



WHY DO PEOPLE MAKE VIRUSES?

Over our past seven years in this business at Computer Care Clinic, the most-asked question we've received is "Why do people make viruses?"

Years ago, as strange as it sounds, we're now talking decades ago, the source of a computer virus was some very bright teenage prankster looking to cause some mischief for bragging rights.

It was no big deal until the mob found out there was a way to make big money with this kind of nonsense. Writing an effective malware program is time consuming. And sustaining a piece of malware – making sure it is undetected by antivirus scanners, updating its functionality, and maintaining its command and control servers takes time and concerted effort on the part of a group of cybercriminals.

The game has changed substantially since the first national news reports you might still be referring to when you think "virus," so it's time to update some definitions. Viruses are only one of many forms of software created for malicious software, now known collectively as "malware."

TYPES OF MALWARE

Viruses and worms are still the superstars of the malware category, known for the manner in which they spread rather than any other particular behavior. The term computer virus is used for a program that has infected some program and, when run, causes the virus to spread to other programs. Viruses may also contain a payload that performs other actions, often malicious. On the other hand, a worm is a program that actively transmits itself over a network to infect other computers. Worms too may carry a payload.

One of the more common ways people make money writing malware is by writing a program that masquerades as legitimate computer protection. People become alarmed at the number of detected viruses these illegitimate programs seem to find on their machines and buy the program that does nothing and continually needs to be renewed. When that malicious program is disguised as something useful or desirable, users may be tempted to install it without realizing they have just installed a Trojan horse, or Trojan for short, similar to its Greek mythological counterpart. A Trojan horse is any program that conceals a harmful or malicious payload. The payload may take effect immediately, in the future, or

on demand when it receives an initialization command over the internet and can lead to many undesirable effects, such as hiding or deleting the user's files or further installing more harmful software. Trojan horses known as droppers are used to start off a worm outbreak, by injecting the worm into users' local network.

Infected computers may be used as proxies to send out spam messages. A computer left in this state is often known as a zombie computer. The advantage to spammers of using infected computers is they provide anonymity, protecting the spammer from prosecution. Spammers have also used infected PCs to target anti-spam organizations with distributed denial-of-service attacks. In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware logs itself into a relay system. The attacker can then give instructions to all the infected systems simultaneously. Botnets can also be used to push upgraded malware to the infected systems, keeping them resistant to antivirus software or other security measures.

Adware is software that displays advertising banners on Web browsers such as Internet Explorer and Mozilla Firefox. While not categorized as malware, many users consider adware invasive. Adware programs often create unwanted effects on a system, such as annoying popup ads and the general degradation in either network connection or system performance. Adware programs are typically installed as separate programs that are bundled with certain free software. Many users inadvertently agree to installing adware by accepting a craftily worded End User License Agreement (EULA) on the free software. Admit it, you never read those either. Adware is often installed in tandem with spyware programs. Both programs feed off each other's functionalities – spyware programs profile users' Internet behavior, while adware programs display targeted ads that correspond to the gathered user's web surfing habits. It's pretty clever stuff.

Spyware programs are produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator. Some spyware programs redirect search engine results to paid advertisements. Others can overwrite affiliate marketing codes so that revenue is redirected to the spyware creator rather than the intended recipient. That's big money these days, well into the millions in some cases.

It is possible for a malware creator to profit by stealing sensitive information from a victim. Some malware programs install a "key logger," which intercepts the user's keystrokes when entering a password, credit card number, or other information that may be exploited. This is then transmitted to the malware creator automatically, enabling credit card fraud and other theft. Similarly, malware may copy the CD key or password for online games, allowing the creator to steal accounts or virtual items.

Grayware is a rarely used term, but refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on a network and introduce significant security. Often grayware performs a variety of undesired actions such as irritating users with pop-up windows, tracking user habits and unnecessarily exposing computer vulnerabilities to attack.

WHY DO PEOPLE CREATE MALWARE?

It's all about the money. Identity theft, fooling people into purchasing Trojan horse software, earning thousands of dollars from forcing unsuspecting people into clicking on 'pay-per-click' advertisements, and a competitive advantage from a denial of service attack are just a few of the ways one can create a large return on investment from malware. It's possible to make millions of dollars in a malware scam in less than one hour.

Today's cybercrime economy is made up of a complicated yet organized mix of specialists, each of whom makes money doing their individual part. The kingpins typically operate in Eastern Europe or China, where the law enforcement reach of Western countries is inconvenient if at all possible.

