

Symantec notes that this high percentage probably indicates that U.S.-based command and control servers are running bots in other countries as well as domestically. And the company noted another trend: The number of command and control servers fell 25 percent from the first half of 2006 to the second.

That's not a good thing. "A drop in the number of command and control servers, combined with a rise in the number of bot-infected computers indicates that, on average, bot networks are increasing in size," the report states.

"Bot networks are thus becoming more consolidated. Consolidated bot networks will likely mean that organizations will have to deal with a well entrenched, experienced and dedicated group of bot network owners instead of a population of hobby hackers."

Conclusion

And that's pretty much the thread that runs through the most recent Symantec report: The hacker landscape is increasingly dominated by professionals, not script kiddies. And the key factor is scale—the most serious threat is from going criminal concerns, rather than someone out for the one big score.

"Frankly, this stuff isn't being sold for that much—you'll see a credit card going for like a dollar to \$6," said Dave Cole. "You see a full identity going for \$14-\$18. So really the way they're selling this stuff is in bulk and trying to make it in mass, as opposed to ripping off any one individual in particular."

Eric Krapf is editor of BCR.

How A New German Law Affects U.S. Content Business

Dr. Axel Spies

Germany is Europe's largest market for online content and multimedia services. And a new law has just been passed that may affect U.S.-based companies that provide online content to German users.

As of Mar. 1, 2007, a new German law called the Telemediengesetz ("TMG") replaces the German Teleservices Act, the Teleservices Data Protection Act and the Federal Media Services Treaty. The TMG covers basically all

online services that are not telecommunications services (such non-telecom services are called Telemedia Services). The new law could have an impact on U.S. content providers.

Mobile commerce, Web shops, music download platforms, video on demand, Internet search engines, emails and even simple company websites are covered by the new law. The TMG imposes a number of new responsibilities for Telemedia Service providers. Companies established outside of Germany need to at least take a closer look at the following issues:

■ **German law applies to a Telemedia Service provider established outside Germany**—The TMG implements the EU's "Country of Origin Principle," which is aimed at facilitating the provision of cross-border tele-services within the EU. The Country of Origin Principle stipulates that each member state must ensure that service providers established in its territory comply with the national provisions applicable in that state. It is sufficient for providers of such services to comply with their local laws—in other words, even if their service is received in another EU country, they need not check whether they comply as well with the laws of that other EU country.

There are exceptions, however—most importantly, data protection laws, gambling and unsolicited emails (i.e., spam). Art. 3 (5) of the new TMG declares that German law applies to services established outside the EU (for instance, services of U.S. providers) if certain circumstances are present—namely, circumstances that pose a "grave and severe danger" to consumers' interests, public security and/or health. Furthermore, based on recent rulings in German courts, it's not even clear whether services that originate outside the EU that *do not* meet this "grave and severe danger" standard are exempt from German law.

■ **"Telemedia Services" is defined very broadly**—There is also some confusion about the difference between services that are a matter of personal communication, and services that are offered for public consumption. The TMG defines a "telemedia service" as every electronic information and communication service apart from those services that (instead of providing content) merely transmit signals via telecommunication networks and/or broadcast signals. Any provision of services closely related to the mere transmission of signals (e.g.,

value added network services) is also excluded.

The TMG thus applies to all kinds of services, without regard to whether they are provided for a fee, for example: Mobile commerce, Web shops, music download platforms, video on demand, Internet search engines, emails and even simple company websites; but it does not apply to live-streaming of video or web-casting that is not directed to the public.

■ **Various duties for Telemedia Service providers**—The TMG has not altered the scope of the service providers' liability as compared to the law's predecessors. This means that:

—As a general rule, Telemedia Service providers are always liable for their own content. Exemptions exist for third-party-generated content, most often coming from the user of the service. Provided the telemedia service provider does not intentionally collaborate with any third-party infringer of the law, the provider is exempted from liability *if*:

(a) they merely relay data or grant user access without initiating the transmission, selecting the recipient of the transmission or selecting or altering the data; or

(b) they use an automated process for caching data for the purpose of more efficient accessibility, without altering the data and while using proper industry standards for collecting, using and updating the data. This exception requires that the service providers immediately take down the content from their servers on notice of a deletion of/denial of access to the infringing data at the data's original source and/or due to any court or administrative order to do so; or

(c) they host data for a user without knowledge of the infringement and take down the data from/deny access to the data on their servers as soon as they gain knowledge of the infringement or, in a claim for damages, of circumstances that clearly imply an infringement. This exception requires that the infringing user is not an employee or otherwise under the supervision of the service provider.

As a result, providers are under no general duty to monitor third-party content for possible infringements. If, in the case of caching and hosting (as compared to mere relaying of data), an infringement is brought to the provider's attention, however, there is a duty to take down the content.

■ **Various disclosure requirements;**



BRIEFING

spamming prohibited—The TMG requires service providers to meet certain basic disclosure requirements, such as company name, place of business, etc. The TMG further allows authorities to seize information on a user's identity for the purposes of criminal prosecution, preventing danger and the (private!) prosecution of intellectual property violations.

The possible scope of this provision remains unclear, and these rights are highly contentious at the moment. The relevant article of the TMG law is likely

to be challenged as unconstitutional in Germany's Federal Constitutional Court, since it may infringe on privacy rights granted by the German Constitution. There are also various restrictions in the law on when providers may use their user data for other purposes.

Finally, the TMG aims at preventing spam, i.e., email that intentionally disguises its sender and/or the subject of its contents. A breach constitutes an administrative offense and can result in fines up to 50,000 euros in each case against the spammer.

Conclusion

To sum up, companies in the U.S. that provide telemedia services to customers in Germany should carefully check that they comply with the TMG, in particular with the anti-spam rules and disclosure requirements□

Dr. Axel Spies is a German telecommunications attorney with Bingham McCutchen law firm in Washington, DC.