IDC
Analyze the Future

WHITE PAPER

The Risks of Obtaining and Using Pirated Software

Sponsored by: Microsoft

John F. Gantz
Al Gillen
Christian A. Christiansen

October 2006

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

IN THIS WHITE PAPER

This White Paper presents the results of an investigation by IDC into the prevalence of malicious code and unwanted software at Web sites that offer pirated software, counterfeit product keys, crack tools, and key generators for Microsoft Windows XP and Microsoft Office. The investigation also looked for such code in key generators and crack tools that are available for download at various Web sites and from peer-to-peer networks.

The intent of the research was to test the degree to which users obtaining and using pirated software are exposed to computer security risks in doing so.

EXECUTIVE SUMMARY

- There are number of methods for obtaining and using counterfeit software. The commonly used ones are obtaining and using counterfeit product keys, obtaining "key generator" programs and using them to create product keys, and obtaining "crack tools" and using them to bypass licensing and activation mechanisms. *Our investigation tested exposure to security risks by (1) visiting Web sites that offer counterfeit product keys, key generators, and crack tools, and (2) downloading and using crack tools and key generators from these Web sites and from peer-to-peer networks.*

- Simple Web searches easily led to sites that offer pirated software, counterfeit keys, crack tools, key generators and so on. It was also easy to find key generators and crack tools for Microsoft Windows and Office on peer-to-peer networks. *It is not difficult to find the kind of software we were looking for.*

- 25% of the Web sites we accessed offering counterfeit product keys, pirated software, key generators or crack tools attempted to install either malicious or potentially unwanted software. *There are a significant number of sites that will attempt to install malicious or unwanted code.*

- 11% of the key generators and crack tools downloaded from Web sites and 59% of the key generators and crack tools downloaded from peer-to-peer networks contained either malicious or potentially unwanted software. *There is a*

significant amount of malicious or unwanted code to be found in key generators and crack tools.

- The cost to organizations to recover from a single incident of malicious software on a single workstation can run over a thousand dollars. The cost to organizations from lost or compromised data can run into the tens of thousands of dollars per incident. *The "savings" of using pirated software can be wiped out with a single security breach.*

- The kind of malicious and unwanted code we found is symptomatic of the transformation noticed by security professionals in the motivations of attackers – from hacking for fun to seeking information held on computers as a means to ill-gotten gains. *Offering pirated software, crack tools, key generators can be just another way for attackers to lure victims into their scams.*

IDC believes that we found enough malicious or unwanted code in our tests to conclude that obtaining and using pirated software can pose a serious security risk to those who do so.

OBTAINING PIRATED SOFTWARE

There are a number of ways for end users to obtain unlicensed, counterfeit, or pirated software.[1]

In addition to obtaining it unknowingly through a distribution channel or by violating the terms of a volume license, the most common methods are:

- Obtaining counterfeit product keys from Web sites and using them with software obtained from sources such as friends or download sites. Counterfeit product keys are fake product keys (keys that appear to be authentic but have not been generated by Microsoft) and stolen product keys (product keys which are stolen from a legitimate copy of Windows or Office, for example, by copying them from the sticker on the personal computer). These product keys are used to bypass licensing and activation mechanisms present in Microsoft software.

- Downloading key generators from Web sites and peer-to-peer networks and using them to generate product keys for use with software obtained from sources such as friends or download sites. Again, the keys generated are used to bypass licensing and activation mechanisms present in Microsoft software.

- Downloading crack tools from Web sites and peer-to-peer networks and using them with software obtained from sources such as friends or download sites. The crack tools are programs that tamper with the Microsoft software itself to

[1] What's the difference between pirated and counterfeit software? By most definitions, "pirated software" is software that is improperly licensed or not licensed at all, and "counterfeit software" is software that is deliberately presented as genuine when it is not. In this White Paper we may use the terms interchangeably because of the common need to find the software on the Internet and bypassing licensing and activation mechanisms by using counterfeit keys, keys produced by key generators or crack tools. Regardless of the source of the actual programs, the journey to find and use them entails the same risks.

bypass licensing and activation mechanisms. Examples of these tools include programs that delete timers in Microsoft software so that the software is always in grace period, programs that tamper with Microsoft binaries responsible for enforcing licensing and activation mechanisms, and so on.

