

ThreatRadar with Eldad Chai:

Listen to Podcasts: <http://www.imperva.com/resources/podcasts.asp>

Brian Contos: Welcome to the Imperva Security Podcast. I'm Brian Contos, Chief Security Strategist for Imperva. Joining me today is Eldad Chai, Imperva Product Manager. Welcome to the show, Eldad.

Eldad Chai: Hey, Brian. Good to be here.

Brian Contos: Eldad, before we get going, I know we're going to be talking about ThreatRadar today, but please give our audience a little bit of background on yourself and exactly what it is that you do here at Imperva.

Eldad Chai: Sure, Brian. I'm the product manager of Imperva, for the web applications firewall, or, in short, our WAF. And what I do at Imperva is define the strategy and roadmap for the solutions.

And just a brief overview: Imperva WAF helps organizations protect web applications and business data from external threats. And it's positioned in the organization's perimeter and blocks attacks on internal or external web applications and prevents sensitive data leakage. And the WAF also helps organizations to be compliant with data security regulations. For example, PCI DSS where it covers the criteria related to application security.

Brian Contos: As I mentioned a little bit earlier, today we're talking about a new capability called ThreatRadar, which, of course, is associated with web application firewalls. So, I guess, the most logical question: what is ThreatRadar and how does this extend the capabilities of WAF?

Eldad Chai: So, ThreatRadar is a new offering by Imperva, and we're really excited about it. It's something new in web application security, and we think it can bring a lot of value to our customers. ThreatRadar is being launched during the RSA Conference (San Francisco 2010).

And what ThreatRadar basically is, is it's a new add-on for Imperva WAF. It provides automated near real-time and adaptive defense against large-scale industrialized cyber attacks. It's based on a reputation technology. And what it can do, it can track attacks on a global scale.

So it has a global perspective on the Internet on the malicious activity that is happening. And based on that, it provides continuous feeds for the WAF and automatically adjusts security policies to block attacks from identified threats.

What ThreatRadar actually does, it allows stopping attackers early before they can reach the web application. And it does that by identifying these malicious sources and this malicious activity, again, on a global scale based on what is happening on other web applications.

On top of that, ThreatRadar provides analysis and forensics tools based on source intelligence that actually takes the guesswork out of security events analysis. You can know, with ThreatRadar, who is sitting behind the computer and executing these attacks or this traffic to your web application.

Brian Contos: So, if we were to put, in a nutshell, the top one, two, or three things that really separate ThreatRadar from what existing WAF capabilities offer, such as dynamic profiling, and user session reconciliation, and blacklists, and white lists, and correlation-all these great things, in a nutshell, what are the top things that ThreatRadar will bring?

Eldad Chai: I think what is special about ThreatRadar is that it can react very quickly to the threat landscape or, as we like to call it, the "threatscape," and make sure that you are always protected from the current threats.

So definitely, the more reactive tools like signature and correlation rules which examine traffic and, based on that, decide whether it's malicious or not, ThreatRadar is proactive. This is the main difference. It goes out there and it identifies the threats to your web application before they can even reach you.

So you can imagine, then, your security or your perimeter as your fortress. You put bars on the windows, you build the high walls, you put a security guard in the front-all that to prevent attackers from executing attacks.

What ThreatRadar is it's actually handing your security guard a book with the pictures of all the bad guys. So these bad guys can't even reach your fortress because the security guy knows who they are. It can prevent them from even reaching your web application.

You know sometimes hackers, they don't attack in the first visit to the web application. They do some preliminary scanning. They do some recon activity to collect data so they can execute that attack later. With ThreatRadar, you are also protected from these activities, actually stopping the attacker on the first time he enters the web application.

Brian Contos: So, you mentioned something very interesting about the threatscape. And we have been talking about this for some time, this evolution of the threatscape and how attacks have changed. Why is ThreatRadar such a critical capability today?

Eldad Chai: Over the recent years, our research team, called Application Defense Center, which actually does all the research on web application security that we eventually build into our product. So they were doing their regular research and they have identified a substantial increase in automated attacks against web applications.

