BLACK BOX®
NETWORK SERVICES

A Beginner's Guide to Cybercrime

Understanding attack methodologies and a more proactive approach to defence.

0118 965 6000 | www.blackbox.co.uk

Table of Contents

We’re here to help! If you have any questions about your application, our products,
or this white paper, contact Black Box Tech Support at 0118 965 6000 or
go to www.blackbox.co.uk and click on “LiveChat.”
You’ll be live with one of our technical experts in less than 30 seconds.

Introduction

If you are a regular reader of Hakin9 magazine, you probably already know a great deal about hacking. But do you know the difference between traditional crime and cybercrime? Do you know where the cybercrime magnets are?

And do you know why nothing with an IP address is secure and why traditional countermeasures such as firewalls, anti-virus, and intrusion detection fail? Would you like to learn new methods to proactively defend against attacks? If so, read on.

Let's start with the difference between traditional crime vs. cybercrime. There are parallel crime methodologies between "real-world" crime and "digital-world" crime, which is enabled by Internet protocols and the World Wide Web.

Traditional criminal techniques involve burglary, deceptive callers, extortion, fraud, identity theft, and child exploitation, to name a few. With cybercrime, the end results are often the same but are done through hacking, phishing, Internet extortion, Internet fraud, identity theft, and child exploitation (sources: uscert.gov, cybercrimes.gov, and privacyrights.org).

If you take a few moments to visit privacyrights.org and click on the "Chronology of Data Breaches," you'll notice more than 350 million personally identifiable information (PII) records have been lost, stolen, or hacked. And this information only refers to breaches in the U.S. So do you still think you are secure or believe your anti-virus and firewall can truly secure your network or personal computer?

Comparing Traditional Crime Techniques with Cybercrimes

Traditional Crimes	Cybercrimes
Burglary Breaking into a building with the intent to steal.	Hacking Computer or network intrusion providing unauthorised access.
Deceptive callers Criminals who telephone their victims and ask for their financial and/or personal identity information.	Phishing A high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.
Extortion Illegal use of force or one's professional positions or powers to obtain property, funds, or patronage.	Internet extortion Hacking into and controlling various industry databases (or the threat of), promising to release control back to the company if funds are received or some other demand satisfied.
Fraud Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain an unfair or a dishonest advantage.	Internet fraud A broad category of fraud schemes that use one or more components of the Internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.
Identity theft Impersonating or presenting oneself as another to gain access, information, or a dishonest advantage.	Identity theft The wrongful obtaining and using of another person's identitfying information in some way that involves fraud or decption, typically for economic gain.
Child exploitation Criminal victimisation of minors for indecent purposes such as pornography and sexual abuse.	Child exploitation Using computers and networks to make it easier to criminally victimise minors.

The prevalence of new malware

Most of the breaches happen because of new and more innovative malware. To start, you need to understand the basics of malware. What is it? Is it a virus, Trojan horse, worm, rootkit, botnet, zombie, keylogger, adware, or spyware? It is all these things, and some are combined into what are known as "blended threats."

Is your computer infected with malware? It is highly possible, as one study claims that 30,000 computers are becoming infected every day with new malware, known as zero-day (this means the day it was released and before an anti-virus vendor has a signature test for it), while still running firewalls and anti-virus software.

Do you think some of the Web sites you visit could be infected with malware? At least half of the Top 100 sites, particularly social networking sites such as Facebook® or YouTube®, support user-generated content, which is becoming a significant way to disseminate malware and conduct fraud. Part of the problem is that on Facebook, MySpace®, and other social networking sites, there's an explicit sense of trust.

Do you pay your bills on-line? Criminals seized control of the CheckFree Web site and attempted to re-direct users to a Web site hosted in the Ukraine that tried to install malware on victims' computers. CheckFree has more than 24 million customers and controls 70 to 80% of the online bill-payment market.

