

07
OCTOBER

NEWS

ISSN 1377-0675
VOLUME 14 ISSUE 1

European Institute for
Computer Anti Virus
Research (eicar) e.V. Office
Hauptstrasse 4
D-85579 Neubiberg

EDITOR
Eddy Willems
press at eicar dot org

CONSULTING EDITOR:
Rainer Fahs

CONTRIBUTORS:
Paul Cowan, Bluecat Network
Henning Ogberg, SurfControl
Yuval Ben-Itzhak, Finjan
Ian Kilpatrick, Wick Hill Group

EDITORIAL ADDRESS:
Ter Borchstraat 17
B-1982 Elewijt (Zemst)
Belgium

- 1 From the Board –
Chairman’s Corner
- 2 Editorial: The Birth of a Wider Range
of Information Security issues
- 3 EICAR Virus Prevalence Table
August 2007
- 4 DNS Security And Cache Poisoning
- 5 Raising the level of protection ...
- 6 Securing corporate networks ...
- 7 Work is where you are...

FROM THE BOARD CHAIRMAN'S CORNER

(By Rainer Fahs (RFA))

The last EICAR News was published in October 2006 with a positive reflection on a successful EICAR conference 2006 in Hamburg and an outlook into a promising future with some thoughts about the EICAR Task forces.

I would have loved to take the same approach for this issue and report about another success story, but because of the recent developments, I am afraid I have to start with a short summary of an internal incident with huge impact on EICAR as an organisation and its reputation.

An internal case of fraud and embezzlement has virtually paralysed EICAR as an organisation which resulted unfortunately in the cancellation of the EICAR conference 2007.

EICAR has been in stormy weather over the years for all sorts of problems and issues but we always found a way ahead and never had we to cancel a conference. Even a short notice cancellation of the conference venue some years ago – surely a major challenge – but we managed to organise the conference at a different venue in very short time.

The EICAR conference is more than just an annual event at a nice location where people meet for a beer at the bar in the evening. It was always the place where the leading experts in anti virus and later in all areas of information security got together to exchange their views on the latest development and technology, trying to keep pace with the bad guys coming up with ever more sophisticated methods of attack.

The cancellation of the EICAR conference 2007 was therefore a deep cut into the core of EICAR and its members and supporters from all over the world. Beside of the financial damage to the organisation there was deep personal disappointment and dissolution for those directly involved.

However, the Board reacted with immediate actions

for recovering from the financial loss and managed – thanks to the diligent work of mainly Robert Niedermeier and Manuel Hüttl – to ensure business continuation with minimum administrative service and financial commitment. Emergency regulations were put in place and replacement for admin support was hired enabling business continuity for the core admin functions of the organisation.

Despite of all efforts, there was regrettably no way to organise a conference for the year 2007 with a budget of acceptable levels of risk and therefore the Board had no other options than to cancel the planned conference.

After initiating legal proceedings the Board concentrated on the recovery of the money and we had to learn about some extremely and time consuming administrative procedures. However, while I am writing these lines, we are in the final stage of a long process and there is a realistic chance that at the time you are reading this EICAR News, we would have our financial situation re-installed with full recovery of the losses.

We are fully aware of the negative impact and the disappointment and frustration caused by our decision to cancel the 2007 conference. The impact is wider than most outsiders would recognise. Some people had already made flight reservations and planned their trip and papers were submitted with the expectation to be presented at the conference and published in the proceedings. Being aware of the detrimental effects of the decision to cancel, we deeply regret any inconvenience for our members and for all who had submitted papers and planned to present them at the conference.

Thanks to Vlasti Broucek and Eric Filiol we found a way of publishing at least the scientific papers planned for the conference in Eric's "Journal in Computer virology".

Vlasti, as the scientific director of EICAR and the Conference Chair, has in the meantime stepped down

from his Board position and has also declared that he would not be able to commit the necessary time and efforts any longer for the work as the Conference Program Chair.

I would like to take the opportunity to thank Vlasti for his professional and diligent work with the conference organisation and the paper review process of the past years and his personal commitment. I personally thank him for his comments and inputs also for the work of the Board and his ideas for the conference organisation with a strong emphasis on the scientific character of the conference. He has surely contributed considerably to the image of the EICAR conference. We all owe him a great thank and wish him and Paula all the best for their future.

In the mean time we are steadily recovering from the financial damage because of incoming membership fees and some outstanding sponsoring commitments from last year's conference.

The damage impact however to EICAR as a worldwide recognised organisation is still much wider than the sheer financial aspects. Money can be paid back – reputation must be restored; and we have been working on that issue as well.

We had several meetings with Board members and experts who we know do have a positive attitude towards EICAR and its goals and objectives. It was rather unfortunate that Board members like Vlasti and James could not physically participate because of the long distances, but we tried to keep up communications as required.

Back in July we came together in Bavaria for a meeting over the weekend with roughly twenty participants who all contributed to a fruitful discussion on the future of EICAR.

The essence of these meetings is the following:

1.

We do believe that there are good reasons to continue with the work of EICAR.

