Computer Crime in 2002, an Insider's Opinion

By Robert Lyttle A.K.A. Pimpshiz – www.sub-seven.com | robert@sub-seven.com
Thanks: RevDisk, Matthew Fox, Tarrant

January 25, 2002

In the near future, securing your computer will be as routine as locking your front doors. We all strive to keep ourselves from becoming a victim of circumstance; however the threat of digital malice seems only to grow. Reports show that even when new security measures are deployed, computer crimes do not decrease; often times they increase. This only goes to prove that hacking is expanding as our society moves in the wrong direction.

Digital Epidemic

Less than a month old, the year 2002 is already susceptible to many new attacks. On New Years day an International non-profit security team released an advisory warning of a large vulnerability in AOL Time Warner's Instant Messenger software. The hole left millions of users open to further dangerous flaws. Fortunately AOL Time Warner quickly applied a server-side fix to prevent any widespread damages.

Another uprise in effect is the amount of webpage defacements recorded by www.alldas.de and www.safemode.org. The year 2001 catapulted to over 20,000 defacements from a mere 5,000 reported in the year 2000. Figures shown should not be taken lightly considering that there are thousands of other incidents that aren't being recorded. Regrettably, in 2002 we will continue to see these numbers boost.

Virus programmers aren't coming into the New Year sitting down either. In recent weeks a new breed of virus has been released. The new method infects users through Macromedia Flash. Luckily the "proof of concept" virus can only contaminate users who have the Macromedia Flash Standalone player installed.

With multiple momentous factors already introduced in 2002, the increase of individuals who delve into the inner workings of computers will more than likely discover original weaknesses. And by this showing that hackers are only getting smarter. An unbridled curiosity in the unknown and unobtainable will always be the greatest advantage in the rapid growth of the structured hacker community.

As today's new computer hackers fall into the insatiable feeling of Black hat curiosity, yesterday's will have moved onto being inclined enough to launch massive attacks. Sometimes conversion will take place, either using the sought skill as a White hat hacker, or remaining on the more secretive side. What we are seeing on an unstoppable basis is the rising of a community that will one day be more powerful than the foes in this comic-like duel..."Once a hacker, always a hacker."

What makes the hacker community even more dangerous is the fact that tools to help simplify tasks such as scanning for holes in networks are being released regularly. Programmers constantly author utilities ranging from exploit scanners to Denial of Service tools. Today it doesn't take a genius to launch a worldwide attack, but only a few easily acquired resources. With this in mind, some hackers are beginning to realize that they are already equipped with the knowledge to accomplish larger and more destructive missions. All of this leading to nothing, but more insecurity, demolition, and derby towards a “secure digital space.”

Law?

These days it is extremely hard to live a legal life on the Internet, and because of this, people will become accustomed to illegal activities. Eventually they won’t know the difference between good and bad, which makes the Internet a scary place to think about. I personally have witnessed authority figures openly discuss their activities about mild computer crimes, as I'm sure others have as well. When the Internet was established, nobody thought of the enthralling effect it would have on individuals. The Internet was not raised with super-strict legal guidelines in mind which makes it what it is today, a widely illegal locale. There is no remedy for this, re-establishing the Internet is quite impossible. Only improvements and adjustments in the system can be applied to help its users live a legal digital life.

Infatuation

The majority of people love to see the hacker community in an entire stereotypical way. This only leads to underestimation from the public and anger from individual hackers. In some cases, one would think the exact opposite of the truth, obviously a very dire mistake. Underestimation is the largest vulnerability that a person can have. Anger is the last mood you want to put a hacker into. Most disgustingly, hackers are widely looked at as terrorists. And one thing that hackers hate the most is ignorance. So add those together with the most common physical stereotype: spectacle wearing, underweight teenage male, with no life. There is bound to be a lot of mad people. Fear of the misunderstood leads to a stereotype. Stereotype leads to rage, rage leads to damage, and damage leads to consequence. The never ending cycle continues to revolve.

