IPkey
2010
Information Security
Outlook

Prepared by

IPkey.com

Confidential

(Internal Use Only)

Introduction

The IPkey Information Security Outlook is compiled to assist clients in gaining a clear perspective on current information security trends. It is not intended to be definitive or exhaustive, but rather an attempt to extract and position those precursors that we believe signal significant changes in the coming year.

The Outlook also includes recommendations. These are based on criteria that includes industry research, interviews, feedback from clients and our many years of experience in the field. A recommendation identifies a particular risk management challenge, and then offers a durable strategy to address it in a cost effective manner. A given recommendation may not be appropriate for every client, and obtaining professional guidance is always a good policy.

One area of Information Security this report does not cover is compliance with laws and regulations. This subject is already very well covered and quite predictable in nature.

The sole ambition of this report is to clearly provide information that is useful in a way that makes sense to you. As many commercial organizations face unprecedented economic challenges, we understand that Information Security is probably not what wakes you in the middle of the night. Yes, other more immediate concerns such as cash flow dominate your radar screen. However, we should not forget that a single security incident can put you out of business within minutes. Productivity can halt, customer and HR data can be breached and account balances disappear; all before you realize what hit you. And yes, it really does happen that quickly.

Like any business owner, I have to take calculated risks to grow the business; we all play the odds to some extent. However, what I am certain of is that in the next 12 months, the chances of avoiding an adverse security incident by playing the odds of 2009 will be near zero. It’s simply not the same game anymore.

Marcus Clarke

President

Executive Summary

This year, we are facing unprecedented growth in both the scope and sophistication of cybercrime. The scale of this global enterprise (close to $100B) impacts all of us. It has grown so fast because the recent economic climate has created a 'perfect storm' of stimulus for cybercrime. First, much of the developing world saw a drastic reduction of legitimate employment for those with computer skills. This has encouraged career paths toward illicit activities. Next, there is widespread global resentment against the US for causing economic woes, which has fueled the legitimacy of cybercrime as an acceptable, even patriotic endeavor. Finally, cybercriminal organizations have exploited this climate to expansively fund the development of new generations of malware. These, and other factors have spurred a new generation of talented, professional criminals to unleash a new class of malicious software (malware) that can evolve faster than the technology available today to stop it. Although it rarely makes the front pages, there is alarm among law enforcement and information security professionals that so little seems capable of slowing this ominous growth.

The impact of this development on US organizations is just now starting to be felt. The goal of these criminals is to infect as many computers as possible with malware, allowing them to be remotely controlled for various illicit purposes. The infected computers, called 'bots' are corralled into groups of thousands, called 'botnets,' which are then used as a launch platform for criminal activities. To grow these 'botnets,' cybercriminals have developed extremely stealthy exploits that evade detection by most traditional security measures. Commercial organizations particularly targeted because budget cuts in IT have caused layoffs and postponement of security upgrades. Perversely, these cuts come at a time when the traditional methods of protection against malware are increasingly ineffective. Additional investment, not reduction, is urgently needed. We recommend that every organization re-examine their fundamental information security assumptions, preferably with professional guidance, as soon as possible. Although each client is different, we have two general recommendations for organizations to defend against this new threat landscape.

First, the best strategy to sniff out this stealthy new, unknown malware is to carefully monitor, and intelligently correlate, abnormal behavior in computers, networks and security gateways. Traditional detection systems are based on the unique 'fingerprints' of malware, called signatures, that match previously discovered threats. When these systems fail to detect new threats, behavioral systems will have to be ready to augment or replace the older systems, which we predict will become becoming marginalized by the end of 2010. While its easy to spot something you've seen before, detection and identification of brand new threats is much more complex, so more sophisticated technology and expertise is required. While this next generation of security technology is now commercially available, the expertise is very constrained and consequently expensive. For this reason, deployment and management of behavioral detection technology is a likely candidate for outsourcing except in the very largest organizations.

Second, the distinction between business and non-business use of the Internet is blurring, making it much more challenging to control the content entering organizational networks. We see no effective long-term solution, so we recommend that clients plan now to isolate user PCs from production systems containing protected data. With careful design and the right technology, this approach can pay dividends in mitigating risk, easing regulatory compliance, facilitatiing remote access and business continuity planning. In fact, we project savings sufficient to more than pay for the cost of next generation security technology.

In summary, our recommendations for clients in 2010 are to recognize that today's economic reality has tipped the scales in favor of the cybercriminals. This requires strengthening defenses and planning the transition to a sustainable security architecture that limits the proximity of users' PCs and protected data. This twofold strategy will minimize exposure to new and unknown risks, and maximize productivity for those who make information security a priority in 2010.

