Psst... Hey Buddy, Wanna Create a Virus?

David Pearson

Psst…Hey Buddy, wanna create a virus?

David Pearson
Version 1.2f
February 13, 2003

Introduction

So, you think there are only a handful of virus creators out there? Just a couple of guys sitting in a back room in some third-world country clunking away on what we would consider a boat anchor of a PC? Think again. The person in the cubicle next to yours could, at this very moment, be creating a virus. Viruses will continue to be generated in greater numbers than ever before. Why? First of all, the number of people with access to computers and the Internet will continue to escalate. Secondly, creating viruses has become easier with the development and availability of virus authoring kits such as the (K)alamar Virus Creation Toolkit or Triniti's VBS Worm Toolbox. The ability to write viruses has also become easier. Languages such as Visual Basic and Visual C, C++, both of which make use of GUI interfaces, make it so that very little actual programming knowledge is required. Virus authoring kits are also available for free on the Internet, and have made it fairly easy for someone to generate a virus or learn enough from the source code generated by the kits to write their own virus. With this truth and ease of availability, we are likely to see a dramatic increase in viruses as the potential virus writing community increases in number and the means for developing viruses and malicious code becomes easier.

Here's what one aspiring virii creator had to say about his craft:

"Virii are wondrous creations written for the sole purpose of spreading and destroying the systems of unsuspecting fools. This eliminates the systems of simpletons who can't tell that there is a problem when a 100-byte file suddenly blossoms into a 1,000-byte file. Duh. These low-lifes do not deserve to exist, so it is our sacred duty to wipe their hard drives off the face of the Earth. It is a simple matter of speeding along survival of the fittest."
That quote was found at http://www.webgurru.com/viruses/vtut1.htm.

Comforting, huh? I think not. Disturbing to say the least. Now think about it, people like this, with the talent to create destruction and ensue mayhem are highly revered in the newsgroups, chat-rooms and dark alleys where they exist. Even to the point of infamous stardom and god-like stature. People, young and old alike admire, look up to and even follow, with cult-like spiritualism, these rather twisted individuals. Adopting their same philosophies, beliefs and practices. Believing that they are doing good, providing a service to their fellow man and computing community.

Should we be concerned? I mean, doesn't it take a computer sciences graduate to create a virus? Or, someone with a masters or doctorate degree in a programming language to create one? There's no way someone, anyone with a computer, Internet

connectivity, a web browser and a search engine URL such as www.yahoo.com could create a virus, could they? That's the question this research paper is going to answer for you. This study will show just how easy it is for Mr. or Ms. Average Computer User to find ready made viruses, the tools, advice and instructions on how to create and propagate their very own virus and malicious code.

Setting the Stage

Let's begin our journey by defining the tools that will be used in this endeavor. Listed will be the hardware, operating system and applications utilized. Why? Good question. In any reputable experiment, baselines must be established so that true measurements can be taken. Since this study publicizes the idea that an average person can achieve the results as documented, the hardware and software used must be readily available and obtainable by the average person.

Hardware:

- **Processor:** Intel® Celeron™ processor at 1.1GHz.
- **Memory:** 128MB
- **Storage:** 20GB.

http://www.dell.com/us/en/dhs/products/series_dimen_desktops.htm

- Modem: 56Kbps, V.92 external Data/Fax modem

http://www.cdw.com/shop/products/default.asp?EDC=276670

Operating System:

- Microsoft Windows 98 Second Edition

http://shop.microsoft.com/Referral/productInfo.asp?siteID=10025

Applications:

- Microsoft Internet Explorer 5.5 SP1 and Internet Tools

http://www.microsoft.com/downloads/search.asp?

Internet Service Provider:

- EarthLink

http://www.earthlink.com/home/

We now have our baseline created. The vehicle by which we will explore, search and discover our targeted prize is powered on. Our modem has negotiated and established

a connection to the Internet through our ISP. Our hand firmly grips the mouse and our clicking finger is poised for action. But, before we actually start clicking on hyperlinks and diving head first into the vast jungle known as the World Wide Web searching for our "Holy Grail", let's define the criteria for what exactly we're looking for and hope to find with as little imaginative creativity as possible. I believe the term is "keep it simple":

1. Web site that contains information about computer viruses.
2. Web site that contains actual live computer viruses ready for downloading.
3. Web site that contains information or tutorials on how to create a computer virus.
4. Web site that contains a computer virus creation toolkit.

The Treasure Hunt

Okay. We have our vehicle for traversing the World Wide Web and we have listed our primary areas of interest and focus. Let's begin our informative journey by mapping out our destinations and documenting our findings along the way.

