ceocfointerviews.com

Issue: July 3, 2017

CEOCFO Magazine

Using AI, Behavioral Analysis and Predictive Analytics to Deliver Cybersecurity and Protect Customers from Malware and other Malicious Attacks with their 24/7 365 Monitoring System

Richard Malinowski
Founder, President, Senior Enterprise Architect

REMTCS, INC.
https://www.remtcs.com

Contact:
Richard E Malinowski
201-274-5000
rmalinowski@remtcs-secure.com

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

"We can detect known malware but also unknown malware (known as zero day attacks) in 15 seconds to 2 minutes (somewhat longer for more sophisticated malware and variants), and we can typically remediate the malware in 2 to 15 minutes."
- Richard Malinowski

CEOCFO: ***Mr. Malinowski, what is the philosophy behind REMTCS?***
Mr. Malinowski: Our philosophy is based upon the widely accepted industry fact that over a million pieces of malware are being produced daily which undetected and unresolved creates complex system vulnerability issues. Accumulatively, this results in 273 to 365 million possibilities of system penetration. We believe the required solution is a fully integrated and autonomous end to end system including an EndPoint solution that incorporates Artificial Intelligence (AI), behavioral analytics, supercomputing, and up to the second threat information data. The benefit from our solution is that it provides, in near real time, the ability to predict, detect, contain and destroy malware across the entire enterprise in lieu of traditional solutions which take upwards of 273 days to detect and secure an enterprise against a specific piece of malware. Given the volume of malware being produced daily, the task of effectively combating the malware can be overwhelming if not done daily (in near real time) and thoroughly.

CEOCFO: ***Lots of people are looking at the problem and attacking it. How do you go about using the elements at your disposal to stay ahead or even up to date?***
Mr. Malinowski: Automation within our unique approach is key versus the traditional highly manually intensive process in combating malware. We are breaking the malware paradigm through the combination of AI, behavioral analytics, supercomputing and up to the second threat data with an EndPoint product in a complete fully integrated end to end solution, from the network to the desktop, smart phone, tablets and laptops, enabling us to not only detect known malware but also unknown malware (known as zero day attacks) in 15 seconds to two minutes. Our capability to do this in the rapid timeframe is based upon over 70 patents combining all of the critical elements of our technology.

CEOCFO: ***Would you explain how it works?***
Mr. Malinowski: Imagine you download a piece of malware and do not know it is malware. Our solution continuously monitors your enterprise 24 x 7 x 365 and we deep inspect every single packet of data crossing the network. As this malware is transiting across your network we stop and examine it and if has any characteristics of malware, we run it in a sandbox (a safe zone to examine the malware). Once we run it in the sandbox, we can detect whether it is in fact malware and if it is trying to connect to a remote server or hacker. We then proactively initiate a kill command for the malware. We are utilizing a high performance computer as an appliance to do this. Additionally, after we identify a piece of malware, we create a signature and then generate anywhere between five to eighteen possible and highly probable variations of that malware. The additional signatures are added to our centralized threat database. We are not only detecting the malware in its present form, we are also calculating what its future generations could conceivably contain or look like.

CEOCFO: ***Are people skeptical?***
Mr. Malinowski: No. Given the high volume of malware, organizations are desperately seeking any advantage they can obtain to help their understaffed security teams catch up to or possibly get in front of the malware war. Most of the competitors in the market place are offering singular solutions ("One Trick Ponies). What we have done is to approach the malware problem from a completely clean slate. Most state that they have a real time solution, but the truth is nothing is in real time- https://www.brighttalk.com/webcast/14723/263399?utm_campaign=knowledge-feed&utm_source=brighttalk-portal&utm_medium=web. We are able to complete our process within fifteen seconds to two minutes which we define as near real time. We have the ability to detect the malware, and many folks say they do that, but we also have counter measures to go out and destroy it. We have a fully integrated EndPoint solution on the front end as well. To be more succinct we have the ability to spawn a search and destroy action at any time (User definable). When we find something particularly insidious, we know where it went as we have captured the IP address and the MAC address of the computer hit by the malware, we can go out and do an immediate scan within seconds to go find and destroy the malware on the infected machine as well as all other endpoints.

CEOCFO: ***If you discover a piece of malware for a customer, does that malware go on to your "bad list" for all of your clients?***
Mr. Malinowski: Yes, but we do not attribute any piece of found malware to a specific entity. As new malware is discovered, or variants are discovered, we update our centralized threat information database and then we push that out to every client on a continuous basis. This is all happening in near real time.

CEOCFO: ***What types of companies are using your products today?***
Mr. Malinowski: We have customers from various industries ranging from financial service firms, to defense contractors, and large global internet providers. We are currently working to form a joint venture with a large insurance firm to create a specialized cyber insurance exchange, whereby our technology will be used to protect participants thereby reducing their cyber insurance premiums. Additionally, our solution has been discussed as the primary means to protect power grids and IoT installations from malware attacks.

CEOCFO: ***When you are able to talk with the right people at an organization, is it an easy concept for people to understand?***
Mr. Malinowski: It depends upon the size of the organization and their level of sophistication. In larger organizations that have been dealing with this issue for years they immediately understand our value. Because we are protecting and mitigating the effects of malware across the enterprise in near real time, our customers have told us they experience a significant reduction in the time their security teams spend on chasing erroneous security alerts. In fact, we have been told that we are a force multiplier in that we provide an extra five full time equivalents to their security staff for a medium sized organization and even more for large organizations. We have calculated that the ROI for our solution is under nine months and most see that right away.

CEOCFO: ***Is it getting easier to defend an attack?***
Mr. Malinowski: No, in fact it is getting much harder. This is due in large part to the fact that there is tremendous profit in hacking and specifically ransomware. Ransomware alone has been reported to be a multi- billion dollar business. You are also seeing that with state sponsored attacks there has been a loss of Intellectual Property (IP) across the United States over the last ten years. We have lost a significant amount of our IP. The attacks are getting more ingenious and more frequent and there have been multiple vector attacks inside of one package. Due to the increased complexity of these new multi vector attacks, more processing power is required to identify the risks. Thus, we use the power of a super computer appliance that we produce.

CEOCFO: ***What surprised you throughout the process of developing the concept and evolving the company?***
Mr. Malinowski: Fortunately, we have been in the right place at the right time. I think the evolution of this company was based upon a lot of knowledge of financial services, analytics and quantitative analytics and different products. It is also based upon knowledge gleaned from biotech and pharmaceutical. Persistency to provide the best solution possible has been evolutionary and spurred by the increasing sophistication of the possible attacks.

CEOCFO: ***Why choose REMTCS?***
Mr. Malinowski: We can proactively predict, detect, contain and resolve malware attacks in near real time. While others claim they can do this, we are the only ones who have backed up our claim with numbers in terms of time to detect and time to remediate against malware attacks. We can detect known malware but also unknown malware (known as zero day attacks) in 15 seconds to 2 minutes (somewhat longer for more sophisticated malware and variants), and we can typically remediate the malware in 2 to 15 minutes. We have the ability to detect malware and ransomware and the ability to use countermeasures to eliminate it. Again, we offer all this in near real time.