Outlook: Cybercrime & Botnets

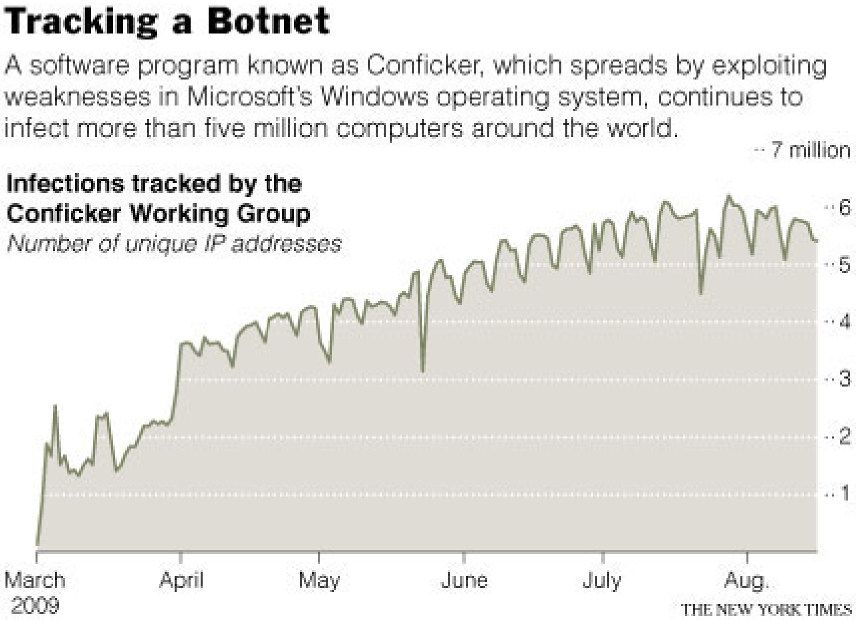
This section of the annual IPKey Outlook identifies key trends in information security going into 2010. This year, our forecast consists of the merging of several patterns. Our dependence on the Internet, the rapid evolution of cybercrime, the purpose and sophistication of malware and the failure of traditional defences. A good place to start is back in late March of 2009.

In the days leading up to April Fools Day, you probably couldn't avoid the buzz about the Conficker Worm. Described in sensational terms by the mainstream media as a 'time bomb' , the studio 'experts' predicted it would cause havok on April 1st. The public was dutifully whipped up into a minor panic by the hair-trigger media, completely ignoring those security experts who were trying to tell a very different story.

When nothing bad actually happened on April 1, the same media who created the frenzy now blamed the very same security experts for crying wolf, even though they had downplayed the impact all along. It was bad day for information security, and yet another blow to any public understanding of a much more serious problem which to this day receives almost no media attention.

This serious problem is that the global computer security community has been quietly, but inexorably losing ground in a critical war. Simply put, the threat of malicious computer code (malware) has been evolving faster than the technology available to stop it. For better or for worse, the global economy has now become so totally dependent on the Internet, that the ability of cybercriminals to critically damage our economic infrastructure is rivalled only by the imaginary villains in a Bond novel. Unfortunately, this is not a movie script; it is today's reality.

Back to Conficker. What security professionals did know back in March was that while April 1 was indeed a date coded into Confiker, it was simply the next date to check in to its Command & Control (CnC) servers which provide new instructions. Such check-in dates had occurred previously and there was no evidence that an attack was imminent. So April Fools Day wasn't anything special, and the treatment by the media was dismaying but not suprising. But IS professionals weren't taking it lightly; Conficker was by far the most sophisticated malware package ever seen. While it had been around since late 2008, it took almost months for a team of researchers to intricately unravel the amazing contents of this tiny, jewel-like package of code. Confiker's ability to evade detection and spread across networks was unprecedented. Far from being a bust, by August 2009 Conficker had succeeded in infected 6 million PCs creating a huge 'botnet'. (see diagram)



As impressive as the technology appeared, what really puzzled the experts was the motive. Whoever created Conficker was capable of having their way with virtually every unprotected Windows computer on the planet. These people could have brought the Internet to its knees, but didn't. Why hadn't they done anything? What were they up to? Between IS professionals, our worst fear was that Conficker was doing something, but we just couldn't detect it.