When embarking on a quest within the World Wide Web on the Internet, and the exact destination or site, URL (uniform resource locator) is not known, tools known as search engines are of great value and importance. One of the greatest attributes of a search engine is this, if all you know about a web site are a few descriptive words, part of the company or website name or even the subject matter in which you are seeking, you can place that information in the search engine and it will deliver to you all of the choices that it was able to find. You have the ability to search on keywords, a group of words, a partial or complete phrase or you can use Boolean, a technique available to most search engines by which you use operands such as AND, OR and NOT in your search. Once you have entered in your search criteria and executed the search, you then scan through the results produced by the search engine until you find what you were looking for. Now, the search may take a retry or two. You may have to refine your search criteria to help in finding what you're looking for or even narrowing down the results produced by the search. As with just about everything else in life, practice makes perfect.

Since this study is based on the ability for an average person to find virus material, we'll utilize one of the most recognized search engines on the Internet, Yahoo!. The URL for the search engine is http://www.yahoo.com/. The first item in our criteria list is; Web site that contains information about computer viruses. So let's type in our search engine the phrase, "computer viruses", you'll notice that we've enclosed the phrase in quotation marks. This is to indicate to the search engine that we want to find that exact phrase in each of the websites it searches through. We'll begin by clicking on search, once the search engine has completed it's task, we'll examine the results produced. One of the many references displayed in our search is the world leader in Internet Security software and makers of Norton Antivirus, Symantec Corporation, found at the URL http://www.symantec.com/avcenter/. Here, at the Symantec Security Response website

we find a vast array of information about computer viruses. Information such as, what types of virus they are, what damage that particular type of virus can do, the viruses characteristics, if it is a hybrid of another virus, is it Polymorphic or macro? Included in all this information is probably some of the most important information about viruses, how to clean them and remove them from your computer systems.

Areas of information found at this website include:

- Latest Virus Threats – a listing of the current viruses found active.
- Security Advisories – detailed information on the latest vendor vulnerabilities.
- Security Alert – up to date information on the latest virus threat.
- Virus Definitions – downloadable files to keep the antivirus software current.
- Removal Tools – downloadable tools to assist in the removal and cleanup of viruses.
- Am I Protected – a web based tool to help you determine just how vulnerable you are.
- Top Virus Threats – detailed information on the latest computer viruses.
- Reference Area – Security articles, white papers, virus encyclopedia and more.

From this site and all of the hyperlinks associated with it, we can glean enough information to develop a substantial baseline of understanding for the computer virus. Once we understand how a thing works, we can then discover how to create a thing and destroy a thing.

Continuing our expedition, let's now investigate our next item of criteria; Web site that contains actual live computer viruses ready for downloading. Be careful though, this is tricky stuff. These sites, as harmless and friendly looking as they may be, could be hazardous to your computers health and well-being. Pay attention here, before proceeding, make sure your antivirus software is current with its virus definitions and the antivirus software is running and functioning properly. If it is not or if any portion is not operating correctly or is out of date do not go any further until the obstruction has been remedied. If everything is ready, let's proceed. In our search engine, let's type the phrase "how to create a virus", click on search and let's examine the results produced by the search engine. The first listing we'll go to is under the heading Viruses, http://www.geocities.com/screamatawall/viruses.html. Let's look at the very first link on this site, http://brianjan.virtualave.net/. Listed across the top of the site, in a menu are the headings; Virus, E-Zines, Utilities, Join P.V.W., Boardroom, Services, Zoom23, Links, Get Paid, Subportal and Email. How easy they make it by making the very first menu choice Virus. After clicking on the menu item, we are presented with a warning box that you have to click on the OK button to remove. Once past the warning box, we are taken to a page that has a list of downloadable viruses. Here's the list from the URL http://brianjan.virtualave.net/virii.htm

- A134-95 Strain A Overwritting virus
- A134-95 Strain B Appending virus
- HappyB Strain A Appending virus

- HappyB Strain B Appending virus
- No Overtime Appending virus
- HungryV Appending virus
- Cheska Appending virus
- Margaret Trojan
- Siri Virus
- Inquisitor Macro virus
- 213 Macro Virus
- Nalen Appending Virus
- Jojo Appending Virus
- Pinoy Freak ! Spawning Virus
- Carol C. Appending Virus
- Lugad Appending Virus
- Sui Generis !
- Siri Virus
- Cheska Virus Strain B
- MVT2 Macro Virus
- Mad Cow Virus
- Mykah Macro Virus
- Baby Blue Appending Virus
- Hiwaga by: PsK
- BlackDay v3.6 by:PhileT0a$t3r [rRlf]
- BlackDay *New* by:PhileT0a$t3r [rRlf]
- N4matics macro by:Ppacket