- Downloading full copies of the packaged software from download Web sites or peer-to-peer networks. Some downloads can take as long as 24 hours.
- Obtaining physical media for sale over the Internet from sites such as eBay.
- Obtaining physical media from street vendors or computer stores.

Our investigation was limited to the first three methods. The time and energy to download full copies of software or to obtain physical disks either from sale over the Internet or from street vendors and computer stores was outside the parameters of the project (see sidebars *What About Physical Media?* and *EBay: Trouble in the Neighborhood.)* However, even for the software acquired via the other three methods, counterfeit product keys, key generators, or crack tools may still be necessary to use the software.

TEST METHODOLOGY

To assess the risks of obtaining and using pirated software, IDC investigated whether visiting the Web sites offering tools and techniques for using pirated software and downloading and using key generators and crack tools would expose users to malicious or potentially unwanted software.

IDC set up a testing lab within its own IT department and ran tests on Web sites offering pirated or counterfeit software, key generators, or crack tools for two weeks in August 2006. The latest versions of commercially available anti-malware software were used to identify malicious and potentially unwanted software. The security team at Microsoft then added to the research by actually downloading key generators and crack tools from the Web sites we analyzed and from peer-to-peer networks.

More details on the testing methodology and the IDC lab can be found in the section *Testing Protocol*.

TEST RESULTS

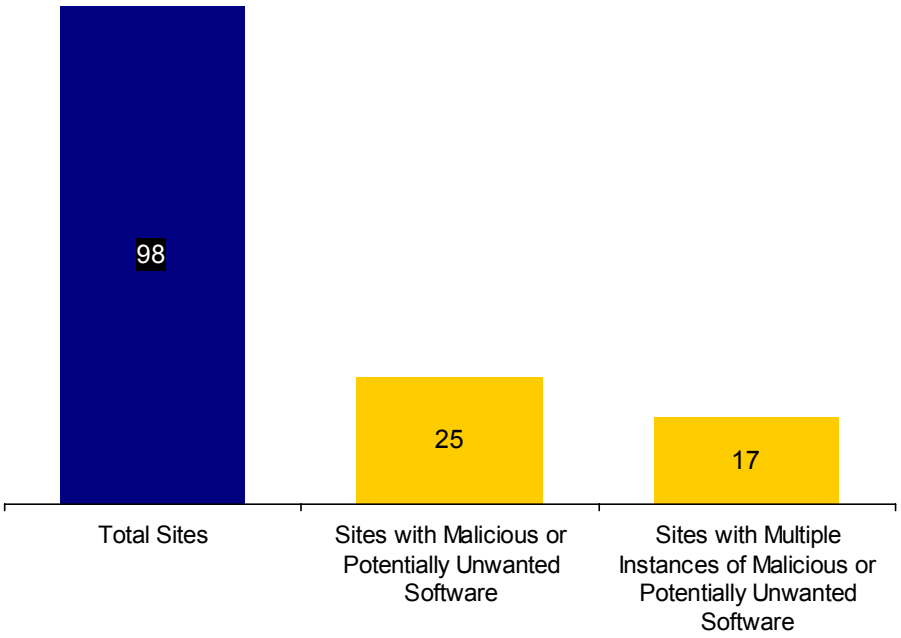
This section presents the results of the investigation, detailed in three subsections. *Seeking Counterfeit Software* details the security risks a user is exposed to when visiting Web sites offering tools and techniques for using pirated software. *Using Key Generators and Crack Tools* details the security risks a user is exposed to when using the key generators and crack tools downloaded from Web sites and peer-to-peer networks. *Makeup of Malicious and Unwanted Software* presents an overview of the malicious and unwanted software discovered during our investigation.

SEEKING COUNTERFEIT SOFTWARE

In all we found and tested 98 unique Web sites offering access to counterfeit product keys, pirated software, key generators and crack tools for Windows XP and Office. Figure 1 shows what we found at these Web sites with our anti-malware software.

