Global Information Assurance Certification Paper

Aggressive Counter-Hacking - Past, Present, and Future

Eric Pollinger
December 29, 2003
GSEC Version 1.4b Option 1

Abstract

This document will describe the history, elements of, and possible future of Aggressive Counter-Hacking employed against the malicious Hacker community. It will also describe the current threat as an escalating one requiring a more aggressive and proactive response. Proposed future offensive measures will be presented with particular attention paid to intrusion detection and response, proactive anti-hacking, the use of new technologies, and the legal concerns of all of these.

Table of Contents

Introduction

The goal of Aggressive Counter Hacking is to defend the network tomorrow by stopping the attacker today.

The tactics employed against malicious hacking are often defensive ones – firewalls, encryption, and switched networks function to make network intrusion difficult while human vulnerabilities are minimized through education and policies. These are defensive measures. Even the sporadic uses of intrusion detection and honey pot systems are more often used for compliance or to distract a hacker rather than to actually catch one. These defensive measures, on their own, do little to dissuade the attacker from continuing his assault – at best they may cause him to temporarily adjust his attack to another target but he can still return if a new exploit is discovered.

A defensive approach can be argued to be sufficient when the likelihood and potential damage of an attack is considered low enough. However, both these factors are on the rise and the cost to business and governments is expanding rapidly. There are also predictions that hacking may play a leading role in future terrorist attacks and so the need for a more aggressive approach is greater than ever.

Aggressive or Offensive Counter-Hacking (ACH) is a possible expansion in how these attacks can be countered. ACH is defined (for the purposes of this document) as any anti-hacking measures that take place outside of the secured network or defended company. ACH can be proactive, as in the case of Microsoft's recent bounty[1] for information leading to the arrest of hackers who target its software, or reactive as in the case of a hacker being tracked down and caught by a targeted company or individual. Also, although not recommended or condoned by the author of this document, ACH can also include measures such as hacking the hacker or the spreading of a counter "good" worm in the attempt to thwart a worm attack.

The Current, Escalating Threat

The overall threat posed by malicious hackers is expanding. This is due to an escalation in the number and skill of the attackers which is a natural progression of the expansion of the Internet, an increase in the potential reward for these hackers, the inability/reluctance of software/network companies to keep up with security as their features escalate, and the reluctance of companies and individuals to take common sense security precautions in the defense of their own networks.

The expansion of the Internet into certain countries is providing the foundation for some of this increase as hacker activities in places where the law may not be

[1] Diana, Alison. "How Much Is a Hacker's Head Worth?" E-Commerce Times. 19 May 2003. URL: http://www.ecommercetimes.com/perl/story/32163.html (1 Dec. 2003).

sufficient will help attract it. The case of Onel de Guzman is an example of this lack of judicial power. Onel is the assumed author of the "I Love You" virus that made the rounds on millions of systems in 2000. Although the evidence clearly pointed to him being the author (or at least one of the authors) he wasn't prosecuted due to holes in Philippine law[2].

The potential reward for hacking is also on the rise with activity involving the hiring of mercenary hackers who will attack for a price rather than for the fun or fame[3] – this, of course, opens up the ranks of malicious hackers by an order of magnitude.

There are two parts of the threat equation – risk of an attack (number of attackers, skill, vulnerability) and the overall impact of the assault (assuming success). The second part of this equation, the impact of a successful assault, is the bigger problem. We have become more dependent on our networks and systems for the running of all aspects of our lives. Virtually every profession owes its productivity efficiency and possibly even its existence to these networks and systems. Also, all of our key infrastructures are vulnerable to these attacks.

> "Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation."
> - Condoleezza Rice, National Security Advisor March 22, 2001

When the US Government conducts simulations into Terror attacks it will usually include hacking assaults as well. These attacks are rarely the main thrust but act as a force multiplier – they make the main attack more powerful by amplifying it or impeding the authorities' response. When the government performed simulations for the 2000 Winter Olympics in Salt Lake City[4] (code named Black Ice) they used hacking to cripple the 911-phone system (by using a cell phone worm) as well as direct hacking against the electrical infrastructure.