Much of the new malware is specifically designed to propagate across USB sticks. For example, the picture frame you just bought online that uses a USB connection might have come with zero-day malware from China. In addition, malware makes its way onto file servers using the structured message block (SMB) protocol—that includes Linux® and Windows® file servers and network-attached storage devices. Some of this malware is so sophisticated, it finds data files such as .doc, .xls, .wav, .mp3, .pdf, and others to infect so when someone else opens them, they too become infected.

Don't think you are safe at home either. Cable networks are loaded with peer attackers. Most likely, a telecommuter is using an insecure, hacked laptop with a key logger and coming in "securely" into your network through an encrypted Virtual Private Network (VPN) tunnel.

Cloud computing—a malware magnet

Cloud computing—in which shared resources and software are available over the Internet— is also a cybercrime magnet. Why? Because cloud computing has shifted the framework for risk. The cloud offers low overhead in return for powerful remote business functionality. In return, you face the risk of data leakage, cloud attacks, and cloud infections. You most likely will not know if and when it happens because of the remote aspects and the pervasive nature of the cloud.

Secure wireless networking—easily hacked

Wired equivalent privacy (WEP) was the first commercial algorithm and attempt to secure wireless networks using the IEEE 802.11 standard. Because wireless networks broadcast messages using radio waves, they can more easily be eavesdropped on than traditional wired local area networks. WEP was released in 1997 as an attempt to provide confidentiality that would be comparable to that of wired networks. However, in less than four years, various weaknesses were uncovered in WEP. Today, it can be cracked in minutes.

Then in 2003, along came Wi-Fi protected access (WPA), which was updated to WPA2 in 2004. Today, both WEP and WPA are widely deployed, yet with new tools such as BackTrack v4.0, anyone can gain access to a "secure" wireless network in a matter of minutes. In addition, most wireless routers have critical flaws known as Common Vulnerabilities and Exposures (CVEs). You can now break into the administrative interface of a wireless router by sending malformed packets from your laptop without worrying about cracking the encryption. Just visit the National Vulnerability Database (NVD) located at http://nvd.nist.gov and type in "wireless" to see where the holes are located.

Vulnerable wireless devices

What about wireless communication devices such as a BlackBerry ®, an iPhone ®, an iPod Touch ®, or an iPad ™? The question is: Do they really belong on the "corporate" network? If so, how do you know when they come and go, along with other portable devices and laptops? How do you stop them from bringing malware into the network? How do you stop them from being used to steal or leak confidential data? If you can't control, track, and manage assets, how can you claim that your network and your data are secure? You cannot. In fact, nothing with an IP address is secure. No device is safe. All IP-based devices are exposed to exploitation. Why? Because they are all targets— they can be spoofed, infected, and remotely controlled, and probably already are infected with some form of zero-day malware.

Is VoIP secure?

But is Voice over IP (VoIP) secure, as it is usually physically wired? The answer is no. There are dozens of VoIP holes also found under the NVD. Some of these can be exploited by tools that are freely available on-line. These tools will enable you to take over the administrative console of the VoIP server by exploiting just one CVE—remember, all it takes is one hole and you can find many exploits. VoIP is also easily susceptible to a "man in the middle" attack. A sample exploit known as voice over misconfigured IP telephony (aka VOMIT) enables you to play back conversations that occurred earlier. Hackers simply use a TCP/IP ethertrace utility such as Wireshark ®, save a "dump" file of network traffic, and then run the file through VOMIT to get a WAVE file of prior conversations.

Traditional countermeasures all fail!

Anti-virus utilities are usually one to seven days behind the current malware threat. With today's malware, they are usually infected without knowing it. Just try "AVKILLER" as one of 400,000 sample pieces of malware to find out for yourself how serious this problem has become. Firewalls are easily circumvented or used as part of an exploit because of their exploitable holes (CVEs). Finally, Intrusion Detection System (IDS) detects odd or mal-behaving traffic after the infected system or hacker system has breached the gates. To understand why these security countermeasures all fail, you need to understand the root cause of exploitation. CVEs are holes and are exploited daily. Here's a simple example: Although there might be 9,000,000 signatures in your McAfee® or Symantec® anti-virus scanner database (and growing exponentially), there are only about 36,000 CVEs.

