

# NEWS

## SEPTEMBER | 09

EICAR  
European Expert Group  
for IT -Security  
Office  
Obergasse 28A  
86943 Thaining  
Germany

CONSULTING EDITOR:  
Rainer Fahs,  
Manuel Hüttl

EDITOR  
Eddy Willems  
press@eicar.org

CONTRIBUTORS  
Prof. Eric Filiol, EICAR Scientific director;  
Lynn Collier, Hitachi Data Systems;  
Eddy Willems, Director for  
External AV Relationships EICAR  
Ian Kilpatrick, Wick Hill Group;  
Boris Sharov, CEO Dr. Web

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

KONZEPT I DESIGN  
www.designheit.de

<b>01</b>	<b>FROM THE BOARD – CHAIRMAN’S CORNER.....</b>	<b>1-2</b>
<b>02</b>	<b>EICAR 2010: ICT SECURITY – QUO VADIS?.....</b>	<b>2-4</b>
<b>03</b>	<b>BEYOND THE CALL OF DUTY: DRIVING BUSINESS VALUE FROM COMPLIANCE</b>	<b>5-6</b>
<b>04</b>	<b>THE INCREASING PROBLEM OF DRIVE-BY DOWNLOADS.....</b>	<b>7-10</b>
<b>05</b>	<b>TEN TIPS TO KEEP IT SECURITY COSTS DOWN IN THE RECESSION.....</b>	<b>10-11</b>
<b>06</b>	<b>SIX MONTH VIRUS ACTIVITY REVIEW FROM DOCTOR WEB.....</b>	<b>12-15</b>
<b>07</b>	<b>FIREWALL OR UTM FOR LARGER COMPANIES?.....</b>	<b>16-17</b>

## FROM THE BOARD CHAIRMAN’S CORNER

*Rainer Fahs*

Though time is running quick and it was back in May this year, but I think it is still worth mentioning that the EICAR Conference 2009 was a great success. First of all, the level of papers presented was excellent, which is even more worth mentioning knowing that only an average of 40 to 50 percent of papers submitted are accepted by the review board.

Secondly, the hotel with the conference area just newly renovated and a staff flexibly responding to our demands was surely an asset and has contributed to the overall success.

Finally the city of Berlin with its history, flavour and thousands of things to explore was the peak making it easy to have a successful conference.

However, it would be an omission not to mention the absolute highlight of the conference, which was the key-note speaker Dr. Fred Cohen with his presentation “Computer viruses Then – Now – Then Again.” Fred gave an overview how everything started by “searching for the most efficient way to distribute a computation” and how it all developed. Interesting in Fred’s story is that his early ideas of utilising “benevolent viruses” in real environment (i. E. Maintenance Virus) got him more trouble than credit. However,

when I asked him the question: “why is it that the negative annotation of viruses became so prevalent from the beginning? In an interview with the German TV, he took the blame on himself, stating “It is my entire fault, we were so focused on the negative aspects and nobody wanted to talk about “benevolent viruses.”

Now, 25 years later, nothing has changed in principle. The situation has only become more complex due to the different stakeholders in the AV community.

As usual at our conference we had the Annual General Meeting and some changes were made to the Board. James Wolfe’s terms were up and he was not nominated for Board member again. We thank James for his contributions over the past four years and hope he stays attached to EICAR and its objectives.

Newly elected to the Board was Marc Schneider whose company is hosting the EICAR Web-page for a number of years. In our Board meeting on 8th August Marc was appointed Technical Director to the Board and we are looking forward to his contributions for the near future.

At the same Board Meeting Eric Filiol was confirmed Scientific Director and Robert Niedermeier was confirmed as Executive Secretary and Legal Advisor. Manuel Hüttl was appointed Director Public Affairs and Eddy Willems Director for External AV Relationships.

The conference was completed by a panel addressing the issues of AV product testing with panel members from AMTSO, Product Testers, EICAR and CARO and I think it is already worth mentioning, that – probably for the first time – all key players were represented in one panel.

However, though generally agreement about principles of AV product testing were formulated and a common approach with participation of all stakeholders was agreed, no concrete working approach was agreed.

Though EICAR as an independent organisation probably does have a say, EICAR is not in a position to tell other organisations how to proceed. We have offered our co-operation because we think we could be real contributors. However, for no reaction from either side

since the EICAR conference, at our Board meeting in August we decided to go our own way and we have initiated first steps. (See Eric Filiol’s article). The great challenge seems to be to get scientific research and the AV industry together – if that is possible at all. The issue will be further pursued by EICAR and results will be presented at our next conference which will be held on May 10th and May 11th 2010, with a pre-conference program on May 8th and 9th at the ESIEA Engineer School/Institute of Computer Science in Paris, France.

The Call for Paper can be found further back in this EICAR News and I would like to encourage submitting papers to the EICAR conference to give the necessary diversity and the ability to reward the best papers.

---

## EICAR 2010: ICT SECURITY – QUO VADIS? OVERVIEW OF THE CONFERENCE: WHY TO ATTEND EICAR 2010?

---

*Professor Eric Filiol, EICAR Scientific director*

The 19th EICAR (European Institute in Computer Antivirus Research) conference will take place in Paris from May 8th to May 11th including a pre-conference program that should be a milestone in the history of computer antivirus research. In fact the whole conference itself is intended also to be a major event in the field and thus for many reasons.