The increased threat posed by malicious hacking is the driving force behind ACH – it will force innovation in law, technology, and personal/corporate conduct to combat it.

Historical Examples of Aggressive Counter-Hacking

Counter hacking, I suspect, has been around as long as hacking itself. It has only been in recent years, with the advent of a defense only strategy among many that it now stands out. The clearest example of ACH is when the victim of

[2] Staff "Power 50 " AsiaWeek. 2001. URL: http://www.asiaweek.com/asiaweek/features/power50.2001/p11.html (6 Dec. 2003).
[3] Blank, Dennis. "Hacker Hit Men for Hire " BusinessWeek. 3 May 2001. URL: http://www.businessweek.com/bwdaily/dnflash/may2001/nf2001053_930.htm (1 Dec. 2003).
[4] Verton, Dan. " Black Ice: Cyber-terrorism and the Private Sector" ComputerWorld. 11 Aug 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,83841,00.html (6 Dec. 2003).

a hacker attack uses legal methods to stop the attacker and bring him to justice - an example of this is the case of Kevin Mitnick.

Kevin Mitnick was a hacker who used sophisticated techniques as well as social engineering to facilitate break-ins first at the Phone Company, then against the US government and other corporations. In the end his victims included Digital Equipment Corporation (DEC), Sun Microsystems, Motorola Inc, and Nokia. Law Enforcement's attempts to catch him were thwarted by his ability to manipulate the phone system – he would hack their trace attempts sending authorities to incorrect locations. In a clear example of ACH Kevin Mitnick was caught by Tsutomu Shimomura, one of his victims, who used cell phone technology to track him down[5].

The progression of self-replicating worms is one of the chief threats on the Internet. Worms usually use known exploits to gain access to a system node and then use it as a distribution sight to propagate to other victims. An ACH way to counter them (though a poor and probably an illegal one) is through the use of a "good" worm. This worm would use the same exploit to gain access to the node, and would still use it as a propagation point, but would not include a destructive package, would close the exploit, and would delete itself when done. 'Welchia'[6] is an example of an attempt at creating a "good" worm. This worm, released in August of 2003, used the same exploit as the Blaster worm and would attempt to download the fix for the exploit from Microsoft and was designed to delete itself at the start of 2004. Even though this worm worked as designed it caused significant havoc due to the bandwidth it consumed from its propagation as well as from the fix download it initiated. The US Navy[7] and State Departments[8] both took outages due to "Welchia".

Attempts at catching criminals have often included the offering of rewards. While the Federal Government offers limited rewards for information leading the apprehension of criminals Private Industry is finally following suit. Microsoft has recently set aside 5 million dollars to be used in rewards against Hackers who target their products[9]. At this point the reward is more reactive as it targets only certain prior attacks but, if successful, this type of system could be expanded to help counter attacks before they cause damage.

---

[5] Gach, Gary. "Internet Security Threatened" Cyberspace Today. 1 March 1995. URL: http://www.cybertoday.com/cybertoday/v1n1/mitnick.html (1 Dec. 2003).
[6] Virus Definition http://www.viruslist.com/eng/viruslist.html?id=65727 (6 Dec. 2003).
[7] Messmer, Ellen. "Navy Marine Corps Intranet hit by Welchia worm"Network World Fusion. 19 August 2003. URL: http://www.nwfusion.com/news/2003/0819navy.html (8 Dec. 2003).
[8] Labott Elise. "'Welchia worm' hits U.S. State Dept. network" CNN. 24 Sep 2003. URL: http://www.cnn.com/2003/TECH/internet/09/24/state.dept.virus/ (8 Dec. 2003).
[9] Diana, Alison. "How Much Is a Hacker's Head Worth?" E-Commerce Times. 19 May 2003. URL: http://www.ecommercetimes.com/perl/story/32163.html (1 Dec. 2003).

The Elements of Aggressive Counter-Hacking

Although there are many types of ACH methods most have components of one or more of these core elements - Preparedness, Detection, Action, and Follow-up.

