Michael Guidry
March 15, 2017

Tracing connections online from the virtual landscape to the physical world

Hacking is the intrusion of a computer by an unwanted guest, and is usually used to express gaining access to corporate, or government networks. It requires either installing using malware, phishing, or directly connecting to machines and attacking their software with exploits. It is currently impossible to accurately trace hackers online unless they use the same software, and techniques for all their targets. It has become a major problem within the last decade due to globalization, and corporate networks directly connected to the Internet.

Tracing Transmission Control Protocol (TCP) connections across the Internet is inaccurate due to how routing is performed across global backbones. The global routing table is modified constantly with nodes, and routes being adjusted for optimization, or quality of service needs. TCP is the most used protocol therefore it is the only protocol which really matters to attempt to trace. User Datagram Protocol (UDP) is state less therefore less reliable for tracking, however has the same vulnerability. UDP is usually used by hackers for exfiltration, or remote control after other actions have been performed.

It is currently impossible to track connections over the Internet accurately. Several cases relate to The Onion Router (TOR) sites aka “Dark Web,” which were somehow uncovered using private technologies. Technologies used for those cases do not work properly over regular hacking via proxies online. Its an issue for the landscape of political hacking worldwide which has been increasing annually across the globe.

China, for example, has been having a lot of blame lately due to Internet Protocol (IP) addresses assigned within its borders being used in massive amounts of attacks. Some of these attacks have been supposedly verified, however it is impossible for China to have performed them all. Proxy servers being used in chains may just be victims themselves. The problem arises due to possible evidence planting being similar to proxying through their others networks, or borders. It is completely different comparing cyber war to traditional conflicts due to evidence being traceable, and soldiers physical evidence being easily recovered.

Hacking back is a concept any government, or corporation is now detailing within their playbook to understand how the liabilities may affect them. It is the terminology used to attack the source of an intrusion by means of hacking itself. Repercussions of hacking a country due to incorrectly assuming an attack was originating there is highly possible. Cyber war policies exists for a lot of nations, and it may easily escalate their attention on whom they believe is performing the attacks. The same happens with ‘proxy wars’ currently within the middle east, etc. Proxy wars traditionally will have global evidence allowing verification of weapon deliveries, or monetary exchanges to determine the origin of funding. Soldiers training methods, and other strategies may be impossible to cloak. It is generally accepted once verified, and escalation is directed towards the proper perpetrator.

Internet Service Providers (ISP) have the ability to perform various tasks internally to determine the pathways through their networks which would reflect lateral hacking movements. Connections leaving a single network that enter the realm of dynamic routing via Border Gateway Protocol (BGP) become a nightmare. The percentage of accuracy decreases

exponentially as each separate network is used to route the connection to its destination. It becomes nearly impossible to trace after just a few gateways at least publicly, or academically.

Unorthodox methods are required to allow tracing of connections under these circumstances. Distributed Denial of Service (DDoS) is a solution that allows you to turn the internet's own packet distribution system into a tracking mechanism. Most people do not consider performing DDoS attacks for positive reasons. DDoS may have been used by targets to "quarantine" their hacking source temporarily from the Internet. This strategy is beyond the scope of this technique, and is literally only a bandaid for a single attack originating from possibly just a proxy.

DDoS is also illegal in most nations which have advanced their cyber crime laws. The fact that this technique requires many computers performing attacks strategically placed across the globe also ensures that they will be performed from countries where these laws are being enforced. The attack requires attacking all networks that you wish to verify against therefore you are immediately breaking laws on the destination side of most of the world simultaneously. It should not be used lightly, or regularly without cause and understanding.

DDoS attacks transmit more data to a destination than a that network can handle which forces it to stop responding in a timely fashion. The latency is so high that the TCP timeouts are reached, and connections break. New connections are also impossible during these attacks. It has only had negative effects since it began being used globally regularly. This technique could be considered a reverse DDoS.

The approach is to attack the entire world in a very strategically timed manner using worldwide machines. Each separate DDoS attack using machines worldwide would use different synchronization, and timing information which would allow embedding information directly into the latency it causes on those networks. The purpose is to compare that latency with the hack taking place to verify its source location. If the attack disrupts networks your attempting to verify against for milliseconds up to a few seconds then you can perform several of these sequentially to embed information in this timing itself. DDoS then becomes a positive useful solution even though technically illegal to a currently difficult problem.

You wouldn't necessarily have to attack the entire world. Conceptually it would be better to use databases of networks wishing to verify against. Residential, and commercial IP delegations throughout most nations would cover a large portion. Government hacking groups have their IPs leaked often as well. It is possible to just perform the attacks on these particular sets of IP addresses rather than the world as a whole. It is also equally possible to perform the attacks on entire ISPs, and countries to quickly determine although this would not be accurate due to possible proxies in between being within that country.

If the technique is used on a major ISP network rather than a gateway going into an office then it is possible that a proxy exists within their network which would read off as a false positive. Accuracy relies on the networks your verifying against to be actual end user machines which would have human attackers. If you were to attack a network, or router of a network which has an office then it is highly likely they are going to notice other hackers using their network to hack externally on scales which would involve this type of solution. If you were to attack an entire country then you are going to have a problem of not recognizing from timing alone whether or not a proxy (of possibly several) just exist in that country. It is imperative to understand this, and always attempt to get as close to the networks in question being verified.