Many of us now believe that Confiker started out as a technological proof-of-concept, perhaps to demonstrate expertise to potential cybercriminal clients. While it seems to be doing nothing other than occasionally checking in with its creators, there's absolutely nothing to prevent Confiker and its descendants from waking up at any moment and unleashing whatever it's creators choose. A cybercriminal can cause a great deal of damage with a botnet of 6 million computers. That's what's frightening to all of us who understand its capabilities. We don't know who created Confiker and we don't know what their motives are. What is clear is that they are very, very talented programmers and they are apparently very patient. What will they do next? For a more in-depth look, read the New York Times article "Cyberwar: Defying Experts, Rogue Computer Code Still Lurks[1]" published 9/27/09. It's described Conficker and provides a rare, honest glimpse at the true state of Internet vulnerability.

The 6 million PCs controlled by Conficker are just the tip of the iceberg. There are now enough computers around the planet controlled by cybercriminals to leave no doubt that they have the capability to paralyse the global economy. Just ask any Estonian about what happened with Russia in 2007[2]. This is the computer security war that we are losing. It a war that changes the rules on a time scale that few of us can imagine.

Contrast this to the world just a few years ago. In these 'good old days' of the early 2000's, computer viruses might try to delete files or crash your PC. While their actual efficacy was questionable, the common thread was that the authors of these viruses appeared to crave notoriety. Often, strange messages would appear on screens claiming credit in a way that refelected the sophomoric humor of the mostly teenage authors. Most of these viruses were so poorly written that some of us wondered whether any damage was by design, or simply a result of bad programming. Nevertheless, they called themselves 'hackers' and became part of Internet folklore.

As the level of sophistication increased, worms joined viruses and the threat became more real and actual damage resulted. Still the goal was largely for bragging rights, and in 2004 we witnessed a 'war' between rival hacking groups who competed to 'own' the most infected computers. This competition gave rise of something completely new, the 'botnet.' A new form of malware emerged to take over, or 'own' as many Windows computers as possible and recruit them into a large botnet. This brilliant strategy was an important milestone in cybercrime. An attack coming from a single source on the Internet can be easily blocked; an attack coming from 10,000 sources around the world is much, much harder to defend. A botnet is like a global hornet's nest that can be stirred into malice at the touch of the keyboard. The motives of these gangs was often political or social, and their power of their code was primarily disruptive.

Since then, the threat landscape has taken yet another quantum leap. Malware has evolved, and today's threat is a tool to achieve sophisticated, well financed criminal objectives. Here's an example how it works today:

You incorrectly typed a website name on your PC, which hasn't been updated in a few weeks. Unfortunately, the strange looking website had been hacked and your PC is now infected with botnet malware. But you don't have a clue. The malware silently takes control of your computer and starts its instructions to make it part of a botnet. First it 'explores' your network and tries to spread to any other computers. It then 'phones home' for new instructions and updates. Its likely your infected computer will later be ordered to send spam or phishing email in short bursts of 100 or so to avoid being blocked by email filters. Occasionally, your computer may be instructed to join in a DDoS attack. Mostly these activities occur in the dead of night when you are least likely to notice and when Internet connections are fastest. And when it's not busy doing anything else, it will record your credit card or bank account numbers for later transmission. Last and most importantly, if that malware is well written and executed, it will create a loophole in your security software so that you will never even suspect that your PC has been compromised. While botnets historically have used home PCs owned by complety unsuspecting, innocent families, the newer malware is targeting corporate PCs; no one is immune. Today's malware is truly the Swiss Army knife of malicious code.

We can track traffic from these bots to Command and Control (CnC) servers hidden away in former Soviet Republics, China or any other nation that fails to prosecute cybercrime. And because of the recent recession, the financial contribution that cybercrime makes to these local economies has become so large that it has become a 'quasi-official' export providing a valuable source of foreign currency. In some countries, these criminals have become patriots and folk heros; any attempt at prosecution would probably cause a local uprising.

This basic strategy has been executed so successfully that cybercrime is arguably the most profitable and least risky criminal activity in history. Cybercriminals are rarely tracked down, even more rarely prosecuted and almost never convicted. Unlike other criminal activities like running drugs or robbing banks, people don't shoot at you. For well educated criminals, it's a dream career. More often than not, the large western banks end up paying for the fraud which are passed along to the consumer as higher interest rates. Because of this and other cultural jealousies, many outside the US look at cybercriminals as Robin Hoods.

The truth is far from a Robin Hood story. Cybercrime has spawned a vast underground economy that is siphoning huge amounts of capital out of western banks. It is important to understand that this economy is not yet considered illegal in many countries; indeed it is even considered a new, emergent form of capitalism. An even stranger twist is that some of these powerful cybercriminal syndicates are closely allied with the 'black' security agencies of foreign governments and provide 'cover' for state sponsored cyberwarfare. This makes for some very strange bedfellows indeed.

