



Complete. On Demand. Affordable.

Top 9 Network Security Threats in 2009

Kevin Prince
Chief Security Architect
Perimeter eSecurity

2008 is nearly in the rear view mirror and as we prepare for 2009, one must ask the question “what threats (new and old) are we going to have to deal with in the coming year?” But first, let’s analyze 2008 compared to what we expected a year ago.

2008 IN REVIEW

Malware, especially from compromised web sites, was a huge issue. Many legitimate sites such as MSNBC.com, History.com, ZDNet.com and many others were compromised, in some cases for days. Unlike the past, the sites looked normal but unsuspecting web surfers with vulnerable systems were exploited when they visited these sites.

Search engines were used, such as Google, to compromise systems. There were several ways this occurred including:

- Tricking the search engine indexing and results logic to escalate malicious web sites to the top of the list where users were more likely click on it.
- Using the “paid for” or “sponsored links” areas of search engines to direct users to compromised sites.

There was (as predicted) a movement towards compromising end points (individual systems such as desktops, laptops and servers) and less emphasis on external direct attacks (although this still frequently happens).

On the flip side, we expected botnets to play a larger role in 2008. While they increased in size, scope, and sophistication, they weren’t used to the scale expected. Basically, botnet controllers were “sowing” more and “reaping” less in 2008.

Also, out of the blue, we had the whole “DNS exploit” issue come back from the dead. We saw a lot of these in the 90’s when DNS was first used and then we went nearly a decade without many DNS flaws. I don’t think anyone expected a core DNS vulnerability on a worldwide scale. The good news is that very few known cases of serious exploits occurred.

Vista had fewer serious security vulnerabilities than expected. This may be because so few people are migrating to Vista and many even downgrading to XP. I imagine that if more people were using Vista 1) we would find more vulnerabilities and 2) more attackers would spend time trying to exploit it. Attackers are all about “bang for the buck.” If most people are still using XP, they will focus on XP. It is just that simple.

LOOKING FORWARD TO 2009

What data security threats will be most prevalent? Let me first start with some general predictions.

- The volume of attacks from international sources has and will continue to increase especially towards government and military networks. The fog is beginning to lift and as it does we will see the vast majority of these attacks coming from China and being tied to government sponsorship.
- Data security breaches tied to theft will significantly increase. It will not surprise anyone that mobile devices are stolen most often.
- The sophistication of application level attacks such as SQL injection, buffer overflow, cross site scripting (XSS) and others will increase. These will be directed towards high traffic web sites (news sites or social networking sites) that when compromised will install malware to a large numbers of users.
- For the most part, botnets will not need to be the concern of small business or consumers. Service providers and large enterprises have added steps (perhaps just in time) to reduce the challenges of botnets.
- Bandwidth consumption will percolate higher in the list of IT challenges for organizations of all sizes. More and more users will use the web to download content. Our appetite has changed from text with a few graphics to streaming high definition video, huge downloads, and YouTube.

Annually I have listed what I believe are top threats for several years now. This year the list is different. This is due to the environment in the US from an economical, legislative, and political perspective. The different perspectives are so volatile that the environment alone will spawn some new threats we have not dealt with. The type and volume of information that is now available on the Internet creates additional threats. The following list is my top 9 threats for 2009.

#1. **MALICIOUS INSIDERS** RISING THREAT

Employees with malicious intent have always been the biggest threat to their organizations. According to www.infosecurityanalysis.com, when a data security breach occurs as a result of a malicious insider, more records are compromised than any other breach source (including hackers). In 2008 we learned about Dwight McPherson, who worked in the admissions office at NY-Presbyterian Hospital/Weill Cornell Medical Center. Dwight was approached by a man who told him he would pay him for medial records of males born between 1950 and 1970. Dwight took nearly 50,000 records and sold two batches

of 1,000 records for \$1,350 before getting caught.

Several studies indicate that only a small percentage of data breaches are reported. Many companies still choose not to report these because it shows a systemic failure of hiring practices, policies, procedures, auditing, enforcement and technology safeguards. As economic times get worse, we will likely see desperate and malicious employees compromise security for a few extra dollars.