FIGURE 1

Web Sites Hosting Keys, Key Generators, or Crack Tools



Source: IDC Study, *Risks of Obtaining and Using Pirated Software, 2006*

25 of the 98 Web sites (25%) that we encountered hosted malicious or potentially unwanted software; at two-thirds of those we found multiple instances of such software. In some cases, the Web sites exploited vulnerabilities in an attempt to install the unwanted software automatically. In other cases, the user was required to take manual action, such as installing an ActiveX control. Where this install was absolutely required (e.g., to download a key generator or a crack tool, or to navigate the website), we took this manual action, assuming the user would as well.

Although the exploits used by the Web sites targeted vulnerabilities that have been addressed with security patches, nonetheless, the intent of the individuals hosting these exploits was malicious. And remember, not all users have up-to-date anti-malware software or are up-to-date with the latest security updates.

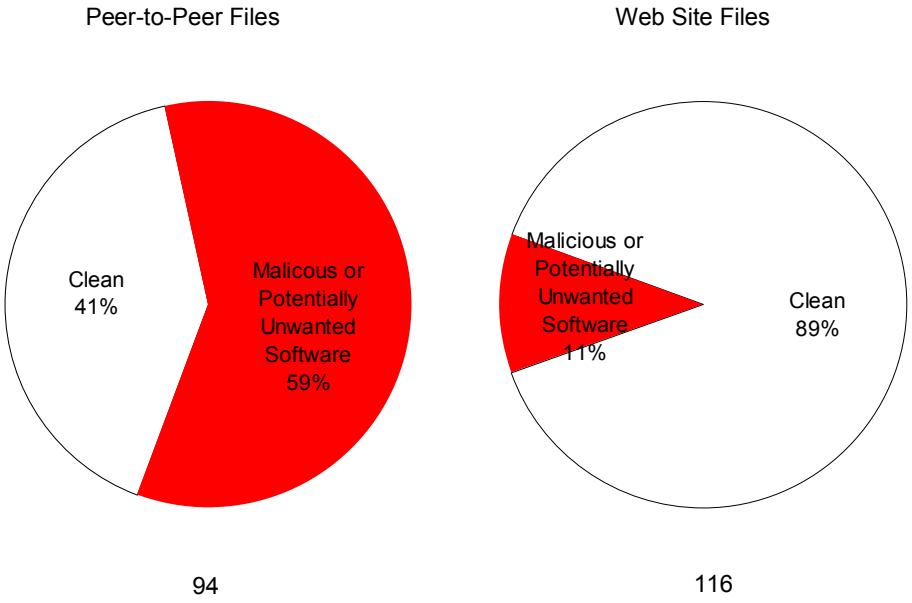
USING KEY GENERATORS AND CRACK TOOLS

The key generators and crack tools were downloaded from two sources, Web sites and peer-to-peer networks. Figure 2 shows what we found in this downloaded software.

116 files were downloaded from Web sites and 13 (11%) were found to contain malicious or potentially unwanted software. 94 files were downloaded from peer-to-peer networks and 55 of these (59%) were found to contain malicious or potentially unwanted software.

FIGURE 2

Downloaded Keys, Key Generators, and Crack Tools



Source: IDC Study, Risks of Obtaining and Using Pirated Software, 2006

It is important to note that peer-to-peer networks themselves can be extremely useful for sharing data, and some peer-to-peer networks have integrated virus scanning for uploading and downloading content. This strips out most of the malicious software before it is shared.

However, as our findings indicate, users need to be diligent about the type of software downloaded from these networks.

MAKEUP OF MALICIOUS AND POTENTIALLY UNWANTED SOFTWARE

During our investigation, we found a wide range of malicious and potentially unwanted software[2], from software that is designed to open connections on a user's system and allow third parties the ability to download and execute programs on the

[2] Note, the names and classifications of the malicious and unwanted software, as presented in this section, conform to McAfee VirusScan Enterprise 8.0i, Symantec's Norton AntiVirus 2006 and Computer Associates' eTrust Antivirus r8 for Windows.

infected system (W32/Beagle) to software that injects advertising content at the top and bottom of web pages (Zquest).

