Product Review

of

SecureLive Website Security

Cyber security is a popular topic in both Hollywood movies and in the Beltway through the appointment of Jeff Moss aka "Dark Tangent" of Both Defcon and BlackHat fame[1] to Homeland Security . Additionally there is NO shortage of security products available for the many devices, sites and other gadgets of modern life. One would think that with all the security products available, there would be no place for a cyber criminal to hide. Think again - they are hiding in desktops, servers and mobile devices worldwide. In actuality, the criminals are getting smarter and your site is likely a target. As a site owner or administrator, your top priority should be security of your digital border above profit, clever content or Search Engine Optimization. Without security, you won't have a safe site.

Today's posting is a review of a new websecurity offering known as SecureLive, from SecureLive.net.The product suite, according to the companies website "*Blocks attack attempts first AND alerts YOU and our LIVE admin in real-time. During blocking and alerting, the system also records vital data about the attacker including attack strings used, geo-tracking and other information that cannot be disclosed in this article due to patent disclosure*."[2]

I took the opportunity to give the product a test drive, evaluating how it responded to various attempts to break in, probe and footprint the site in question. In this article I'll discuss this and at the end my thoughts on the service and my recommendation.

Background

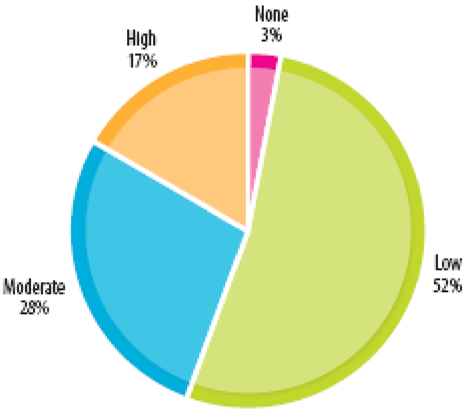
[1] http://www.wired.com/threatlevel/2009/06/hacker-dark-tangent-joins-dhs-security-council/
[2] http://www.securelive.net/index.php

Given that true information security is largely ignored, or people are simply uneducated, I thought it would be helpful to present a few facts from a recent report by the Verizon Business Risk Team[3]entitled, "2008 Data Breach Investigations report."

Most site attacks take very little to NO effort to break in. In fact, in the Verizon study, the level of difficulty was broken down as follows[4]:

- None—No special skills or resources were used. The average user could have done it.
- Low—Low-level skills and/or resources were used. Automated tools and script kiddies.
- Moderate—The attack employed skilled techniques, minor customization, and/or significant resources.
- High—Advanced skills, significant customization, and/or extensive resources were used.

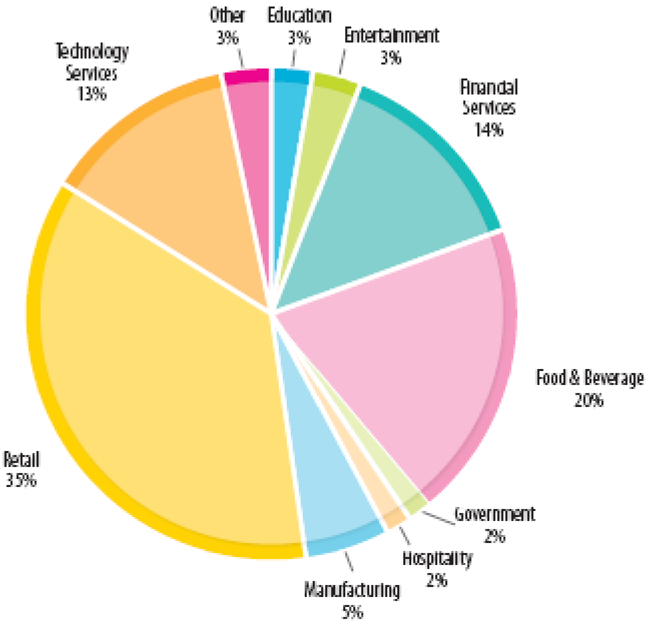
This translated in their case study, conducted for four years and over 500 forensic engagements to this graph:



Source: Verizon Report - Page 18

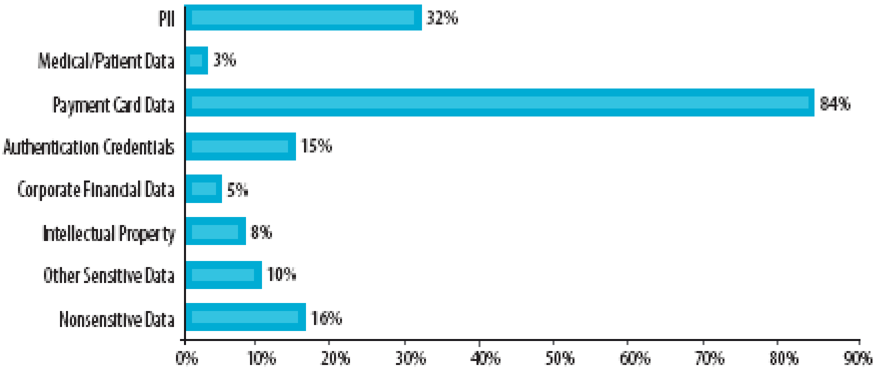
Yes - you are reading that right 3% takes NO knowledge, 52% takes a LOW amount of knowledge -let's see, basic math, that's right at 55% of the attacks they reviewed, took little or no special knowledge. To put that in context, the types companies according to Verizon were as follows:

[3] http://www.verizonbusiness.com/resources/security/databreachreport.pdf
[4] Verizon report - Page 17



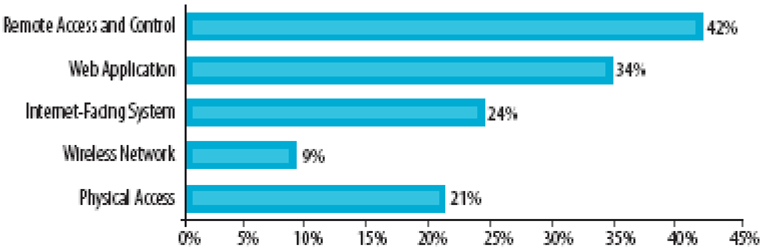
Source: Verizon Report - Page 8

The types of data that the bad guys were after is well, easy to guess:



Source: Verizon Report - Page 21

And the report goes on to cover the who, what, when and so on, but the last and most important fact they presented was that the second most attacked area of sites are through the web application itself:



Source: Verizon Report - Page 19

You are encouraged to read the report at your leisure, as it contains a great many facts and details pertinent to staying secure. Suffice is to say that small amount of the report tells us that many different sizes and types of companies are easily breached by easy to obtain, simple to use 'attack-tools.' If they are vulnerable you can bet you are likely or will be soon.

***Disclaimer: Entering a computer network or system without permission is a Illegal Act. These tests were performed with the site owners permission and cooperation. Neither the author nor this site supports any illegal activity.**

Intro to the attack

Before starting an actual attempt to break through this servers defenses, we needed to understand what we were dealing with. We did a number of passive tests, that did not alert anyone. These included, browsing the site with my XP box running FireFox. This gave us an idea of how the site was laid out, what it was built from and so on.

During this we quickly discovered it was a Joomla 1.5.x based site running a plethora of extensions. Some we knew, some we didn't.

We Googled and checked a few databases to establish as much as we could passively about our target.

Out of this effort we knew the IP, the owner, where it was hosted and where the DNS server was located. None of this would alert anyone to any wrong doing.

Knock - Knock -

We used a basic IP scanner to confirm the presence of our target, then moved to a more advanced scanner to gain a deeper understanding of it. Out of this part, we did not set off any alarms and found some very interesting ports opened, that we would attempt to exploit as part of the test.

Gaining that traction we then moved up to a direct SQL attack on the machine -- hitting a component that did not exist on the site. I wanted to test the 'alertness' of the software. It did not trigger anything -but that is what I would have expected - it in essence ignored my feeble attempt on attacking a non-existent component.