If you close just one CVE, for example, you can block more than 90,000 variants of the W32 malware. If you aren't visiting http://nvd.nist.gov to see what kind of exploitable holes you have in your network, cybercriminals certainly are. Because everything with an IP address has a CVE, you need to figure out which ones are critical holes and how to patch, reconfigure, and remove them. This is also known as "system hardening," and most folks seem too busy to find the time to go after the root cause analysis. Instead they stay in reactive mode—cleaning old viruses, patching one hole while opening another. You might think you are defending your castle with traditional countermeasures like bows, arrows, and spears, however, today's cybercriminal is flying into your castle, behind the moat, using an Apache helicopter, night goggles, and a silencer.

Proactive defence—learn and use the "secret" formulas

Here are a few simple formulas to help you understand how to reduce risk, comply with regulations, and harden your systems. The first formula is based on U.S. military basic war tactics and is called the four Ds. They are:

1. Detect – awareness of a threat
2. Deter – preempting exploitation
3. Defend – fighting in real-time
4. Defeat – winning the battle!

The second formula is well known in network security circles and is called the "Risk Formula":

R = T x V x A

(R)isk = (T)hreats x (V)ulnerabilities x (A)ssets

So, to fully understand your risks, you need to deal with:

Threats = Cybercriminals, malware, malicious insiders

Vulnerabilities = Weaknesses that threats exploit

Assets = People, property, your network, devices, etc.

Now, let's put these two formulas together—the 4Ds and the Risk Formula—to build a more proactive, next-generation defence:

4Ds x R = [4Ds x T] x [4Ds x V] x [4Ds x A]

You'll never be 100% secure, but you can dramatically reduce your risk and proactively defend your organisation by containing and controlling threats, vulnerabilities, and assets. Using the 4Ds with the Risk Formula:

- Threats need to be detected, deterred, defended against, and defeated in real-time or expect downtime.
- Vulnerabilities need to be detected, deterred, defended against, and defeated (i.e. removed by system hardening, reconfiguration, patching, etc.) as quickly as possible or expect to be exploited.
- Assets need to be controlled—which ones gain access to your network/infrastructure and those that are trusted but weak or infected need to be quarantined in real-time or expect malware propogation.

Proactive defence—employee awareness and training

With these two formulas in place, you’ll still need to account for the most important challenge to network security: untrained and easily exploited employees. You should begin to invite employees to a quarterly “lunch and learn” training session and give them “bite-size” nuggets of best practices information. Consider even giving an award once per year to the best INFOSEC-compliant employee who has shown an initiative to be proactive with your security policies, the 4Ds, and the Risk Formula. Remember, if you can keep them interested, they will take some of the knowledge you share into their daily routines. That's the real goal.

Launch a 4D and Risk Formula educational campaign so all employees in your organisation join your mission to protect corporate information. Create your own “security broadcast channel” via e-mail or really simple syndication (RSS) and get the message out to your corporate work force. You can also give them “security smart” tips, alert them to a new phishing scam, or let them know that the corporation had to dismiss an individual who was attempting to steal corporate information. It’s important to understand that keeping the entire team in the loop helps bolster the corporate security posture.

There are other tools available such as INFOSEC awareness posters, which you can get from one of the security awareness training companies. If you are creative and have the time, make postcards with dos and don’ts/best practices for employees so they can pin them up in their offices as reminders. The bottom line: Knowledge is power, so start empowering your fellow employees to gain a basic toehold in what they should and shouldn’t do. This will help you in your mission of more uptime and fewer compliance headaches.

There are also some great corporate security policy tools available for free, such as the powerful COBIT model at http://www.isaca.org, the e-tail/retail-oriented Payment Card Industry (PCI) model from the PCI Security Standards Council found at https://www.pcisecuritystandards.org, and the extremely comprehensive international model called ISO 27001/17799 from http://www.iso.org. Any of these models will be a great starting point.