An impressive list of viruses to choose from for someone just looking around. Quick recap, how did we get here? First, by searching on 'how to create a virus', then clicking on a heading titled Viruses, which took us to http://www.geocities.com/screamatawall/viruses.html. We then clicked on the first link on the page, http://brianjan.virtualave.net/virii.htm and then clicked on the menu heading, Virus. That was definitely not rocket science and we have obtained one of our objectives. Not only that, but if I'm curious, which most people are, if I click on the heading Links I can find a website that contains the following list of authors that I obtained from URL http://vx.org.ua/links.shtml:

· ***Virus Authors***

- anarchriz' webpages - a few viruses
- (A)ntisocial (B)it (C)ombinations - Freestyler/Kefrens
- b e n c h
- Bahay Kawayan the Home page of Putoksa Kawayan - Bahay Kawayan, the home page of Putoksa Kawayan, a Filipino virus author with source codes and live viruses of his works available for download.
- Benny's Bi0 Laboratory (www.coderz.net/benny/) - Benny/29A
- Bhunji's page - (Swedish)
- Black Jack's VX page
- The BugHunters Homepage
- Bumblenet - Bumblebee's page
- Cybernetik Systems - Griyo/29A

- CyberShadow's Home Page (www.coderz.net/ABS)
- Dark Slayer
- Del Armg0's page
- Eddow's Page
- eLIFE by Paul Zest
- Flyshadow's page
- f0revir - f0re's page
- FRiZER's homepage
- Frog's Print Homepage
- GeneCite - Gene Source of Chaos
- Gigabyte's Homepage (www.coderz.net/gigabyte/)
- Homepage of Darkman/29A (www.coderz.net/darkman/) - A few sources with links to AVPVE descriptions.
- Jackie's World (www.coderz.net/jackie/) - Jackie/LineZero
- Knowdeth's Virus Utils & More (www.coderz.net/knowdeth/) - Knowdeth's Virus Utils & More is the location and source for virus utils/vck/compilers
- Les Virus par UnKm
- Lifewire Virus Laboratory (www.coderz.net/lifewire) - Win32asm virus coding
- Lord Dark
- Lord Julus's Page - A page mainly on programming, security, virus and anti-virus and others.
- LordArz
- Macro Viruses By Psyclone X
- Mandragore'z Infectious - Personal web site about vx stuff.
- MidNyte's Lair - MidNyte/Ultimate Chaos
- Moebius' site (www.coderz.net/moebius/)
- ORIFICENET
- Prizzy's Cubby
- Raid's VX website. (www.coderz.net/Raid/)
- R-E-V's page (www.coderz.net/rev/)
- Silvio Cesare - Linux viruses
- SMOOTHiE Da HuStla's Macro Virii
- SpyjureNet - SpyjureNet - Where you can find original texts and source code relating to system and network security and viruses.
- SSR
- T-2000
- TheWizard LABs
- Vicodine ES and melissa central - Mirror of VicodineES page.
- VXF (www.coderz.net/vxf) - VX-Faerie
- WalruS - Macro Virus and Virii Site
- Yanush Milovski's WWW Page
- Yozis Network
- Zhuge Jin
- Z0MBiE's HomePage - Z0MBiE's HomePage: Sources/Viruses/Trojans/Hacking/Tools/VX E-Zines/Hi-Tech/Programming and more...
- Zulu (www.coderz.net/zulu/)

Have I died and gone to virus heaven? Honestly, look at what we found with just a few clicks, an actual list of several virus writers' websites. Are they for real? If I click on one of the hyperlinks will I actually go to the described website? Or will I be redirected to a place that I really didn't want to go to? That my friend is the chance each of us will have to take. What did you think, that this would be trouble free? That the type of information

we are searching for would be free of anything malicious? Wake up and remember what you are trying to find, malicious, destructive, harmful code. Furthermore, what about the people that create this code, do you think there are nice people, not wanting to do any harm to your computer system? Remember what we found at the very start of this journey, the quote from a virus creator? Let me paraphrase for those of us with short memories, “Virii are wondrous creations written for the sole purpose of spreading and destroying the systems of unsuspecting fools.” So maybe it’s not heaven but actually hell, I’ll let you discover which one it is. On a different note, doesn’t this look like a virtual Yellow Pages listing for Virii and all of the nastiness associated with it? Do I need to search on Yahoo any further for what I am looking for? I’ll let you answer that.

