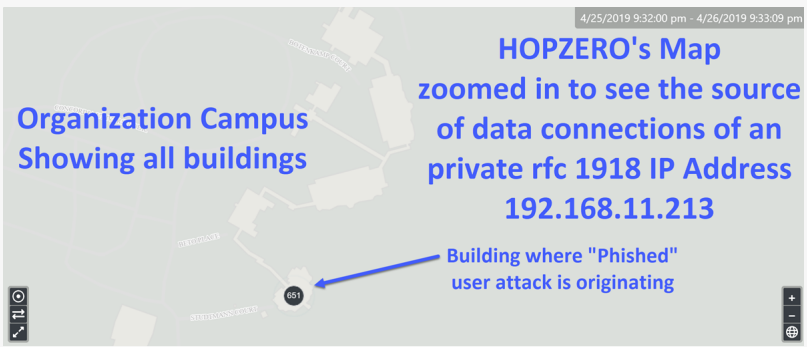
HOPZERO Now Visualizes The Private Organization Location Of Hacker Attacks To "Catch Phish"

HOPZERO Internal (rfc 1918) Private Address GeoIP Creates a Visual Representation of the Network to Determine Who is Trying to Access Restricted Resources

HOPZERO.com



HOPZERO's Pinpoint Position Of Internal Phish Attacker

AUSTIN, TX, USA, April 29, 2019 /EINPresswire.com/ -- HOPZERO Corporation, creator of HopSphere Radius Security, announced that its unique flagship product, HopSphere Radius Security, has the ability to utilize Internal GeoIP data to find the location of computers attempting to access unauthorized data. HOPZERO Internal GeoIP provides a visual representation of an internally-based threat actor or rogue employee or a machine that has been compromised and is being used by an external threat actor. Now security operators can see on a map where attacks are coming from inside an organization, not just from outside to actually catch phish.

> Being able to visually see where data travels on the internet and across a global private network is a massive achievement that will allow security teams to... catch a cybercriminal red-handed"
>
> *Bill Alderson, CTO*

With its latest product, HOPZERO has created an intelligent data control system to classify and protect data that should stay inside an organization, out of reach from outside or inside cyber criminals. The system protects information, and prevents data exfiltration, with a virtual perimeter that puts a networking enforced limit on how far data can travel. Attempts to breach that perimeter and transport data farther than allowed are blocked and an alert issued indicating precisely where the attack came from and what they were after for rapid remediation.

"Being able to visually see where data travels on the internet and across a global private network

is a massive achievement that will allow security teams to both shut down the possibility of a data breach as well as catch a cybercriminal red-handed." said Bill Alderson, "The result will allow major corporations and universities and governments to see where data travels and the risks to its key devices around the world.

While external GeoIP location services have existed for years and offer many productive solutions, the internal use of GeoIP has been limited. By placing an absolute limit on how far high-value data can travel or from what distance someone can access a high-value resource, the Security Operations Team can find the computer used in the attack.
HopSphere Radius Security uses a customized internal address table as well as hop count to determine the location of a computing device on the organization's own network. A mapping of internal activity now augments the visualization map already incorporated into the solution to boost swift investigative and remediation abilities. The maps can work together to see a possible relationship between external and internal activity.

The internal location awareness in HopSphere Radius Security provides the ability to: 1.) Determine the user and computing device attempting to access a resource protected by HOPZERO 2.) Locate a computing device that may have been compromised by an external attacker and is being used as a pivot point to conduct an internal attack and data breach and 3.) See where data is going from a particular internal resource. Internal location awareness is fully incorporated into the HopSphere Radius Security solution at no extra charge. The capability is immediately available.

Ben Merritt
HOPZERO INC.
+1 833-467-9376
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
