February 2013

Microsoft Security Intelligence Report

Key Points

- The Microsoft Security Intelligence Report offers a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide.
- Microsoft's Trustworthy Computing group is responsible for implementing a long-term, collaborative effort to create and deliver more secure, private, and reliable computing experiences through the Security Science initiative, critical infrastructure protection, delivery of secure products, and defense against malware.
- Microsoft believes that industry cooperation with authorities is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort.

BACKGROUND

The Internet has become an integral part of everyday life, and as the number of people online grows, so too have concerns about their safety. With good reason: increases in Internet traffic have resulted in dramatic increases in online crime, which has heightened the security concerns of governments and organizations around the world.

Online threats have evolved from petty crimes by attention-seeking hackers to multi-front attacks by sophisticated criminal organizations. Cyber criminals exploit users through email, web browsers, social media, online games, and fake security software. Compromised computers can be used to breach security systems and the data of financial institutions, target political organizations for attacks, and steal people's money or identity—and their sense of security.

As a partner in the global response to online crime, Microsoft provides resources and expertise, including its semi-annual Security Intelligence Report (SIR), to help discover the latest threats. The report offers a comprehensive, up-to-date, and geographically relevant analysis of the cyber threat landscape of exploits, vulnerabilities, and malware using data from more than 600 million computers worldwide and some of the busiest online services on the Internet. The latest SIR, Volume 13: January–June 2012,[1] is over 900 pages of data and analysis with views of 105 countries and regions around the world.

Recent editions of the SIR have shown that cybercriminals are gravitating toward the use of fake software activation keys that contain malware. This emerging social engineering tactic is the number one threat facing consumers worldwide. The SIR also shows that social engineering and similar attacks can be mitigated through security best practices such as implementing effective technical safeguards.

Microsoft appreciates the scope and changing complexities of online security—and the tremendous value of collaborative effort in the event of an attack to provide support, guidance, and the latest information. To that end, the company continues to promote the global imperative of sharing knowledge with industry leaders, governments, and security organizations.

[1] **aka.ms/SIR-V13**

MICROSOFT APPROACH

The Trustworthy Computing group at Microsoft is responsible for implementing a long-term, collaborative effort to create and deliver more secure, private, and reliable computing experiences. Areas of the group's focus include:

- **Security Science.** Building on a body of research about how systems are attacked and ways to prevent or mitigate those attacks, Security Science is a Microsoft initiative that develops tools and techniques to make attacking systems more difficult. Through Security Science, Microsoft continually monitors threat trends and looks for software vulnerabilities. The company then uses that information to create mitigation tools and techniques that developers can draw on to improve overall security.
- **Protection of critical infrastructure.** With technology becoming ever more important in people's daily lives, the Trustworthy Computing team engages with governments around the world to help them protect critical infrastructures as well as the safety of their citizens online. The team is committed to sharing its research and innovations to help establish policies that make meaningful improvements to global cyber security.
- **Delivery of secure products.** The Microsoft Security Engineering Center helps protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL). The SDL is the industry-leading software security assurance process, which embeds security and privacy through every phase of the development of Microsoft products.
- **Combating malware.** The Microsoft Malware Protection Center analyzes malicious software and develops solutions that Microsoft uses in its security technologies. When a vulnerability in Microsoft software is discovered, the Microsoft Security Response Center monitors and responds to the incident. It also manages the company's process for releasing security updates, and serves as the single point of coordination.

POLICY CONSIDERATIONS

- Microsoft welcomes the support of governments in fighting online security threats. The company believes that industry cooperation with authorities is the most effective means of reducing cyber threats, and supports balanced regulation as part of that effort. Microsoft believes that less onerous restrictions on industry allow for greater innovation and flexibility in developing and implementing responses to cyber crime.
- Microsoft has joined with industry partners to encourage countries to adopt the Convention on Cybercrime ratified by the Council of Europe, which requires signatories to adopt and update laws and procedures that address online crime.
- Microsoft supports the government funding of basic security research to help improve the security of online systems.

Helpful Resources

Microsoft Security Response Center
www.microsoft.com/msrc

Microsoft Security Intelligence Report
www.microsoft.com/sir

Microsoft Malware Protection Center
www.microsoft.com/mmpc

Convention on Cybercrime
aka.ms/Convention-on-Cybercrime