You May Think You Have Never Been Hacked...You Just Have Not Realized It Yet

Security Vendors are finally launching solutions that will help protect the SMB community from targeted and untargeted web attacks

Published: 25 Jun 2013
By Alexander Michael,
Director of Consulting, Information & Communication Technologies

I have been talking and writing for years about the need to protect intellectual property from cyber criminals, but I had actually never met a hacker... until three days ago, in the coffee shop at London City Airport, during a two-hour delay.

Out of boredom and frustration, the hacker showed me how – in just one minute – he could hack into the website of the destination airport, changing the way departure times were listed. I was shocked to see for myself how easy it actually is to compromise someone's website, and the well-known concept that we are all vulnerable, all of a sudden became very real, up close and personal.

My new hacker friend told me that the criminal hackers – or "Black Hats", as they are commonly called – run huge markets of information for sale upon request, and that most people whose confidential information is on sale do not realize that they have been hacked in the past, probably even several times. Cloud technologies, social networks and shared web hosting's make everyone vulnerable. A number of serious, recent hacks could have disturbing consequences far into the future.

On 21 February 2013, cPanel detected an intrusion into a workstation used by its technical service team. cPanel provides a web hosting control panel, used by thousands of web hosting companies globally. It gives server and website owners control over their information assets, providing simple and powerful web interface to manage website content, e-mail accounts and backups. Although, at the moment, there is no evidence that sensitive data or the actual database were compromised, the truth is that no one can know for sure. It certainly does not bear thinking about a single intrusion potentially exposing dozens of millions of websites around the world that are managed via cPanel. In the beginning of June 2013 an exploit was published for another web hosting control panel – Plesk - that allowed attackers to remotely execute arbitrary code on any web hosting that used Plesk, putting all their websites at critical risk

During the month of May 2013, it transpired that Twitter accounts are vulnerable. The Associated Press became a high-profile victim when a false tweet said: "Breaking: Two Explosions in the White House and Barack Obama is injured." The AP's Twitter account was suspended, and it advised its followers to ignore all tweets until further notice, but in the meantime the Dow Jones had plummeted 150 points. All was revealed and the markets quickly recovered, but in financial trading – where latency is measured in milliseconds – it is easy to understand how criminals can take home staggering profits, on the basis of a single bogus tweet. Twitter has been quick to react, tightening security, but what if many more Twitter accounts were compromised? What if the entire Twitter database was compromised and is now available on the black market? I asked the hacker's opinion about the compromised Twitter accounts. Based on his experience, he thought the concerns were definitely real.

LinkedIn was hacked exactly a year ago, in June 2012, and millions of user accounts were stolen. If Twitter and LinkedIn accounts are vulnerable then so are e-mail accounts. Last week (on krebsonsecurity.com), a thought-provoking writer on cybercrime, Brian Krebs, discussed the value of a hacked e-mail account, providing estimates of the black market "price lists" of e-mail accounts, asking the very pertinent question: "If your inbox were held for ransom, would you pay to get it back?". He pointed out how, until recently, some of the Web's largest providers of online services offered little security beyond a username and password.

However unpleasant the thought, we should never forget that Black Hats are all about money. They are highly skilled and trained, and highly motivated only by profit. Before vulnerabilities are publicly discovered and patches are released, bugs and zero-day exploits can cause a lot of information to be stolen, invisible to the victims. SMBs are just as vulnerable as large corporations – but they lack the resources to protect themselves – and they are more likely to use open source platforms (e.g. WordPress), which are vulnerable to many common attack vectors. A recent study by the security company Checkmarx shows that more than 30% of the most popular WordPress plugins have one or more critical vulnerabilities.

Often, a website is an open door to a company's IT infrastructure, including all corporate e-mails. Frost & Sullivan recently published a whitepaper on web application security (**http://www.frost.com/prod/servlet/press-release.pag?docid=265950808**), highlighting the damage that a vulnerable website can cause. In many cases, compromised websites result in emails and other valuable digital assets being compromised. Entire e-mail archives may be stolen, for example, and that may seem harmless, because it is old information, but e-mail archives will invariably contain recovered password to other resources, like social networks or internet banking, allowing countless new attacks to be perpetrated. Also, a lot of people rely on their web e-mail accounts as a form of cheap cloud-based storage. It is a big mistake to assume that an e-mail account will be safe, just because it is delivered by one of the World's top e-mail service providers. Not realizing how easily an e-mail account can be compromised, people lay themselves and their customers open to unspeakable damage.