The hard fact is that Cybercrime keeps growing and currently appears unstoppable. At IPkey, we actually use the term Cybercapitalism to reinforce the fact that in much of the world it's not even regarded as criminal. We have to remind ourselves that in the former Soviet Union and in much of Asia, it's just good business. By their own words, the very definition of capitalism is inherited from ours when it comes to the rest of the world; the US does not have a stellar history of ethical dealings with foreign nations, and neither do these 21st century capitalists. Whatever we may think, they see no ethical distinction between what they do today and what US corporations have done for decades.

As long as there are nations that do not fully cooperate with authorities, cybercapitalism will keep growing. As long as ordinary people fail to adequately protect their personal computers from being taken over and used in a 'botnet' to launch attacks, cybercapitalism will keep growing. As long as any version of Windows has flaws, cybercapitalism will keep growing. The math is that simple. If you doubt the motivation or the capability of organized crime to operate globally, I invite you to watch an excellent presentation on 'The Global Illicit Economy' by Nils Gilman[3].

Even if tomorrow, a new version of Windows was suddenly made secure, we still face the problem of hundreds of millions of computers around the world still running old, highly insecure Windows versions. Almost all of these computers run pirated copies of Windows, which means they cannot obtain security updates without downloading the much-despised Microsoft Genuine Advantage software. Almost no-one is willing to do this for a variety of reasons. While we understand Microsoft's concerns of pirated intellectual property, who are they really hurting by virtually inviting these computers to become botnet members? All of us who have paid Microsoft. We believe this decision by Microsoft to be one which all of us will be paying for one way or another, and one that they will ultimately regret.

Microsoft's shortsighted decision means that botnets will easily proliferate in the indefinite future, and their capacity for illicit activity will only escalate in capacity and maliciousness. Even if our clients use the latest Windows versions which are always updated, we will still have to deal with the hundreds of millions of compromized Windows PCs in China, Russia and the developing world with whom we intimately share the Internet. The challenge to all of us is that without a change in Microsoft's policy, almost all of these vulnerable PCs will end up in the control of cybercriminal organizations, and they will be coming after us in any way they can.

As a shareholder, executive or manager, there are practical steps that you can take to defend your business and employees from this challenging future. These steps will lower the attack profile of your organization so that it's less likely to be exploited, and use robust technology to prevent protected data leaking out of your firm onto the Internet. We caution against believing anyone who tells you that there's a silver bullet that will make this problem go away. There isn't one now and we don't see anything on the horizon. This is a complex and evolving challenge that can change daily; it requires a agile, multifaceted strategy to stay in business. We will provide actionable steps you can take in the recommendations that follow this forecast.

Question...

We end this section of the 2010 Outlook with three questions that we have recently been asking members of the Information Security community.

1. What would it look like, as if by some new technology, viruses, worms, botnets and cybercriminals were to be defeated and disappear?
2. What would it look like, as some might fear, cybercriminals perfected malware and we became incapable of defending ourselves?
3. How would these two situations differ in appearance?

I would welcome your answers and thoughts at mclarke@meridian-grp.com

Recommendation: Complex threats require behavioral detection

In our Outlook, we described in detail how new malware, similar to Conficker, is designed to evade traditional anti-virus and anti-malware software that's based on matching unique fingerprints, called signatures. Our first recommendation is that clients start now to critically reassess their information security defenses. If this is delayed, we believe that 2010 may bring some very unpleasant and costly suprises.

The reassessment process requires giving up thinking that we can depend solely on the positive threat identification provided by signature based systems. This means that we also need to give up the luxury of automatic blocking of viruses and worms that have enjoyed for so many years. To automatically block traffic, you need to have a very, very high confidence level that what you are blocking is indeed malware and not legitimate traffic. Otherwise productivity nosedives and users start complaining to management that they can't get their work done. Only signature based systems can currently provide this very high level of confidence. In 2010 and beyond, while many legacy threats will still be detectable by signature and can be automatically blocked, these will constitute a decreasing minority. It is for this reason that we have to think less about detection & blocking and more about behavior and containment.

