Global Information Assurance Certification Paper

David Benton
11/28/2000

What's Inside a Cracker?

Introduction

"Think what your enemy will do and beat him to the draw" – George Patton

As security specialists we are constantly faced with new threats in the form of malicious code, denial of service attacks and the like. There is always a reason for the Security Officer to get up in the morning, as well as lock the "doors" at night. For better or worse, the career opportunities for both "black hats" and "white hats" show no sign of slowing down. Just the opposite. New tools to combat cyber crime are being marketed to IT professionals like tofu-pups at a PETA gathering. While paranoia and Black Ice become a way of life, it is important to understand the psychology and motivation of the cracker.

First. we need to understand the terminology. Hackers and hacking are sometimes used synonymously with crackers and their deeds. However, there are technically two different profiles:

Profile of a hacker

Hackers generally like to think of themselves as an elite group of information seekers who are adept at exploring computer systems and networks. Although hacking into network computer systems is illegal, hackers believe it is ethically acceptable as long as a hacker does not commit theft, vandalism or breach any confidentiality -- the so-called hacker code of ethics. In fact, many hackers believe it is their responsibility to seek out security holes in computer networks so that systems administrators may fix them. "If we can share what we've learned with everybody and then publish it," L0pht hacker Wedge stated in a NewsHour interview, " that's great." *(1)*

Profile of a cracker

But not all hackers follow a code of ethics. Those who break into computer systems with malicious intent are known in the hacking world as *crackers*. The word itself was devised by hackers who wanted to differentiate themselves from crackers. Whereas hackers possess a great deal of knowledge of computers and generally write their own hacking programs, crackers tend to be young and unskilled.

As Jeff Schiller, head of network security at M.I.T stated, "most of the crackers we are dealing with are not experts, they are not very sophisticated." *(1)* They do most of their cracking by downloading free hacking software from hacker Web sites. Although they lack the technical skills of hackers, crackers are considered dangerous because of their irresponsible use of sophisticated software.

Eric Raymond, author of "The New Hacker's Dictionary," argues, "Real hackers call these people 'crackers' and want nothing to do with them... being able to break security doesn't make you a hacker any more than being able to hot wire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word 'hacker' to describe crackers; this irritates real hackers no end... "*(2)*

The motivation of Crackers/Hackers

Whether its described as a hack or a crack, lets look at some of the categories of malicious behavior:

Script Kiddies

Many believe that crack attacks on computer networks are the work of sophisticated hacker/crackers who spend hours writing complicated code and meticulously probing a target computer for a security hole to breech. Much to the surprise of most people, the typical network cracker is a 12-16 year old boy who found some cracking code on the Internet and decided to try it out. What makes the script kiddie so dangerous is not the vast amount of knowledge that they possess, but rather their lack of knowledge. Often a script kiddie will run a script on a system without having any understanding at all of what he or she is doing.

In the hacker/cracker community a script kiddie is considered to be at the shallow end of the gene pool. Their motivation is not based on showing off their own hard work but rather causing chaos with scripts they can steal or find on the internet.

Political Hacks/Cracks

On Tuedsay, November 7, 2000, the official Republican party Website was cracked and it's normal content was replaced by a rant on why you should vote for Al Gore. The Website defacement was noted at 4:00 AM EST and was not restored until after 9:00 AM EST. Keynote systems, a firm that monitors high profile and special events Web sites for performance, noticed the crack after their monitors showed a significant slowdown at the GOP.org Website.

This attack is being called by security experts an "articulate" attack. Unlike many Web defacements and other cracks and attacks, no one has claimed responsibility for this attack. Most cracks that come from script kiddies are less sophisticated and mature and most of the time the attack is immediately claimed by one cracker group or another. This was a form of hacktivism, or a computer hack with activist overtones, which is covered latter in this discussion.

The Democratic National Committee Website was also attacked early election day morning. In contrast to the GOP attack, there was no defacement. This was a DoS attack or Denial of Service attack. According to a Democratic National Committee spokesman the DNC Web site suffered "...repeated attacks" until it was forced to shut down. *(3)*

Hacktivism

Hacktivism put *crackers* in a whole new category. While the script-kiddie is causing mayhem with trojan horses, worms, DOS attacks and web defacement for no other reason than a personal "fix", Hacktivism is cracking with a political or activist mission. It is know as electronic civil disobedience. The future battle ground for political and social movements including acts of global terrorism may very well be the internet. As we becomes more cyber-dependent, we also become more venerable to malicious code.