The AV world -- and more widely the computer security world-- is facing for a few years big challenges. BUT contrary to partially wrong feelings those challenges are not only coming from the bad guys: usually all those ugly actors who think to be intelligent or having some sort of power by distributing malware. While all the instances (the defenders, e.g. AV vendors, governments, researchers, IT experts...) involved in fighting those malevolent guys (the attackers), the motivations has begun to diverge substantially for a few months, in such a way that it not only becomes more difficult to make the difference between defenders and attackers but also finally the result is that the activity of

the attackers is made easier: here precisely lie the new challenges that the EICAR 2010 has decided to address. Hence the main theme of the event: **ICT Security – Quo Vadis?** I would be tempting to use an equivalent formula: is the AV world and the ICT world going mad? Let us see why through two illustrative but worrying recent issues.

The first one refers to AV evaluation – which will be addressed at EICAR 2010 as a one of the major topics. The situation is somehow worsening making that evaluation, from an independent, technical perspective more and more difficult not only from a technical point of view but also from a legal point of view. To realise how things are evolving, anyone can read any AV software licence document (the one which nobody reads in fact): you will discover, according to the product, in a jumble that you cannot use the product in any automated way (which is quite limiting in a context of black box evaluation), you cannot even analyse the product, you are warned that your data

can go outside for analysis (but where), that the encryption embedded in the product is weak on purpose in order to facilitate US governmental decryption... Is it really serious and does it take the needs and interest of the end-user which are not simple "consumers". In this respect, the reaction of the AV community goes in the wrong direction and is perceived as just trying for 20 years more just to protect their commercial interest. On the contrary it should work deeply and in a trustful way with the scientific community. Nobody has the right to forget that there is ONLY one target: malware and those who spread them. The recent evolution of the use of cryptographic primitives into malware (remember Conficker), the rise of metamorphic like techniques require now that all good wills work together. That is why EICAR 2010 will focus on the evaluation of AV software, in such a way that we provide a useful reflexion for better products while taking into account the end-users needs, the ethical and legal aspects and the scientific/technical challenges we are bound to face in a very near future. Aside the classical academic and industry papers which will be presented, the two-day preconference program will propose tutorials, student/industry sessions around the topic of AV software and AV policy evaluation. Especially, we intend to offer and promote new tools and tutorials with respect to them, that everyone could use to evaluate himself his own AV security and policy. It will be the occasion to recall that the only independent way to test an AV without using any malware – a critical issue in itself – was, and still is, the EICAR test file. We will propose, especially for the industry, a tutorial on that file and on new open forthcoming tools that will be disclosed and presented during EICAR 2010. Those tools are directly inspired by the EICAR test file but go far ahead to address the new challenges and needs. So it should be a good reason to attend the conference.

The second case is the very worrying evolution of the use of malware for so-called "investigation" and "copyright protection" purposes. A number of countries (USA, Germany, UK, France, Austria, Switzerland, have officially announced that malware-like technologies (e.g. Trojan horses for the most part) are now authorized to enforce the law. More worrying is the use for commercial purposes (as it is the case when trying to monitor users' downloading in order to fight piracy). The question is: is the remedy not worse than the

disease? Such issues should be addressed at the EICAR 2010 conference. BUT the main consequence of that evolution lies in the way the AV community will react and what it will decide: either AV vendors accept not to detect those malware-like technologies (which is bound to be very difficult from a behavioural detection point of view, unless closely collaborating with the governments) or they refuse and will detect them anyway. Well, it reminds us the critical issue of the FBI Trojan horse Magic Lantern, except that now we have a lot of Magic Lantern codes which are about to be used. If the AV community chooses the first solution – to cooperate with the governments – they are going to lose their credibility and legitimacy very quickly, making precisely the game of the bad guys. Why? Because they implicitly would accept the fact that there is such things as good and bad Trojan Horses. What is quite impossible to manage from a technical point of view, would be a nightmare from a legal/society/privacy point of view. In fact, they are just about to open the Pandora box? That is the reason why we have decided at EICAR 2010 to also address these kinds of topics. The ICT world has now invaded our society and personal lives and we cannot remain blind to its evolution. I would like to quote Francois Rabelais, a famous French writer, from the 16th Century: "Science without conscience is the soul's perdition". It could be the EICAR 2010's motto. So you now know why you must attend the conference. Look for the EICAR website. More details will be published by mid September. You can also register to the EICAR forum where you will find a lot of useful information.

# EICAR 2010: „ICT SECURITY – QUO VADIS?“ CALL FOR PAPERS

EUROPEAN EXPERT GROUP FOR IT-SECURITY



eicar

2010

## CALL FOR PAPERS

<b>SUBMISSION DEADLINES:</b> Peer reviewed papers due Other papers (non reviewed)	December 20 <sup>th</sup> , 2009 December 20 <sup>th</sup> , 2009
<b>ACCEPTANCE NOTFICATION TO AUTHORS:</b> Peer reviewed papers Other papers (non reviewed) - Initial selection Other papers (non reviewed) - Final selection	February 21 <sup>st</sup> , 2010 December 22 <sup>nd</sup> , 2010 January 31 <sup>st</sup> , 2010
<b>FINAL PAPERS DUE:</b>	March 21 <sup>st</sup> , 2010

# BEYOND THE CALL OF DUTY: DRIVING BUSINESS VALUE FROM COMPLIANCE

*Lynn Collier, Hitachi Data Systems*

The regulatory environment is becoming increasingly complex for UK-based enterprises, with the UK and EU governing bodies as well as industry-specific bodies imposing a growing level of legislation.

Companies and public sector organisations alike must stay alert to compliance if they are to avoid public embarrassment, fines, undertakings or even legal proceedings. Adding to this problem, new regulations are expected over the next 12 months that will continue to challenge businesses across all sectors.

