The New York Times

Blog

Getting a Clear Picture of a Computer Network's Security

By NICOLE PERLROTH
August 30, 2014

Security experts say the only hope of protecting corporate networks from hackers is something the industry calls "defense in depth."

The phrase simply means that plugging in one traditional defense — antivirus software, or a firewall, is no longer going to cut it. To stay ahead of a determined and sophisticated adversary, a security officer's best hope is to layer on many different defenses — strong passwords, two-factor authentication, antivirus software, firewall protection, breach detection plans that can sift through vast amounts of employee data in search of anomalies — then pray they never make the headlines.

But the dirty little secret of this growing online industrial complex is this: Even those who are layering on as many defenses as possible are still getting crushed. Why? Because their time is now spent maintaining software, chasing false positives and placating employees who suddenly find themselves locked out of the network, or unable to gain access to a file on the go.

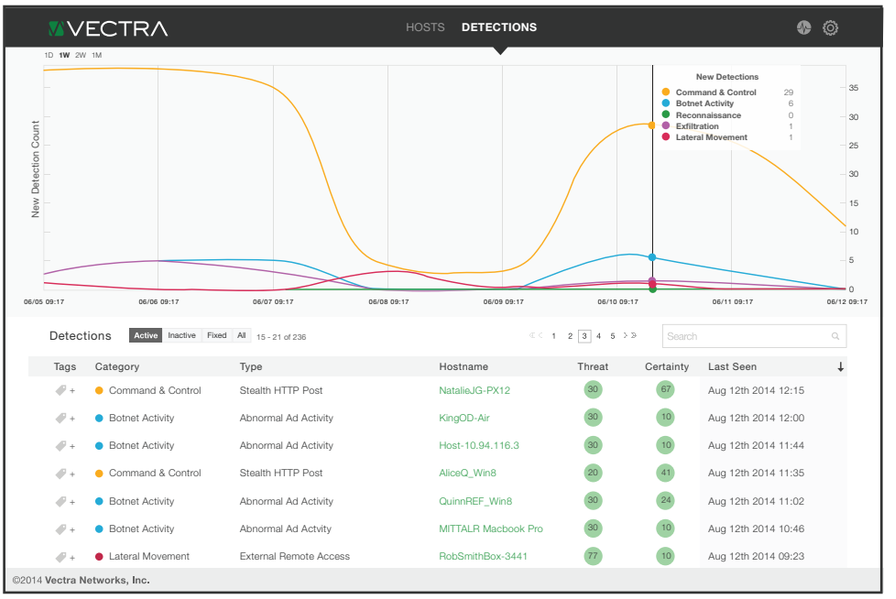
"It's a race you cannot win," said Hitesh Sheth, the chief executive officer of Vectra Networks, a start-up in San Jose, Calif., that is trying to help chief information security officers, or CISOs, deal with the deluge of data. "CISOs are getting crushed."

Mr. Sheth left his post at Aruba Networks and Oliver Tavakoli, Vectra Network's chief technology officer, left his at Juniper Networks to start their company this year. With funding from Vinod Khosla's venture capital firm, Khosla Ventures; Accel Partners; AME Cloud Ventures and IA Ventures, which invests in data solutions, they created Vectra.

Vectra does not claim to stop attackers from coming in. The goal is to quickly find out what's inside the network, with an advanced degree of precision, so that chief information security officers don't have to spend all their time chasing down false leads. Once they plug Vectra into their network, they can monitor suspicious network activity on a dashboard.

On a recent Monday, one security officer used Vectra to get a full picture of a network. There were alerts to threatening activity, but Vectra also gave a sense of how threatening the activity could be.

Up popped an alert when an employee installed Tor, software that enables online anonymity, which is sometimes used by cybercriminals to mask their whereabouts. Had the same user's device made another suspicious move — like scanning the network for an administrator's account and then trying to guess at her password by trying to log in multiple times — Vectra's tool would highlight the employee's computer and inform a security officer that the employee was a threat with a high degree of certainty. Had the odd behavior stopped at Tor, it would have also been flagged, but not been perceived as an immediate threat.



"We have to make sure a security solution can provide us with enough credible intelligence to investigate thoroughly, so we're not bogged down with false positives and unnecessary work," said Sam Kamran, a chief information security officer at Riverbed Technology. "Vectra helps us know the unknown."

"The alerts we see have a higher level of confidence, and that allows us to concentrate our resources and chase down credible threats," Mr. Kamran added.

Vectra's tool uses machine learning and data science to listen, think and anticipate an attacker's next move. It learns the typical traffic patterns and behaviors on a network, then remembers and correlates any abnormal behavior it has seen over days, weeks or months.
That gives security officers the ability to drill down and see where, in an attack, a device's behavior may be. Based on any abnormal activity, Vectra's tool tells CISOs that that activity would indicate whether hackers are conducting reconnaissance, have broken into the network, or are, at worst, pulling data out of the network.

An employee who inadvertently clicked on an ad and installed tracking software would be flagged as a low priority and remediation issue, whereas an infected device that was being used to pull data out of the network would pop up as a high-threat priority.

Vectra started shipping only in March and has less than 100 customers. Beyond Riverbed, Mr. Sheth's former employer, Aruba, installed the tool to help it prioritize threats. Mr. Sheth said the tool had gained the most traction with financial services firms, technology firms and educational organizations.

But he said he was also choosing to market the service beyond major companies to smaller ones that simply could not afford an army of analysts to dig into every possible threat.

Vectra devised the tool to be very basic. Customers work off a simple dashboard and can click on various threats and drill down if they need to, but the tool lacks any flashiness or extra features that might cause confusion.

"We wanted it to be as easy to set up as an iPhone," Mr. Sheth said. "If a complex device like the iPhone can be made easier to use, why can't you extend that to a security product?"