti-virus and policy enforcement and protect against spam, scams and all three email-borne aspects of a virus outbreak (virus-generated message delivery, virus-driven email notification blooms and unwanted malicious attachment types)
- Deploy multi-tier anti-virus protection to protect against the most common attack and distribution vectors: email, downloads and remote users
- Invest in well-supported spam protection from vendors that operate anti-spam labs to update both technology and current data
- Establish patch management policies and processes to update systems and minimize zero-day threats when vulnerabilities are discovered
- Extend protections and policies to home and remote users to ensure that all systems are hardened against infiltration and infection
- Monitor outbound email traffic to ensure compromised systems are detected and eliminated before they are able to damage systems and reputations

To ensure consolidated protection from the spam economy, organizations should choose a vendor such as Sophos, with resources dedicated to actively analyzing, anticipating and protecting worldwide customers from all aspects of spam and viruses 24 hours a day.

SOPHOS
WWW.SOPHOS.COM

More information on spam/virus convergence and how to protect your organization can be found at www.sophos.com/spaminfo