GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Script Kiddies and Packet Monkeys - The New Generation of "Hackers"

Denis Dion

January 29, 2001

Over the last couple of years a new type of hacker has become more and more prevalent on the Internet scene. These cyber-bandits are known in hacker jargon as script kiddies and packet monkeys. They have been responsible for quite a few notorious attacks such as the Distributed Denial Of Service (DDOS) attacks on Yahoo, eBay, eTrade, Buy.com, ZDNet and CNN as well as defacing sites ranging from Pepsi to NASA. This article attempts to take a closer look this new breed and what motivates them as well as discussing some of the consequences resulting from their actions.

Here are some definitions according to a couple of internet-related dictionaries:

script kiddies pl.n.

> The lowest form of cracker; script kiddies do mischief with scripts and programs written by others, often without understanding the exploit.
> Source: The New Hackers Dictionary
> http://www.hack.gr/jargon/html/S/script-kiddies.html

packet monkeys pl.n.

> The exploits of individuals who perform denial-of-service attacks on websites, for no apparent reason, seem silly, pointless and downright simian.
> Source: partial definition from The Word Spy
> http://www.logophilia.com/WordSpy/packetmonkey.html

distributed denial of service n.

> A computer attack that hijacks dozens or sometimes hundreds of computers around the Internet and instructs each of them to inundate a target site with meaningless requests for data.
> Source: The Word Spy
> http://www.logophilia.com/WordSpy/distributeddenialofservice.html

The hacker community contains several different types of which the prominent ones are:

black hat

> A hacker who uses his or her talents for malicious or criminal ends. (Also known as a cracker.)

gray hat

> A hacker who supplies information about a security issue both to the vendor and to crackers

white hat

> A hacker who, upon discovering a vulnerability in a computer system, alerts the system vendor to the problem.

Note: All definitions were obtained from The Word Spy
http://www.logophilia.com/WordSpy/whitehathacker.html

At the bottom of the pecking order and the newest addition to this collection are the wannabes. Script kiddies and packet monkeys are exactly that. The old school hacker community generally looks down upon them. This is due to their lack of technical skill. In the past, a hacker usually spent years to learn the inner workings of computer technology. Script kiddies and packet monkeys, generally, have very limited computer skills and rely on the work of other, more experienced computer experts. "Bottom feeder" is one term I have read being used to describe them. Ironically, it is the exactly the group of hardcore

hackers who disdain these wannabes that are finding and publishing security exploits as well as providing the tools to take advantage of them.

In addition, one of the main goal of hacking was not to be discovered, but rather get into a system, see how it works and then leave as quietly as possible. This is not the case with script kiddies who tend to deface websites with digital graffiti containing greetings to friends or cause sensational headlines by bringing large business sites to their knees. The old-time hackers do not seem to appreciate all the unwanted attention this new generation is bringing down upon the entire community

A script kiddy is someone looking for an easy kill and his or her methodology is quite simple. They are not searching for specific information and their targets are mostly random. They focus on a small number of exploits and then search the Internet looking for systems with which they can use these exploits on. Most of the tools are automated and use the same strategy; first develop a list of IP addresses that can be scanned and then scan these addresses for a specific vulnerability. Whole blocks of IP addresses and ports are swept. The attacker need only run the scan, come back in a couple of hours, get the results and start attacking. The results of such global scans are often archived or shared among other users. List of servers are even kept in databases, which, in turn, are traded or sold like baseball cards. These databases remove the need to scan addresses making the job that much more efficient and quicker.

The tools being used by script kiddies and packet monkeys are extremely simple, most being limited to a single purpose with a few options. Traditional hackers usually use Unix-like operating systems and spend much time developing utilities to be used with vulnerabilities they have discovered. These days many of the utilities are being ported or are even originating on systems running Microsoft operating systems. The Antionline group, for example, provides a wide range of exploits for different operating systems on their web site. Not only are the scripts and programs readily available for downloading but you are even provided with step-by-step instructions on how to use them. In essence, the new generation of hackers needs only to follow cookbook instructions or run pre-canned scripts to attack a system.

Even the distributed denial of service attacks against well-known sites early last year was referred by one hacker as being just "old, tired technology being run in a big way ". DDOS attacks are based on a single user controlling up to hundreds of compromised systems spread all over the globe. These compromised systems are then remotely coordinated to execute denial of service attacks against a victim or victims. The attack on Yahoo, for example, was launched through at least 50 locations. Software was planted on these "slave" machines and at a given time they ran programs to send a flood of destructive messages to the targeted servers. The utility Stacheldraht (barbed wire) used in the DDOS attacks of February 2000 was created by a gray hat hacker in Germany known as "Mixter" but the actual culprit is apparently a teenager from Canada going by the name of "Mafiaboy".

