SPOTLIGHT ON SECURITY

Deep Learning App Targets Malware

By John P. Mello Jr.
Nov 10, 2015 4:29 PM PT

Print
Email

Here's the problem with most programs aimed at killing malicious software: They need someone to tell them something's malicious.

What if, however, the programs had the smarts to identify bad code on their own? That's what a company called Deep Instinct says its security solution, launched last week, can do.

The offering works its magic with a technology called "deep learning."

"Deep learning draws its inspiration from the human mind. It organizes itself into a structure of synthetic neurons," explained Bruce Daley, principal analyst at Tractica.

"It's another term for neural networks," he told TechNewsWorld. "It was rebranded because there was so little progress with neural nets."

Better Brain Emulation

Deep learning applications will be a hot commodity in the future, becoming a $10 billion market by 2024, Tractica forecasts.

A fertile area for those apps may be security, which is what Deep Instinct is counting on.

Classical neural networks in the 1980s and '90s had one or two layers of several hundred neurons.

"Nice results, but nothing spectacular," observed Deep Instinct CTO Eli David.

Now with advances in hardware, processing power and algorithms, deep neural networks that are more than 10 layers deep with hundreds of millions of neurons can be created. That kind of power can be harnessed to approach software development in a different way.

Chess Master vs. Chess Program

"With traditional programming, as you code, you have to anticipate all the situations that arise that you have to deal with. What deep learning does is take the data and build a model from what it finds in the data that's statistically relevant," Tractica's Daley said.

"So you don't have to anticipate all the relationships the program will encounter," he added. "It turns the process into something like making beer or making bread."

For example, computer chess programs play the game by brute forcing every move. They use massive processing power to figure out every possible move after a piece is moved on the board.

A person can't do that. Yet chess masters have more than held their own against computer programs. With deep learning, a program approaches a problem more like the chess master than chess program.

In classic machine learning, a facial-recognition program contains information about a face, distance between pupils, shape of the face and so forth, Deep Instinct's David explained. "With deep learning, you just feed it raw input and it learns the features itself."

Cats From Cat's Tail

That kind of "thinking" can be very important in a security app. What makes malware difficult to detect through traditional programming methods is that the slightest change in malicious code can fool a program.

"It's as if I show you the picture of a cat, then I modify a few pixels, and you can't recognize it's a cat," David said.

"With deep leaning, you can show just the tail of the cat, and it will return with high confidence that it's a cat. It is extremely resilient to variance and modification," he continued.

Deep Instinct's security solution has a small agent -- it takes up about 10 MB of memory -- installed on each endpoint -- laptop, mobile device or server -- with deep learning technology in it.

Road Ahead

"Most of the time this agent does nothing. When it detects a new file -- any type of file -- it passes it through the deep learning module on the device. If the file is malware, it will remove it or quarantines it," David said.

"We compared our solution to 61 other solutions, and in all the benchmarks we conducted, we have 98 to 99 percent detection," he noted. "The other solutions average 79 percent."

The solution requires a network appliance. It's used for collecting information so a network administrator can have a bird's-eye view of a network down to the individual user. It's also used to upgrade the agents on the endpoints.

Deep Instinct is marketing its security solution to Fortune 500 companies.

On the drawing board is a version for network monitoring, the company said. That version will be able to detect malicious traffic faster than current solutions because it can look at fewer packets before identifying that traffic.

Better Sharing Needed

Security pros recognize that sharing information with others is important to the security of all, but they acknowledge that barriers remain preventing effective sharing from taking place.

That's what researchers for IID and the Ponemon Institute found when surveying 692 IT and IT security practitioners for a report released last week.

Nearly half the respondents (47 percent) said their organizations had suffered a material security breach. Nearly two-thirds of those respondents (65 percent) said they could have prevented or minimized the impact of attacks if they'd had the right threat intelligence.

Liability and trust remain major barriers to sharing, the researchers found. More than half the organizations represented by the survey sample (62 percent) said potential liability prevented them from sharing information, and 60 percent said trust issues with others kept them from sharing.

Barriers Beyond Liability

A bill in Congress -- the Computer Intelligence Sharing and Protection Act -- could address the liability issue. It has received Senate approval and is now hung up between the houses

"If Congress passed and the president signed into law tomorrow a bill limiting liability, I don't think that will open up the sharing flood gates," said IID Vice President Mark Foege.

"It is a barrier, but it is not the only barrier," he added.

Trust would remain a barrier, Foege noted -- organizations not trusting others they don't have a relationship with or might compete with or that just don't have any information they need or want.

There are technology barriers, too. "Not every organization is set up to exchange their threat indicators. Most are set up to receive them, but not everybody is set up to send them," he said.