In the Web site search, one piece of software we found multiple times (xpladv470), was written up earlier this year in a Websense Security Lab alert[3] as having been observed getting more malicious over time. Originally it was typically used to install unwanted software, like counterfeit anti-spyware removal tools, toolbars, and adware. But by early 2006 Websense noticed the files downloaded by the Trojan performing functions like logging keystrokes when users accessed banking sites and redirecting traffic to fraudulent PayPal Web sites

The key generators and crack tools that we downloaded contained worms such as Win32.Alcra.F and Win32.KwBotF.Worm; Trojan droppers such as, Win32.VB.GK; backdoors such as, Backdoor.Bifrose and Infostealer.Ld.Pinch.E; and adware such as, ZangoSearch and DollarRevenue. The latter programs can monitor the contents of Web browser windows and install additional adware programs.

WHAT DOES THIS MEAN FOR YOU?

The test results speak to the dangers of seeking and using pirated software. IDC's security market analysts classify those risks into three types of threat:

Infection from unwanted code—running from mild to severe. On the mild side is annoying code, like adware, with its constant barrage of pop-up ads and potential home page hijacking. More destructive code, like Trojans, can potentially consume system resources until a device becomes inoperable. Finally there is potentially devastating code, like bots and keyloggers, which can take over a machine to relay spam, store illegal files, or give third parties access to sensitive data.

Degradation of security protections—malicious and unwanted software like that found in our tests has been known to prevent antivirus software and firewalls from running and/or receiving updates. Some adware even produces pop-up ads for counterfeit spyware removal tools—sometimes asking the user to pay for software to clean the ads just created.

Degradation of application performance—security problems don't always present themselves as such. In many cases, the user simply notices a system problem and calls the IT department. Spyware is especially known to slow network performance or Internet access or to create log-in problems and remote access issues.

Our research shows that even up-to-date systems running latest anti-malware software are vulnerable. New viruses, Trojans, worms, and spyware programs appear all the time. And how many users stay right on top of security updates or use the very latest anti-malware tools?[4]

[3] http://www.websense.com/securitylabs/alerts/alert.php?AlertID=395

[4] For a sobering view of trends in security threats like some of those discussed here, see *The Trend of Threats Today, 2005 Annual Roundup and 2006 Forecast,* by Jaime Lyndon, A. Yaneza, and David Sancho, of Trend Micro, available at http://www.trendmicro.com/en/security/white-papers/overview.htm#annual-roundup.

WHAT ARE THE FINANCIAL RISKS?

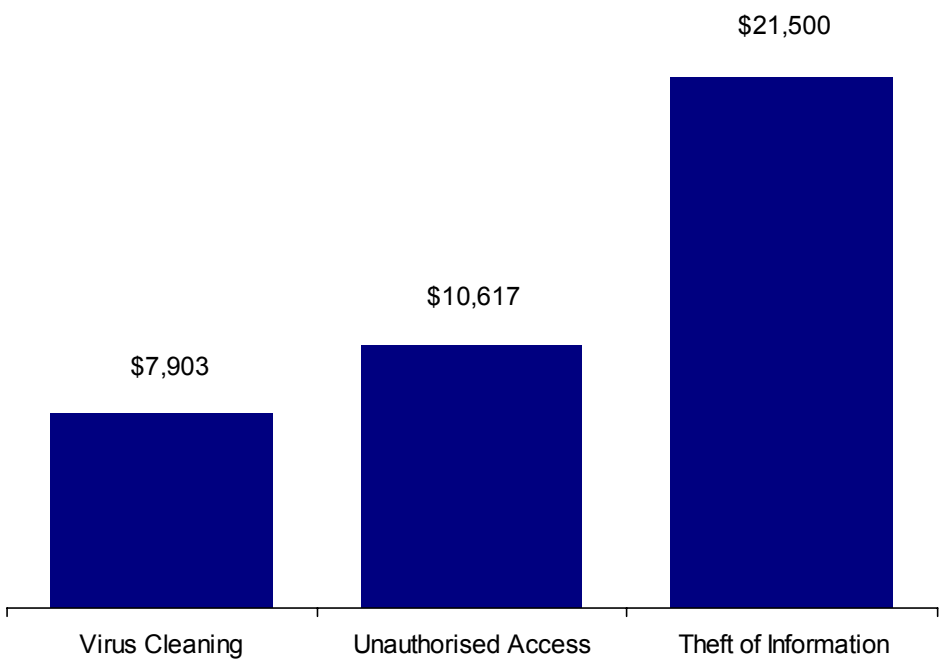
To a consumer, given the security risks, the cost of obtaining and using a pirated or counterfeit copy of Windows or Office can include the cost of one or more service calls to clean the system, the loss of data or information on an infected system that needs to have its hard drive reformatted, or the much larger cost of identity theft.

