BURTON GROUP'S 2007 MALWARE PREDICTIONS

In forward extrapolation, it helps to have a clear understanding of what is and what is not different from the malware of the past. Almost everything we see in the space—advanced viruses, Trojan horse programs, cybercrime, and worms, as well as many of the defenses—have been around for 10 to 20 years. In recent years, however, the Internet has become massively interconnected, which has allowed malware to propagate more widely. And currently, malware creation has become much more automated, the number of criminal adversaries operating internationally has greatly increased, and there are more targeted attacks.

Malware is getting better and better at doing what it always did, which is to expand and cover the available environments. We're also watching with fascinated dismay as malware creation evolves from a hobby into an underground cybercrime industry. There are simply more resources and tools than ever working on the dark side to perfect cyberattack machinery, such as vulnerability finders, exploit generators, modular attack construction kits, botnet control, malware localization, intelligence gathering, anonymity, money laundering, and other tools of the trade. With this in mind, Burton Group offers the following predictions:

1. Malware will eventually attack every IT environment, including endpoint security components. Smartphones, Windows Vista, Mac OS X, and other sophisticated operating environments will attract malware interest in proportion to their installed base. Infrastructure will not be immune; users could be misdirected through compromised routers, DNS, or search engines and computers attacked through compromised software update services.

2. Useful IT environments will have cracks into which malware can creep, even if many of the component services are themselves bulletproof. Social engineering will often speed or simplify the penetration process.

3. Cybercrime will remain a growth industry, launching waves of malware in mass attacks and targeted attacks. The world can no more eliminate cybercrime than it can crime.

4. Attack tools will become more sophisticated in cybercrime's underground economy. Vulnerability research (on or used for the dark side) will evolve alongside secure software development practices.

5. Malware will continue to be used for denial of service, sabotage, theft, fraud, and industrial espionage as well as economic warfare and information warfare.

6. Heuristic and behavioral detection (so-called "proactive" security) will become more important; but signature detection will still be required for scanning performance and positive identification of malware.

7. Protection will continue to be limited by the deeper problems of defense, but from time to time improvements (such as Intel's NX chip feature that resists buffer overflow attacks, or Microsoft's address space layout randomization) will be made that significantly reduce risk and force attackers to adapt.

8. Small but talented vendors will often provide more effective protection than widely used products—until attacks are tested or developed against them too.

9. Security suite vendors and enterprises will integrate NAC, vulnerability management, security information management, and other control layer technologies with malware defense.

10. Absent mature risk management, organizations will enjoy malware-free honeymoons with new software or other IT facilities, become complacent, and later fall victim to dramatic attacks that will be sensationalized in the press.

11. Technical defenses are subject to failures, but organizations that develop a full spectrum defense can manage the risk much more effectively than those who do not.

Source: Burton Group Security and Risk Management Strategies report: Malware, Cybercrime, and a Full Spectrum Defense. v1 7 Dec 2007