The days of late night sittings with overflowing ashtrays, cold coffee and half empty bags of Doritos is a thing of the past at least where script kiddies and packet monkeys are concerned.

Fortunately, this new generation of "cyber punks" tend do dumb things like draw attention to the crime and leave a trail of evidence that even relatively clueless law enforcement can follow. In other words, they usually get caught. Most of the attacks are quite easy to trace back to the culprits. As they do not know the inner workings of the systems they are attacking (logging, auditing, etc.) they fail to clean up their tracks and leave evidence all over the place.

Even more obvious are the script kiddies who deface web sites. They usually mark the site with their Internet aliases and post shout outs to friends. It does not take a genius to find these people, especially when they brag about their "exploits" in chat rooms and over IRC (Internet Relay Chat).

Packet monkeys, on the other hand, are a bit harder to find as usually many compromised machines are being used simultaneously for the attack. Finding the culprits either means sifting through a ton of logs back through several machines or getting tips from other hackers. This does not mean that packet monkeys are smarter, they are just attacking on a grander scale that makes the volume of evidence to be checked greater.

So, why do they do it and why are there so many of them out there? There is no consensus as to the reasons for the attacks and more than one theory regarding the motives. Most think that it is just a digital form of adolescent mischief comparable to graffiti spraying or prank phone calls. Even many hackers say a great amount of Internet vandalism is juvenile stuff. It seems that there are a bunch of rebellious teenagers out there with little technical skill but plenty of mean spirit. Boredom with their real existence, disconnected from schools, politics or dispirited with today’s society – these could all be reasons why these attacks are increasing.

Another reason could be that hacking has become, to some degree, socially acceptable. The attacks can be considered a vehicle used to gain acceptance, a feeling of power, belonging and control. Script kiddies, after all, typically advertise their exploits to gain acceptance with their peer group.

Still others consider the attacks a protest against the growing commercialization and regulation of the Internet. Buy.com, for

instance, was hit just before the stock went public and the other sites hit with DDOS attacks were all more or less business sites. Many of the sites that have been hacked into and defaced belong to governments or big corporations (McDonalds, Nike and Pepsi to name a few). If this is so, the disabling of e-commerce sites can interpreted as a protest against the "strip-malling" of the Internet or a form of class resentment. Possibly, these teenagers see themselves as defending territory against the encroachment of big money, regulatory power and the closing off of the Internet by proprietary companies. A lofty goal which apparently is not working.

The one odd thing is that none of the attacks seem to be for personal monetary gain. At least no evidence has been forthcoming even though the threat of such attacks could be used as a means of extortion against companies that are heavily dependant on their Internet presence. Black hat hackers or crackers use their abilities and knowledge to exploit and damage systems for personal gain or political motives. White and gray hat hackers tend to use their skills to find and correct security problems. Script kiddies and packet monkeys just attack randomly and without any specific motives.

However, Script kiddies and packet monkeys are much more dangerous then their monikers would suggest. As stated earlier, their attacks are mostly random. It is this random selection of targets that make them such a dangerous threat. Sooner or later they will probe everyone's network and machines. In other words, no one is safe. The sheer number of these culprits gives way to a new era. The pool of Internet users, and thus potential vandals, is far greater than in the early '90s. Society has become so reliant on computers and the networking of them that damage to these systems has a far greater impact then a decade ago. Not only widespread access to the internet but easy access to the tools needed to carry out attacks have been making it easier for almost anyone with basic computer and networking skills to become a "hacker". Most of the tools are easy to use and widely distributed. A rapidly growing number of people are obtaining these tools at an alarming rate. The information about exploits and how to use them are free and posted publicly. There is no natural screening process. Lastly, the process the script kiddies use in scanning for systems to crack make the attack less personal. It is harder for them to identify with their victims and easier to do damage without feeling remorse for their actions.

What can be done to prevent attacks from script kiddies and packet monkeys from succeeding? It may be that even if you secure your system as well as you are able it will not be enough. Distributed denial of service attacks are devilishly difficult to prevent. As an administrator you have to find every possible vulnerability while they only have to find something that you have missed. In any case, you should at least make it harder for them. Every machine hooked to the Internet should be made as secure as possible. This security should be kept up-to-date. You need to secure your machines before you connect them to the network for the first time. It has been reported that script kiddies have compromised some machines within minutes of being connected to the Internet.