2.

We also believe that continuation has to follow the

path of the last two years with the concentration on the core business of IT Security and the wider scope of all aspects of IT security centralised around aspects of malware.

3.

We further believe that the annual EICAR conference is essential for the continuation of EICAR.

4.

There was further consensus that the work of Task Forces and Working Groups in EICAR has to be based on strict Goals and Objectives agreed by the Board prior to the establishment of such groups. Concentrating on the way ahead, we are looking forward to the EICAR Members Meeting on 21st October in Munich and the first

EICAR Information Security Summit

22nd October in Munich at the Congress Centre Fairground Munich, being held in parallel to the "Systems", the leading business-to-business trade fair for IT, Media and Communication,

At the Members Meeting we will discuss the way ahead inclusive dates and venue for the next year's conference. I am happy to report that we have with Eric Filiol not only a volunteer taking over the conference organisation and paper review from Vlasti, but also has an interesting proposal for a conference venue in France.

Currently we are in the process to create an EICAR Forum on our Web-Page, which is meant to provide a place for secure information exchange between EICAR Experts worldwide on specific topics of interest. For more information .please check the EICAR web page (<http://www.eicar.org/>)

QUESTIONS & ANSWERS

Within this new column you can get answers from the specialists themselves. If you have some questions or some problems related to Anti-Virus or Security please send them to newsletter@eicar.org and we will try to give your questions to the most respected specialists in the Anti-Virus and Security world.

No questions received this time.

(By Eddy Willems, EICAR News Editor)

THE BIRTH OF A WIDER RANGE OF INFORMATION SECURITY ISSUES

By Eddy Willems, Director Press & Information EICAR – September 2007

During the first 9 months of 2007 we examined a wider range of information security issues concerning the INTERNET, new technologies, threats and vulnerabilities, the areas in which today's key challenges lie and where the problems are that security vendors may have to solve. However the questions are as well:

Are the threats really new?

Are the threats really smarter than before?

We saw a steady flow of reports on a great variety of data security threats during this period which is considerably different compared to the former years. The underlying trend to note is the spread of malicious activity across various technology platforms and applications during the first 9 months of 2007.

It appears that those carrying out security attacks are conquering more and more foothold to build themselves their own, stronger and sustainable commercial economy based on carefully crafted security attacks targeting consumers of INTERNET services, companies and public sector organisations.

So what happened really?

One typical case is the example of social engineering developed to a new level of sophistication via the „Zhelatin-Stormworm gang“—named after the trojan it installed on infected PCs. This gang was responsible for what started out as the „storm worm.“ First spotted earlier this year, the spread of the „storm worm“ started via e-mails purporting to provide information on some dangerous storms in Europe at the end of January. Users who fell for it were directed to a web site containing malicious code aimed at turning Windows PCs into spam bots. Over time, e-mails containing links to the „storm worm“ took on many forms, from supposed missile strikes to reports of genocide. Unlike the typical „comment spam“ that many of us know now, the worm is actually getting into people's

Blogspot accounts and creating new blog posts with links to the Trojan itself. Over 2 million computers were infected worldwide as part of this massive bot-net, with this number still increasing.

The banking industry continued to be a key target for phishing scams. As Trojans become more technically complex, scammers implemented new techniques in their attacks, including content filters that keep closer track of consumers' online banking activity. Such detection methods make it easier and more effective for fraudsters to collect more account details using a variety of methods. We even saw very advanced and dedicated Dutch phishing and spyware attacks for the ABN Amro bank and other large banks.

The link between cyber crime and real-life political unrest was tightened as a form of ‚Cyber War‘ which caused general unrest in Estonia. Disputes over the re-location of a Russian Red Army monument not only led to arrests over ground, but several governmental and other public sector and media websites were heavily targeted via Distributed Denial of Service (DDoS) attacks by an extremely active network of hackers. Several key sites were unreachable for extended periods.

Adding to the construction of a stronger malicious economy of sophisticated security breaches, the mobile malware industry became more active during the last months. ‚Personalised‘ SMS spam, financial lotteries, and Trojans masking themselves as utility programs are some of the examples of the fast-developing mobile scams. New spyware was also reported for some Windows Mobile and Symbian S60 3rd Edition devices.

It is fairly alarming to see increasingly complex mobile Trojans and spyware being developed by growing commercial entities, making solid profits to support further development of the malicious economy.

Spammers took the next step ahead by using images instead of text to defeat hash filtering and string

matching. Spammers also used malware infected computers (eg. StormWorm botnet) to launch spam e-mails to defeat network/sender reputation filtering. Excel, RTF, PDF, and RAR archived spam are just next generation anti anti-spam techniques spammers discovered they can use to avoid detection. This "catch-me-if-you-can" game is similar to the development of anti anti-virus techniques used by malware writers. When viruses were being detected heuristically, virus authors employed polymorphism to make anti-virus detection a lot harder.