Frost & Sullivan strongly believes that organizations must maintain a holistic view of their vulnerabilities and that some of the most important innovations of the next couple of years will take place in the vulnerability management space. We gave our 2011 Award for Entrepreneurial Company of the Year (**http://www.frost.com/prod/servlet/press-release.pag?docid=234804194**) to VUPEN, in recognition of how it has positioned itself to provide advanced and reliable vulnerability intelligence for chief security officers, security professionals and their respective organizations. Because of the dynamic nature of information security, vendors with a strong entrepreneurial drive are best placed to fill the gaps in the security market, as these gaps develop.

Another entrepreneurial, innovative security vendor to watch is High-Tech Bridge. Early in 2012, High-Tech Bridge gave Frost & Sullivan the first briefing about its development of ImmuniWeb® (**https://www.htbridge.com/immuniweb/**), a pioneering web application security assessment concept which supplements automatic vulnerability scan combined with manual web application penetration test in parallel. In December 2012, the up-coming launch was publically announced, and on 15 May 2013 ImmuniWeb was launched in a way that would enable SMBs to configure and order assessments online, in just 15 minutes. Until I have seen it tested against substitute solutions, I only want to be cautiously optimistic, but it certainly appears that the hybrid approach, introduced to the global market by ImmuniWeb, represents a highly efficient, new generation solution for SMBs, offering speed, simplicity, cost-effectiveness and additional quality, afforded by the parallel manual penetration testing.

The basic concepts of speed, simplicity and cost-effectiveness are catching on, and several other security vendors have been taking up this particular challenge. Express Lite for Small Businesses (**http://www.qualys.com/company/newsroom/news-releases/uk/2013-06-10-qualys-introduces-express-lite-for-small-businesses/**), introduced by the well-known security company Qualys little more than a week ago, on 10 June 2013, promises to bring the "Power of the Cloud to SMBs with Easy-to-Deploy, Affordable, All-in-One Security and Compliance Solution." Although Qualys' Express Lite is not a hybrid solution, it does addressing the SMB need for simplicity, doing away with paperwork, enabling small companies to process everything online. Its entry-level price of $795 certainly makes it affordable to SMBs. Qualys is highly regarded in the security industry, and the many basic free tools it makes available to the SMB community are helping to educate IT decision-makers with limited resources about the seriousness of information security and compliance.

An example that the mainstream security industry is beginning to take web application security seriously has come from Trend Micro, one of the World's leaders in antivirus software. A series of acquisitions during the past 5 years clearly show Trend Micro's ambition to break the antivirus mold and become an end-to-end security company. Little more than a week ago, on 11 June 2013, Trend Micro announced the pre-launch of its Trend Micro™ Web App Security (**http://webappsecurity.trendmicro.com/**), a comprehensive offering which duplicates the hybrid approach previously introduced by ImmuniWeb. Although the global roll-out of Web App Security will not take place until next year, it is clear that the larger security vendors are waking up to the needs of SMBs, and that is hugely positive.

Despite the recent positive moves by the security vendors, I unfortunately believe that hackers will always exist, and that even the security vendors themselves are vulnerable. Several days after the Trend Micro™ Web App Security pre-launch, one of the oldest and most respected information security communities @attritionorg (**https://twitter.com/attritionorg/status/345330064562454529**) tweeted a couple of pictures of a Trend Micro website which had been shown to be vulnerable to Cross-Site Scripting (XSS) attacks. Another tweet (**https://twitter.com/attritionorg/status/348202970296496130**) later demonstrated that the Web App Security is running on the WordPress platform and had a publicly exposed admin panel. That is an unsubtle message to the security industry that it needs to take its own medicine and that the security industry must continue to innovate and be on its toes constantly.

Organizations need to realize that websites are not just websites. Businesses have a fundamental dependence on their websites, and a compromised website can destroy a healthy business in no time at all. Security needs to be an integrated part of everything we do – not an afterthought – and everybody must understand risk and change their behavior accordingly.

I have every reason to believe that Black Hats are also skilled librarians, able to cash in on the seemingly worthless information stolen years ago, which becomes priceless when a person becomes famous. There is not a lot we can do about the ticking time bombs of e-mail archives that have already been stolen, but we can absolutely make sure that web vulnerabilities are discovered and eliminated.

Innovative and creative approaches to security, like ImmuniWeb's hybrid assessment, are essential. By continuing to innovate, I hope that the security industry will bring some peace to the many SMBs worried about their confidential information.