Cutwail Botnet Feeling Effects of Blackhole Takedown

By Michael Mimoso

Published: 2013-12-18 · Archived: 2026-04-05 23:06:01 UTC

Without the Blackhole exploit kit around to inject malware such as the Zeus Trojan, keepers of the Cutwail spam bot have been forced to resort to some old-school methods of sending malware such as direct email attachments.

The arrest of alleged hacker Paunch and the subsequent dismantling of the Blackhole Exploit Kit operation has cybercrime groups scrambling to find another automated means of delivering exploits.

In the meantime, some are settling for old-school tactics that include infected email attachments and an increased investment in the social engineering used to entice users into double-clicking and executing the malware stored in the attachment.

The most recent evidence of this comes from a major cybercrime group reliant on the Cutwail botnet to send out spam that had been fiddling with a relatively new exploit kit called Magnitude before deciding to go the direct-attachment route.

Researchers at Websense said that since Paunch's arrest, reported in early October, the company has captured emails with links that used to redirect to Blackhole now redirecting to Magnitude and others redirecting to phishing pages with American Express, work from home and diet remedy themes.

Apparently, however, Magnitude didn't serve the attackers' needs sufficiently as more and more samples included direct attachments, said director of research Alex Watson.

"That gives us an interesting look at the criminal community that leaves you open to speculate why they experimented with Magnitude and then moved away," Watson told Threatpost. While the group was using Blackhole, the number of Cutwail messages containing malicious URLs was markedly higher than post-Blackhole when the number of emails containing infected ZIP files shot up.

"The overall levels of malicious activity have stayed somewhat consistent, but I would say the success of campaigns since moving to direct attachments and things like that is dramatically lower," Watson said. "We've seen slightly more sophisticated social engineering attacks that are more convincing to users, but not nearly the same success rates they had when Blackhole was available for use."

Cutwail is one of the most established spam botnets and most prolific, sending at one point, millions of spam messages daily. It was two million compromised machines strong and used to distribute spam and financial malware targeting not only credit card data but credentials. The Cutwail emails often included links that would lead victims to sites hosting Blackhole, which would then inject downloaders for other malware such as ZeroAccess or Zeus.

The arrest of Paunch and the Blackhole takedown has turned cybercrime economics on its ear in some parts. Attackers have been forced to find other avenues to recover lost revenue.

“They’ve had to put more work into the social engineering and having sophisticated-looking emails to get users to click,” Watson said. “A second thing we’ve noticed is an increased aggressiveness with malware installations on computers that are compromised.”

Where attackers would be satisfied with leaner attacks because the volume provided by Blackhole web injections was so high, that’s now changed.

“Often we’ll see a Pony downloader which will steal credentials, which will then download Zeus, which will then download Cryptolocker, all in the matter of a couple of minutes,” Watson said. “So you’re looking at very aggressive installation of malware on computers that are targeted, which could be another way of making up lost revenue due to not infecting as many machines.”

Compromised computers are more than ever cash cows for attackers, some of whom invest significant money in purchasing exploit kits such as Blackhole. When that goes away, a number of infection vectors go away with it. Some of that dynamic has given rise to ransomware in recent months, in particular Cryptolocker, which encrypts files on shared drives in return for a ransom. Other malware variants have taken to anonymity networks such as Tor or I2P to hide communication and hopefully preserve the longevity of their enterprise.

Ransomware, however, gives an attacker an immediate shot at collecting a payout, Watson said.

“With Cryptolocker, I think there have been some cases where it’s been very successful,” he said. “If you look smaller companies that don’t have really strong controls around file sharing or backup, and those businesses that don’t really have an established disaster recovery plan would be vulnerable to this.”
