

As PC Virus Turns 25, Attack Toolkits Arrive

Twenty-five years ago, the Alvi brothers of Pakistan gave the world the Brain Virus, the first bit of malware capable of infecting a DOS-based PC. The brothers embedded their real names and business address in the code and later told Time magazine they had written the virus to protect their medical software from piracy. Twenty-five years later, most malware is anything but benign and cyber criminals pull off exploits the Alvi brothers never envisioned.

Using Web based statistics from a number of sources, including Kaspersky Labs, the following two tables show the birth of viruses from 1990 to 2008, and the number of known viruses in Jan 2011.

Table 1 Virus Growth from 1980 to 2010 from Internet Sources

| Year | Number of Viruses Reported | Year | Number of Viruses Reported |
|------|----------------------------|------|----------------------------|
| 1990 | 200 to 500 | 1991 | 600 to 1000 |
| 1992 | 1,000 to 2,300 | 1994 | 4,500 to 7,500 |
| 1996 | Over 10,000 | 1998 | 20,000 |
| 2000 | 50,000 | 2008 | Over 1 Million |

| Total # of viruses in their database | Viruses added in their last update | Viruses added in last 7 days | Recent number of viruses added per hour |
|--------------------------------------|------------------------------------|------------------------------|---|
| 4, 671, 288 | 4,066 | 64,284 | 306 |

Table 1 Kaspersky Labs 2011 Virus Statistics

Malware is now a tool attackers use to use to steal from consumers and institutions alike. Hackers now mimic legitimate business owners, by creating and selling kits that produce malware. Recently, online sales of

Jan 2011: Malware Development Kits Now On Sale on the Internet

these "kits" that allow relatively unskilled hackers to create and launch malware attacks against production systems have been noticed. The kits, sometimes called crimeware, are used to facilitate the launch of concerted and widespread attacks on networked computers. According to a Symantec report, these kits are usually composed of prewritten malicious code for exploiting vulnerabilities along with various tools to customize, deploy, and automate widespread attacks.

With careful scrutiny, you can find cheap attack kits selling on the Web for various prices, ranging from \$40 or \$50. The top two attack toolkits in terms of malicious Web activity are **MPack (48%)** and **NeoSploit (31%)**. **The ZeuS attack kit is only third at (19%)**, but it costs between \$4,000 and \$8,000 depending on how much support you purchase. ZeuS can be used in Botnet form to steal financial data and execute fraudulent transactions. ZeuS prices range from \$4,000 to more than \$8,000. Some kits come with online support and subscription services, so customers can get updated versions of the malware. Symantec has also observed advertisements offering to help install and set up purchased attack kits for a fee. "It's like a mirror of the legitimate software business!"

Symantec says that two-thirds of malicious Web activity can be traced back to Botnets and exploit code built using these popular attack toolkits sold in the underground economy. Symantec also notes the kit builders are in an all out war to oust rivals and gain criminally-minded customers willing to pay, especially those interested in ZeuS.

Symantec has to delve into attack toolkits since they must design countermeasures to ZeuS built viruses. Most consider that developing attack kits is not a crime. Symantec's report suggests that the tremendous growth of malware we've seen in the last two years is driven by these toolkits. These attack toolkits make it fairly easy for anyone to get into rackets that include everything from running Botnets for spam, financial crime and denial-of-service attacks, or simpler tasks like compromising PCs with malicious Trojans through Web drive-by downloads, often from legitimate websites that have been compromised. Known adult entertainment and video streaming websites, along with their misspelled-

typo equivalents, are said to be the most likely sites that attackers load up with malware.

VULNERABILITY TARGETS

Most often exploited by these attack toolkits were **Microsoft Active Template Library Header Data Remote Code Execution Vulnerability** at 41%; **Adobe Flash Player** at 25%; and **Microsoft Windows Media Player** at 9%, with various other Microsoft and Apple protocols also popular.

In general, Symantec's research indicates that attack toolkit developers don't particularly rush to get new vulnerabilities into their attack code, nor do they strive to incorporate zero-day attacks. There is now even an attack toolkit open-source project, the Hybrid Botnet System. Symantec depicts an underground world where attack toolkit developers worry about piracy and install backdoors in their code to monitor their customers whom they don't trust.

The successful attack toolkits are activity updated and have led to a thriving business in providing post-sales services, Symantec reports. Attack kits are now "prevalent enough to support a services-based economy whereby the kit developers and others provide a range of additional, post-purchase services to enhance the profitability of the kits."

A cheaper version of Zeus, called **SpyEye**, even had a "Kill ZeuS" feature when it discovered ZeuS malware. The SpyEye developer announced in October 2010 that he had acquired the ZeuS source code from its developer. The original ZeuS developer claims to be no longer involved in the ZeuS project, but the SpyEye developer is providing existing ZeuS customers with support services.

In its post-script, the Symantec report emphasizes the need for computer users to keep their software patched and running security-protection software as means for protecting against the proliferating variants of malware spawned by the attack toolkits in the hands of cybercriminals.

Here are five reasons to be concerned about these kits:

1. Attack kits make it easier for relatively unsophisticated hackers to launch an attack. Not just any computer user could successfully use one

of these kits, but for those who can, it's much easier than building a virus or other malware from the ground up.

2. The prevalence, simplicity and effectiveness of the attack kits are contributing to an upward spike in cybercrime. One major kit, called ZeuS, has accounted for more than 90,000 unique malicious code variants as of August 2009, and millions of computers have now been attacked by ZeuS developed viruses. ZeuS is designed primarily to steal financial details, such as the online banking credentials of a victim. Its ease of use and ability to generate income makes it an appealing purchase for even novice cybercriminals.

3. Cyber criminals seek a return on their investment. Since they're spending money to buy a kit, it's likely they'll want to use them. Because buyers of the kits can get updates, they're using the newest and most potent versions of the malware, which means that it is likely that users will be hit even harder. So the changes of kit produced malware evading your existing virus protection are good.

4. Increasingly, attack toolkits include exploits for vulnerabilities that encompass multiple applications and technologies. This increases the likelihood that an attack will succeed because there is a greater chance that the victim will be using one of the vulnerable applications and that one of the applications is unpatched.

5. The attack kits spew out malware that can attack multiple platforms; so users of Macs or computers running the Linux operating system, which are usually considered safer than Windows, are at risk as well.

Naturally, you want to defend yourself from these cutting edge attacks. So be sure you're running reputable defense programs and keep them updated. And since many of the kits rely on "poisoned" Web sites, make certain that if your malware detector questions the authenticity of a site you pay attention and get out of there without clicking on anything.

It's tempting to make jokes about the Alvi brothers, and to be sure, the story of the Brain Virus has its place in computer lore. **But ultimately, this stuff isn't funny, and it's not really a happy 25th virus anniversary.**