For enterprises, the costs can be even greater. In its 2006 survey of 616 US IT security professionals,[5] The Computer Security Institute found that 65% of companies represented had experienced a virus attack, 32% unauthorized access to information, 15% system penetration and 9% theft of proprietary information—all threats enabled by malicious software applications like those identified in our testing.

The data from that survey, shown in Figure 3—which plots the cost per security incident by type per respondent—demonstrate that the financial risks of using such software can be high.

FIGURE 3

The Costs of Malicious Code



Source: IDC calculations using data from the FBI/Computer Security Institute survey, 2006; N=616

While the data in Figure 3 show per-incident costs per respondent, they don't show per workstation cost. What would it cost to fix just one incident on one computer?

[5] *Eleventh Annual CSI/FBI Computer Crime and Security Survey, 2006,* Computer Security Institute, http://www.gocsi.com/; published with permission.

The answer obviously varies by company or individual and by incident type. However, according to a 2002 study[6] by Trend Micro, Inc., the cost to stop a workstation, scan for and clean malicious or unwanted software, and document everything is over $1,000. Would these costs hold today? Probably. IDC's own internal costs to diagnose a system problem resulting from malicious or unwanted software, back up the existing data, reformat the hard drive, and re-image the system are in the same ballpark. And these costs don't include the value of lost data, the loss of end user productivity, or the cost to an organization of losing proprietary information.

It's true that not *all* attempts to obtain and use pirated or counterfeit software will lead to a security event, but our research indicates that the risks are nevertheless real.

FUTURE OUTLOOK AND ESSENTIAL GUIDANCE

In the US, according to the Business Software Alliance, more than one in five PC software packages is pirated or counterfeit—a ratio that has barely lowered over the last decade. At the same time, security threats have increased dramatically.

Not only have attacks increased in number and type—from computer viruses and worms to viruses, worms, Trojans, denial-of-service attacks, spyware, adware, downloaders, Phishers, bots, and rootkits—but the motivation behind the attacks has changed. Last year, according to Trend Micro,[7] "the vast majority of threats were for financial gain, rather than the apparent desire for notoriety or bragging rights that influenced malicious behavior in prior years."

As an example of some of the economics of the "malware" world, in July 2006, Websense Security Labs discovered a fraudulent World Cup 2006 Soccer Web site that would infect visitor's system with a Trojan that downloaded additional software onto the PC. The site used a tool kit, called Web Attacker, sold by a Russian Web site. The tool includes a graphic user interface and the ability to collect statistics on infections created.

Attackers are finding new and better ways to compress files, link multiple sets of malicious code together, for example by using one Trojan to download another, and even sending malicious code out with components that remove competing malicious code. Producing malware has become an industry.

In this atmosphere, it seems logical to infer that the risks faced by users seeking to use pirated software can only increase.

There are ways to prevent attacks like those we detected, by installing firewalls, using up-to-date anti-malware software and keeping your system up-to-date with the current security releases. But the best prevention of the security risks from obtaining and using pirated software is simply to use the genuine item. In the long run it can cost less.

---

[6] *The Real Cost of a Virus Outbreak,* March 1, 2002. http://www.trendmicro.com/

[7] See http://www.trendmicro.com/en/security/white-papers/overview.htm#annual-roundup.

SIDEBAR: WHAT ABOUT PHYSICAL MEDIA?