These kinds of attacks, it's not a human sitting behind the traffic. It's either a bot and it's coming from an anonymous proxies --these are actually software programs that attackers write in order to attack web applications on the large scale.

And there is one very famous example I think everybody knows. This is the mass SQL injection attacks happening throughout the past three years and actually taking down thousands of sites with SQL injection vulnerabilities. These are bots, bots that automatically identify the targets and automatically hit them. Another example is the increase in denial-of-service attacks, or distributed denial-of-service attacks, again, aimed on breaking web applications.

So looking at these attacks and the hackers' ability to quickly shift locations and attack techniques, Legacy quickly understood that in order to fight automation, you must use

automation. There is no manual way to deal with these kinds of attacks. And we see them taking a real large part of the threatscape today. So ThreatRadar is built for that. It's built to be fully automated and it's built to be adaptive and designed to deal with such attacks.

And you can think about it as thousands of sensors scattered around the Internet identifying malicious activity. ThreatRadar consolidates all of this information and makes sure that our customers are protected from these kinds of threats.

Brian Contos: That's very interesting. I think we understand at a high level now what ThreatRadar gives customers, but let's get to the nuts and bolts of it.

I have an Imperva SecureSphere Web Application Firewall, or I'm thinking about buying one. I want to leverage ThreatRadar. What exactly will it do, and how does it work, and what will it give me? What are the real deliverables I will see as a user of the product?

Eldad Chai: ThreatRadar services cover a couple of threats. It's built on five types of services. The first is malicious sources. These are traffic sources that have repeatedly performed malicious activity on other web applications. Again, for example, the 10 million bot-nets active every day.

The second type of service is anonymous proxies. These are traffic sources that use anonymous proxies to conceal their identity. This is usually an indication to malicious activity.

The third service is the Onion router network that is called the TOR Network. Again, the TOR Network is some kind of an anonymizer. It's usually used by hackers for all kinds of automated attacks like common spam, or web email spam, or click fraud.

The fourth service is phishing URLs, which provides our customers with real-time indication on phishing activity on their domain. So if one of their customers is a victim to phishing incidents, they are going to be notified in real-time.

And the fourth element of ThreatRadar is the IP forensics tool, which allows you to analyze security events based on source intelligence. So that is what you get with ThreatRadar, all these five services.

And what really happens in the web application firewall is that the WAF opens a direct connection with the ThreatRadar servers and there is a continuous feed of data about these threats and malicious sources streaming to the WAF in a near real-time manner. So ThreatRadar collects that data and feeds that to the WAF, and then the WAF adjusts their security policies based on that data on threats.

So all security rules are always aligned with what is going out there. What is the threat and what do we need to stop to make sure the web application is secure?

Brian Contos: So it sounds to me the bad guys are using the power of the Internet-Google searching capabilities, anonymous proxies, and TOR Onion routers, et cetera. They're using capabilities out there to launch the attacks.

And it's almost like the defensive mechanisms are leveraging the same capabilities, but for purposes of good to sort of take this global perspective and understand what is happening on the rest of the Internet to protect the individual's web application or the individual's organization.

ThreatRadar with Eldad Chai

Is this something that might also be related to help prevent and/or detect business logic type attacks, as well? Are we seeing industrialized hacking attempts and automated attacks going after these business logic flaws, as well?

Eldad Chai: To your first point, and you are exactly correct, we need to fight fire with fire. And that is the only thing that will do the job. Regarding business logic attacks, it definitely happens in some cases.

So if you take, for example, business logic attacks around scraping, when someone systematically downloads all the web application content to use it in its own business, definitely ThreatRadar will be able identify these scraping activities and then protect your web application from them.

It's not true for all types of business logic attacks, but what we identify is that in many types of business logic attacks, like a Brute Force, some spam, web email spam, there is a great amount of automation involved. In these cases, ThreatRadar will definitely be the right countermeasure.

Brian Contos: Fantastic. Well, Eldad, thank you so much for your time today.

Eldad Chai: Thank you, Brian. I was happy to be here.

Brian Contos: If you would like to learn more about this subject and Imperva, please visit <http://www.imperva.com> or send us an e-mail at blog@imperva.com.



Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004