One of the most celebrated and talked about acts of hacktivism is when the NY Times site was defaced by the group that called themselves HFG or Hacking For Girliez. On September 13th, 1998 at 4:50 AM, the NY Times home page was replaced with a page created by HFG. This act was aimed primarily at the NY Times reporter John Markoff who co-authored the book "Take Down". It is this book that chronicled the exploits and eventual arrest of Kevin Mitnick. This act of hacktivism received a flurry of press coverage because it was one of the first attacks on a mainstream publishing company that had political overtones. *(3)*

Psychology of the Cracker

As documented by *Marc Rogers M.A., Graduate Studies, Dept. of Psychology University of Manitoba(4)*, there are basically seven psychological profiles of crackers or *malicious* hackers:

Tool kit/newbies (**NT**), cyber-punks **(CP)**, internals (**IT**), coders (**CD**), old guard hackers (**OG**), professional criminals (**PC**), and cyber-terrorists **(CT**). These categories are seen as comprising a continuum from lowest technical ability (NT), to highest (OG-CT) .

The **NT** category includes those persons who have limited computer and programming skills. These persons are new to hacking and rely on already written pieces of software, referred to as tool kits, to conduct their attacks. The tool kits are readily available on the Internet.

The **CP** category is compromised of persons who usually have better computer skills and some programming capabilities. They are capable of writing some of their own software albeit limited and have a better understanding of the systems they are attacking. They also intentionally engage in malicious acts, such as defacing web pages, and sending junk mail (known as spamming). Many are engaged in credit card number theft and telecommunications fraud.

IT can be made up of disgruntled employees or ex-employees who are usually very computer literate and much of the time work in computer releated jobs. They are able to carry out their attacks due to the privileges they have been or had been assigned as part of their job function. This group accounts for nearly 70% of all computer related criminal activity (Power, 1997).*(4)*

The **OG**, appear to have no criminal intent although there is an alarming disrespect for personal property. The OG appears to be interested in the intellectual endeavor.

The **PC** and **CT** groups are probably the most dangerous. They are professional criminals and ex-intelligence operatives who are guns for hire. They specialize in corporate espionage, are usually extremely well trained, and have access to state of the art equipment. It has been theorized that the professional category has expanded since the dissolution of several of the eastern block intelligence agencies.

It seems the majority of research has been done on the **CP** category. They Cyber-punk is probably the most well known in hack/crack discussions and their actions may be the most preventable as attention is

brought to discovering and addressing this behavior early on. Therefore I have included in this document the results of Marc Rogers research on the psychological profile of this offender…

"The available data indicates that individuals classified as **CP** are; Caucasian, 12-28 years, from middle class families. They are loners, who have limited social skills and perform poorly in school (Chandler, 1996; Littman 1996; Hafner & Markoff, 1995; Sperling, 1992). They are usually not career oriented, but show an aptitude with computers and other electronic equipment. Their families are usually considered dysfunctional, single parent, abusive, and in some cases sexually abusive (Goodell, 1995). Often these individuals display obsessive traits, staying online for days on end with no sleep (Goodell, 1995). ***Cyber-punks*** have a tendency to brag about their exploits. This may be due in part to their desire to be admired by their hacking peers (Post, 1996; Sperling, 1992). The bragging often results in them coming to the attention of law enforcement. The bragging and willingness to talk about their exploits continues even while in custody and during interviews with law enforcement (Hafner & Markoff, 1995; Littman, 1995).The fact that many of the attacks are malicious in nature suggests that these individuals have unresolved anger and feel a need to strike out at something or someone (Post, 1996; Sperling, 1992). They are not comfortable with people so they strike out at computers and networks, rationalizing that corporations are immoral and need to be taught a lesson (Post, 1996)."*(4)*