Smart organisations are preparing for compliance but the smartest ones are aiming beyond this and looking to drive business value out of necessity. If approached strategically, compliance is not a burden but an opportunity.

Despite being forewarned about impending regulatory changes, companies are often ill-equipped to deal with the legislation. This is generally because the true impact of compliance is not immediately obvious. For example, the Markets in Financial Instruments Directive (MiFID) introduced in October 2007, to which the majority of financial services companies need to comply, demands on average that three times the current amount of contact records be stored than under previous guidelines.

After a few months of complying with MiFID, CIOs and IT managers began to hear their storage infrastructure creak under the strain of the data deluge. In some cases, under-provisioned storage systems saw the influx of new data volumes begin to cost the organisation serious money as it was stored on expensive, high-availability disk systems.

For many financial services companies, MiFID has meant a lengthy retrospective overhaul of their data storage processes and infrastructure. Switching to highly scalable storage systems to avoid expensive upgrades; implementing a tiered storage architecture to lower storage management expenses; introducing virtualisation to maximise capacity and running data

deduplication software to reduce data volumes are all common approaches.

While these are all very effective steps to take in the face of growing data volumes, they are much easier to implement prior to new legislation coming in, rather than afterwards, when the new data is already flooding in. Currently, storage environments in the financial services sector are leading the industry in terms of fitness for handling spiralling data volumes but many have achieved this the hard way.

One much-talked-about example of upcoming regulation is EuroSOX, which will affect every European business with more than 2,500 employees. The Sarbanes-Oxley Act of 2002 in the US (SOX) only impacted companies trading in the US but in 2008 the European version, known as EuroSOX, comes into effect.

This set of regulations brings together disparate directives already in place and harmonises them, with the aim of restoring investor confidence in the EU. In essence, EuroSOX places greater demand on an enterprise's financial reporting – meaning more information must be stored, tracked, modelled and made available to relevant authorities as and when required.

The archive requirements of EuroSOX will be significant. The need to store greater amounts of financial data, which can be retrieved and presented accurately within tight time frames, requires companies to adhere to strict data storage processes. The relevant data needs to be indexed so it is easily searchable and stored on a system with relatively high levels of availability so that it can be quickly retrieved.

Most importantly, this information needs to be secure in order to prevent leaks and avoid attacks by hackers. In the current economic climate, this usually needs to be achieved on a shrinking IT budget, so only rarely can a company rip out an ineffective legacy system and introduce a new, best-of-breed infrastructure. However, it is important that non-financial sector

companies learn from the experiences of their financial sector counterparts and prepare in advance for the demands placed on their storage infrastructure by EuroSOX compliance. It is key to select a robust and adaptable solution which will support compliance requirements today and which will offer an agile infrastructure to encompass future requirements.

There are three important things to consider when re-engineering your IT infrastructure to support compliance objectives:

The vast increase in data volumes often associated with compliance can require an organisation to implement an archiving platform, which specialises in the effective storage, search and retrieval of large volumes of data. When choosing an archiving infrastructure, it is important to select an open system with no proprietary lock-ins. Many archival systems store data in a format unique to that vendor, which can cause problems when the system has to be upgraded and the data transferred to a new format. In some cases this can lead to volumes of unreadable data or a lengthy and expensive migration process.

Remember that processes are just as important as technology. When it comes to retrieving data, the storage process is key. Files saved without the correct descriptions (metadata tags) attached will be almost impossible to find. Ingraining a culture of uniform tagging throughout the organisation will pay dividends when regulatory authorities request specific data at short notice.

Future-proof technology is more cost-effective than cheap storage methods. While tape storage is appealing for its price and familiarity, winding through

miles of tape under time constraints to find a critical piece of archived information is every IT manager's nightmare. Tape can degrade over time and this, added to the challenge of managing data deletion in such an environment, make it an unsuitable medium for compliance archiving. The reliability and longevity of disk-based systems makes them the obvious choice for critical information archives.

Forward-thinking enterprises are increasingly looking to drive business value from the necessity of compliance. As organisations log more and more data relating to customer contacts and financial information, it makes sense to harness this knowledge for business advantage, ultimately generating profit for the company. A great deal of financial information, for example, can be used to generate superior levels of business intelligence.

EuroSOX is not the only regulatory change set to impact IT departments in the near future, with updates to the EU Data Retention Directive and MiFID expected within the next year. The rate of new legislation does not look likely to abate for some time, requiring businesses proactively to address potential compliance issues before they arise.

By planning your IT strategy to support compliance objectives well in advance, your company will be able to deal with upcoming regulations with relative ease. If this forward-thinking approach becomes more common, it is likely that we will see many more companies derive significant business value from compliance. In this way, enterprises can look to mitigate the costs involved in compliance and take the opportunities that it offers.

# THE INCREASING PROBLEM OF DRIVE-BY DOWNLOADS.

*Eddy Willems, Director for External AV Relationships EICAR*

Unfortunately, the maturity and sophistication of the web has attracted the attention of well-organized malware purveyors who are now intent on using the Web to deliver their viruses, spyware, Trojans, bots, rootkits, and fake security software. The anti-virus industry refers to this covert downloading of malware, which occurs at Web sites without the user's awareness, as a "drive-by download." In this article, we will explore what actually happens during a drive-by attack, the lures used to perpetrate attacks, the technology behind the attacks, and the use of drive-by download attacks in personal data theft and computer takeovers.