A Bot can completely take over a computer and set it up so that the bot writer has control over that computer and several thousand others. For a website that is able to protect itself very well in terms of hacking, the idea is to instead overload its servers. Thousands of simultaneous website requests sent by infected computers can overload a web server and take it down, allowing other websites to get a competitive edge via a damaged reputation or additional sales. Other bot variations might use the infected computers as SPAM (junk e-mail) sending robots, collecting thousands of dollars for that service from some rogue advertiser.

In 2010, a group of organized cyber criminals who are alleged to have made \$14m from advertising fraud were arrested in Estonia. The FBI alleged that the gang infected more than four million computers in 100 countries with code that redirected users to online ads. About 500,000 of the affected computers were in the US and many of the millions inadvertently enrolled in the fraud scheme were in government offices, schools, and corporates. NASA first discovered the malicious software on 130 of its computers. Security firm Trend Micro also provided key intelligence during the long investigation. The FBI claimed that the "massive and sophisticated internet fraud scheme" revolved around servers set up to surreptitiously reroute traffic to websites where the gang would get a cut of the advertising revenue. Victims would start out trying to visit sites such as Amazon, Netflix and ESPN but instead end up on sites displaying adverts put together by the gang, said the FBI in a statement. "These defendants gave new meaning to the term, 'false advertising'," said Manhattan US attorney Preet Bharara in a statement detailing the take down which the FBI dubbed "Operation Ghost Click". Describing the gang as "cyber bandits", Mr Bharara alleged they collected "millions in undeserved commissions for all the hijacked computer clicks and internet ads they fraudulently engineered".

Perhaps Eugene Kaspersky, founder of anti-virus maker Kaspersky Labs said it best, "It's a different world today. 10 years ago, we were fighting against smart kids who hacked as a hobby. Now, we're dealing with criminal gangs that control your computer to make money."

ARE MACs VIRUS-PROOF?

Apple's now famous and very misleading advertising says "Mac OS X doesn't get PC viruses. And its built-in defenses help keep you safe from other malware without the hassle of constant alerts and sweeps."

Technically, since Mac too is a PC, or Personal Computer, the preceding statement is an outright lie. It is true Mac OS X doesn't get Windows-based viruses – Mac OS X gets Mac OS X viruses. And there are plenty of them. Visit Apple's website (<http://support.apple.com/kb/ht4650>) for proof.

And those Mac viruses are just as nasty as the PC viruses, but they'll cost twice as much to remove. Nicole, one of our interns, got infected with one of those Mac viruses before she started working with us. Not knowing what else to do, she had Apple handle the removal. They fixed it – by asking her to mail her computer to Cupertino, then reloading her operating system, and charging her almost \$500. With Apple market penetration nearing 10%, you'll see more and more Mac malware. It's not as prevalent as Windows based infections today, but the organized cyber criminals are very much aware that there are millions of Mac users with their pants down. When that storm hits, It ain't gonna be pretty.

If you have a Mac, invest in some antivirus software as soon as possible. Symantec, McAfee and Sophos provide pretty good protection. Regardless of what lies your Mac salesman tells you (and we've heard some doosies personally, but Florida law prohibits us from recording them), there is no 'perfect' antivirus solution. There are security flaws and backdoors to every operating system that exists.

On the PC side, it's rare that someone explains why PCs are more vulnerable to malware. Unlike Steve Jobs and his tyrannically closed systems, Bill Gates and his associates decided to leave their operating system a bit more 'open' so many different vendors could produce hardware and software that would run on his DOS and later Windows platforms. Programmers will tell you it's nothing short of a small miracle that Windows runs well on so many varied hardware platforms, which is obviously why Microsoft is the world leader in operating systems. This 'openness' initiative unfortunately comes with the sacrifice of several more areas that may be exploited by malware.

WHAT CAN I DO TO PROTECT MYSELF?

There are several things you can do to protect yourself from today's malware. You've used computers long enough to notice when something just doesn't 'look right.' Websites with obvious advertising pop-ups. Emails with misspelled words. Poor English. Domains (dot-coms) that look a little too descriptive for what you're trying to search for. Fortunately, malware people are very poor marketers and even worse social engineers – so far.

Otherwise, here are some tips you can use to protect yourself.

- *Keep your Windows operating system software up to date.*
- *Install a good antivirus program and set it to auto-update daily and auto-scan weekly.*
- *Install a complementary antimalware program and set it to auto-update daily and auto-scan weekly.*
- *Keep your Java software up to date. Java's automatic updater will show up in the bottom right hand corner of your screen periodically.*
- *Keep your Adobe Flash software up to date. The Adobe automatic updater will show up in the bottom right hand corner of your screen periodically.*

- *Avoid visiting websites that just don't look right. You can tell from their listings in the search engines.*
- *Do not open attachments to email that just don't look right.*
- *Call Computer Care Clinic and have us install our super-secret 'Virus-Free Internet' solution.*