John Vranesevich, founder of AntiOnline, describes the **CP** in this way, "I often refer to this group as my 'gang mentality' group. If these people weren't breaking into computer systems, they'd be out on the streets trying to spray paint their initials on the tallest buildings they could get their hands on. They hack to try to gain peer acceptance, a feeling of self-superiority, or a feeling of control," *(5)*

Let's Chat

Documented below *(6)*are actual (sanitized) excerpts from an IRC session between two young crackers, they are called "Dick" and "J4n3". There are two distinct characterizations you can discern from this conversation. They are most likely teen-agers and their motivation seems to be more for fun or excitement than any sort of financial or intellectual gain.

```
:J4n3! :oye deface kardo

yo let's deface (them)

:D1ck! :he's 'OK'
:D1ck! :oki
:J4n3! :lekin yaar ye pass kyon nahi chal rahay :?

but dude why arent these pass(words) working?

:D1ck! :?
:J4n3! :the pass from that shadow file :
:D1ck! :dunno jani

dont know pal

:J4n3! :they r fresh they should work naa
:D1ck! :;P
:D1ck! :?
:D1ck! :oye brb rebooting to win
:D1ck! :brb
:J4n3! :kkz
:atlanta.ga.us.undernet.org 005 pencil SILENCE=15 WHOX WALLCHOPS USERIP CPRIVMSG CNOTICE MODES=6 MAXCHANNELS=15 MAXBANS=30 NICKLEN=9 TOPICLEN=160 KI
:D1ck! :J4n3
:D1ck! :there?
:D1ck! :ACTION is away: (Auto-Away after 15 mins) [BX-MsgLog On]
:J4n3! :D1ck
:J4n3! :D1ck
:J4n3! :lets deface
:J4n3! :wow
:J4n3! :mera jooota hai japani , ye pathloon englistaani , sir pay laaal topi rooosi phir bee dil hai balochistani :p

[Note: lines from a popular hindi movie song, except at the end he
says my heart is Baluchistani. Baluchistan is a province in Pakistan.]
!
!
!
:J4n3! :yeah from where u getting this server ? and till when u get it ?
:J4n3! :it should be on redhat ok ?
:D1ck! :easilyhosted
:D1ck! :yep
:D1ck! :it is
:D1ck! :i`ll make it ultra secure
:D1ck! :redhat 6.2
:J4n3! :haha kewl
:D1ck! :i`ll upgrade to new kernel
:J4n3! :give me 2 days for web
:D1ck! :2.2.16
:D1ck! :kewl
:D1ck! :okies
:J4n3! ::)
:D1ck! :the day u do it
:D1ck! :the next day ill get the seerver
:D1ck! :online
:J4n3! :hmmm
:J4n3! :talked to ur dad bout it ?
:D1ck! :ofcourse
:D1ck! :he sed 'yes'
:D1ck! :and i have his cc in my hand
:D1ck! ::P
:J4n3! :haha cool
:J4n3! :woooo
```

Conclusion

Of course, the motivations and psychological profiles listed in this paper are not extensive or mutual exclusive. However, I trust this will give a sketch of what's behind the major threats in today's cyber world. As the "good guys" struggle to keep up with cracking methodology, much more research is needed with regard to the motivations and psyche of the perpetrator. As we monitor our networks and systems to curb malicious activity at the onset, so should we apply this proactive strategy to the behavioral "flags" of the ***cracker***.

Bibliography

(1) Hacker Profile Online NewsHour Special

http://www.pbs.org/newshour/bb/cyberspace/jan-june98/hacker_profile.html

(2) Happy Hacker Whats a Hacker http://www.happyhacker.org/define.shtml

(3) In the Spotlight Internet/Network Security http://www.netsecurity.about.com/compute/netsecurity/

(4) Psychology of Hackers: Steps Toward a New Taxonomy , Marc Rogers M.A http://www.infowar.com/hacker/99/HackerTaxonomy.shtml

(5) A Profile of the Web 'Crackers' **Elinor Abreu, The Industry Standard**
Tuesday, February 15, 2000 http://www.pcworld.com/news/article.asp?aid=15268

(6) Know Your Enemy: Motives Written by the Honeynet Project
Last Modified: 27 June, 2000 http://www.enteract.com/~lspitz/motives/