So what is the next step for viruses and information threats? Despite the emergence of new operating systems (such as Windows Vista), new services (mobile content) and devices (the iPhone), cyber criminals continue to lack own initiative and are using tried and tested ways of attacking internet users instead. Furthermore, we are seeing a significant return to "the sources": computers are increasingly the targets of DDoS attacks and attacks that use browser vulnerabilities and legitimate functionality to penetrate the system. Probably the only thing that distinguishes the present from several years ago is the fact that email is not being used as the primary vehicle for spreading viruses. Instead, instant messaging services are one of today's key means of distribution. Another difference is that there has been an explosive increase in Trojans targeting the users of online games. The threats however are not becoming smarter. Innovation has stagnated as development is now focused on cosmetically changes and wider techniques have been used to achieve the same objectives. Security threats however are crossing technology borders towards a new malicious economy and that's another problem.

Antivirus and security vendors have considerably improved their technologies and introduced several new technologies. Presently, end points or pc's are protected much more effectively than several years ago. The average time that most new malicious programs survive in the wild has been cut down to a number of hours, and is rarely ever counted in days anymore. However this last point may not be the case for every attack as some attacks are still dedicated and could be exploiting just one new specifically created malware against your company.

The gain of data from your company is worth a lot of money if you see the prices on the dark sides of the web.

But let's predict what will happen next. Malicious users will attempt to reach beyond the security solutions – a task that is a shift from "getting around" antivirus programs or security devices and implies more action in fields that have not yet been mastered by normal security and anti-virus protection, or areas in which protection is not an option for any number of reasons. Based on our experiences from the first 9 month of the year, this is more than likely where the new front will be in the information war:

- *online games*
- *blogs*
- *instant messaging and*
- *file swapping networks.*

VIRUS PREVALENCE TABLE

TOP 10

(TOP 10 – August 2007 Version)

1. W32/Netsky
2. W32/Bagle
3. W32/ Mytob
4. W32/ MyWife
5. W32/Sober
6. W32/Stration
7. W32/ Mydoom
8. W32/Lovgate
9. W32/Bagz
10. W32/Zafi

– Virus Families –

(By Eddy Willems, EICAR WildList Reporter)

What members could do!

We ask you to send your statistics or incidents to us. Also, if you are looking at a new undetected specimen or if you have some problems with a document, spreadsheet or executable which could be infected, please send us this in a zipped file to the address vsample@wavci.com. We can provide you with a solution within a few days from receiving this sample in case of infection. The samples or reporting of the statistics or incidents will be used for input for our report to the WildList.

DNS SECURITY AND CACHE POISONING

By Paul Cowan, Technical Product Manager, BlueCat Networks

After functioning well for almost a quarter of a century at the heart of the Internet and other networks, DNS (Domain Name System) servers are arguably the most overlooked component in modern network security. DNS services represent the number one entry point for hackers; they also represent the most critical, basic link in a network. With a majority of the anti-virus focus placed squarely on email functions, in fact, a DNS failure of any kind can completely bring down a network – from firewalls to mail servers to everything in between.

DNS is after all, the system that allows the Internet to be navigated in real time. DNS servers match the names of network resources and websites with their numerical addresses. Given the power of DNS cache poisoning, many believe that it will ultimately become a major tool for on-line identity theft. This article explores the mechanics of DNS cache poisoning and examines the principles and best practices that can aid in prevention.

Let's review the activities DNS performs before discussing DNS cache poisoning. The bulk of DNS usage is either in providing authoritative answers to domain name queries or resolving Internet addresses for clients.

Authoritative servers provide trustworthy answers for a network or a small portion of the Internet. These servers will only respond with an IP address to queries for the domains that they are authoritative for, resolving queries for members of these domains into the associated IP addresses. There are 13 "root" servers that the entire world uses to navigate the Internet. These root servers direct servers making DNS queries to the appropriate Top Level Domain (TLD) servers that are authoritative for areas of the Internet such as .com, .org and .net. The TLD servers point to the next level below them for domains such as example.com. This hierarchy can be extended to any desired depth in order to limit the number of domains and resource records that a server is authoritative for.

When a client is requesting information on a domain and the server is not authoritative for that domain, the DNS server must manage this query until an answer can be found elsewhere, or forward the query to another server to perform this task. The DNS server managing the query contacts a root server, is redirected to a TLD server, and is then further redirected down the DNS hierarchy until the authoritative DNS server for the desired domain is found. The authoritative server for the domain that the query is referen-

cing will then respond with an IP address that can be returned to the client. These responses are stored on the server that is managing the query in temporary memory or “cache”. This cache prevents the same query from needing to be run again, allowing the network, or the Internet to operate more efficiently with less traffic. This process, known as a recursive DNS query, is the most commonly exploited feature for DNS cache poisoning.