Before we explore drive-by downloads in more detail, it is useful to understand how this type of attack has exploded in recent years. It is also helpful to understand that the same malware, and often is, delivered in different ways – sometimes by e-mail, sometimes by visiting a Web page, sometimes by other methods. Drive by malware delivery is of increased appeal to cybercriminals simply because it is, in general, a more stealthy form of infection that results in more successful attacks. According to more recent data from ScanSafe 74 percent of all malware spotted in the third quarter of 2008 came from visits to compromised Web sites. Let's explain now how the attacks work, the techniques used to lure targets to rigged Web sites, the sophisticated exploit kits and the applications they target, the complicated maze of Web redirects, and the payloads used to conduct identity theft and computer takeover attacks.

## *Browser Attacks*

To fully understand the dramatic shift to using the Web browser as the attack tool, it is useful to revisit the history of major Internet-based computer attacks. During the "Internet worm era," when attacks like

Code Red, Blaster, Slammer and Sasser wreaked havoc on corporate networks, hackers used remote exploits against Windows operating system vulnerabilities. (A remote exploit is one in which the malware resides on a network-connected server, exploits legitimate code on the user's computer, but doesn't require prior access to the user's computer to exploit the vulnerability in the code.) Malicious executables, such as Melissa, were also attached to e-mail or they arrived via instant messaging or peer-to-peer applications. Microsoft reacted to the worm attacks in a positive way. They added a firewall, which is turned on by default in Windows XP SP2, and implemented several anti-worm mitigation mechanisms in the operating system. With automatic updates enabled on Windows, end users got some assistance with regularly applying operating system patches. Businesses and consumers also got smarter about blocking attachments or not clicking on strange executables. Both factors forced attackers to shift tactics, moving up the stack to target third-party applications and to perfect the art of social engineering.

This evolution also drove the emergence of a stealthy new technique – the drive-by download – that uses the browser as the mechanism to connect computer users to servers rigged with malicious exploits. In the drive-by attack, the malicious program is automatically downloaded to your computer without your consent or even your knowledge. The attack actually occurs in two steps. The user surfs to a Web site that has been rigged with code that in turn redirects the connection to a malicious third-party server hosting exploits. Figure 1 shows the basic structure of a drive-by download attack. These exploits can target vulnerabilities in the Web browser, an unpatched browser plug-in, a vulnerable ActiveX control, or any other third party software flaws.

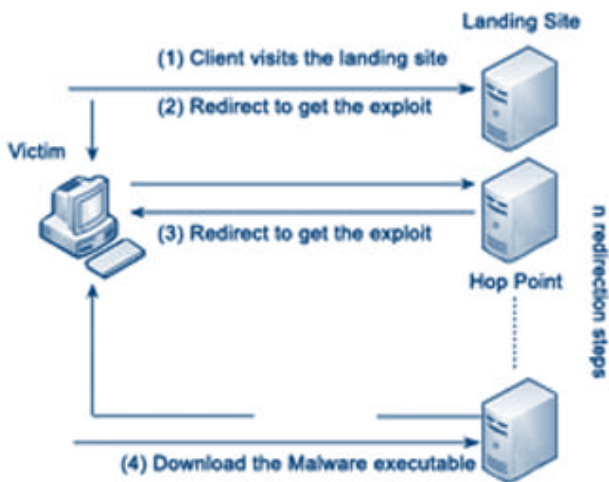


Figure 1 – Structure of a Drive-by Download Attack

As the figure indicates, there may be any number of redirections to different sites before the exploit is actually downloaded. According to data from Kaspersky Lab and others in the security industry, we are in the midst of a large-scale drive-by download epidemic. Over a recent ten-month period, the Google Anti-Malware Team crawled billions of pages on the Web in search of malicious activity and found more than three million URLs initiating drive-by malware downloads. In the early days of drive-by downloads, attackers typically created malicious sites and used social engineering lures to attract visitors. This continues to be a major source of malicious activity online, but more recently hackers have compromised legitimate Web sites and either secretly exploit script or planted redirect code that silently launches attacks via the browser.

### Exploits, exploits and exploits

One high-profile Web site compromise in 2007 provides a glimpse at how drive-by downloads are launched against computer users. In the weeks leading up to the NFL Superbowl game, Miami's Dolphin Stadium site was hacked and rigged with a snippet of JavaScript code. A visitor to that site with an unpatched Windows machine was silently connected to a remote third party that attempted to exploit known vulnerabilities described by Microsoft's MS06-014 and MS07-004 security bulletins. If an exploit was successful, a Trojan was silently installed that gave the attacker full access to the compromised computer. The atta-

cker could later take advantage of the compromised computer in order to steal confidential information or to launch DoS attacks. Later in 2007, the high-traffic "Bank of India" Web site was hijacked by hackers in a sophisticated attack that used multiple redirects to send Windows users to a server hosting an e-mail worm file, two stealth rootkits, two Trojan downloaders, and three backdoor Trojans. These are just two examples to highlight the extent of the problem on legitimate Web sites. In its tracking of Web-based malware threats, ScanSafe reported that by the middle of 2008, the majority of malware was being found on legitimate sites.

Malware exploit kits serve as the engine for drive-by downloads. These kits are professionally written software components that can be hosted on a server with a database backend. The kits, which are sold on underground hacker sites, are fitted with exploits for vulnerabilities in a range of widely deployed desktop applications, including Apple's QuickTime media player, Adobe Flash Player, Adobe Reader, RealNetworks' RealPlayer, and WinZip. Browser-specific exploits have also been used, targeting Microsoft's Internet Explorer, Mozilla's Firefox, Apple Safari, and Opera. Several targeted exploit kits are fitted only with attack code for Adobe PDF vulnerabilities or known flaws in ActiveX controls. Identity thieves and other malware authors purchase exploit kits and deploy them on a malicious server. Code to redirect traffic to that malicious server is then embedded on Web sites, and lures to those sites are spammed via e-mail or bulletin boards.