From here we can go to other websites that contain live viruses and tutorials. Here’s the actual table from http://www.geocities.com/screamatawall/viruses.html listing the other links:

Pinoy Virus writers http://brianjan.virtualave.net/
http://Hackers.B3.Nu Copyright Pinoy Virus Writers ® All rights reserved 1997-2001 Zoom23 Webmaster.
Doctor Owl http://www.security-informer.com/english/crd_virus_440766.html
Interview with "Doctor Owl" virus writer
Virus writing http://revenger21.freeyellow.com/VIRUS.HTM
Taken from "Revengers text files homes page".Includes files on how to create a virus and more. This website has also resources for lock picking, hacking, phreaking and more.
Virus Tutorial http://www.ummah.org.uk/mhc/virus_tut.html
A tutorial on viruses and how to make them.
Develop a virus http://www.webgurru.com/viruses/vtut1.htm
An indepth tutorial on how to develop a virus.

That was found just by looking under a heading named Viruses. Let’s continue looking at the results that Yahoo has provided. Under the heading, Sirkus FAQ -- coding, virus programming, computer virus ... we find this link;

http://www.sirkussystem.com/sirkus/sirkusfaq.html

Sections within this site include Coding, Virii, and Links and of course Email. Although, at the time of this writing, the Coding and Links sections were under development, the Virii section was quite filled with useful information. Information such as tutorials from the group Phalcon/Skism. Tutorials that include the “basics” and “zines” (pronounced

"zeens," from fanzines). Okay, we understand what “basics” mean, but, what is a zine? Here’s an excerpt from The Book of Zines by Chip Rowe.

“Most zines suck. There's no nice way to say it. The truism coined by Theodore Sturgeon applies: Ninety percent of everything is crap. Most people forget what Sturgeon said about the remaining 10 percent. He said it was worth dying for.

I'm dying! Zines (pronounced "zeens," from fanzines) are cut-and-paste, "sorry this is late," self-published magazines reproduced at Kinko's or on the sly at work and distributed through mail order and word of mouth. They touch on sex, music, politics, television, movies, work, food, whatever. They're Tinkertoys for malcontents. They're obsessed with obsession. They're extraordinary and ordinary. They're about strangeness but since it's usually happening somewhere else you're kind of relieved. You can get to know people pretty well through their zines, which are always more personal and idiosyncratic than glossy magazines because glossies and the celebrities they worship are so busy being well known.

Most zine editors can recall the moment they first saw *Factsheet Five*, the zine that reviews zines, and asked themselves (1) that's what I've been doing? or, more likely, (2) I can do that, and why not? Everyone cleared space on their kitchen tables, and estimates flew like confetti—10,000 zines, 50,000 zines, a million readers. Nobody knows. A zine dies, a zine grows. Over the years since I assembled the first issue of Chip's Closet Cleaner and sent copies to my puzzled relatives, I've exchanged zines and letters and e-mail with hundreds of underground publishers and found we share the same desire—the same *need*—to create. Factsheet Five used to ask its readers a deceptively simple question, "Why publish?" and always received passionate (if sometimes long-winded) responses.

Most zines suck, but you find that golden 10 percent and you're hooked for life. Found mine.”—Chip Rowe

The information doesn’t stop there it continues by providing actual virus source code, nearly 400 examples for us to learn from. You have the choice of viewing the code directly from the site by just clicking on the desired one, or, you can download it for later viewing by simply right clicking and ‘save target as’ right from your browser. One small deterrent at this site for the beginner is that the downloadable code is still in a decompiled state. This makes it a little more difficult for the absolute beginner to utilize this right away. They would first have to compile the code, and that would require a compiler that would compile assembly. Not too many beginners would have or even know how to use a compiler.

So far, we have been able to obtain three of our four objectives with very little work or expertise. Our fourth objective may be a little more difficult to find, virus toolkits. Since we were so successful with the formula used on the previous three, let’s continue in that frame of mind.

Let’s return to the website, http://www.geocities.com/screamatawall/viruses.html and click on our old friend, http://brianjan.virtualave.net/virii.htm. Scanning across the top at the menu choices, let’s click on Links. Right there, under the very first heading Virus

Links, we find our first toolkit, Triniti's VBS Worm Toolbox. Clicking on the hyperlink takes us to http://www.batchlabs.net/batchlabs/. Listed on the right side of the page, at the very top of the page is the hyperlink vbs worm toolbox. All I have to do now is click on the link and I am presented with a download confirmation box for VBS Worm Toolbox.exe. There it is, a virus toolkit. Not too hard to find after all.