#2. MALWARE STEADY THREAT

This is where I feel a bit like Nostradamus. If I use words that are so generic and apply to almost anything, I of course will be right in a prediction. Malware means malicious software which can include viruses, worms, Trojan horse programs, etc. I don't want to generalize, I want to be specific. What I am referring to are web sites that host malware. When a vulnerable user accesses this web site, their system becomes infected. The system then falls under the control of the attacker.

This is such an effective method to distribute malware and compromise systems that it has become the most prolific method. I believe this will continue and become a greater threat in 2009.

#3. EXPLOITED VULNERABILITIES WEAKENING THREAT

Exploiting a known vulnerability is the normal process when people talk about "hacking". Hackers find a weakness and exploit it for their gain. There is nothing new here, except the location of the systems.

In times past, it was external systems such as email servers, web servers, and firewalls that would be broken into. These attacks are moving inside the network. Systems on the inside of the network are not patched and updated as frequently. Networks have a hard outer edge and a gooey center from a security perspective. Organizations rely on Microsoft SUS (system update service) that patches and keeps the systems up-to-date. The problem is that SUS only patches Microsoft which leaves all the non-Microsoft operating systems applications vulnerable.

IT professionals make the mistake of thinking, "well it was only the administrative assistants machine that got compromised and it didn't have any sensitive information on it." If a system gets compromised, the attacker may have control of more than just that one system. From that system they could launch additional attacks to other systems. They can "sniff" the credentials of anyone on that system to access other systems. Typically, the first system to be exploited is just the base camp to compromise more valuable assets.

When an internal system is compromised, the bad guys now have ways of bypassing your entire network and edge based security controls. They use encrypted tunnels over commonly used ports to make their deeds virtually invisible.

#4. SOCIAL ENGINEERING



RISING THREAT

Gartner has stated that the greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses. Kudos to Gartner, they were right, and I believe 2009 will be the year of more social engineering attacks. Why spend days trying to crack a username and password using sophisticated software and potentially get caught, when you can trick someone into just giving you theirs? With hacking you are compromising a computer, and with social engineering you are compromising a human.

In 2009 we will see the common use of many social engineering ploys. Any method of communication can and will be used to perpetrate fraud including telephones, mobile phones, text messaging, instant messaging, and social networking sites. Additionally, many people will fall prey to their own natural curiosity. For example, leaving a CD infused with malware entitled “2008 employee compensation & bonuses” by the elevator or a USB thumb drive near the door of the building that will infect a system when plugged in.

#5. CARELESS EMPLOYEES



RISING THREAT

Careless employees are not a threat I have listed in the past. Not only have I seen a trend that includes more mistakes made by careless or untrained employees that lead to a security compromise, but this will be fueled by the economic climate. With a recession, business will have to do more with less. The strain this puts on employees causes them to cut corners on important duties. Systems will not be updated, logs will not be reviewed and alerts will go unchecked. This creates gaps that can be exploited by the attackers.

A poor economic climate may lead to less formal employee training. This leads to policies and procedures not being followed. Liability issues arise. Data exposure can occur. One example of this is how my wife’s personal information was compromised. The local University Hospital had a procedure to have their backup tapes (with thousands of sensitive patient records) taken off-site by a third party provider. The employee of the data archive and transport company decided not to follow procedures and instead of dropping the tapes off at their destination, went to his second job. While at his 2nd job, his car was broken into and the tapes were stolen.

#6. REDUCED BUDGETS



RISING THREAT

As you can see, there are many threats that have roots in a downward economy. A weak economy leads to companies tightening their budgets. This results in lower headcount and less money for upgrades and new systems. Just because the economy slows does not mean that criminals slow down. In fact, it is often the opposite. There are always those system upgrades, process improvements, and new technologies that were put into next year’s budget that may now be put on hold. 2009 may see reduced budgets, which means more exposure and security gaps that can lead to a data security breach.

#7. REMOTE WORKERS STEADY THREAT

Companies that support telecommuting are on the upswing. Remote workers and travelers all pose unique security risks. Often I see organizations install a VPN box without much thought to security. A VPN only encrypts the traffic between the remote user and the company. If that system is compromised, you are effectively encrypting (keeping private) all of the hacker's traffic. VPN's are usually installed in a way that bypasses edge based security devices such as the corporate firewall. Remote workers have greater exposure to system compromise for several reasons.