Preparedness can include any Policy and Education items added to facilitate ACH. From the Policy perspective the ranking of attacks should clearly include either those that will necessitate an ACH reaction and follow-up or a clear approval process governing the activation of ACH for certain attacks. For example, a port scan or a mischievous, poorly targeted attack on a well-defended Web interface should not have an ACH response but an attack in which confidential information was exposed would. Careful control of the activation of an aggressive response to an attack is important since the response can be costly and disruptive. Having clear Policy elements also allows organizations to sort out the legal and logistic concerns prior to an attack and should clearly define not just the internal response but the external as well (I.E. the contacting of Law Enforcement). Education is as important as Policy in preparing an organization. Security Engineers need the tools to detect, record, and defend a network while the decision makers need to be prepared to make the key decisions in activating the policy.

The **Detection** element includes all methods whereby an attack is detected. Intrusion Detection is an example of this but detecting confidential information on external systems (post attack) or being sensitive to an imminent attack (learning that a worm it propagating before being infested) are also methods.

Intrusion Detection operates either on individual systems (Host-Based (HIDS)) or on the network as a whole (Network-Based (NIDS)). HIDS can be difficult and costly to install as it requires agents on every defended server and possibly a central monitoring server (with its own set of defenses) but it can be very effective in tracking unauthorized changes on a machine as well as attacks on the communication between two defended systems. NIDS operates by scanning network traffic for signs of known attack vectors or suspicious activity and logs (or, in some cases, blocks) the transmission. NIDS acts as a buffer between the systems it protects and the outside world and as such can act as a bottleneck – limiting network throughput. It also requires careful monitoring to the logs it produces.

Intrusion Detection has been criticized in recent days due to its poor fit in the defensive model and some have argued that it should be replaced with Intrusion Prevention systems[10] but ID is a central component of ACH. By its nature ID is either a significant piece of an offensive strategy or a means of reporting the failure of a defensive one. As a means of reporting failure ID probably doesn't

[10] Wickham, Timothy. "Intrusion Prevention is Dead. Long Live Intruder Prevention" SANS GSec. 21 Apr 2003. URL: http://www.sans.org/rr/papers/index.php?id=1028 (7 Dec. 2003).

provide the ROI that an organization expects from it but, with the correct and enforced policies in place, it can be used as an effective tripwire against the malicious hacker.

When ID fails and the attack succeeds the organization may have to face that all they can do is to catch the attacker – the damage from this attack will need to be absorbed. The reward Microsoft posed in the Examples section is an instance of this. Another version of this technique, especially when confidential information like source code is involved and accessible through multiple sources, is to manipulate the information so that, if exposed, the vulnerability (and/or the culprit) can be detected. This technique can be limited to the addition of spaces, misspellings, or the changing of variable names but these are easily masked. A better technique is make certain fundamental changes in the file such as the changing of word usage or tense in a document or reordering logic in source controlled files. Four changes will yield sixteen versions of the file to be categorized and tracked. While this technique has limited uses it can be very effective in the detection of the method of attack when multiple files are in play.

The **Action** element of ACH consists of the appropriate and calculated response that is geared to not only defend the network but also to catch the hacker. This action can take the form of offering a bounty or the creation of a worm designed to stop the propagation of another worm but is usually achieved through the employment of Forensics to aid Law Enforcement in the apprehension of the criminal. Computer Forensics involves the careful and legal detecting and saving of key pieces of evidence so that they can be used to find and prosecute the attacker. This process may require allowing an attack to continue for a short period so that evidence can be gathered. This gathering process often includes saving pristine versions of hard drives and logs and working with copies to piece together details of the attack. Computer Forensics is a specialty and would require that the company practicing ACH invest some time and resources into training or engaging appropriate outside staff.