DNS Attacks and Vulnerabilities

Although DNS is essential to modern networking, it has some security vulnerabilities that can cause issues unless they are accounted for. The server on which the DNS service is running can provide a major point of vulnerability for DNS. Therefore, this server should be as secure as possible. This can target the program providing the DNS service through a vulnerability such as a buffer overflow. A server-based attack could target any program or service running on the operating system, the operating system itself, or even the hardware on which the server is running. Any ports that are open to the Internet provide increased exposure to hacking attempts. There are almost endless possibilities for vulnerabilities to emerge. The more complex a server or a network gets, the more likely a small vulnerability could be overlooked long enough to become a large liability. A compromised server could be used to provide a poisoned cache, but could also provide falsified authoritative DNS information too.

When the caching server sends out a DNS query, there is no way for it to know that the server responding to it is legitimate. The server performing the recursive query, if it is an early version of BIND, might not even be keeping track that it made a request for the update it is being given. One of the primary tools that attackers use for cache poisoning is generating fake recursive DNS queries by guessing the correct Transaction ID. This allows an attacker to make a false update to the DNS information in the cache. If the attacker can guess the next transaction ID, and contact the caching server with it before the real authoritative server can respond, the server will accept their fake or “spoofed” update and the cache can be poisoned. Often the attacker will simultaneously mount a denial-

of-service (DOS) attack on the legitimate responding DNS server to prevent it from responding faster than the attacker, thus guaranteeing that the cache poisoning will succeed.

Cache poisoning is often referred to now as pharming. Pharming actually uses DNS cache poisoning to mimic sites and pass false information or trick users into conducting financial transactions or installing malware and other unwanted programs. These activities could eventually result in the erosion of public trust in the Internet, both in terms of privacy concerns and as a platform for commerce.

In a pharming attack, web surfers can unknowingly be redirected by the poisoned DNS server simply by entering the URL of a well known, commonly used Web site. The user's requests never reach the legitimate site, despite the user's browser indicating that the site at that address is being displayed. Since the DNS server that helped the user's browser to navigate to that site has been compromised, the user is actually at a completely different site. The user is then often asked to enter information such as banking credentials or a social security number that can be used in perpetrating frauds against the victim.

Another variation of this attack involves a “man-in-the-middle” scenario, also known as DNS hijacking. In this type of attack, the attacker uses a cache-poisoned DNS server to intercept a user's communications to a website. The attacker can harvest all of the intercepted information, such as credit card numbers, bank account information, or social security identifications before passing it on to the legitimate website. Thus, the transactions look legitimate while identity and information theft is actually occurring.

DNS Security

The problem of DNS cache poisoning is quickly gaining momentum, and is becoming increasingly common due to the large number of outdated and unsecured Web servers in use, outdated implementations of BIND, and insecure implementations of recursive DNS resolution. DNS was designed at a time when network security was not a primary consideration, and

it was often sacrificed for functionality. DNS security today requires a complete, system-wide approach. All aspects of the DNS implementation, as well as the platform that it is running on, must be considered.

New DNSSEC standards for secure DNS such as Secret Key Transaction Authentication for DNS (TSIG) are available, but not widely implemented yet by vendors. To address many of these kinds of legacy issues left over from the early days of the Internet, there is a new proposed version of the Internet protocol called IPv6. The proposed IPv6 Internet protocol offers many solutions to the DNS issues discussed here. Due to complexity and migration costs however, IPv6 has not yet been widely implemented. This creates a situation in which the current service must be hardened to the greatest extent possible and then be monitored in order to maintain security.

Despite some past vulnerabilities, the most popular and secure DNS software in the world is the Berkeley Internet Name Daemon (BIND) by the Internet Software Consortium (ISC). Version 4 and 8 implementations, still widely used, suffer from vulnerabilities based on buffer overflows, input validation errors, and information leaks. Even version 9.2.1 suffered from a buffer overflow that allowed DOS attacks. The BIND service must be updated to its latest version to be most secure from cache poisoning and to be able to implement BIND Views. The newest versions of BIND are more secure thanks to the use of the `/dev/random` randomization engine from the operating system to provide superior randomization of transaction IDs. Also, newer versions of BIND are more likely to switch the port that they use for each subsequent transaction.

Common recommendations when implementing DNS services include using a purpose-built server that does not provide any other services, except possibly DHCP. Appliance servers in fact have proven themselves to be the simplest, most effective and affordable solution to ensure secure DNS caching. Using a dedicated appliance reduces the number of potentially vulnerable

programs and services running on the server and reduces the risk in the areas of operating system and hardware vulnerabilities as well as open ports. Adonis uses known and secured hardware, as well as a hardened, Linux-based operating system with few open ports.

DNS services should be separated between authoritative and caching functions in order to minimize the possible impact of cache poisoning. Recursive queries should not be allowed on a server answering requests from external servers and clients. This can be accomplished through the use of two different DNS servers, or by using a single server that uses a packet-filtering firewall on its external interface and implements BIND views.

BIND views enables a DNS server to respond with different DNS services and information based on the origin of DNS queries. A single server then appears to be different DNS servers depending on who is sending a request to it. Queries from external addresses would receive only authoritative DNS services, but internal addresses on the local network would not experience restrictions.

Administrators responsible for DNS implementation and operation must embrace a system-wide security approach in order to maintain the highest possible level of DNS security in the face of the known vulnerabilities.

