Bamital Botnet Takedown Is Successful; Cleanup Underway

Published: 2013-02-22 · Archived: 2026-04-10 02:36:06 UTC

Feb 22, 2013

*The following is a post by **Richard Domingues Boscovich**, Assistant General Counsel, Microsoft Digital Crimes Unit.*

Two weeks after Microsoft and Symantec's collaborative takedown of the Bamital botnet, I'm pleased to report that the Bamital botnet remains offline. Additionally, since Microsoft was able to receive all of the computer traffic that had been connecting to the Bamital botnet, we are also seeing very positive cleanup results firsthand. For instance, our preliminary data shows that as of February 18th, approximately 32 percent of the infected computers we had observed since the February 6th takedown are no longer part of the Bamital botnet. This promising reduction rate is largely due to the takedown of the botnet and victims taking action in response to the proactive notification process and available cleanup tools. We expect that the number of victim notifications and cleaned computers will improve as we fine-tune our process over the course of the next several weeks.

I also want to take this opportunity to acknowledge the cooperation of the Indian Computer Emergency Response Team (CERT-In). Bamital's command and control structure was using several ".In" top level domains to control infected computers around the world. CERT-In played an integral role by implementing a crucial component of the notification process that allowed us to contact and offer cleanup tools to victims affected by Bamital. CERT-In's support is the reason why this cleanup effort has been effective. Additionally, we will soon be working with Internet service providers and Computer Emergency Response Teams around the world, as we have in the past, to help rescue those remaining computers infected with this malware.

Meanwhile, we also have positive news to share on the legal side. Early last week we entered into a confidential settlement agreement in the case with defendant John Doe 12. We believe the agreement is in the best interest of the case. Finally, at a preliminary injunction hearing on February 13th, the Federal Court for the Eastern District of Virginia granted Microsoft's motion and entered an order granting the preliminary injunction. The granting of this motion helps to keep the domains that the bot-herders used to operate the botnet offline, and allows Microsoft to continue pointing all of the malicious IP addresses to Microsoft's domain name system (DNS).

Helping protect people is at the forefront of Microsoft's proactive fight against botnets and other forms of cybercrime. We do this by applying a three-pronged approach which includes helping advance security in our products and services, taking proactive, disruptive measures to help protect people, and educating people about the dangers of cybercrime and how they can protect themselves from online threats. As DCU recently held its fourth annual Digital Crimes Consortium (DCC) in Barcelona, Spain, a week-long conference that provides a rare opportunity for law enforcement and members of the technology security community from around the world to discuss the latest cybercrime issues and challenges, I want to stress that cybercrime cannot be fought alone. However, with continued successes in cooperation among all players – industry, academic researchers, law enforcement agencies and governments worldwide – the global community has the power to turn the tide in the

fight against cybercrime. I look forward to continuing to work with partners like Symantec and CERT-In to shut down cybercriminal networks and protect innocent people around the world.

To stay informed on what Microsoft and others are doing to help make the Internet safer for everyone, follow the Microsoft Digital Crimes Unit on Facebook and Twitter.

Tags: botnets, Digital Crimes Unit