Although hackers are looked at as terrorists now, and as a result face much stricter laws, there will not be a change in the community. There are some terrorist hackers out there, but nobody wants to give up the lust for endless knowledge. They are aware that knowing everything is impossible, which is what makes things all the better. Sacrifices must be made along the path to knowledge. Some of the sacrificing means to hack into your own countries government systems before a malicious foreign enemy does. Would you rather have a US hacker or a foreign hacker defeat our government’s security measures? Would you rather witness the humiliation and severe damage caused by the enemy or witness US hackers help point out the holes among the critical components of our country? Because when it comes down to the bottom line, these are the two main factors.

If it weren't for hackers there would be no sense of insecurity, and therefore no drive to create stronger security. In fact, there wouldn't be a lot of things. Hackers are the pioneers of everything around us. They have helped our lives evolve into something that was once driven by dreams. This is why you will never see a hacker fall, no matter how many hits he or she takes.

Whether the government realizes it or not they have hackers working for them. Hackers aren’t just people who infiltrate transparent security lines, among a lot of other things, they are inventors. You believe, you invent, and you live. They invent ways to stay ahead, they invent ways to look ahead, and they invent ways to feel ahead. They will always be ahead of the public, which is why the government has them. Ironically enough, the government wastes a notable amount of time making hackers look bad. So are they saying that their own employees are terrorists who should be feared? In reality, that’s how it is. Not many recognize it this way, but that’s how it’s imposed on us. The eyes of a hacker dilate to the real things in this world. The human eye does not have to be naked.

What about, “Two wrongs don’t make a right”? – True, however in many events, this has been proven opposite. Socrates was put on trial. Hackers have been put on trial. Socrates strongly believed in his studies as do hackers. Socrates broke society’s laws at the time, as some hackers are breaking today’s laws. It may seem wrong now, but years ahead hackers could be widely read about in a positive way; just like Socrates is read about to this day. The many philosophers who broke laws to do what they believed in, compare to the many hackers of today. So, maybe it does take two wrongs to make a right? It’s been proven and it is being proven as you read this text. Only time will fix our world’s unjust imperfections as it has before. You shouldn’t read this as a completely accurate analogy, but more as a valid point to help alleviate your evil thoughts of the everyday hacker.

Breaking laws could be the key to success that the public yearns for in this digital wild. You will not stop a person from contributing to this world. Socrates was imprisoned and killed, unafraid of the consequences following his actions. He is dead for breaking the law, yet his contributions in the evolution of human thought are still here.

Put two things together, fill in the blanks, and complete the puzzle that we’ve been living in for so many years; to realize the flaws that are present.

Nonchalant

Comfortably being illegal is no big deal these days. This only makes the speedy growth of all other computer related crimes even less complicated. Bringing down websites to their knees, easily stealing identities, and snooping for secret documents are all a part of the entire hacker community. Who you hear about in the news is the community that is in full control over the Internet. Most of the hackers you hear about are these types of hackers. The ones who are considered semi-smart, but in reality do not possess any true knowledge or morals. This is not necessarily true for every malicious hacker out there, but a large fraction falls under these terms.

Stealing credit cards and launching Denial of Service attacks do not require a large amount of skill. There are people who live for these types of things which make the threat of falling into the digital line of fire even greater. Even some of these people make a financial living by committing Identity Theft on a daily basis. Making a profit, earning a buck from everything illegal done, is their specialty. Is it hard? No. Are we all possible victims? Yes. It shouldn’t be overwhelmingly scary to think about, considering that it takes half a brain to prevent you from suffering any of the possible consequences. What you should be worrying about are the companies that store your vital information.

Oh, so your PC has been remotely hijacked by a hacker right…scared? You shouldn’t be. As stated earlier, it takes half a brain to prevent being infected by a Trojan Horse. It is extremely easy to rid yourself of and avoid such threats. For the past 5 years I've used the same anti-virus scanner. It’s called my brain. It only takes common sense to make sure that you aren't about to step into a self initiated catastrophic situation. The risk is high because of the large amount of people that do nothing except look for users who are open to such mindless attacks. Don’t watch your important documents get wiped before your eyes; instead use your mind's judgments.

