WhatWorks:
Blocking Complex Malware Threats at Boston Financial

with

WhatWorks is a user-to-user program in which security managers who have implemented effective internet security technologies tell why they deployed it, how it works, how it improves security, what problems they faced and what lessons they learned. Got a story of your own? A product you'd like to know more about? Let us know.
www.sans.org/whatworks

About Boston Financial Data Services, Inc.

Boston Financial Data Services, Inc. is one of the industry's premier outsourcing providers servicing the financial marketplace. Founded in 1973, Boston Financial is a joint venture between DST Systems, Inc. of Kansas City, MO. and State Street Corporation of Boston, MA. The joint venture has enabled Boston Financial's clients to utilize DST's industry-leading software and technology while benefiting from the institutional support and global reach of State Street. For more information, visit www.bostonfinancial.com/fia.

About the Users

Mike Rizzo is the Chief Information Officer and is responsible for the Global Information Technology Strategy for the International Financial Data Services (IFDS) and Boston Financial entities and the Business and Technology Services team at Boston Financial. He has over 30 years of domestic and international experience in the technology field, with an extensive background in managing technical environments, people, and projects.

Yalmore Grant, Information Security Officer, is responsible for the security program and oversight of all security initiatives at Boston Financial.

SANS Summary

Concerned with the ever-increasing complexity of malware and the high rate of user-targeted attacks, Boston Financial's security team began to investigate additional options for end-point security. The new solution needed to combat all types of user targeted attacks from spear-phishing, to watering hole attacks, to drive-by-downloads. It needed to stop attacks without the use of signatures, have a low rate of false positives and couldn't impact employees' job performance with unnecessary security procedures. Boston Financial implemented Invincea's Enterprise Edition, version 2.4.1, to its entire base of more than 2,000 employees. The company found it very effective in stopping incidents at the endpoint, and has found Invincea's tech support team to be a very responsive, committed and partnership minded In helping to hardening the Boston Financial environment.

~~~~~~

Interview

Q: What prompted you to look at proofs of concept for moving beyond antiviral endpoint security?

A: I generally pay attention to the security environment because of my natural curiosity. In multiple conversations with the security officers, in paying attention to attacks detailed in the news, reading trade industry information, etc. I tended to agree with the thinking that the end-point was becoming more and more important as the complexity and volumes of malware and the creativity of the malware developers continued to increase. Eventually, some of this was going to slip through whatever we put in place so we needed better end-point protection at the desktop. The security officers then brought the Invincea product to my attention and it seemed to be a move in the right direction.

“Invincea support has been great. They are a really good team and they've been very responsive and great to work with.”

Q: Since you're the CIO, did you have money in your own budget to fund this? Or did you have to get additional money?

A: I had money budgeted for information security tools that were as yet undefined simply
~~~~~~

because the environment is changing so quickly. It's not always prudent to name a tool that you later don't use, so we had some money that was set aside for tools to be developed. The first proof of concept certainly was well within the budget that I had available. We looked at our broader rollout, and by the time we got to that point I knew what was coming and we had budgeted for that tool.

Q: Did you look at more than one solution, did you set up any criteria for success? How were you going to know whether it worked or whether you should move forward?
A: We looked at some alternatives in this space but they weren't for us. They required far too much computing resources and weren't as flexible as Invincea. We did set up some criteria, but the malware stuff is really hard to measure because you don't know what you didn't catch. We wanted to see that there were significant numbers of incidents that we were able to trap at the desktop and isolate without having a huge number of false positives. We wanted to be able to prove that it was actually catching things that are real and not just making a nuisance of the desktop and making it difficult for people to work. One of the criteria was that we couldn't impact people's day-to-day jobs in terms of making them go through things that were unnecessary in the name of security.

Q: I assume you have some sort of anti-viral end-point protection suite that was already on your PCs. Did you add Invincea to the mix and then look at what it was seeing in addition to what your other suite had been doing?
A: Yes. When I talked about it catching things at the desktop that we would not have otherwise seen, they were not false positives. The anti-virus tools do not stop spear phishing or watering hole attacks. With Invincea, it was clear that URLs that were providing a gateway to access malicious downloads were now being denied and the user browsing environment was being rebuilt without any requirement from the user.

Q: How did you get started? Did you have a prototype or a test bed?
A: We implemented it on a test bed of desktops. We first rolled it out mostly to our technology desktops, people within my organization who have a little more tolerance for interruptions than some of the business folks. We installed it on probably 30 to 50 desktops within my team, did some tracking, ran into a few issues that you would find normal in an early release and worked really closely with the Invincea folks. Our on-site team is great and helped us resolve all those issues and get things rolled out. We slowly increased that number and eventually completed the full rollout earlier this year.

"We are stopping more (bad) things at the desktop than we have before. Invincea is performing well."

Q: How long did it take to move from your initial prototype rollout until going to full production rollout?
A: I would say it was probably 12 to 13 months that we were playing around with it by the time we got to final implementation.