The DNS system, as we know it, will not last though time without a major overhaul in the area of security. With emerging technologies such as VoIP beginning to massively increase DNS usage, all possible precautions should be taken to ensure continued confidence in the Internet as a medium of knowledge transfer and commerce.

RAISING THE LEVEL OF PROTECTION AGAINST TODAY'S MORE COMPLEX INTERNET THREATS

By Henning Ogberg, Country Manager DACH, SurfControl

Enterprise protection is a tricky business in today's world. As Internet-borne threats proliferate and evolve at an unprecedented rate, even the most diligent company can have its defenses penetrated by the one threat they didn't anticipate—and it only takes one lapse to expose the business to a broad spectrum of serious risks. Consider three examples:

Company A:

"Traditional" Protection Falls Short

This firm deploys bulletproof defenses against "classic" Internet threats such as viruses, Trojans, worms, and spyware. It licenses security technology from a top vendor, and keeps its software and subscriptions up to date. As a result, the company's network environment is perceived as safe, and its IT team sleeps soundly at night. But the dream of a secure enterprise is quickly becoming a nightmare.

Employees cripple network performance through illicit podcasting and peer-to-peer downloads of music, video, and software that violate copyright law.

Intellectual property is leaked via e-mail by careless or unscrupulous employees.

Rampant instant messaging places the company at risk of regulatory non-compliance.

One compulsive gambler plays online poker continuously while vital tasks go uncompleted, and porn surfing brings the further possibility of lawsuits. Unable to enforce its acceptable use policy, the company has no way to ensure user productivity, protect network resources from abuse, or avoid the serious business risks associated with abuse.

Company B:

Mobile Workers Undermine Perimeter Security

This company takes protection one step further. Robust perimeter defenses are complemented by strict policy-based control over P2P, IM, podcasting, and Web usage.

Problem solved? Far from it. The company's employees are constantly on the go, working at client and partner sites, home offices, hotels, airports, commuter trains—anywhere a network connection is available. And every time they operate outside of the company's own network, they unknowingly load up their laptops with the kind of malware the company has worked so hard to counter—then, bring it back inside the company's secure perimeter, where it is free to spread. Removable storage devices like USB drives fly under the company's radar to deliver additional threats. Back to square one.

Company C:

The Threat of Complexity

This firm has done its homework, and boasts best-of-breed defenses across every threat vector—including mobile and disconnected workers. Its Internet protection infrastructure would be the envy of any enterprise ... if only it weren't so difficult and costly to administer and maintain. In reality, the solution remains only partly implemented, having pushed available IT resources to a limit. Overtaxed IT staffers have been unable to customize the solution to fully address the company's policies, risks, and compliance mandates, resulting in a generic deployment with too many gaps.

Calls to technical support are met with offers of costly add-on consulting services.

Updates fall behind as IT dollars and manpower run short.

For all the time and money spent, the company is no closer to effective protection.

Clearly, there's more to Internet protection than meets the eye. To avoid serious business risks, companies need to understand and address the full scope of the challenge—and work with a partner who does, too. Key factors for achieving comprehensive, cost-effective Internet protection State-of-the-art defensive technologies and functionality are obviously essential for effective protection.

Today's blended threats, devised to exploit multiple attack vectors, call for the best possible countermeasures across every point of vulnerability, from the gateway to the desktop and everywhere in-between. But this is only one part of the picture. Every organization's business is unique, and so are its protection requirements. In general, the effectiveness of an Internet protection solution will come down to six factors:

1. *Protection at critical points of vulnerability;*
2. *Protection at key points of management;*
3. *Proactive defense;*
4. *Flexibility in deployment;*
5. *Customization and control; and*
6. *Best value based on need.*

Protection at Critical Points of Vulnerability

Because today's blended threats can arrive in many forms, through many Internet channels, companies

need to deploy consistent protection across Web, e-mail, mobile devices, and desktop clients. Each of these vectors should share access to a common threat database so that, for example, a virus will be recognized regardless of whether it arrives via e-mail, Webmail, removable storage device, or public hotspot.

Layered protection can provide added assurance against threats: a database of known threats is complemented by heuristics and other techniques to recognize and filter previously unknown threats. Protection technologies and human analysis work hand-in hand to identify and stop emerging threats. Standard threat definitions are supplemented by company- and industry-specific definitions, and encryption works in tandem with intelligent content filtering to prevent data loss. No matter what types of risks a company faces, a multi-layered approach offers the highest level of protection.

Protection at Key Points of Management

Depending on a company's IT architecture, infrastructure, and security objectives, protection can be deployed on the server, on the client, or in the cloud (as an on demand service). Companies should evaluate this critical matter—and, ideally, deploy protection in all three places. In this way, threats can be neutralized no matter how or where they enter the network environment. Even remote users working disconnected from the network can be protected through client-level or on-demand applications.

