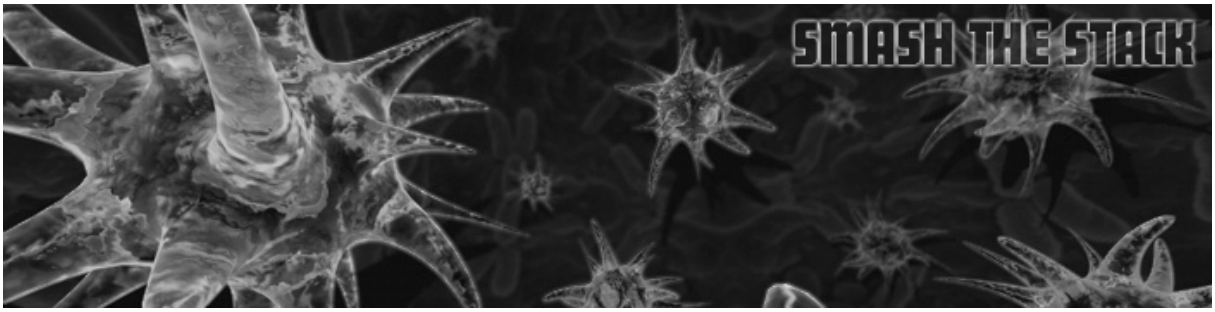

VX – The Virus Underground

(27th Dec. 2007 at the 24c3 in Berlin/Germany)

About me

Name: Marcell Dietl (SkyOut)
Website: www.smash-the-stack.net
Email: skyout@smash-the-stack.net

Age: 18 years
City: Wiesbaden/Germany
Company: MK Mediaconcept (www.mymk.de)
Characteristics: Gothic, Social Engineer, Autodidact
Addicted to: Cecurity, Cigarettes and Coffee (CCC)

The term VX

- Also stands for a gas with the chemical structure $C_{11}H_{26}NO_2PS$
- In our case it means Virus Coding
- The term has been made in the early days of the scene
- VXers are the Virus Coders and groups are named VX Groups

Groups of the scene

- 29A (www.29a.net)
- rRlf (www.rrlf.de.vu)
- DoomRiderz (www.doomriderz.co.nr)
- Purgatory (www.purgatory.net.tf)
- F-13 Labs (www.f13-labs.net)
- EOF-Project (www.eof-project.net)
- NE365 (wwww.vxer.cn)

The ideology behind it

- People can be divided into several categories
- Criminals making viruses to earn money
- Hobbyists, that only code some viruses for fun and leave again
- Ideologists, that stay in the scene for years
- WhiteHats, who code without the intention to harm anyone
- BlackHats coding viruses and spreading them

History, Present and Future

- History: Viruses were made to get attention, mostly spread by floppy disks, the first worms fort he Windows OS came out
- Present: Many worms are coded to build up botnets and earn money, cross-platform malware as a new trend, more malware for *nix based operating systems, much Spyware and Adware
- Future: Much more mobile device malware

Cross-Platform malware

- Several techniques to build a virus, that works cross-platform
- Macroviruses for Office Suites like MS Office or OpenOffice
- .NET (Mono) viruses
- Scripting languages, that normaly have an interpreter for different platforms
- Most difficult: Coding a virus in a LowLevel language, that changes ist behavior at start, example: Winux

Typical spreading techniques of modern viruses

- Floppy disks (not used anymore)
- Autostart function in CDs or DVDs
- USB flash drives with autostart functionality
- P2P Networks
- Sharehosters like Rapidshare (In forums and blogs the virus author links to the file and makes the users interested in downloading and executing it)
- Email

- Bluetooth
- IRC (Over the DCC function)
- Instant messenger like ICQ, MSN etc.
- Network shares, that are writable by others in the network
- Warez infected with malware
- Exploits automatically attacking a common weakness

Types of reproduction

- Appender = The virus puts its code at the end of the original file and does a jump to this part at the start
- Prepender = The virus puts its code at the beginning of the original file and starts this code and after a little delay the original code gets executed
- Overwriter = The virus overwrites the whole file with its own code

Types of payloads

- Payload = The routine the virus starts apart from reproduction
- Conspicuous payload = The user shall realize, that he got infected with a virus, for example with a message box
- Inconscpicuous payload = The user shall NOT realize, that he got infected, for example by putting the whole OS into a VM
- Polymorphism/Metamorphism = The virus code is not static and changes during reproduction
- Anti-Debugging features

Types of malware

- Virus = Self-reproducing code starting with a host file
- Worm = Malware with the ability to automatically spread
- Trojan Horse = A program, that acts as a normal application and starts the evil code silently
- Hoax = Malware, that does not harm any system as it is only a joke

Ways of communication between VXers

- Central file servers to store source code and sometimes binary viruses, for example vx.netlux.org as a central website for viruses
- Websites (see the section about the groups of the scene)
- Emails and instant messenger used for personal information exchange
- IRC channels used for public information exchange (#eof-project, #virus, #vir, #vxers, #vx-lab @undernet.org)
- Electronical magazines (E-Zines) coming out once a year by a group

Connection between the VX scene and AV (Anti Virus) companies

- It is a continuous fight
- Both groups are observing the other side, for example AV companies blogging about the VX scene
- Some AVers even tried to get in touch with the scene to get internal information and bring some VXers into jail
- In best case the connection between both groups works as follows: VXers coding a virus and sending it to Avers -> AV companies are doing an anylsis and can protect their customers -> VXers have some like a trophy

Used programming languages

- .NET languages are getting more and more popular
- Programming languages for Windows are still the most used ones, for example Visual Basic
- Many new viruses are coded in scripting languages like PHP
- Assembler is still the language, that VXers respect most

Problems of the scene

- Very small scene, only about 50 more or less active people
- Many virus coders only code some viruses and leave the scene again (see above -> Hobbyists), that leads to no continuity

- Decentralization, which means, that every groups tries to do their own thing instead of working together
- The whole community is based on a few websites and a few big VX hosters

Social Engineering and VX

- Social Engineering is needed for Worms to spread
- Examples are texts in Emails to make the user click on the attachement or good messages while spreading over an instant messenger

CONCLUSION

Most VXers are not coding viruses to harm anything or anybody. For them it is a way to express their feelings and ideas in a technological and often misunderstood way. That is why most VXers do not make their viruses available in binary format and only upload the source code to show it to others. Doing so they want to conduct a knowledge exchange between each other without destroying something. So in relation to Hacking: VX can be considered playing with technology and finding out new ways of coding, that have not been there before, therefore it is hacking and most VXers can be considered WhiteHats as a conclusion of this paper!

Thanks for your attention – SkyOut