One question that still haunts my mind as it probably does yours seeing that we are well-educated people with high morals and established values. So what if a beginner or even a well-versed computer user finds this stuff, can any real harm be done? Take a look at this news article excerpt published on www.wired.com. You can find the entire news story at http://www.wired.com/news/print/0,1294,41817,00.html

You, Too, Can Write an Anna Worm
by Michelle Delio

2:00 a.m. Feb. 15, 2001 PST

The Anna Kournikova e-mail worm that whacked networks this week was not the work of a skilled cracker. It was created using one of the many virus-generating kits that are easily available on the Internet.
The kits, which have names like Satanic Brain Virus Tools 1.0, Instant Virus Production Kit, and Ye Olde Funky Virus Generator, make writing a virus a straightforward and uncomplicated task.
If you can install a program on a computer, you can also -- using one of these kits -- write and release a virus just like the authors of Cartman, Poppy and Kenny did.
Anna was created by a 20-year-old Dutch man who calls himself "OnTheFly" using the VBS Worm Generator, an application credited to a cracker known as [K]alamar, who is believed to be based in Buenos Aires.

[K]alamar's VBS Worm Generator 1.5 includes a well-written readme file, and an easy-to-understand point-and-click interface.
"A 10-year-old could use [K]alamar's VBS Worm Generator 1.5 to create a worm," said Ken Dunham, a senior analyst with SecurityPortal."

Now, let's look at this news article, also found on www.wired.com. The entire news article can be found at http://www.wired.com/news/technology/0,1282,41761,00.html

New Virus: Now Anna Loves You
by Michelle Delio
1:00 p.m. Feb. 12, 2001 PST

"A new worm is making its way through e-mail boxes, and it seems to be spreading more rapidly than last year's Love Bug, which infected 15 million computers and is regarded as the worst e-mail virus ever."

Cause any damage you asked? Only if you consider “15 million computers and is regarded as the worst e-mail virus ever”, damage, then I guess they can.

Conclusion

Now, in the course of our journey did we uncover any new undiscovered technology or malicious code lingering in the wilds of the Internet? Did we happen to stumble upon a cure for many of our modern day diseases? Did we discover the Lost City of Atlantis? No, but that wasn’t our quest. That’s not what we were looking for. We were looking for the ‘beginners’ route to viruses. Did we find it? Let’s recap:

We started with common hardware, software and Internet connectivity.
We utilized a popular search engine, www.yahoo.com.
We searched with simple phrases, ‘viruses’ and ‘how to create a virus’.

Results. With the use of just three primary websites we were able to find all of the information, source code and links to other websites that we needed to begin the process of creating viruses. Did we find every source for virus information and creation? No. Could we have found more? Yes, much, much more. Just think, in a matter of a few mouse clicks I was able to find source code, tutorials, live viruses and a VBS Worm tool kit, what if I researched even more, what would I have found?

At the onset of this paper we asked the question, “Could someone, anyone with a computer, Internet connectivity, a web browser and a search engine URL such as www.yahoo.com create a virus?” Through the use of research techniques, available hardware and software and common sense, we have been able to prove decisively, yes. Someone, anyone with the basic, necessary tools and intelligence could not only find, but also create and deliver havoc by the vehicle we know as a virus.

Resources

Webgurru. URL:
http://www.webgurru.com/viruses/vtut1.htm

Dell Computer Corporation. URL:
http://www.dell.com/us/en/dhs/products/series_dimen_desktops.htm

CDW Computer Centers. Inc., URL:
http://www.cdw.com/shop/products/default.asp?EDC=276670

Microsoft Corporation. URL:
http://shop.microsoft.com/Referral/productInfo.asp?siteID=10025

Microsoft Corporation. URL:

http://www.microsoft.com/downloads/search.asp?

Earthlink, Inc.. URL:
http://www.earthlink.com/home/

Yahoo!, Inc.. URL:
http://www.yahoo.com/

Symantec Corporation. URL:
http://www.symantec.com/avcenter/

Wake the Dead. URL:
http://www.geocities.com/screamatawall/viruses.html

Sirkus Systems. URL:
http://www.sirkussystem.com/sirkus/sirkusfaq.html

Pinoy Virus Writers. URL:
http://brianjan.virtualave.net/

VX Heavens. URL:
http://vx.org.ua/links.shtml

BatchLabs. URL:
http://www.batchlabs.net/batchlabs/

Delio, Michelle. “You, Too, Can Write an Anna Worm”. Wired News. Feb.15, 2001. URL:
http://www.wired.com/news/print/0,1294,41817,00.html

Delio, Michelle. “New Virus: Now Anna Loves You”. Wired News. Feb.12, 2001. URL:
http://www.wired.com/news/technology/0,1282,41761,00.html