An exploit kit server can use HTTP request headers from a browser visit to determine the visitor's browser type and version as well as the underlying operating system. Once the target operating system is fingerprinted, the exploit kit can determine which exploits to fire.

In some cases, several exploits can be sent at the same time, attempting to compromise a machine via third-party application vulnerabilities. Some of the more sophisticated exploit kits are well maintained and updated with software exploits on a monthly basis. The kits come with a well-designed user interface that stores detailed data about successful attacks. The data can range from operating system versions exploited,

the target's country of origin, which exploit was used, and the efficiency of exploits based on traffic to the malicious site.

### *The real problem: patching your systems...*

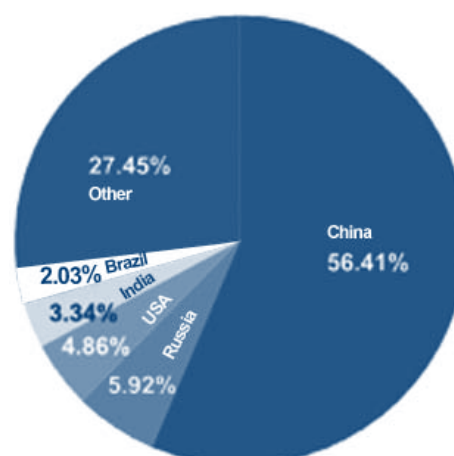
The drive-by download epidemic is largely attributed to the unpatched state of the Windows ecosystem. With very few exceptions, the exploits in circulation target software vulnerabilities that are known – and for which patches are available. However, for a variety of reasons, end users are slow to apply the necessary software fixes. Microsoft's Automatic

Updates mechanism offers end users a valuable way to keep operating system vulnerabilities patched, but the same cannot be said for third-party desktop applications. Secunia, a company that tracks software vulnerabilities, estimates that about one-third of all deployed desktop applications are vulnerable to a known (patched) security issue.

### *Which countries*

The following table shows the countries which rank most highly in terms of attempts to infect computers via the web.

<i>China:</i>	<i>56,41%</i>
<i>Russia:</i>	<i>5,92%</i>
<i>USA:</i>	<i>4,86%</i>
<i>India:</i>	<i>3,34%</i>
<i>Brazil:</i>	<i>2,03%</i>
<i>Other:</i>	<i>27,45%</i>



### *Some solutions*

It is important to note that most modern Web browsers – including Internet Explorer, Firefox, and Opera – have added anti-malware blockers that provide early-warning systems when users attempt to surf to a rigged Web site. These blockers provide good value but, because they are blacklist-based, they do not provide 100 percent protection to Web surfers. The most practical approach to defending against drive-by downloads is to pay close attention to the patch management component of defense. Let's try to sum up the most important solutions:

- *Use a patch management solution that assists with finding – and fixing – all third party desk*

*top applications. Secunia offers two tools – Personal Software Inspector and Network Security Inspector – that can help identify unpatched applications.*

- *Use a desktop browser that includes anti-phishing and anti-malware blockers. Microsoft's Internet Explorer, Mozilla Firefox, and Opera all provide security features to block malicious sites.*
- *Enable a firewall and apply all Microsoft operating system updates. Avoid using pirated software which has its updates disabled through WGA.*

- *Install anti-virus/anti-malware software and be sure to keep its databases updated. Make sure your anti-virus provider is using a browser traffic scanner to help pinpoint potential problems from drive-by downloads.*
- *Try to browse in a virtual environment and quit to return to a safe snapshot from the clean situation before, this method can help to avoid the possible new attacks. This method can be done by use of a virtual environment or some AV vendor package functionality. For instance Kaspersky lab is calling this the Green Zone. This application can even roll back all the system changes made by an application.*

These steps toward managing the vulnerabilities continue to offer the greatest, most valuable protection against drive-by download attacks.

However it's not over yet ... Recently there has been a clear trend for cybercriminals to use a range of sophisticated drive-by downloads to install malware on victim machines. Overall, cybercriminals are becoming increasingly Web-oriented. This makes it particularly important for users to update their operating systems and application software regularly and to keep their antivirus solutions up-to-date. I hope we all can stay safe for the next wave of drive-by downloads by using these solutions.

Thanks goes to Ryan Naraine in helping me out with this article.

---

## TEN TIPS TO KEEP IT SECURITY COSTS DOWN IN THE RECESSION

---

*Ian Kilpatrick, Wick Hill Group*

### *1. Move to UTMs (unified threat management systems)*

UTMs save money over multiple point solutions. They can cost just a quarter of the price of multiple solutions.

With UTMs you have fewer devices, so you can save on energy costs, rack space and air-conditioning. If you deploy multiple UTMs throughout an organisation, and use centralised management and reporting, you can significantly reduce the time spent on admin and management. There are also fewer ongoing management costs from factors such as training, maintenance and upgrades. And you only have one dedicated platform to support. Companies such as Check Point, WatchGuard and NETGEAR have solutions in this area

### *2. Beef up your web filtering*

List-based web filtering security tools don't provide effective control against proxy anonymisers, which allow staff to browse restricted sites undetected by many web filtering systems. Consider moving to solutions that provide protection against anonymisers, so you can significantly increase productivity, as well as improving security. Marshal8e6, Barracuda Networks and Finjan are among the companies who offer products here.