"That being said, we have to work together to make sure that liability as a barrier gets removed so we can move forward across all organizations," Foege added.

Breach Diary

- Nov. 2. Imperva Incapsula releases third-quarter DDoS report finding a quarter-to-quarter increase in DDoS attacks of 116 percent. DDoS botnet traffic from China increased during the period from 14.9 to 37.5 percent, it reported.
- Nov. 3. Dow Corning files for a preliminary injunction against two former contractors, Anjaneyulu Chaganti and Homi Syodia, to prevent them from destroying, altering or transferring any data taken from Corning's computers. The contractors allegedly downloaded illegally confidential information about Corning's employees.
- Nov. 4. JPMorgan Chase CSO Jim Cummings is transferred to Texas to work on veteran and military housing initiatives following a data breach last year that compromised confidential information of 83 million customers, Bloomberg Business reports, citing a confidential memo.
- Nov. 4. The U.S. Office of Personnel Management, which suffered the data theft of personal information for 21.5 million people earlier this year, announces hiring of Clifton Triplett as a senior cyber and information technology advisor to the acting director of the agency, Beth Cobert.
- Nov. 4. ShowTix4U notifies an unspecified number of customers that their payment card information may have been compromised in data breach that occurred from April to September.
- Nov. 4. UK Home Secretary Theresa May unveils legislation to give government sweeping surveillance powers, including the right to discover the websites that

anyone visits.

- Nov. 5. Ninety 90 percent of 276 board directors and senior executives believe regulators should hold companies liable if they don't properly secure their data, a survey by the New York Stock Exchange and Veracode reveals.
- Nov. 6. Communications and broadband provider TalkTalk discloses that 156,959 customers were affected by data breach discovered two weeks ago.
- Nov. 6. Cox Communications agrees to pay a $595,000 fine to the Federal Communications Commission in connection with data breach in August 2014. During the attack, a Cox customer service representative and a contractor were persuaded to enter their credentials into a rogue website.
- Nov. 6. Touchnote sends email alert to its users that their identity information is at risk due to a data breach discovered Nov. 4. No financial information was accessed in the attack, the company says.
- Nov. 6. Personal information of law enforcement officials that appears to have been stolen from an FBI Internet portal is posted to the Web. Group that hacked into the email account of CIA Director John Brennan claims responsibility for breach.
- Nov. 7. Four Winds Casino in Michigan alerts patrons that their payment card information may have been compromised in a data breach at three of its locations between October 2014 and Oct. 21, 2015.

Upcoming Security Events

- Nov. 13-14. B-Sides Delaware. Wilmington University, New Castle Campus, 320 North Dupont Highway, New Castle, Delaware. Free with registration.
- Nov. 14. B-Sides Charleston. Tides Folly Beach Hotel, Charleston, South Carolina. Free with registration.
- Nov. 14-15. B-Sides Winnipeg. King's Head Pub, 120 King St., Winnipeg, Manitoba. Admission: $20 (includes a meals on each day).
- Nov. 18. Leverage Machine Learning Using Splunk User Behavioral Analytics. Noon ET. Webinar sponsored by Splunk. Free with registration.
- Nov. 19. The Business of Phishing: How Phishing Erodes Corporate Trust and Decreases Revenue. Noon ET. Webinar sponsored by Agari. Free with registration.
- Nov. 21. B-Sides Vienna. NIG - Neues Intitutsgebäude, Universitätsstraße 7 1010, Vienna, Austria. Free.
- Nov. 21. B-Sides Jacksonville. The Sheraton Hotel, 10605 Deerwood Park Blvd., Jacksonville, Florida. Free.
- Nov. 24-25. Cyber Impact Gateway Conference. ILEC Conference Centre and Ibis London Earls Court, London, UK. Registration: Before Oct. 9 -- end users, 1,799 pounds plus VAT; solution providers, 2,799 pounds plus VAT. Before Oct.

30 -- end users, 1,899 pounds plus VAT; solution providers, 2,899 pounds plus VAT. Standard -- end users, 1,999 pounds plus VAT; solution providers, 2,999 pounds plus VAT.

- Dec. 7-9. Gartner Identity & Access Management Summit. Caesars Palace, 3570 Las Vegas Blvd. South, Las Vegas. Registration: $2,695; public sector, $2.225.
- Dec. 12. Threats and Defenses on the Internet. Noon ET. Northeastern University, Burlington Campus, 145 South Bedford St., Burlington, Massachusetts. Registration: $6. ECT

John Mello is a freelance technology writer and contributor to *Chief Security Officer* magazine. You can connect with him on Google+.

Reader Comments

Be the first to comment!