When the black and white, signature based prevention systems can't reliably detect threats, we enter the gray zone of what is known as Behavioral Anomaly Detection (BAD). While signature based systems positively identify malware, behavioral systems look for the anomalies that malware typically might cause. For example, if a PC gets infected by new malware and nothing is detected by the signature based anti-virus system, how would we know something is wrong? We might see a sharp increase in the number of connections to the Internet, the use of a unusual port for the first time, or a new process started on a PC. While none of these occurences individually constitute a smoking gun, the combination of them in short order can be a very strong indicator of something bad going on with that PC. However someone, or something, has to be watching for these indicators 24x7 to correlate the symptoms and validate the problem. There's far too much data for humans alone to do this, so a combination of specialized software and skilled analysts are needed. Behavioral Anomaly Detection can never provide the 100% certainty of a signature match, but it can quickly alert you to something bad which nothing else even notices and quarantine the suspect PC.

To illustrate the distinction between detection/blocking and behavior/containment, lets take a look at an example of each in detail.

Detection & Blocking

The traditional emphasis is inspecting traffic from the Internet to the PC. If a signature based system can inspect, detect and block a virus before it reaches the PC, this is an easy win. The PC doesn't need to be cleaned up, the virus wouldn't spread to other PCs and cause a massive infection that would cripple productivity. This older style of malicious code wasn't acquisitive, just destructive. No-one was too concerned about the traffic from the PC to the Internet because the network was usually so messed up that little or no traffic flowed anywhere. Our worst fears about a crippling loss of productivity rather than a data breach.

Behavior & Containment

Today the emphasis is on inspecting traffic from the PC to the Internet. Signature systems at the gateway may not be able to detect all malware coming from the Internet to the PC, but Data Leak Prevention and other specialized sensors examine outbound traffic very carefully to make sure that no protected company data gets out. We may not be able to reliably recognize the latest malware

> coming in, but we certainly can detect our own protected data trying to go out. But until that happens, we're in the dark. To continue our example, the PC has become infected, but we don't know yet because no AV or IPS signature has been matched and the computer is running just fine. The PC is now probably ready to join a botnet and it sends a message back to it's Command & Control servers probably located somewhere in Russia or China.
>
> Meanwhile, our perimeter security system is using egress port filtering, and very carefully inspecting all outbound traffic. It's blocking non-essential ports such as ICQ, which botnets have often used in the past for CnC communication. However, the malware on our PC is very well designed and uses HTTP or HTTPS to communicate back to its masters because those ports are almost always open. This time, when the CnC traffic is inspected on the way out to the Internet, it trips a behavioral detection sensor and generates a red flag. Within minutes, that is correlated with another indicator from an agent on our infected PC showing that a new, unknown process recently started running. The security team is immediately alerted and our PC is then quarantined. The affected user is notified that their PC has been quarantined and any work should be saved to a special quarantine server. To make it more challenging, let's assume that we didn't recognize the CnC traffic because it's using a new, unknown technique. So the PC succeeds in joining a botnet, but still nothing is detected. However, at 1:37am it attempts to open 300 SMTP connections to mail servers around the world to send spam. This activity is a dead giveaway to the detection systems and the PC is immediately quarantined. Either way, the PC is stopped from sending out any protected data or performing any illicit activities that could cause liability issues. In 2010, that's going to be considered an easy win.

The key to designing the Behavioral Anomaly Detection strategy is to understand the intent of the malware, and what it may do that reveals it's presence. First, we throw out all our past assumptions. For starters, malware may not even be the correct term anymore. In the past, the title was earned because the intent was indeed malicious and destructive. The only purpose was to disrupt and propagate. This new malware has a far different agenda. Now the purpose is to employ the host PC for its own purposes for as long and effectively as possible. This means that it will go to great lengths to remain undetected; a complete reversal of past behavior. Work loads are usually run in short bursts to avoid detection, and late at night or when the PC is idle so that it doesn't give itself away. Amazingly, the malware in many cases actually cleans the PC of any other malware infections and even gives it a 'tune-up.' Botnet malware wants to have its host in good working order so that it can put it to work when needed. In short, well designed botnet malware should act like an invisible houseguest who lives in your house when you are not home and leaves no traces. Unfortunately, this well-behaved houseguest is also stealing your bank account numbers, using your address and ultimately even stealing your identity.

As we have already seen, to trap this unwelcome but clever visitor, we have to gather and correlate several 'clues' that our computer is not behaving normally. While each clue is useful in itself, these clues grow tremendously in effectiveness when they are combined. Seen together, these techniques can detect the previously undetectable threat by seeing it's 'trail.' The devil, of course, is in the details. While it's simple to say 'when combined,' it's actually a complex challenge to correlate the results of these individual sensors. It's even more difficult when the data from these different security tools come from different vendors.