IDC did not test physical media. We did, however, review the work Microsoft conducted earlier in the year analyzing disks obtained by Microsoft employees who purchased mid-grade counterfeit software in various countries around the world.

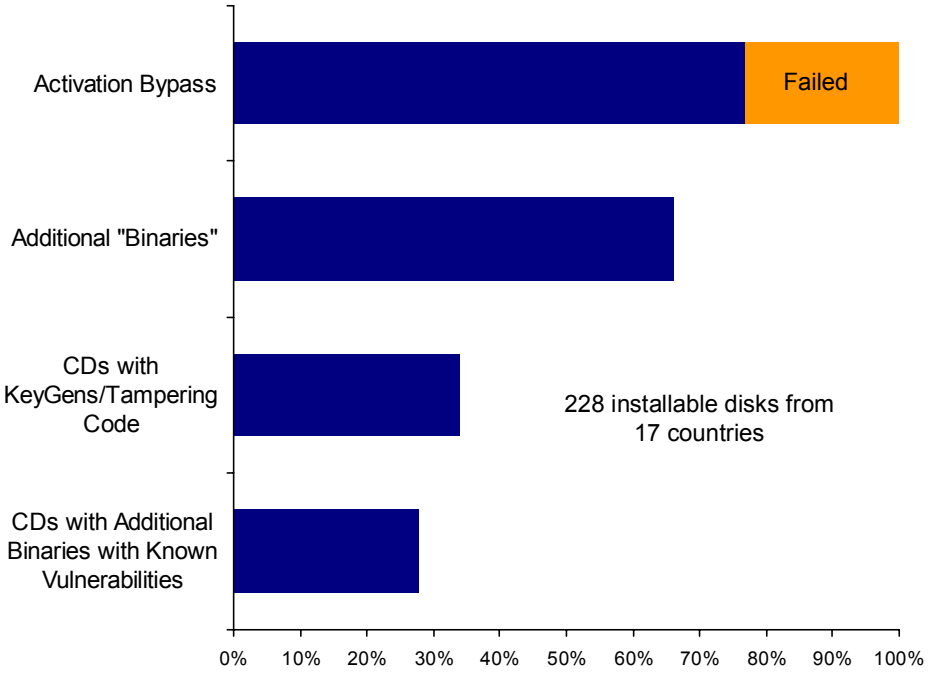
How did the physical media fare?

Here, the issue wasn't embedded malicious software, but vulnerabilities introduced through additional software and software that changed the nature of original packages. These came in several ways:

- Some packages came with software that wasn't part of the genuine Microsoft Windows program ("additional binaries").
- Some of the additional binaries represented key generators or code that actually changed the nature of the original program.
- Some of the additional binaries represented third party software with known security vulnerabilities.

And, although not a vulnerability, in some cases the software could not bypass Microsoft's activation mechanisms. (In fact, 34% of counterfeit disks coundn't even be installed). A summary of the results is shown below:

Risks in Counterfeit Media (Percent of Installable Disks)



Source: Microsoft Study, 2006; 348 disks obtained, 228 installable, 17 countries

SIDEBAR: EBAY: TROUBLE IN THE NEIGHBORHOOD

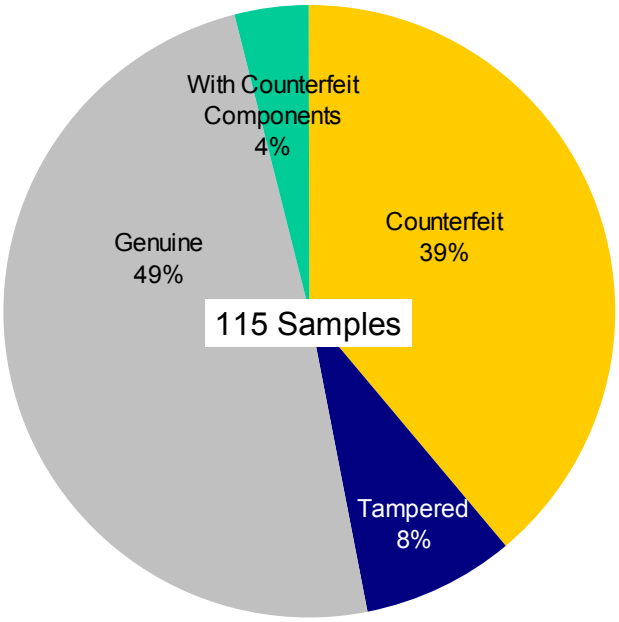
Searching for a deal? Why not buy your software on eBay? For many people, that can be a legitimate way to obtain genuine software at a discount.