All instances of ACH require **Follow-up**. This follow-up hopefully involves the informing of Law Enforcement with the evidence obtained through the use of Forensics. Reporting a cybercrime can be done at the Internet Fraud Complaint Center[11]. Further information on the governments' role in cybercrime can be found at the FBI Cybercrimes division[12]. If not, or if the ACH wasn't successful, this follow-up should involve an analysis of the methods used to detect and take action against the attack. The follow-up should involve an analysis of whether further preparation or education is required.

One element of ACH is that the company practicing it has made a decision to report the attack so that the attacker can be found. This may be difficult for a

[11] Internet Fraud Complaint Center: http://www1.ifccfbi.gov/index.asp
[12] FBI Cybercrimes Division: http://www.fbi.gov/libref/factsfigure/cybercrimes.htm

company as it might give a competitor an advantage but the action of hiding attacks can only benefit the attacker. SB1386, a new California Law[13], requires that an attacked company alert its customers of the attack and is a step in the right direction though it will have some painful repercussions for the first companies forced to comply with it.

A Discussion of the legal issues involved in Counter-Hacking

The relationship between the Law and hacking/computer crime has always been a troubled one. In the attempt to thwart malicious hacking activities lawmakers have often not been up to the task of creating enforceable, correctly targeted, and otherwise effective laws. Like many examples of lawmakers stepping into the technical realm they have shown poor understanding of the core issues and how to assess and counter the threat as well as an underestimating of how their new laws may affect legal activities.

A good example of poor legislation with respect to electronic security is New Zealand's Crimes Amendment No 6 Bill[14]. This bill, which was recently passed after years of debate, has some provisions that may make legal activity illegal and currently illegal activity legal. The bill defines 'interception of electronic communication', which the bill states is illegal, in such a way that proper security measures such as Intrusion Detection may be included. The bill also gets confusing around 'unauthorized access' in that it may allow a user who has partial authority on a machine (an email or FTP account) full legal authority so that breaking into another user's account **may be legal**. The bill also falls under scrutiny with respect to its treatment of Law Enforcement, as most anti-hacking bills seem to, in that authorities are granted substantial rights to search electronic communications without a court order.

One might think that in the U.S. laws against malicious hacking would be finely tuned but that is not the case. The main law protecting systems and information from attack is the Computer Fraud and Abuse Act (Title 18, Part 1, Chp 47, Sec 1030[15]) and a quick reading of the section may leave one wondering whether their home or company system is actually protected. The law is careful to define exactly what a 'Protected System' is and what kind of data is regarded as protected (mainly government, financial, and medical). In fact, from a criminal perspective, many examples of hacker activity are difficult to prosecute under U.S. Law. Often the government is forced to ignore major parts of a hacker's crime and concentrate their case against him by finding a part of the attack which involved a system involved in Interstate or Foreign commerce - a practice similar to convicting known Mob defendants on tax evasion charges. A good example of

[13] Poulsen, Kevin. " **California disclosure law has national reach**" Security Focus. 6 Jan 2003. URL: http://www.securityfocus.com/news/1984 (21 Dec. 2003).
[14] Bell, Steven. " Anti-hacking law niggles set in" ComputerWorld. 10 Jul 2003. URL: http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http://computerworld.co.nz/webhome.nsf/UNID/91201106EC2844A2CC256D5E000E3663 (20 Dec. 2003).
[15] Computer Fraud and Abuse Act: http://www4.law.cornell.edu/uscode/18/1030.html

this practice would be the case of '*Shurgard Storage Centers v. Safeguard Self Storage*'. In this case the judge used the Interstate and Foreign commerce part of the law in a broad way to cover an employee's stealing and distribution of company proprietary information…

> *"The judge concluded that the CFAA was "intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature." The court had no difficulty in quickly concluding that Shurgard's computers, attached to the Internet, were indeed "protected computers" within the ambit of the CFAA."*[16]

Even with this loose interpretation of 'Protected Computer' the 'Computer Fraud and Abuse Act' may not protect a home user's system and not even define as illegal certain attacks on corporate systems. In fact it seems very possible that certain hacker activity, which is assumed illegal, may not be. For example, if a hacker creates a worm with the purpose of stealing CPU time from systems to achieve some (arguably) legal goal and the worm is constructed in such a way that it doesn't cause damage in propagation, execution, or cleanup the release of the worm and subsequent propagation is not clearly illegal. The stealing of the CPU time, by itself, doesn't appear to be illegal.