Data correlation is a notoriously tricky art because a security engineer has to program the systems with his or her expertise that can tell the system that particular combinations of activity are indicative of an exploit. Furthermore, correlation programming requires frequent 'fine tuning' to minimize alerts, or false-positives, while maintaining sensitivity to suspicious activity. We see a market developing in the future for 'plug-ins' that imbue behavioral anomaly detections systems with expert intelligence for newer and more sophisticated threats.

In such a brave new world, clients face a significant uptick in the complexity, expertise and cost required to deploy and maintain defensive systems to protect assets, limit liability and maintain compliance. For many, this comes at a time when IT costs are being severely squeezed. For reasons of both economy and scarcity of needed expertise, we see the core management of these systems being contracted to outside specialists. Some larger vendors, such as Cisco and Symantec will no doubt offer proprietary systems that promise correlation capabilities, but only with their own security offerings. These may or may not work well, but we are cautious that these systems will be used to lock customers into a proprietary framework that may not ultimately be in their own best interests.

For this reason, we recommend a more vendor agnostic approach that allows for data gathering from disparate systems. Otherwise we see vendors perpetually promising security nirvana if customers buy just one more product, rather than using what the cutomer has today, and making it work today. Our experience is that most security vendors are still product focused, and rarely look beyond the current quarter's sales. We recommend our clients utilize Managed Security Service Providers who can provide the monitoring infrastructure and deploy Behavior & Containment based defenses. MSSPs inherently have a longer term mindset which is likely to be more successful for clients, and at a lower cost.

Recommendation: Isolate Protected Resources in a Private Cloud

For nine years our firm has been studying information security trends. During that time we have seen some dramatic improvements, but we also have seen areas that just seem to be making no progress at all. One of these areas is PC security. Given malware developments in the last year, we have now thrown in the towel. We now feel that any device in the physical or logical possession of a user is insecure, and cannot in fact be secured. This applies to any company owned PCs and notebooks, home PCs, PDAs and others. It's time for us to acknowlege that users' computers cannot be sufficiently secured to reliably meet typical risk management and compliance goals.

We have come to this conclusion partly because the new breed of polymorphic, blended threats all too easily subverts the traditional protections installed on a PC. It is also partly because the distinction between business and non-business use of the Internet is blurring, thereby making it far more challenging to control the content coming into organizational networks. Traditionally personal sites such as YouTube, Facebook and other are entering the business mainstream for legitimate business purposes, such as marketing and training. Many organizations have given up restricting access to personal email sites such as Yahoo, Gmail and MSN. This is particularly troublesome because personal mailboxes commonly contain a variety of toxic spam, phishing and other malicious content. The problem is that all communication between the user's PC and these sites is encrypted and typically passes right through almost every perimeter security gateway on the market. This means that users can unintentionally download what they believe to be a friend's photo, and instead download malware to the internal network. Defense is therefore left to the often inadequate End Point Control (EPC) protection on the user PC. All other defenses are bypassed, and one just hopes the EPC software is up to date and functioning correctly. This is not to take anything away from Symantec, McAfee and the like, but every security information professional knows that a single line of defense is far from sufficient.

In the short term, this threat can be mitigated by using one of the new perimeter security gateways that can inspect encrypted traffic and block threats using this method. One provider of these that we recommend is Fortinet whose products we have tested and found to be effective. When this is combined with well managed, effective EPC software, this combination can deliver a cost-benefit that's hard to beat.

The only viable, cost-effective and long-term resolution of this situation is to completely isolate user PCs from production systems containing sensitive data or mission critical applications. Any user computer that has Internet access, or is in any way exposed to other computers that have Internet access, should be considered suspect and contained on a separate network in a DMZ-type zone.

We recommend this approach for our clients. With careful design, clients can very effectively mitigate risk and achieve regulatory compliance with room to spare. The first step in this design is to install a properly configured security gateway to act as a 'traffic cop' between the user network and the protected network. With the right equipment, this can be very effective, but vulnerabilities can still propagate via Windows traffic beween PC and server. This first step can buy you the valuable time you need to prepare for the second, bigger step.

The second step of our recommendation is to use Virtual Desktop Infrastructure (VDI) technology, recently named 'Private Cloud,' as the best way to truly achieve the isolation needed for the long term. With this, the only connection between the two networks is through the security gateway (Step 1) that now passes only KVM (keyboard, video & mouse) traffic.

While the VDI approach is a major change, it has a very valuable side benefit; it vastly facilitates a central remote access strategy. The low bandwidth requirements of KVM traffic and the isolation of protected resources is a fortuitous combination. It means that authenticated access to protected applications is possible from almost any device, using almost any connection (a process called 'consumerization'). Secure access from thin clients at the workplace, PCs or Macs at home via DSL, iPhones via 3G cell networks and even satellite phone modems now becomes realistic. Given that almost all organizations are trying to enable remote access for a variety of productivity reasons, the VDI approach can deliver many valuable benefits at very little additional cost. For certain financial institutions, this will also help satisfy requiring for pandemic contincency planning.