### *3. Close down the bad guys*

Close down the areas that you weren't too happy about but may have ignored in the past. For example, P2P, streaming media and IM. Not only do they

represent a significant security risk, they also have an extremely high cost in wasted staff time. Solutions are available that let you manage these areas, alongside traditional web risks. They include those from Marshall8e6 and Barracuda Networks.

#### *4. Deal with non-work related emails*

Inappropriate and non-work related emails not only carry major legal risks for organisations but also have a huge security and productivity cost. Yet many organisations are completely blind to the level or nature of the activity. Solutions are available that allow you to manage non-work related emails and increase productivity, without upsetting staff or disrupting business.

#### *5. Deploy encryption*

The lack of encryption can lead to data being viewed by unauthorised people, both inside and outside an organisation. The cost of dealing with such data leakage incidents is massively larger than the cost of preventing them in the first place. In a recession, the damage to reputation can be even more expensive. We are all too painfully aware now, that data leakage is not an isolated thing and can strike all sorts of companies. Encryption used to be expensive and disruptive to install, but this is no longer the case, and most companies can afford to use it. Solutions are available from Check Point (Check Point Endpoint Security) and HP.

#### *6. Two factor authentication*

The cost of managing passwords can be extremely expensive in terms of helpdesk resources. And weak passwords put your business at risk. Two factor (soft or hardware) tokens cost only a few pounds, less than the price of one helpdesk call. They can secure your business effectively, particularly where you have a lot of remote and mobile users. Suppliers include CRYPTO-Card and VASCO.

#### *7. Hosted security*

For some companies, hosted security can be a more cost-effective option than handling all security needs yourself. It can cover any type of environment and includes office based systems, remote locations, home offices and mobile laptops. You can host all or just some of your security needs. Cost savings can come from areas such as not having to pay all the costs associated with installing and managing hardware and software. There are many companies in this area including Kaspersky Lab and CRYPTOCARD.

#### *8. Compliance*

The burden of proving that your IT security is compliant to an ever-increasing range of laws and regulations can take up costly manpower. Solutions are available which can automate the collation of security data from devices and systems across your organisation, and make it readily available when you are called upon to prove your compliance. They save on manpower and on the possible cost consequences of not being able to prove you are compliant. These include solutions from ArcSight and LogLogic.

#### *9. Bring staff on board*

Using your own staff is a major way to secure your systems. Retrain staff and remind them that data security is their responsibility and crucial to the survival of the business. In tough times, the message is more likely to strike home and be appreciated.

#### *10. Review AV.*

Many anti-virus and end point solutions create a large load on PC resources with big updates and processor intensive scans. With budgets under threat, desktop refreshes are being delayed. Using efficient low footprint anti-virus extends the life of PCs and laptops.

# SIX MONTH VIRUS ACTIVITY REVIEW FROM DOCTOR WEB

*Boris Sharov, CEO Dr. Web*

Doctor Web presents the virus activity review for the first six months of 2009. ATM malware, new threats for Mac OS X and the first large botnet comprised of web-resources became the most significant events of the past half-year. On the other hand the expansion rate of the Shadow botnet (Conficker, Dwindup) has decreased significantly.

## Botnets

In the first months of 2009 many users and IT security experts focused their attention on the [Win32.HLLW.Shadow](#) worm.

Computers infected by the malicious program joined the botnet that ensnared millions of machines worldwide. [Win32.HLLW.Shadow](#) had several spreading techniques. It exploited Windows vulnerabilities, used brute force administrator password cracking (it turned out that passwords used by many administrators were rather weak) and travelled between computers on removable data-storage devices.

Authors of [Win32.HLLW.Shadow](#) released numerous modifications of the worm during the epidemics. All of them were promptly added to the Dr.Web virus databases. Now activity of this malicious program has declined and it left the virus top ten.

Virut was another botnet that came into the spotlight in the last six months. In case of this botnet computers were infected by a complex polymorphic virus. The Tdss botnet also became a stand-out among networks of zombie computers. A program that enslaved target machines used rootkit technologies to hide its presence in the system. [BackDoor.Tdss](#) has been spreading rather intensively in the last six months with its numerous modifications discovered in the wild every now and then. It should be noted that the backdoor

can feature different sets of modules meaning that modules responsible for installation and disguise of [BackDoor.Tdss](#) are created and spread on commercial basis. The graph below shows how the number of discovered variations of the program changed through the first six months of 2009.

One of the last but by no means the least botnet that got into the news was created using the [BackDoor.MaosBoot](#) bootkit family. It is ought to be noted that these bootkits are among the hardest to cure. Two new versions of the bootkits have been discovered by Doctor Web virus analysts in 2009.

In April cyber-criminals included Twitter in their botnet control centre domain name generation algorithm. In May a lot of web-sites were found to spread the rootkit. The sites were capable of detecting location of a supposed victim. For example, [BackDoor.MaosBoot](#) wouldn't attack a host unless it was located in Germany or the USA.

## JS.Gumblar

While largest botnets were typically comprised of infected workstations, [JS.Gumblar](#) changed the situation. Malicious programs from this family contributed to creation of a botnet of more than 60000 web-pages.

The mid-May 2009 saw a wave of malicious scenarios implemented using Javascript. This was when [JS.Gumblar](#) came into action.

Malicious scenarios of [JS.Gumblar](#) were injected in the code of many web-resources. For most of them it was the first time when they were compromised.