Proactive Defense

Rapidly-evolving Internet threats require constant vigilance, expert analysis, and continuously updated prevention measures. The best approach for identifying and defending against emerging threats combines world-class technologies, human expertise, and an infrastructure for automatically delivering updated protection around the clock and around the globe. In most cases, this is a service that provides detection, alert and elimination of threats before damage goes unheeded.

Flexibility in Deployment

A full range of deployment options—including software, appliance, and on-demand services—enables a company to choose the solution most appropriate to its specific needs and challenges. While larger organizations often require the extensive functionality and granular policy control of a software-based solution, smaller enterprises may prefer the out-of-the-box simplicity and high performance of an appliance-based solution. On-demand solutions make enterprise-class Internet protection available to all companies. Enterprises with multiple branches or remote workers can utilize this technology to manage their e-mail and web security requirements for those that are not based full-time at their headquarters as well as those companies that may not have the infrastructure to host a server-based solution—or those companies who simply prefer to outsource this function as part of the overall IT strategy.

Customization and Control

To fully manage its risks—from malware to inappropriate usage to business and regulatory non-compliance—a company needs the flexible control to define and enforce policies customized to its own specific environment, business needs, and potential risks. The solution should also allow unique rules to be applied to different users and groups within the company to reflect job functions and Internet access privileges.

Once these policies have been implemented, administrators and managers need comprehensive reporting and visibility to manage and monitor employees' Internet usage, verify compliance with business and regulatory requirements, and adjust their protection and security strategy according to the evolving needs of the business.

Best value based on need

When selecting an Internet protection provider, companies should seek out a trusted partner, not just a vendor looking to make a sale. A trusted partner with a proven track record in Internet protection and

a comprehensive range of best-of-breed technologies can provide the experience, deep resources, and continuous innovation needed to stay at the leading edge of security. By working to understand each customer's requirements, the provider can deliver single-source solutions that satisfy their needs, as well as ongoing support and updates to ensure maximum effectiveness over time.

The solution must also be cost-effective to acquire, own, manage, and support over the long term, so that the cost of protection fits comfortably into a company's IT budget—instead of becoming yet another problem in search of a solution.

Protection in action

Returning to the three companies discussed earlier, we can see how each of these key factors plays into an effective Internet protection strategy.

Company A customizes its Internet protection solution to fit its policies and priorities, and then uses robust reporting capabilities to achieve full control over the business risks it faces.

- Inappropriate usage of peer-to-peer networks and podcasts are shut down completely, freeing vital network resources and eliminating the risk of copyright violations.
- Every e-mail is scanned for keywords and content specific to the company's own intellectual property—so nothing gets out that shouldn't.
- Instant messaging and Web surfing are brought under complete control to aid business and regulatory compliance.
- Unproductive and unsafe websites are blocked, so the compulsive gambler is forced to play on his own time—and without using the company's resources.

Company B extends comprehensive protection from the perimeter to the desktop as well as in the cloud. No matter how a remote employee reconnects to the network—from home or hotel, via a café hot-spot,

through a client's network, or through a wireless ISP—any threats on the mobile PC will be blocked from entering the enterprise environment.

Removable storage devices are similarly safeguarded. Company C opts for an on-demand service instead of a hardware or software form factor for complete protection without breaking its budget. It can still maintain the control and policy management of a network or gateway solution and fast implementation and low overheads are backed by the full support and resources of a trusted industry leader.

SECURING CORPORATE NETWORKS IN A WIRED

By Yuval Ben-Itzhak, Chief Technology Officer, Finjan

The World Wide Web not only helped to create the global village, it also produced a paradigm shift in the way people work. In the "old" offline computing environment, electronic information in most cases was pushed to the desktop, usually either by email or diskette. In today's wired world, corporate users are always connected and use the Web to access information that they need to carry out their work activities. The Web provides endless sources of information as well as exciting business opportunities for the modern corporation.

This universal connectivity empowers corporate users to download and install new software from the web, without needing to bother an administrator. Since users deliberately search for and choose the information they want – this method can be described as "pull" rather than "push". However, while the Internet has become an indispensable part of our business and personal lives, the shift from pushing to pulling information has introduced a new dimension for the propagation of malicious content.

The Invisible Web Threat

Today's wired world has bred a new generation of e-criminals that exploit the very connectivity that has become so crucial to corporate business productivity. Driven by financial gain, e-criminals build their nasty schemes around the fact that users are always connected. Spyware/Adware, Trojans, and Rootkits are examples of malicious content aimed at serving the "new age" criminals' business interests. In addition, free software, toolbars and utilities downloaded by corporate users often include "invisible" malicious content that can compromise an entire corporate network.

Malicious content covers a wide range of web threats, including applications that display pop-up ads, applications that co-opt search results, key loggers that intercept credit card numbers and send them to a remote machine, or even Trojan horses that expose corporate desktops to remote hacking.

The fact that desktops crash less often than in the days of the "I Love You" virus does not necessarily mean that corporate computers are healthier, or that

the valuable data they hold is secure. The reason is that in today's connected environment, a crashed or disconnected machine is useless. A corporate PC is much more valuable to an e-criminal when it is connected to the malicious site and available for "silent" downloads or remote execution, etc.