The key appears to be protecting all of cyberspace from predatory programs. Internet service providers could install filters on the data they ship. RSA Security claims it has created a method that, when an attack is sensed, requires visiting computers to solve cryptographic puzzles. The task should overwhelm the attacking machines themselves.

And what does the future look like? The DDOS attacks of February 2000 were a wake-up call to the fragility of the Internet. The attack was a deliberate attempt to shut down a network operation by overloading it. The importance of the Web to government, business and law enforcement agencies is so great that such attacks threaten the possibilities of new laws, restrictions and policing. The attacks will not stop companies commercializing the Internet. It will, however, speed up the end of an era where the Internet was free. Not too long ago, the Internet was looked upon as the last, best hope for a renaissance of personal expression and political speech, as one of the last bastions of freedom of thought. Now, it is largely viewed as a mega shopping center. The Internet has become so linked with the economy that interrupting commercial sites has been deemed a national security issue in America. It is just a step away from using these attacks to justify legislation, budgets and intrusions by the government.

Society will be forced to make some tough choices. They must decide between making the net safe for capitalism and thus more regulated or leave it as it is with all its vulnerabilities. Over the next few years, society's tolerance of hackers will lessen and be looked on as a form of terrorism. A form of net phobia is arising and the dangers posed by the youthful script kiddies and packet monkeys will cause a rethinking of how we deal with them. It has become far more than just "fun and games".

References:

Copeland, Libby. "Script Kiddies Ruin Our Image – Hackers". Washington Post. 18 Feb., 2000. URL: http://www.infowar.com/hacker/00/hack_021800c_j.shtml (29 Jan., 2001).

Fennelly, Carole. "Idiots in the News: Script kiddies - geniuses or idiots?". April, 2000. URL: http://www.sunworld.com/sunworldonline/swol-04-2000/swol-04-security_p.html (29 Jan., 2001).

Grant, David. "A new improved script-kiddy". Geeknews. 13 June, 1999.

URL: http://geeknews.efront.com/articles/DavidGrant/061399.shtml (29 Jan., 2001).

Kahney, Leander. "Smells Like Mean Spirit". Wired News. 7 Feb. 2000.
URL: http://www.wirednews.com/news/business/0,1367,34228,00.html (29 Jan., 2001).

Katz, Jon. "Attack of the packet monkeys". Online Freedom Forum. 15 Feb., 2000.
URL: http://www.freedomforum.org/technology/2000/2/15katz.asp (29 Jan., 2001).

Katz, Jon. "Script Kiddies Who are These Guys". Time Europe. 15 May, 2000.
URL: http://www.time.com/time/europe/magazine/2000/0515/hackers.html (29 Jan., 2001).

Lemos, Robert. "Script Kiddies: The Net's cybergangs". ZDNet News. 12 July, 2000.
URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2602573,00.html?chkpt=zdnnrla (29 Jan., 2001).

Lemos, Robert. "Why there's an army of script kiddies". ZDNet News. 27 July, 2000.
URL: http://www1.zdnet.com.au/antivirus/stories/au0004358.html (29 Jan, 2001).

mea culpa. "[ISN] Editorial: Script Kiddies". Internet Security News. 7 Oct. 1998.
URL: http://www.landfield.com/isn/mail-archive/1998/Oct/0029.html (29 Jan., 2001).

noeld. "The Danger of Script Kiddies ". RootPrompt.org. 7 Aug., 2000.
URL: http://rootprompt.org/article.php3?article=756 (29 Jan., 2001).

Pond, Weld. "New breed drowning out hacker culture?". ZDNet News. 20 July, 2000.
URL: http://www.zdnet.com/zdnn/stories/comment/0,5859,2605327,00.html (29. Jan, 2001).

Spitner, Lance. "Know Your Enemy ". The Honeynet Project. 21 July, 2000.
URL: http://project.honeynet.org/papers/enemy/ (29 Jan., 2001).

Unknown author. "Hacker inquiry leads to Germany". BBC News. 13 Feb., 2000.
URL: http://news.bbc.co.uk/hi/english/sci/tech/newsid_641000/641921.stm (29 Jan, 2001).

Vest, Jason. "E-Bombs Away! Protest, Panic, and the Politics of Packet Monkeys". Village Voice. 16 Feb., 2000. URL:
http://www.villagevoice.com/issues/0007/vest.shtml (29. Jan., 2001).