While Private Clouds offer many benefits, they do little to alter the fundamental vulnerabilities of the user PC. Protected data is far safer, but an infected PC ultimately requires expensive IT support to clean the PC or re-image the disk. One way to eliminate this support burden is to use 'Thin-Client' PCs that run an 'embedded' version of Windows which does not allow any data or programs to be saved. A user can surf the web, check personal email and print; but when they log out, any changes are wiped out. The next user to login starts with a 'clean slate' with no remnants of the previous use carrying over. Malware may infect the PC and be loaded in RAM, but is wiped out when the user logs off. We feel that a Thin Client solution with embedded Windows is the perfect adjunct to VDI-based Private Clouds.

This approach does effectively prevent any contamination of the protected networks, and even PCs if embedded Windows is used, but one vulnerability remains. This is malware that uses keyboard logging to capture user credentials from the user's PC. Fortunately, there are several viable methods to combat this threat, such as the use of tokens and biometric devices, but it's important that this last piece of the security puzzle not be overlooked.

Finally, there's one more benefit of a Private Cloud. The process of isolating,or abstracting, protected resources also offers an valuable opportunity to move much of the critical contents of your data center to a local, managed co-location facility. This can offer a plethora of benefits and potential cost reductions. Benefits include a far more robust facility for your critical infrastructure, typically offering substantial UPS capacity and backup generator power, mutiple high-speed, redundant internet uplinks and 24x7 hands-on engineering staff. The savings in cost include the reduction or elimination the expense of maintaining and operating your own facility. This includes electricity, HVAC costs and specialized fire control systems.

We anticipate that clients who follow the Private Cloud strategy will spend less on problem resolution, compliance and audit efforts, and costly technology band-aids by getting it right to begin with. Security will be much more manageable and certainly with less stress. If this is supplemented with a co-location strategy to move the data center offsite, the benefits and cost savings can be substantial. Some of these savings can then be invested in upgrading the security infrastructure as recommended previously. While almost nothing in IT is free, our recommendations when implemented coherently can provide many benefits: security, productivity, compliance, remote access, environmental and organizational. All within a typical payback period of 18-24 months.

Appendix: What happens when a PC gets infected?

No computer is perfect; any computers has vulnerabilities that can be exploited. Windows PCs are especially targeted because they are so popular. Here's how it starts:

Researchers and hackers discover a new flaw, or vulnerability, and sometime after it becomes known to the software vendor, typically Microsoft. Windows programmers then work rapidly to correct the flaw from being exploited, and then publish a 'patch' or 'hotfix' that then provides protection against the real or hypothetical threat. During the time between the vulnerability becoming known and the patch being installed, the affected computer is extremely vulnerable. If the researchers who discovered the vulnerability didn't publicize the flaw, there's a good chance that Microsoft will develop and release a patch before the hackers know about it. However, there is a great deal of ethical debate as to whether any flaw should be immediately publicized, and so today it often is. This gives hackers a great opportunity to exploit the vulnerability before Microsoft issues a patch. This is called a 'zero-day' expoit. Ultimately, the importance of the zero-day exploit pales in comparison to the simple fact that millions of PCs don't get updated with the patch for weeks, months or even years. Around the world, there's no shortage of PCs ripe for compromise.

Most of the time, this kind of malware is introduced into the computer by tricking you or your employees, by using what professionals call 'social engineering.' This is invariably done by an email tempting you to click on a link to what appears to be a legitimate web site. The methods by which you suspend your better judgement and impulsively click vary, but they are the usual culprits: greed, lust, fear and sometimes even humor.

After you click on the link to a compromised web site, the malware enters your computer undetected and you are infected. If there wasn't a gateway security device to scan your traffic, then it's up to the security software on your computer to catch it. But maybe the software hasn't been updated in a while so it doesn't recognised this new malware. If that's the case, the game is already over. The threat is inside your network and as yet undetected. Within minutes, it has infected every windows PC and server on your network. Perhaps security software on a server creates an alert. If that's the case, you are lucky because now, finally, you know there's a problem.

If the malware is really good, it will evade all signature-based security detection by rapidly mutating into unique, one-of-a-kind variants. At this point, your organization has been gravely compromised and you have no clue. If the criminals who did this just want to collect credit card info, they may continue successfully for a long time if their malware remains undetected. However, if they want you out of business, it's easy enough for you to be setup by releasing confidental information on clients or employees. Once compromised, the cybercriminals can control your destiny; in their own words, they own you.