Next up - I thought - we need to know more about this machine and its OS. I used a GNU/GPL vulnerability scanner, and ran it against the site. To my surprise, I found the KangA virus on the machine. I laughed to myself, thinking I have a back door - but why? That's a Windows type virus. Then I realized I mistyped the domain by one letter. I had scanned a domain with an almost EXACT name. -- DOH! - [*This is an interesting dilemma though, had I been a real - cracker (attacker) I would have stumbled upon a easier target and likely would have gone on.*]

Rescanning I did not see any compromises, yet I found a couple of items that needed patching, but nothing to really sneak around the software with. What was interesting is that I did not set off any warning bells with the Software (*this has been disclosed to the* *vendor already and a very satisfactory explanation to me was given - so no worries mate*).

I hopped over to my CentOs Linux box, and attempted a few "cheap" hacker tricks - which of course failed, and did not set-off any alarms.

That settled it - I pulled out a commercially available Cross Site Script and SQL Injection testing tool to find any weaknesses in the site.

Test started --- and kept, going, and going...ooops.. I was caught!

SecureLive detected my attempt to run a SQL Injection and a XSS against the site. All of the sudden my other (windows) box could no longer reach the site - 404 Page not found...hmm...Jumping over to the Linux server on a different network - no problem. SecureLive stopped me.

Wow - I was effectively dead in the water unless I wished to move to another location with a different IP. SecureLive stopped me and blocked me from even seeing the website. Wow!!

And that your honor is how it happened...

After the test, I spoke directly with Mr. Jeff Brown, CEO and Founder of SecureLive. We swapped stories about our Tandy/ TRS-80s, and programming in GW-Basic, and the "good-ole" days. Then I disclosed all the tests I had ran; why things behaved the way they did and so on.

Without further delay - here is my opinion.

Web Security is often viewed as "their" problem. Host's see it as the website owners problem- its up to you to keep your site safe, the website owners see it as the host or the OS, or application providers job, and so on. Much like the childhood tale of the Little Red Hen - everyone is always "too busy" - let someone else deal with it.

One thing I must emphasize, you should not depend solely on any single security device or platform to guard you. Defense in layers is the right way to protect yourself. This starts at the HOST and *their* perimeter protection with Firewalls, NAT and other assorted systems. Then it moves inward to you and from there you have the responsibility to maintain your website and possibly the Operating System by staying on top of patching. Software doesn't suddenly go bad, it "rots". In other words, secure software today is the vulnerable software tomorrow. Adding SecureLive to your website is a strong inner defense.

As I stated at the beginning of this article you should put your sites security as the TOP and most well funded priority
that will easily pay for itself by *stopping* a loss of revenue.

Let's reason together, say you take credit cards online, and you are hacked. The press finds out, your loss of business is immediate and then of course the potential fines and legal action. Is security still to costly?

SecureLive is a Premium product that offers more value than you are paying for. With the rise in Cyber Crime, and the sophistication of the attacks and the tools, any serious site owner, who depends on their website for revenue should not be without this product guarding their site. It's simple to install and is monitored as part of the SecureLive service. Should an attacker reach a certain threat level, the "host" of the IP is notified allowing them to take action at their end of the wire, to shut down the bad guys..

What I really liked during my conversation with Mr. Brown, was the under the covers look at the technology. He has developed a very robust and powerful system, that has the flexibility to change and grow as the threats to your site will inevitably change and become even more powerful.

Point your browser over to www.securelive.net and buy it today and start being part of the solution to e-crime rather than a victim.

About the author:

Tom Canavan is author of Joomla! Web security, available from Amazon and a must read for any website administrator, not just Joomla! sites. He has been in the Computer industry for 24 years, and is most recently the former CIO of a large .dot com based in Texas.

He offers a full security service available at joomlarescue.com for diagnostic checks and removal of the bad guys. Use coupon code "compass" and get $200.00off of Health Check two.