It also seems clear that the ACH practice (though not recommended by the author of this document) of counter-hacking a hacker's computer **may** not be illegal – especially if the damage to their system doesn't exceed $5,000 (see subsection a-4 of the 'Computer Fraud and Abuse Act') and even that provision would seem to rely on the hackers' system being defined as 'Protected' – something a judge may not be inclined to do.

The Future

The future of ACH is divided into three areas. How will the Law change in the face of the growing threat and the lessons learned from prior, less than effective, laws? How will companies and governments change their policies and procedures to more effectively counter the hacker threat? How will new technologies help in the detection, tracking, and countering of hacking threats?

Given the cost and importance of this type of law the government should make continuous progress in this area. Part of this progress will involve private industry pushing for changes in order to help defend their systems and property. The RIAA's recent attempts to get legal protection of their intellectual property are a good example. In fact their attempts to gain legal access to search and

[16] Burke, Edmund. "The Expanding Importance of the Computer Fraud and Abuse Act" GigaLaw.com. Jan 2001. URL: http://www.gigalaw.com/articles/2001-all/burke-2001-01-all.html (20 Dec. 2003).

attack home users who possess illegal copies of their music is a pure example of ACH[17].

The case of the W32/Fizzer@MM worm is a good case study to illustrate the direction future legislation may take. This worm was first discovered in June 2003 and quickly propagated. It used an IRC channel to check for and download an update of itself. The IRC operators had the opportunity to shut down the channel or could code a benign update that would clean the worm from the effected system (as some did)[18]. This practice of disabling the worm was quickly stopped due to the uncertainty of the law around in this area but this illustrates one of the clear dividing lines. As governments approach this type of law they will need to consider the difference between an undefended/non-up to date but not yet infected machine vs. one that is trying to propagate a dangerous worm throughout the Internet. Like a gunman shooting randomly from his house can a third party deal with this server? Could a law similar to the 'Good Samaritan' law, which protects those who give first aid from subsequent prosecution, be created to protect self-policing on the Internet or would the government take on this role?

The future role of organizations in ACH is dependent on the effectiveness of their current, largely defensive, measures. However, more and more companies are feeling the sting of these attacks. Recently a hacker gained access to the source code of Valve Software's new 'Half Life 2' game[19] and published it on the Internet making it all but impossible for the company to release the game in the current form (due to the security holes which were introduced by having their source public) – this delay in release will cost the company many millions. The continuing of these types of attacks will soften the public outrage at the company being attacked and will enable them to admit and fight against future attacks – maybe even gaining public confidence and admiration for bold moves to counter the attacker.

New Technology, especially in the realm of exposing the attacker, is the other driving force in the future development of ACH. ACH requires the ability to trace an attack back to the attacker and, although difficult under the best of circumstances, it has been virtually impossible in the case of DDOS attacks in which a hacker has taken over hundreds or thousands of other machines in order to blitz a target system so that it is unable to perform its normal job. Trace Back of this attack would require some sort of fingerprint of the original attacker seeing through source IP spoofing and the use of proxy systems. This type of technology in under development and usually involves a statistical approach to

[17] McCullagh, Declan. "RIAA wants to hack your PC" Wired.com. Oct 15 2001. URL: http://www.wired.com/news/conflict/0,2100,47552,00.html (21 Dec. 2003).
[18] Bradley, Tony. "Ethics: Savior or Vigilante" NetSecurity. URL: http://netsecurity.about.com/cs/generalsecurity/a/aa052103_2.htm (21 Dec. 2003).
[19] Brunker, Mike. "Hacker spoils game for software firm" MSNBC Oct 3, 2003. URL: http://www.msnbc.com/news/975464.asp?cp1=1#BODY (21 Dec. 2003)

sampling authenticatable packets and storing them for a short period so that they can be used to trace the attack back to the source.