Q: How do you manage the use of Invincea?
A: It's managed locally by our information security staff. We have a very close relationship with the Invincea folks; they're here in Boston regularly checking in on us, making sure things are working okay and talking about upgrades. We manage it with them.

The product itself is installed on a central management system with all administrative and forensics information available. The Information Security team is responsible for managing the logistics of the product.

Q: When an employee joins Boston Financial, is Invincea part of the standard desktop image that rolls out to all new desktops?
A: Yes, it is.

Q: Since it is being managed by the same people, is it just part of their duties now or did you have to add any full-time staff or anything for dealing with it?
A: No, actually we did not have to add any additional staff. The volume of log information is growing significantly and very quickly. We're looking at alternative ways to evaluate the logs to trend and correlate information and threats, but you can't attribute that to Invincea. It simply contributes log information.

Q: Do you have security information event management that you feed all your logs to or how are you doing that?
A: We're in the process of outsourcing that as a managed service. We've been doing it ourselves, but in lieu of hiring a couple of FTEs to do nothing but sit down and review logs, we're going to outsource that as a managed service.

Q: Has there been a lot of ongoing tuning where you change it so the users see less or it stops less? How's that going?
A: Generally it's gone pretty well. We work very closely with the Invincea folks; they're here fairly regularly chatting with us and going through upgrades and implementations. We've tweaked it a little bit; occasionally we see a potential performance issue that once investigated, it turns out to not be Invincea, but rather a website the user was trying to visit. I think the product is performing well enough to the point where it's just going to fall into part of the normal routine and people won't even notice it anymore.

Q: Can you give me an idea of the scale of your deployment? Roughly how many desktops is it on and how many will it ultimately be on?
A: Roughly it's on 2,000 desktops today and ultimately it could be 2,500 or potentially more, depending on activity. We have a couple of offices that are hosted on a different network from one of our parent companies, but we're not in control of the desktops at the moment.

“Invincea is a forward thinking group of folks who have a really good handle on what's going on in the security space.”

Q: You said a couple times the ongoing support from Invincea was very good. You've been happy with that?
A: Absolutely. The guys have been great. They are a really good team and they've been very responsive and great to work with.

Q: Are there any features or requirements for the product you'd like to see it have that you've given to them and are hoping to see in the future?
A: In the future, there are a couple of areas that could be developed further. I would like to see a better backward compatibility functionality of the Invincea browser with the native browser. Better error reporting methods would also be very helpful to shorten our response/react times.

Q: What were the criteria for success? Do you have any metrics on what this is finding and allowing you to stop or limit damage?
A: We are stopping more things at the desktop than we have before; we're identifying more. Our main concern was the number of machines that we had to remove from the network due to infections. We were not able to clean those machines because of the variations in the types of infections that were found. Prior to Invincea, we were averaging four machines per week with disruption to the user of an average of 3-6 hours, the improvement has been significant. Invincea has helped us stop a number of incidents that could have been severe.

Q: Is the money you're spending on Invincea replacing anything else or this is giving you added security?
A: It started out as added security. We had several independent tools that were installed performing different functions, whether it was an IDS/IPS, a firewall, or a secure gateway, or a desktop product or anti-virus, but there wasn't a holistic approach. As we go forward we're reevaluating the desktop security environment. We need a more holistic approach that can help us cross correlate the threats that we find at the IPS point as well as the desktop point and make some sense out of whether they're connected. In the future we will probably reduce the number of tools that we have and work with the ones that can work more holistically in addressing the issues; based on what I've seen, Invincea is one of those.

"We want tools that can work more holistically in addressing the issues; based on what I've seen, Invincea is one of those."

Q: Is there anything that you'd like to add?
A: Invincea is a forward thinking group of folks who have a really good handle on what's going on in the security space. I'm very comfortable working with them as a team. Beyond implementing the product here, I know that they're committed to taking our feedback and making the product better to help us get a more hardened environment here at our shop. They seem to have a good vision of the future in this area and we are looking forward to moving forward with them as a partner.

Q. Would you recommend Invincea to your clients?
A. We aren't in the business of making recommendations. With that said, our clients want to know what we are doing from a security perspective to protect their information. We mention the Invincea concept and our clients love the idea and want to know more. We stop short of a recommendation, but do tell them to take a very strong look at this – it is working for us.

SANS Bottom Line on Invincea products at Boston Financial:

1. Effective solution for preventing endpoint security incidents;
2. Stops attacks that are prevalent today – spear-phishing and watering holes – and that bypass other network endpoint security technologies;
3. Low rate of false positives;
4. Doesn't negatively impact employee job performance with unnecessary security procedures;
5. Very responsive tech support committed to adding requested features and strengthening the client's environment;
6. Fast deployment scale in comparison to other types of technologies.

Visit: www.invincea.com
Phone: 1.855.511.5967