Malicious Code for Sale

The evolution of web-based threats is being driven by commercial and financial interests. Adware alone is estimated to generate annual revenues in the hundreds of millions of dollars. Spyware and Trojan SDKs are available for sale, with warranties that if the exploited vulnerability will be patched by the vendor, the hacker will provide a new, unknown one.

Security research reveals that a real market exists for malicious code, including buyers, sellers and distributors. Motivated by the business opportunity, hackers continue to raise the technological bar to find new ways to exploit vulnerabilities.

As the vulnerability market develops, many hackers prefer to sell new exploits for profit rather than disclosing them responsibly to the vendor whose product is affected. Finjan's Web Security Trends Report (Q2 2006) presented indisputable evidence of this growing market for malicious code, governed by the forces of supply and demand, and fuelled by e-criminals who are willing to pay hackers handsome sums for their wares.

New Threats Require Proactive Solutions

In order to address these new types of threats, and to ensure compliance with regulatory requirements, corporations require intelligent, proactive security solutions that complement their existing security infrastructure. According to

Gartner:

"Traditional signature-based antivirus products can no longer protect companies from malicious code attacks. Vendors must execute product and business

strategies to meet the new market requirements for broader malicious code protection."

(Gartner, Feb. 2005 Magic Quadrant)

Reactive, signature-based security solutions, e.g., Anti-Virus, require time to create and deliver a signature update to their databases, and thus cannot offer immediate protection against new, unknown attacks. This creates a Window-of-Vulnerability™, during which networks are exposed and vulnerable for hours and sometimes days to new attacks, until patches or signature updates are installed.

In order to protect themselves and their customers from today's sophisticated web threats, corporations have started to implement proactive, behavior-based security solutions that scan web content for known and new potential threats before they reach the end user's desktop.

Behaviour-based security closes the Window-of-Vulnerability™ to safeguard networks from new and unknown types of malicious code. This technology inspects web content on the fly for suspicious or malicious computer operations, function calls, commands or operations. Using these findings together with smart algorithms, behavior-based security builds the expected execution model of the content and looks for dangerous execution paths that might compromise the end-user machine. Then, in accordance with each organization's specific security policy, the security engine decides whether to allow, block or neutralize the content.

In addition, behavior-based security analyzes each and every piece of content, regardless of its original source. Web pages from Myspace.com or Yahoo.com are analyzed in exactly the same way as pages from smaller or recently created websites. This technology assures that malicious content will not enter the network even if its origin is a highly trusted site. This differentiates behavior-based security from URL Filtering solutions, which automatically mark well known websites as trusted despite the fact that hackers can upload malicious code to personal pages or ads to those domains, like in the recent Myspace.com case.

As behaviour-based security analyzes code behaviour

and understands the context of its execution environment, this approach is highly effective in handling unknown and dynamic web content. Since it does not require signatures or pre-defined patterns to identify malicious content, it is the ideal solution for securing corporate networks from the new and emerging threats in today's wired world.

AUTHENTICATION – MARKET UPDATE

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure infrastructure solutions.

The impact of the Internet over the last few years has meant fundamental changes in the way we access business systems. The network security perimeter has crumbled at all levels while the number of users wanting network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world.

The devices for gaining access have multiplied and diversified. Users now want to access using mobile and wireless devices, including laptops. The information they want to access has widened to encompass all aspects of a business, including e-mail, a greater range of applications and various types of data.

While there are enormous productivity benefits available from increased access, the security risks have greatly increased. The traditional method of securing system access was by authentication through the use of passwords. Unfortunately, traditional password authentication is totally unsuitable for securing the access requirements of today's distributed users.

UK companies are considerably behind the curve in responding to this changing scenario. According to the DTI Information Security Breaches Survey 2006, UK businesses are still overwhelmingly dependant on user IDs and passwords to check the identity of users attempting to access their systems.

The Survey says that UK companies are poorly placed

to deal with identity theft, with only 1% having a comprehensive approach for identity management (authentication, access control and user provisioning).

Types of authentication

Weak single factor authentication

This is the use of single static passwords and still employed by most UK companies. The benefit is that static passwords are easy to remember. However, when you have different passwords for different systems, they start to become very difficult to remember and have to be written down, making them vulnerable. A significant use of Post-It notes is rumoured to be password related.

The many disadvantages of single static passwords include how easy it is to crack them. They are short and based on topics close to the user, such as birthdays, partner names, children's names, etc; and they are typically letters only.

They are also vulnerable to social engineering i.e. people asking for your password or guessing it. Some highly publicised surveys carried out at railway stations have shown how easy it is to get people to reveal their passwords. They can also be picked up by spyware.

The alternative method of password management is to change passwords regularly. Operated correctly, this has the benefit of being more inherently secure than static passwords. A disadvantage of frequently changing passwords is that they can be easily forgotten, leading to very high support costs and significantly increased administration costs. This is particularly relevant for larger organisations with hundreds of applications.