Proactive defence—strong encryption

There's an old saying: "loose lips sink ships.“ The best practice is to look at all aspects of electronic communications and data manipulation throughout your enterprise. That should include all instant messaging, file transfer, chat, e-mail, on-line meetings, and webinars plus all data creation, change, storage, deletion, and retrieval. For example, how are customer records stored? How are electronic versions of other confidential information protected? Backing up the data is not enough.

You should set up a VPN for external network access. Make sure the systems that access your network through the encrypted tunnel are also not the weakest links in your infrastructure by deploying Host Intrusion Prevention System (HIPS) on endpoints. You can encrypt everything from your hard drives to your e-mail sessions to your file transfers. There are numerous free tools out there like http://www.truecrypt.org for hard drives and http://www.openssl.org for Web, e-mail, and instant messaging, plus the “granddaddy” of free encryption at http://www.openpgp.org PGP (Pretty Good Privacy).

You'll need policies in place for key storage and password access so if the end users ever lose the keys and passwords, you'll have a way back in to decrypt the information, reset the keys, or change the passwords. You might find out that some of the servers and services you are running already offer encryption if you simply check the box and turn on this feature.

Proactive defence—physical access control

Piggybacking and tailgating are a major physical security risk—hence the need for more intelligent physical access control (PAC). So, you’ll need to make sure your PAC solution shares data over the network to you and (potentially) to your NAC solution. You should make sure your PAC solution uses two-factor authentication and that if your TCP/IP connections go down, the PAC system still functions mechanically with accessible local logs.

Proactive defence—network access control

Because so many exploits happen behind firewalls, you need to consider deploying network access control (NAC). Simply put, NAC determines who belongs on your network and who does not, so you should make sure your NAC solution doesn’t telegraph to exploiters (i.e. “welcome to NAC portal…please wait, installing XYZ corp trust agent v3.1). Also you’ll need to make sure it has a way to deal with non Windows systems (hubs, switches, routers, BlackBerry devices, iOS devices, etc.). Your network solution needs to be holistic. Try to find a non-inline or “out-of-band” appliance solution and avoid costly, hard-to-manage hacked agents.

Proactive defence—host-based intrusion prevention system

Because so many Windows systems—especially laptops—are compromised, you need to consider host-based intrusion prevention systems (HIPS). HIPS blocks malicious software from functioning. The evolution of anti-virus will always be a newer, faster signature testing engine (even if they try to add HIPS) that’s one step behind the latest malware attack. Look for a purely HIPS solution that blocks zero-day malware without signature updates (heuristically). It should help mitigate malware propagation, quarantine malware in real-time, and not be a CPU or memory hog, which makes the end-user PC unusable.

In summary

Crime and cybercrime are really the same concept, with the same end results, only using different “vehicles” or mediums (i.e. physical vs. logical). Web sites, e-mails, instant messaging, softphones, and portable devices are all malware magnets. If you have an IP address, you are not secure, and traditional countermeasures all fail! You can begin to take a more proactive approach to cyberdefence by using and understanding the 4Ds and the Risk Formula. You will never be 100% secure, and you can never block or prevent all intrusions, so focus on intrusion defence and risk management. In other words, expect it to happen—use the 4Ds and the Risk Formula to contain the damage, if any. Don’t forget to educate your fellow employees—the weakest link—and to document your security policies. Stay vigilant and proactive so you will be one step ahead of the next threat.

About Black Box

Black Box Network Services is a leading network security provider, serving 175,000 clients in 141 countries with 195 offices throughout the world. The Black Box® Catalogue and Web site offer more than 118,000 products , including NACs, secure Internet gateways, biometrics, and remote monitoring and security. For details on these solutions, including our award-winning Veri-NAC™ , go to www.blackbox.co.uk/goto/Veri-NAC.

Black Box also offers networking equipment, digital signage and multimedia products, KVM cables, cabinets and racks, and more—all supported by our FREE, 24/7, live Tech Support hotline.

Black Box is also known as the world’s largest technical services company dedicated to designing, building, and maintaining today’s complicated data and voice infrastructure systems.