- The company does not own the computer they are working from and it does not have the security software like other corporate systems.
- Remote users are more likely to allow their systems to lapse in their security protection. They do not update software because they often pay for it out of their own pocket.
- When something goes wrong, there is no IT person to help them, thus they do whatever it takes to get it working which may disable needed security measures.
- Theft is the #1 cause of data security breaches. Most people house some sensitive corporate or customer data on their laptops. 1 in 10 laptops is stolen within the first year of ownership.
- A remote computer is not subject to the same security requirements as corporate. For example, you may use web content filtering on the corporate network to block access to inappropriate web sites. Remote user traffic is usually not routed through the same system. As a result, the remote user may access a web site that could infect and compromise their system. When that system connects to the network, that compromised system can now spread and attack other internal systems.
- Children and other household members may use the same computer mom or dad use for work. They install a game, hit a web site, or any of a number of things that can lead to the compromise of the system. All you hear is "Dad, the computer is running really slow again!"

#8. UNSTABLE THIRD PARTY PROVIDERS STRONG RISING THREAT

Most providers have begun to see slowing sales and weaker profits. At the same time, regulators are requiring many providers to achieve and maintain strong compliance. While there is an increase in expenses, there is a decrease in revenues. I believe this will lead many providers to go out of business or cut corners that could lead to a compromise. At this time, it is imperative for organizations to streamline their 3rd party providers. Ensure you are using ones that have been in business for a long time and have seen hard times before. Use ones that have been regulatory focused for years rather than ones that are just trying now. Ask for audited financials and ensure your provider is profitable.

Choose a provider that can offer you multiple solutions to gain the benefits of economies of scale. I am a big proponent of outsourcing, but it must be to the right organization.

#9. DOWNLOADED SOFTWARE STEADY THREAT

IT administrators may be tempted to take on more themselves. They may download and install open source software or freeware in an attempt to save money. I have found that these tools in the hands of an inexperienced user may lead to a huge waste of time or a data breach. Almost all security software available commercially has a freeware or open source counterpart somewhere. The installation, configuration, fine tuning and other aspects of a software lifecycle sometimes are more than any individual can handle, especially if they don't have the time and training to do it.

Lastly, users that are allowed to download and install software on their desktops are a huge risk to their company. For example, we have seen unsuspecting users install modified versions of P2P software. Rather than just giving the user the ability to download music and movies (which is a bandwidth problem by itself), these programs can be modified to scan the local system and network systems to catalog sensitive information such as spreadsheets and databases and make them publically available for download anywhere in the world. Your firewall and most other security devices cannot detect or stop this activity.

All software downloaded and used should be done by a trained IT professional. I believe we will continue to see many data breaches as a result of downloaded software in 2009.

CONCLUSION

This doesn't have to be all doom and gloom. By realizing these threats, we can work to ensure our exposure is limited. Additionally, it gives us the opportunity to look at alternative solutions. A company that has traditionally kept their security management and monitoring in-house may use this as an opportunity to look at the cost benefits of outsourcing this to a leading security firm. Some of the technology you have been using to reduce your risk may be outdated and you can replace it with newer systems that can protect your organization better for the same or less money. Challenges such as this give us the opportunity to rethink the way we have done things in the past and find newer, optimized ways of securing our organizations. With data security, it isn't about having more as much as it is about having the right stuff.

Kevin Prince
Chief Security Architect
Perimeter eSecurity
KPrince@perimeterusa.com

ABOUT PERIMETER ESECURITY

As the only provider of complete security On Demand, Perimeter eSecurity makes security easily available and affordable for all businesses. Perimeter's On Demand security services protect thousands of computer networks nationwide, offering more than 50 different services on a subscription basis in the areas of: Vulnerability Defense, Intrusion Defense, Network Defense, Email Defense, System Defense, and User Defense. With the proliferation of security threats and technologies, clients benefit from a single-source provider that offers all services through one pre-integrated platform and web portal. Perimeter's security SaaS services are continuously expanded, enhanced and upgraded for current and future regulatory compliance. With seven geographically distributed technical offices and three redundant data centers, Perimeter's complete, On Demand and affordable security services are always available and have been validated by multiple independent third parties. If you would like to speak with us or view a product demo, please don't hesitate to call at 800.234.2175 Option #2 or visit our web site at www.PerimeterUSA.com.