Hiding in Plain Sight – Cybercriminals Take Advantage of US Cloud Providers

By Michael C. Maschke, Sharon D. Nelson, Esq. and John W. Simek

One long-standing cybersecurity measure has been the ability to block malicious threats by Internet Protocol ("IP") addresses. A public IP address is like your home's street address on the Internet. It's a unique number assigned to your internet connection by your service provider, allowing other devices and websites to find and communicate with you online.

Just like your home address lets mail reach your house, a public IP address helps websites, apps, and other online services know where to send data when you browse the internet.

System administrators and cybersecurity professionals used to spend countless hours updating block lists using the originating public IPs of ransomware attackers, spam and phishing senders, malicious websites, and sources of Denial of Service ("DoS") attacks. Maintaining these lists quickly proved ineffective. Just as soon as an IP address was added, the attacks would continue from a new IP address—like an internet-based game of Whac-A-Mole.

Facing the frustrations of maintaining these lists, administrators sought to block traffic based on geographical locations by blocking IP addresses leased or located in a particular country or region rather than by one at a time. On the face of it, this seems like a reasonable step to take, mainly when a business operates primarily in the United States and doesn't likely need to access information or public websites hosted within countries often present on these lists – for example, North Korea, Iran, Russia, and China.

This approach has also worked reasonably well for law firms, restricting access to resources inside or originating from countries well-known to harbor cybersecurity attackers. An attacker based in China can't obtain an IP address used or belonging to an Internet Service Provider based in the United Kingdom or European Union, right?

Cyberattackers Adjust Tactics

The first significant test to block traffic and malicious attacks based on the geographic location of IP addresses came with the usage of Virtual Private Networks (VPNs), which allows a user to select a VPN server to connect to that will encrypt all internet traffic from the user's computer to the public internet. Typically, VPN software will allow you to choose a VPN server from your desired location, and any internet traffic is then routed through that country. Luckily, many adverse countries prohibit the usage of VPNs to curb and control free speech, so this evasion technique hasn't been as widely successful as once thought.

What if cybercriminals could originate their traffic from within the United States – at will?

That is precisely what cybercriminals have started to do. Rather than originate malicious traffic overseas to attack the U.S. government, businesses, and citizens, which is more likely to be inspected, analyzed, and filtered, cybercriminals based in China and Russia are more frequently funneling their operations through large U.S.-based cloud providers. Amazon Web Services and Microsoft Azure have been targeted to provide services to Chinese front companies, which have been used to attack U.S.-based businesses by hosting fake trading apps, gambling websites, and

retail phishing pages. Using U.S.-based infrastructure, cybercriminals can bypass geolocation and IP-based filtering and rent out their infrastructure to other cybercriminals, akin to sub-letting a spare bedroom in an apartment you are leasing. This practice makes it very difficult to control who is behind the "renting" of Microsoft or Azure's virtual services. All the activity and internet traffic originating behind a single front company may share the same Public IP address – and administrators will not start blocking cloud providers. As an added bonus, activating and deactivating cloud virtual services is very quick. This means back actors can "stand up" an evil environment, run it for a short period of time and then tear it down before victims start taking action.

What can be done about these new tactics? Just last year, the U.S. Department of Commerce proposed a rule that would require cloud providers to collect data from customers to determine whether each potential customer is a foreign or U.S. citizen, in addition to reporting any transactions that may allow a foreign entity to train AI models that could be used in malicious cyberactivity. How they will implement this requirement and its effectiveness remains to be seen. We know that cybercriminals constantly adjust to the changing environment and will most likely find a way around any new measures that we implement. It is a never-ending challenge.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com*