According to Google statistics showing the number of requests to [gumblar.cn](#) (malicious scenarios used to

carry out attacks from infected pages were downloaded from the web-site) looks as follows:

So instead of targeting user machines cyber-criminals created and still control this non-typical botnet of compromised web-resources with numbers of visitors reaching hundreds of thousands. Such web-resources enable malefactors to spread any piece of malware among users worldwide.

### Malware and ATMs

Customers of Russian banks using ATMs were worried by the news about viruses that compromised ATMs of certain Russian banks.

Trojan.Skimer stored information found on bank cards and could also save account balance information if a victim obtained it using the ATM. This information can be used by cyber-criminals to manufacture fake cards to withdraw all funds available on accounts of their victims.

### Ransomware

SMS-fraud where a victim has to send a paid message is becoming even more popular. To force a user to send such a message cyber-criminals create ransomware that can block access to Windows (Trojan. Winlock) or display adult-content banners (Trojan. Blackmailer).

A message prompting a victim to send a paid SMS can also be sent via ICQ or over a social networking web-site.

### Mac OS X

The growing interest to Mac OS X on the part of cyber criminals has been observed since the beginning of 2009. The first outcome of this interest was the Mac.Iservice Trojan that added compromised Macs to a botnet. It was the first case of a botnet consisting of machines running Mac OS X (the iBotnet).

The spring saw a wave of other malicious programs for Mac.

Those were Mac.DnsChange trojans that were spread as links to a malicious video clip. Twitter became one of the channels used to distribute the link.

Activation of the malicious video clip allowed detecting the target operating system using the User-Agent data. After detection of the platform a user was offered a corresponding file – a malicious program for Windows or for Mac OS X.

As popularity of Mac OS X grows among users, so it does among cyber-criminals. By now the number of threats for Mac OS X is not nearly large enough to be compared with the number of threats targeting Windows. However, the situation may change in the future.

### Exploits

In the first two weeks of July a severe “zero day” vulnerability was found in a component of Microsoft DirectX used by Internet Explorer 6 and 7.

Vulnerable operating systems include 2000/2003/XP with all released updates installed (including x64 versions of the systems). incorrect procession of a video stream by the msVidCtl.dll component of ActiveX can be used to spread malicious programs from web-sites that cause stack overflow and launch a malicious program on the target machine.

All exploits of this vulnerability are members of the Exploit.DirectShow family.

### Social networking web-sites

As in 2008, increased activity of cyber-criminals on social networking web-sites was registered in the spring of 2009.

The number of instances of infections by Win32.HLLW.Facebook (aka Koobface) doubled in two summer months. At the beginning of June many modifications of Win32.HLLW.Facebook that targeted users of Facebook, ySpace and Twitter were added to the Dr.Web anti-virus database.

We believe it is necessary to speak about Twitter in more detail. It has already become a popular channel used to spread malicious programs with the number of messages containing links to bogus web-sites increasing.

It should be specially noted that link shortening services make it very hard to guess if a link points to an unwanted web-resource.

The JS.Twitter virus family appeared at the end of May. Now the family is represented by XSS-worms that were spreading using the social networking web-site at the end of the spring.

As for malicious programs spreading over Russian social networking web-sites, the family of Trojan.Hosts ransomware can serve as the most typically example.

## Conclusions

By the summer 2009 the number of infections by Win32.HLLW.Shadow declined significantly. However, its appearance set the trend for the increasing number of large-scale viral threats that persisted in 2009. JS.Gumblar followed Win32.HLLW.Shadow and infected an unprecedented number of web-resources.

Cyber-criminals are clearly interested in Mac OS. Infection methods become more versatile allowing to deliver a malicious program for a detected platform. Popular social networking web-sites attract attention of the growing number of virus-makers. A number of modifications of Win32.HLLW.Facebook surged in the beginning of the summer. The particular interest of cyber-criminals in Twitter should also be taken into consideration.

The growing number of ransomware shows that cyber-extortioners strive for quick and easy illegal money. The special trend of the past six months is the mali-

### VIRUS DETECTED ON USER MACHINES

## TOP 20

(TOP 20 – JANUARY 2009 – JULY 2009 – LAST 6 MONTHS)

1. W32.Gavir.ini	7.76%
2. W32.Shadow.based	4.88%
3. Trojan.Download.36339	4.50%
4. DDoS.Kardaw	3.64%
5. W32.Beagle	3.41%
6. JS.Nimda	2.95%
7. Trojan.Botnetlog.9	2.77%
8. W32.Virut.5	2.74%
9. Trojan.Starter.516	2.45%
10. W97M.Thus	2.28%
11. W32.Virut.14	2.11%
12. W32.Netsky.35328	2.09%
13. Trojan.PWS.Panda.114	1.94%
14. W32.Alman	1.85%
15. Trojan.Download.42350	1.83%
16. W32.Autoruner.5555	1.76%
17. Trojan.MulDrop.16727	1.60%
18. Trojan.Blackmailer.1094	1.56%
19. VBS.Generic.548	1.50%
20. W32.Sector.17	1.17%

### VIRUS DETECTED IN MAIL TRAFFIC

## TOP 20

(TOP 20 – JANUARY 2009 – JULY 2009 – LAST 6 MONTHS)