But not all software sold on eBay is legitimate. Together, Microsoft and eBay intervene in about 50,000 software auctions a year that are deemed to be infringing copyright. Who knows how many sales get through that net?

Those that do run some of the risks we have been talking about. In test purchases of over 115 copies of physical media purchased over eBay in 2005, Microsoft's legal team found that 39% were counterfeit. An additional 12% came with either additional software components that were counterfeit or genuine software that had been tampered with.

This indicates that the chance of an individual customer buying genuine legally licensed software on eBay is less than 1 in 2—not particularly great odds for a product used to store and process important and often highly confidential personal and business information.

EBay Test Purchases



Source: Microsoft Legal and Compliance team, 2006; "tampered" includes both genuine software with counterfeit components and genuine software that has been tampered with

How many of these disks would result in security threats? While our study did not test the purchased media, the pirated or counterfeit software may require a product key, a key generator or a crack tool. If so, users seeking to use them would come across the same security threats that we encountered.

TESTING PROTOCOL

ANALYZING WEB SITES

The analysis of Web sites by IDC was performed on VMware virtual machines (VMware workstation version 5.5.1) running on three standard IDC laptops. The virtual machines ran IDC's standard image of Windows XP (SP2) complete with all Microsoft security updates and Microsoft Internet Explorer 6.02.

The testing protocol was to use anti-malware software (McAfee VirusScan Enterprise 8.0i and Computer Associates' eTrust Antivirus r8 for Windows) to monitor traffic from the Web sites and identify any attempts to install malicious or potentially unwanted software. The anti-malware definitions were up to date as of the day of testing.

The goal was to test the Web sites that offer pirated or counterfeit software, counterfeit product keys, key generators or crack tools for identifiable security threats.

Given below is the step-by-step process for analyzing Web sites:

1. Search for Web sites that offer access to free Microsoft software, product keys, key generators and crack tools for Windows XP or Office. Search engines used were MSN Search, Yahoo, and Google. Search terms included "Windows XP," "Office," "keygens," "cracks" and so on.

2. Once a website is identified, open it using Internet Explorer.

3. Browse the website while searching for counterfeit product keys, key generators and crack tools. In case the website requires manual action, such as installing an ActiveX control, take this action if it is absolutely necessary (e.g., to navigate the website).

4. Record any instances of malicious and potentially unwanted software identified by the anti-malware software.

5. Follow any links on the site that refer to additional sources of "free" software, product keys, key generators or crack tools.

6. Repeat the process for all identified Web sites.

ANALYZING KEY GENERATORS AND CRACK TOOLS

Subsequent to IDC's Web sites tests, the Microsoft security team downloaded key generators and crack tools from the Web sites that IDC identified and from peer-to-peer networks. The goal was to test if these key generators and crack tools contained any malicious and potentially unwanted software.

The analysis of the downloaded software was performed on machines with Microsoft Windows XP Gold (no server packs and no security patches) and Internet Explorer 6.0. Note that the patch level of the operating system is *not* relevant when using downloaded software. Because the software would be run manually by the user, it

would have the same effect independent of whether the operating system was not patched at all or fully patched.

The anti-malware software used to identify malicious and potentially unwanted software included: McAfee VirusScan Enterprise 8.0i, Computer Associates' eTrust Antivirus r8 for Windows, and Symantec's Norton AntiVirus 2006. Again, the anti-malware definitions were up to date as of the day of testing.

The analysis of the downloaded software was similar that of the Web sites, except these were first downloaded (both from Web sites and peer-to-peer networks) and then scanned by the anti-malware software.