Widely known as tools for remote administration, Trojan Horses aren't solely used for controlling a victims PC for fun. They are used to help climb up a ladder. For instance, a common use for Trojan Horses would be to assist in accomplishing a certain task or to obtain information that will ultimately help achieve the initial goal. Better utilities like these will steadily be developed to help ease difficult processes. Plan to see more of these in the future.

I am not going to say that virus authors are the members in the hacker community who should be feared the most, but it is definitely not a good idea to overlook them. Chain reaction type destruction and the learning boost is what get their blood running. The binary code practically running through their veins is what gives them the fuel to continue. The initial process may seem extremely tedious to some, but to the individual, it is a superior learning experience. Even if the formation isn’t released into the wild to cause harm, authors love to see what they have finally created from an acute thought.

Hackers aren't just picking up computer skills; they are acquiring psychological and counterintelligence type knowledge. Expect to see these types of people being born at an increasing rate.

Don't hope for them to disappear, but to continue to help strengthen the quality of our lives.

Solution

Rather than seeing all hackers in a one sided manner, identify the real threatening ones and operate from there. I am not going to get into the philosophies of Black, Gray and White hat hackers. White hat hackers aren't the only good ones out there. There are plenty of Black and Grey hat hackers who help in their own special ways. I guess this could be seen as a form of bigotry. Just because an Asian killed an American, we are going to wipe out their entire continent? It gets you thinking of the current views about hackers, doesn't it?

Currently there are only about 200 agents that are dedicated to the investigation of computer crimes. Sure there are probably more agents that work on computer crimes, but nowhere near the amount of hackers. You won't have a fair game without an equal amount of players. A few hundred special agents against hundreds of thousands of knowledge hungry hackers? It looks like there is quite a difference in pieces on the virtual chess board.

An average special agent compares nowhere close to a hacker. There is no competition, simply a pawn against a queen. Do these agents spend countless amounts of hours learning the unthinkable? Don't count on it. New organization needs to be established. Sadly, the hackers in the government field who have the correct mindset aren't the ones that are leading agencies like the NIPC, when they should be.

Conventional interrogation and investigation tactics may work on regular criminals, but not hackers. During my own interrogation the investigators began with flattering statements, trying to make me spew the details that they were looking for. I came into the room knowing what they were going to say to me. What would seem like a regular conversation to them is actually a technique used by many of us. Later they began underestimation, creating vulnerabilities in themselves. Therefore allowing me to have the upper hand at all times. Not necessarily possessing the upper hand in my court battle, but more in the areas that are of significance to me. In any normal person's eyes, it would seem that I was the one being beaten down, the one being hassled with court fees and other miscellaneous complications, but in reality it is quite the opposite. Diversion, question, and assumption. This is what wins the chess game. To take a hacker out you must beat him/her at their own strategic game. Steps towards imitating their thought process, understanding their lifestyle and matching their skills, is the key. Taking a hacker out means minimizing the threat of insecurity, while minimizing the threat of insecurity means eventually creating a safer place. New tactics and strategies need to be developed against certain situations as these.

They say that their government trained employees work pro-actively against cyber attacks. However, not too many credible situations have been shown to the public. Intensifying this area would be a smart step forward, but of course a delicate step to deal with.

So the question is this: Is it possible to undermine hackers? Yes, but it will never be an easy task. Hackers will stay one step ahead and manifest their thoughts into reality, constantly introducing new obstacles to the Internet. With its current path, there will never be a point in time when illegal activities in the fast paced lanes of the digital highway will cease. Intelligence now needs to be focused on the prevention and minimization of such activities. The majority of people trying to deter attacks against critical infrastructures are unfortunately taking the wrong approach. Rather than minimizing the existence of vulnerability, they are trying to nullify their fears. Until this is realized by the top officials who fall into the Internet, websites will continue to be hacked, sensitive information will continue to be stolen, and other related incidents will continue to escalate.

Only a hacker can defeat a hacker.