Microsoft Releases Security Intelligence Report

May 13, 2011

REDMONT, WA (RPRN) 05/13/11 — Cybercriminals Increasingly Targeting Consumers

Today's release of Microsoft's Security Intelligence Report volume 10 is our most comprehensive global threat report to date, with in-depth regional threat intelligence for 117 countries from more than 600 million machines worldwide. The report highlights a polarization of cybercriminal behavior and an increasing trend of cybercriminals using "marketing-like" approaches and deception methods to target consumers.

Since 2006, we have released 10 volumes of the Security Intelligence Report, providing customers with unparalleled insight into the software threat landscape and guidance to better protect themselves. The threat landscape has changed significantly during those years with advancements in security and privacy technology and general awareness of cybercrime. However, cybercriminals have gotten more sophisticated and continue to evolve their attack methods.

Across the threat landscape, we see a definite polarization in terms of criminal behavior. On one side are a small number of sophisticated criminals whose motives vary from large payoffs to targeted attacks. These attackers may have special intelligence about a target's environment, use customized social engineering to trick the intended victims, or exploit newly-discovered

vulnerabilities in software to compromise networks and systems.

On the other side, there are those who leverage more accessible attack methods, in some cases originally created by the more skilled cybercriminals, along with social engineering to take a small amount of money from a large number of people. Social engineering tactics include fooling people with rogue security software that pose as legitimate protection products, impersonating friends to steal passwords to online gaming accounts, conducting phishing using social networking as the lure, and tricking users to download adware.

From the latest report, we see these attacks being run like marketing campaigns and fake product promotions, especially during significant events that generate a lot of media attention. In the report, there are some key data points that indicate these tactics are on the rise:

· **Rogue Security Software** – Rogue security software was detected and blocked on almost 19 million systems in 2010, and the top five families were responsible for approximately 13 million of these detections.

· **Phishing** – Phishing using social networking as the lure increased 1,200 percent – from a low of 8.3 percent of all phishing in January to a high of 84.5 percent in December 2010. Phishing that targeted online gaming sites reached a high of 16.7 percent of all phishing in June.

· **Adware** – Global detections of adware when surfing websites increased 70 percent from the second quarter to the fourth quarter of 2010. This increase was almost completely caused by the detection of a pair of new Adware families, JS/Pornpop and Win32/ClickPotato, which are the two most prevalent malware in many countries.

Advancements in security and general awareness of threats have a positive impact in protecting the broader online community. According to the National Vulnerability Database, vulnerability disclosures (counted by CVE) in 2010 across the industry are down 16.5 percent from 2009. Additionally, we continue to see that newer products are less susceptible to attack – computers running Windows 7 and Windows Server 2008 R2 showed the

lowest infection rates. Overall, machines with more recent and complete service packs installed fared better than those with earlier versions. It's also notable that Windows 7 operating systems are infected only about half as often as Vista and Vista half as often as Windows XP. This data emphasizes the importance of upgrading to the latest software.

Finally, I am pleased to see the rapid the adoption of Microsoft Security Essentials, which surpassed 30 million active subscribers after one year of availability. It continues to grow. This demonstrates a continued proactive approach to security, and we're proud to welcome all these MSE users to our global family.

We continue to advance our security processes, technologies and resources to keep customers protected from the changing threat landscape. However, we know this cannot be done alone. Through collective efforts – such as the sharing of threat intelligence and guidance, software providers making advancements in security protections and customers keeping their systems up to date - we can help minimize cybercrime and create a safer, more trusted computing experience for everyone.

Media Contact Name: Vinny Gullotto
Media Web Address:
http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/05/12/microsoft-releases-security-intelligence-report-cybercriminals-increasingly-targeting-consumers.aspx

About the author:

RushPR News is a social media newswire service created to help you with content creation and distribution to news outlets and social media networks. RushPRnews can also assist you with your web strategies with experts advices and strategies at an affordable cost. Write us at news@rushprnews.com

---

Filed Under: BREAKING NEWS, Technology, Featured, MICROSOFT

NEWS, PRESS RELEASE

RUSH PR NEWS newswire and press release services at rushprnews.com / Anne Howard annehowardpublicist.com

Content- Legal Responsibility - All material is copyrighted - You may repost but you MUST link back to the original post on your page and acknowledge Rush PR News as the news source. Rush PR News is not legally and/or morally responsible for content of press releases, opinions expressed or fact-checking.

Rush PR News cannot be held legally responsible for material published and distributed through its newswire service or published in its press-room and therefore cannot be sued for published material. Third-party must be contacted directly to dispute content.

Rush PR News is not the contact for material published.