Conclusion

Aggressive Anti-Hacking will continue to have an expanding role in the struggle against Malicious Hacking. As the cost of a 'defense only' strategy increases, both in dollars and ineffectiveness, and as the Law catches up with technology, the role of AAH will be a key weapon in the battle against Hackers.

References

[1] Diana, Alison. "How Much Is a Hacker's Head Worth?" E-Commerce Times. 19 May 2003. URL: http://www.ecommercetimes.com/perl/story/32163.html (1 Dec. 2003).
[2] Staff "Power 50 " AsiaWeek. 2001. URL: http://www.asiaweek.com/asiaweek/features/power50.2001/p11.html (6 Dec. 2003).
[3] Blank, Dennis. "Hacker Hit Men for Hire " BusinessWeek. 3 May 2001. URL: http://www.businessweek.com/bwdaily/dnflash/may2001/nf2001053_930.htm (1 Dec. 2003).
[4] Verton, Dan. " Black Ice: Cyber-terrorism and the Private Sector" ComputerWorld. 11 Aug 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,83841,00.html (6 Dec. 2003).
[5] Gach, Gary. "Internet Security Threatened" Cyberspace Today. 1 March 1995. URL: http://www.cybertoday.com/cybertoday/v1n1/mitnick.html (1 Dec. 2003).
[6] Virus Definition http://www.viruslist.com/eng/viruslist.html?id=65727 (6 Dec. 2003).
[7] Messmer, Ellen. "Navy Marine Corps Intranet hit by Welchia worm"Network World Fusion. 19 August 2003. URL: http://www.nwfusion.com/news/2003/0819navy.html (8 Dec. 2003).
[8] Labott Elise. "'Welchia worm' hits U.S. State Dept. network" CNN. 24 Sep 2003. URL: http://www.cnn.com/2003/TECH/internet/09/24/state.dept.virus/ (8 Dec. 2003).
[9] Diana, Alison. "How Much Is a Hacker's Head Worth?" E-Commerce Times. 19 May 2003. URL: http://www.ecommercetimes.com/perl/story/32163.html (1 Dec. 2003).
[10] Wickham, Timothy. "Intrusion Prevention is Dead. Long Live Intruder Prevention" SANS GSec. 21 Apr 2003. URL: http://www.sans.org/rr/papers/index.php?id=1028 (7 Dec. 2003).
[11] Internet Fraud Complaint Center: http://www1.ifccfbi.gov/index.asp
[12] FBI Cybercrimes Division: http://www.fbi.gov/libref/factsfigure/cybercrimes.htm
[13] Poulsen, Kevin. " California disclosure law has national reach" Security Focus. 6 Jan 2003. URL: http://www.securityfocus.com/news/1984 (21 Dec. 2003).
[14] Bell, Steven. " Anti-hacking law niggles set in" ComputerWorld. 10 Jul 2003. URL: http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http://computerworld.co.nz/webhome.nsf/UNID/91201106EC2844A2CC256D5E000E3663 (20 Dec. 2003).
[15] Computer Fraud and Abuse Act: http://www4.law.cornell.edu/uscode/18/1030.html
[16] Burke, Edmund. "The Expanding Importance of the Computer Fraud and Abuse Act" GigaLaw.com. Jan 2001. URL: http://www.gigalaw.com/articles/2001-all/burke-2001-01-all.html (20 Dec. 2003).
[17] McCullagh, Declan. "RIAA wants to hack your PC" Wired.com. Oct 15 2001. URL: http://www.wired.com/news/conflict/0,2100,47552,00.html (21 Dec. 2003).
[17] Bradley, Tony. "Ethics: Savior or Vigilante" NetSecurity. URL: http://netsecurity.about.com/cs/generalsecurity/a/aa052103_2.htm (21 Dec. 2003).
[18] Brunker, Mike. "Hacker spoils game for software firm" MSNBC Oct 3, 2003. URL: http://www.msnbc.com/news/975464.asp?cp1=1#BODY (21 Dec. 2003)