CRAIN'S CLEVELAND BUSINESS

June 16, 2019

Binary Defense surges amid awareness, product launch

Judy Stringer
clbfreelancer@crain.com

Shane Wynn

Binary Defense Systems CEO Mike Valentine, left, and chief security officer Dave DeSimone stand in the company's Security Operations Center, where analysts — many of them military-trained — assess cyber threats around the clock.

From Crain's Akron Business: Increasing awareness of the digital danger, particularly on the part of its big corporate clients, accounts for part of the Stow cybersecurity firm's growth, officials say. Another factor is the creation of its own security platform, called Binary Defense Managed Endpoint Detection and Response.

Business leaders not yet snagged in the talons of a ransomware gang likely don't realize just how crazy things have gotten, said Binary Defense CEO Mike Valentine.

Today's savvy malware perpetrators offer customer-support lines to help their victims figure out how to buy cryptocurrency, like bitcoin, to pay the ransom. They often will negotiate ransom fees or files to be decrypted. Some offer immunity packages to ensure victims can't get hit again.

"We can actually advise businesses on the probability of getting their data back after payment based on the customer-service rating of the attacker," he said.

Relatively new to the wacky world of cybercrime himself, Valentine aims to keep executives out of this situation altogether.

In 2014, the retired logistics chief teamed up with security guru Dave Kennedy, founder of Strongsville-based consultancy TrustedSec, to build out Binary Defense, which provides cybersecurity services by subscription. The company started in a 4,000-square-foot historic bank building in Hudson but doubled its footprint earlier this year, moving to a 10,000-square-foot suite in Stow.

"We were busting at the seams," Valentine said. "In January 2018, we probably had 30 folks, and we are up over 80 now and hiring."

The new headquarters includes a cutting-edge Security Operations Center (SOC), where analysts — many of them military-trained —assess cyberthreats around the clock and alert and engage clients when necessary. Binary Defense also opened a sales office in Fort Myers, Fla., last year and plans to add satellite operations on the West Coast and in Europe in 2020, if not before.

The private company does not divulge revenue, but in 2018 alone, Valentine said, income surged by 85%. He expects to see another 50%bump this year.

Increasing awareness of the digital danger, particularly on the part of its big corporate clients, accounts for part of Binary Defense's growth, according to Kennedy. Large companies today know they need to keep tabs on the rapidly evolving threat landscape but often struggle to find the skilled manpower to do it on their own, he said.

"This industry is a new one and there are not a lot of folks with a lot of experience working in it, so big corporations can't staff appropriately for cybersecurity," he said.

Another factor in its expansion is homegrown. While Binary Defense's traditional managed services monitor data streaming to and from a company's computer infrastructure via third-party security applications like AlienVault, Valentine and Kennedy focused internal development on the creation of the company's own security platform, called Binary Defense Managed Endpoint Detection and Response (EDR). It was released last year.

Valentine said Managed EDR involves "nano-agents," which are deployed on corporate laptops, desktop terminals and servers throughout an organization. The software identifies suspicious digital behavior and allows companies to remotely lock down any endpoint that might be compromised. A repeated password usage attempt, for instance, might trigger an alert to Binary Defense's onsite SOC for escalation to the customer.

The endpoint offering makes effective cybersecurity a more affordable option for small and medium-size companies, according to Valentine, because the software is faster and easier to install than complex security infrastructure platforms. Installation of the latter can take weeks or months, he said. Binary Defense recently deployed Managed EDR on 2,200 endpoints for a client in about 25 minutes.

"As soon as it is deployed, we can see all the IP addresses across the organization, and once those are seen, the security team in here is monitoring all those computers," he said.

The increased ease and affordability of endpoint platforms like Managed EDR has resulted in proactive security upgrades among some businesses, Kennedy said.

A market report by Gartner found that while only 5% of organizations use managed endpoint technologies today, 15% are expected to do so by 2020.

Still, many of the industry's new customers are reactive, noted Kennedy.

"They get hacked, it causes a lot of pain in the corporation and they don't want to get hacked again," he said.

And there's one big reason why, Kennedy added: Most small and midsize organizations rely solely on antivirus for protection. Antivirus tools block malware based on known signatures, but increasingly sophisticated versions of malware can change their signatures to avoid detection.

"Instead of looking for a signature or some other identified marker, we're looking at the behavior some device exhibits," Kennedy said.
"Like, for example why is your computer now communicating with an IP address out of China when it never has before? That is unusual behavior."

Contrary to its name, Binary Defense has a third service offering, which, Valentine said, involves "scraping" the clearnet (aka non-dark web), dark web and social media to identify information that might be harmful to its clients. The counterintelligence team also performs threat intelligence, working with the FBI and other security outfits to identify new or evolving cybercriminal tactics and feeding that information back into its SOC to stay ahead of possible breaches.

That all may sound like supercomplicated work, but Valentine said educating companies about the danger of depending on antivirus alone is perhaps Binary Defense's biggest challenge.

"Larger companies, really any organization with a security team, are aware of where the exposures are and they're trying to get budget and the people to fill those gaps," he said. "But when you move into the small and midsize — and there's a lot more of those out there — there is a much greater lack of understanding of how exposed they really are."

Source URL: *https://www.crainscleveland.com/technology/binary-defense-surges-amid-awareness-product-launch*