It may seem astonishing that just one employee clicking on a link for an irresistible offer in a spam email can bring an organization to it's knees. Unfortunately, it's the truth. Some might argue that it's unlikely in a well protected network that been subjected to the rigors of a compliance audit. But in a zero-day attack, malware can exploit a new vulnerability before a patch or AntiVirus signature becomes available; there is likely to be no defense at all. Why? Because the vast majority of our defenses are solely based on the highly questionable premise that threats can be detected and prevented by looking for a unique 'fingerprint' in malware that provides positive identification.

This type of detection is performed by inspecting files and transmissions and looking for a match to any one of a vast library of unique fingerprints, called signatures, that researchers have painstakingly derived from samples of malware. The great advantage of signature based detection is that when you get a match, there is no doubt that it's the particular virus or worm. This high level of confidence means that you can block or otherwise prevent it immediately. This is the good news;, the bad news is that if there isn't a signature to match the malware, it's absolutely useless and you are wide open.

This 'loophole' is becoming more and more of a problem for two reasons. First, the authors of malware know that when a new vulnerability is discovered in common computer code such as Windows, there is a 'window' of a few days before signatures can be derived. If they can write a zero-day exploit quickly, they have a short time during which there will be virtually no defense against their exploit. And they don't need much time; researchers have estimated that the SQL Slammer worm spread around the planet in just 15 minutes.

While this is scary, there is a second and far more serious problem. More and more malware is 'polymorphic' which means that it can mutate into a thousand variants in just a matter of minutes. These variants each require new signatures, but there is no way that can happen in time. Until recently, these mutations had enough in common to still be detected, but some new worms have such varied methods of detecting evasion that the resemlance to real-world biological viruses gets too close for comfort.

If the SQL Slammer worm was akin to the flu, then the new malware such as Confiker is like AIDS, and another type called a rootkit is like a cancer. This is no longer just one piece of code that can be fingerprinted; it's an entire collection of related but diverse threats. While there is a flu vaccine; there is no vaccine for AIDS or cancer. How do we protect ourselves from infection by an unknown agent?

The simplistic answer is that you can't. Just as the human body doesn't exist in a bubble, our computer systems aren't locked in a safe. We are exposed to the outside world and this means that we will get infected. What's important in this amazing biological process is that the immune system knows almost immediately when something foreign has invaded the human body. As we know well, all kinds of biology enters the human body every day, but what the immune system looks for is something that is spreading, growing and reproducing using the bodies own resources. This activity is then recognized as atypical behavior. The immune system is a remarkably 'self-aware' system that knows what it is and what it isn't normal, like the 'behavioral anomaly detection' system mentioned previously.

Once detected, the 'foreign' code (bacteria or virus) will be targeted by the immune system which will then try and develop antibodies to fight the infection. If it can't stop it, it will try to contain it. What's interesting is that the immune system 'archives' these antibodies so that whenever that threat shows up again, our bodies have the tools to immediately fight it. What we call 'resistance' in biology is fact a signature based defense system derived from the past activity a behavioral anomaly detection system.

For computers to have the functional equivalent of an immune system, they will have to become self-aware and know when something bad is happening. This is what behavioral anomaly detection is all about. There are various heuristic techniques that compare a known 'good' state to the current condition to determine if there are deviations. The important concept is that the computer has to 'learn' which variations are benign and which are not. As you can imagine, this is a complex field but one that is vital to the future of computing as we know it today.

References

[1] Defying Experts, Rogue Computer Code Still Lurks © New York Times

[2] Digital Fears Emerge Adter Data Siege in Estonia © New York Times
Estonia Computers Blitzed, Possibly by the Russians © New York Times

[3] The Global Illicit Economy by Nils Gilman (Video)

Resources

Emerging Cyber Threats Report for 2009 by GTISC

IBM Internet Security Systems X-Force 2009 Mid-Year Trend and Risk Report

Day Before Zero - Damballa Research Blog

About IPkey.com

IPkey.com, a division of Meridian Group Inc., offers Information Security Management and Monitoring Services to risk-averse clients nationally. Based in Albuquerque, New Mexico USA, Meridian has provided IT related services to business, government and non-profit organizations for over 20 years. IPkey's research group compiles the annual Information Security Outlook to assist clients to better understand the threat landscape in the coming year. The Outlook is made generally available upon request after 90 days from the date of publication. You may contact the author of this document at mclarke@ipkey.com.