1. W32.Netsky.35328	34.82%
2. W32.MyDoom	9.58%
3. W32.Beagle	9.28%
4. Trojan.Download	7.29%
5. W32.MyDoom.44	3.83%
6. W32.Mydoom.based	3.43%
7. W32.Netsky.based	3.21%
8. W32.Netsky.28672	3.12%
9. W32.Netsky	2.83%
10. W32.Perf	2.52%
11. Trojan.Botnetlog.9	2.49%
12. Trojan.MulDrop.19648	2.14%
13. W32.Beagle.32768	1.88%
14. Trojan.MulDrop.13408	1.84%
15. W32.MyDoom.49	1.38%
16. Trojan.PWS.Panda	1.28%
17. w32.Beagle.27136	1.25%
18. Exploit.IFrame.43	1.15%
19. W32.Beagle.pswzip	0.79%
20. Exploit.IFrameB0	0.72%

# FIREWALL OR UTM FOR LARGER COMPANIES?

*Ian Kilpatrick, Wick Hill Group*

*UTMs used to be the domain of smaller companies, but Ian Kilpatrick, chairman of security specialist Wick Hill Group, explains why UTMs are now a serious contender for providing firewall protection, and a whole lot more, for enterprises and larger companies.*

Unified threat management systems (UTMs) have been growing in popularity for the last few years. Traditionally, they have been widely adopted by SMEs, but larger companies and enterprises are now also deploying UTMs, appreciating the benefits they can offer.

UTMs are designed to provide a range of security solutions in a single appliance, reducing costs and simplifying the whole process of security systems management, reporting and installation.

The minimum requirement for a UTM, according to IDC, is a firewall, VPN, antivirus and intrusion detection/prevention. Super UTMs (sometimes called extended UTMs or XTMs) have, however, evolved from this to incorporate additional capabilities which can include URL filtering, spam blocking and spyware protection, as well as centralised management, monitoring, and logging capabilities.

There are many reasons for the growth in popularity of UTMs. Cost is a key issue, with common thought being that a UTM device can cost less than a quarter of the price of equivalent, individual point solutions. Simplified centralised management is a further reason for adopting UTMs. Having multiple security solutions in one appliance makes managing security overall much simpler, as well as enabling easier event consolidation.

Larger companies and enterprises are now also adopting UTMs because they have begun to appreciate the benefits of less expenditure and easier centralised administration. Large companies are typically using

UTMs to centrally secure branch and remote offices; or alongside their existing gateway firewall for the additional UTM functionality. Additionally, many companies are using UTMs as their main gateway security appliance for all functions.

Larger organisations using point solutions are often unable to scale the solutions to the number of sites they have, because of cost, installation, management, reporting and ongoing support issues. This can lead to organisations deploying reduced security and inferior policies at remote locations. UTMs can help overcome these problems.

Where companies use a powerful UTM as their main firewall and also deploy the same brand UTMs at branch offices, they have the big advantage of being able to manage and report on all their branch office security from one central location. This can give much greater control over branch and remote office security, simplify and improve overall company security, reduce support costs in areas such as patch updating, and reduce data centre costs.

UTM models are now available which are aimed specifically at larger sites, with the high performance and multi-gigabit throughput to deal with thousands of users. Such systems might integrate stateful packet firewalls with VPNs, zero day attack prevention, anti-spyware, gateway anti-virus, intrusion prevention, anti-spam, and URL filtering.

The recent importance of green issues is another reason UTMs are becoming more attractive to larger companies. UTMs integrate several security functions into one single appliance and this fact alone could qualify them to be 'green'. One single UTM appliance can replace up to five or six separate security appliances or servers. This saves space in the office and significantly reduces

ces power consumption, both in the rack and in the air conditioning necessary to cool multiple products. Given the increased pressure on data centres in relation to power issues, this is can be a key benefit.

A UTM could also be considered 'green' if it can easily upgrade to add more functionality and performance. This would allow a UTM to grow and change with a company's needs, rather than having to be wastefully ditched when it fails to cope with increased demands.

A stated disadvantage of UTMs over point solutions is that they have a single point of failure with all security systems potentially down at the same time and this would obviously be a serious problem for large enterprises. However, one additional appliance can provide failover protection for perhaps five key security functions.

#### Choosing a UTM

For any company looking at UTMs, it is essential to define requirements and thoroughly research the market, but going for an established name with a proven record in firewall security is a good way of establishing a shortlist. Bear in mind that there is no legal definition of a UTM and that there are significant variations between UTM appliances. The variations are on price, functionality, performance, scalability and most importantly security.

Not all suppliers provide solutions that are suitable for larger companies. Performance is a key element. Many UTMs aren't designed for all the functions to work together, so performance can rapidly decline when all functions are switched on.

You may want considerable room for growth or an appliance that is licence upgradeable for both performance and function. You'll also need a firewall that has deep packet inspection as a minimum, not just stateful inspection.

#### The future of UTMs

As businesses grow, their security platform will need to grow with them. UTM vendors such as WatchGuard and Check Point are now producing UTMs that will adapt to and grow with future security needs. Based on the knowledge that they will increasingly be fulfilling the needs of enterprises and larger companies, UTM appliances will be able to proactively adapt to dynamic network environments, as well as protect against unknown future threats.

UTM appliances will be interoperating in and supporting very mixed network topologies and have the inherent security technology to be flexible. Administrators will be able to pick and choose the security service they want from UTM devices.

#### Conclusion

Enterprises and larger companies are increasingly selecting UTMs as an alternative to firewalls and coupled with multiple point solutions. Costs savings, easier management and green credentials are just a few of the issues which make them attractive.

Powerful UTM appliances with high performance aimed at very large networks are now available. Future development will provide adaptability and future proofing which will help all companies protect in an ever changing and increasingly complex security environment.