Single Sign On (SSO)

Single sign on allows users to authenticate once and gain access, when required, to multiple (permitted) software systems. This is useful where users are wanting to access an ever increasing numbers of applications. SSO has major security and user benefits, as well as significantly reducing the helpdesk costs of password management.

There is a security risk with static password-based single sign on because a breach of password security means all systems accessible by a particular user can be compromised. Typically, SSO deployments are in conjunction with some form of two factor authentication. SSO is now undergoing rapid growth thanks to new technology from companies such as Imprivata, which has dramatically lowered the cost of deployment.

Strong authentication

Strong authentication involves one of a range of elements such as hardware tokens, soft tokens, fingerprint recognition, swipe cards, etc. Most strong authentication deployments are used together with passwords (two factor authentication).

Strong two factor authentication

Strong two factor authentication is a much more secure means of authenticating users onto networks as it requires two separate security elements.

It comprises something you know (a password) and something you have (e.g. a token). Tokens are currently the most popular two factor solution, due to their low cost, ease of deployment, ease of management and the standard of security they provide.

VASCO, one of the market leaders, provides hardware tokens which generate one time passwords (OTP). The rapid fall in the price of tokens means they are now available from only a few pounds per user per year

To put that in perspective, it's less than the cost of ONE password-related helpdesk call. With password-connected calls making up between 30% and 50% of all helpdesk calls (depending on whose research you accept), tokens can represent a cost-saving as well as an improvement in security.

Other two factor options include soft tokens which can be sent to your mobile, swipe cards, USB-based authentication and fingerprint recognition. Proximity authentication is another variation which simply means that once you have authenticated and are within wireless range, you don't need to authenticate again for another system.

Similarly with physical/logical security, physical swipe card entry systems linked to IT systems security, allow organisations to integrate access security with network security. Companies such as Imprivata are providing converged security systems in this area.

Three factor authentication

This is far superior and involves something you know (e.g. password), something you have (e.g. authentication token) and something you are (e.g. fingerprint, retinal scan, facial recognition). While biometric authentication is obviously more costly, it is appropriate for high security applications/departments such as pharmaceutical R&D, finance, etc.

Biometric authentication

Biometric authentication is a more recent and still developing technology. It can be either two factor or three factor. Examples of physical, physiological or biometric characteristics include fingerprints, eye retinas and irises, facial patterns, and hand measurements; examples of behavioural characteristics used for authentication include signature, gait and typing patterns. Biometric authentication is more appropriate than tokens for certain applications, such as some manufacturing environments; or where superior security is required.

Remote, mobile and wireless security

Static passwords, as mentioned above, are still the main way of authenticating users onto a network, but are woefully inadequate for remote and mobile computer users, with huge identity theft risks (particularly for wireless). The answer is to deploy strong two factor authentication, but other measures are also advisable.

Low cost encryption from companies such as Utimaco or PGP, can protect key mobile devices for less than £70 per device. Or, if cost is an issue and performance isn't a problem, there are free solutions available.

It is essential to ensure that network connections from remote users is via encrypted VPNs, which create a secure tunnel over the Internet from the user to the network and are authenticated through the network gateway. Either Secure Socket Layer (SSL) or IPsec VPNs are suitable.

SSL VPNs are more appropriate where you have large numbers of remote users as they are low cost and provide easier to manage connections than IPsec. SSL VPNs are a growing area and there is a wide range of solutions available from vendors such as WatchGuard, Array, Check Point and NETASQ.

Wireless is a particular security issue and it is best to ensure that, together with strong authentication, all wireless traffic is over VPNs and is encrypted. Don't use Wired Equivalent Privacy (WEP) for encryption because it is poor, insecure and weak. Use WPA or WPA2 (also known as 802.11i) and ensure that users always operate with it switched on – the default is with it switched off.

If you have remote wireless LANs, ensure that the service set ID (SSID) is changed from the default and is secured to prevent unauthorised wireless users connecting. Don't change it to something blindingly obvious like your company name (or "control tower", as seen by startled laptop users at a US airport).

Another authentication option is to implement media access control (MAC) filtering. A MAC address is a physical address, so if you restrict access to devices whose

address you have authorised, you can eliminate many ID theft issues. Another variation of this is device authentication, where the device authenticates itself to the network.

The DTI Survey 2006 found that roughly 36% of UK businesses allow some staff to access their systems from a remote location (e.g. from home or via wireless hotspots). Four-fifths of large businesses allow this. Interestingly, respondents who allow remote access are twice as likely to have had an unauthorised outsider try to break into their network as those who do not; they are also more likely to have experienced an actual penetration incident.

Conclusion

The growth of the Internet, the increase in users requiring access to networks and the move to remote working has fundamentally changed the requirements for authentication over the last few years. However, users are still lagging behind developments and relying on single static passwords, which are wholly inadequate.

The need for strong authentication is greater than ever, the cost of solutions such as single sign on and strong two factor authentication has come down, and such solutions are now easier to use. It is time for companies to look at improving their authentication procedures, if they want to remain secure and avoid potential business disruption, financial loss and damage to reputation.

