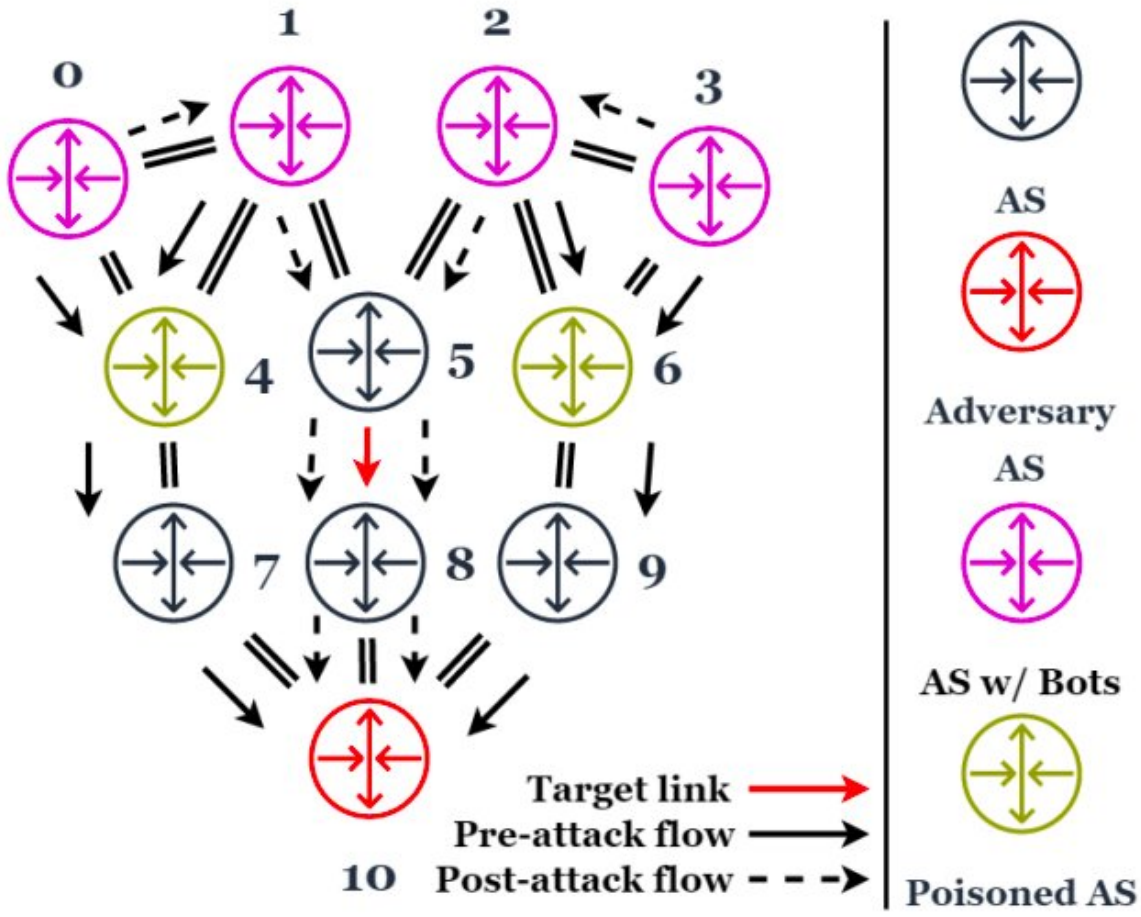
Maestro: a new attack that orchestrates malicious flows with BGP

May 31 2019, by Ingrid Fadelli



Demonstration of the Maestro Attack: utilizing BGP Poisoning to collapse botnet traffic onto a single link. Credit: McDaniel et al.

Researchers at the University of Tennessee have recently identified the Maestro attack, a new link flooding attack (LFA) that leverages plane traffic control engineering techniques to concentrate botnet-sourced distributed denial of service (DDos) flows on transit links. In their paper, recently published on arXiv, the researchers outlined this type attack, tried to understand its scope and presented effective mitigations for network operators who wish to insulate themselves from it.

Distributed denial of service (DDos) attacks work by directing traffic from different sources on the internet to overwhelm the capacity of a targeted system. Although researchers have introduced numerous mitigation and defense techniques to protect users against these attacks, they are still proliferating. Link flooding attacks (LFA) are a specific type of DDoS attacks that target infrastructure links, which are typically launched from botnets.

"While investigating how well an ISP could singlehandedly defend against massive denial of service attacks, we realized the same technique we were using to defend against attacks could be used by an adversary to take down our own defense," Jared Smith, one of the researchers who carried out the study, told TechXplore. "This led to us exploring how well this technique, BGP poisoning, could be used to carry out such an attack."

As they were trying to develop defenses against DDoS attacks, Smith and his colleagues Tyler McDaniel and Max Schuchard explored how an adversary's ability to influence routing decisions (i.e. his/her access to a compromised boarder gateway protocol or BGP speaker) can shape remote networks' path selection processes to their advantage. During their investigation, they identified a new type of LFA attack, which they called the Maestro attack.

"We are researching DDoS attacks against Internet infrastructure links,"

McDaniel told TechXolore. "These attacks are limited by internet routing characteristics, because DDoS sources do not always have a destination for their traffic that crosses a target link. The Maestro attack exploits vulnerabilities in the language Internet routers use to communicate (i.e. BGP) to overcome this limitation."

The Maestro attack works by distributing fraudulent (i.e. poisoned) BGP messages from an internet router to channel inbound traffic (i.e. traffic flowing into the router) onto a target link. Simultaneously, it directs a DDoS attack against the same router using a botnet, which ultimately funnels DDoS traffic onto the target link.

In other words, Maestro orchestrates path selection of remote Autonomous Systems (ASes) and bot traffic destinations, in order to steer malicious flows onto links that would otherwise be inaccessible to botnets. To carry out this attack, a user would need to have two key tools: an edge router in some compromised AS and a botnet.

"For one of our major botnet models, Mirai, a well-positioned Maestro attacker can expect to bring a million additional infected hosts onto the target link vs. a traditional link DDoS," McDaniel said. "This number represents fully a third of the entire botnet."

According to the researchers, in order to insulate themselves from this attack, or at least mitigate the risk of becoming a target, network operators should filter out poisoned BGP messages. Interestingly, however, studies carried out in their lab revealed that most routers do not currently filter these messages out.

"An adversary who can compromise or buy an Internet router can disseminate fraudulent messages to intensify attacks on the Internet's infrastructure," McDaniel said. "This is troubling, because prior work has raised the specter of large-scale link DDoS being weaponized to

isolate installations or entire geographic regions from the internet."

In addition to introducing the Maestro attack, the study carried out by Smith, McDaniel and Schuchard provides further evidence that BGP, as it stands, is no longer an ideal, scalable and secure routing protocol. This was already suggested by previous studies, as well as by recent incidents, such as the 3ve fraud operation and the China Telecom hijack. According to the researchers, although upgrades such as peer locking could help to prevent this specific attack, replacing BGP with an entirely new, next-generation system (e.g. SCION) would be the most effective solution.

"Going forward, we're primarily exploring two directions," Smith said. "First, while talking to ISP operators about Maestro, we found differing opinions of how vulnerable the Internet actually is. Our lab has a history of actively measuring the Internet's behavior and we're working on measuring human operator intuition against the actual behavior of the Internet. Second, we're already seeing strong results for extending Maestro to work even when you don't have a massive botnet available."

More information: The Maestro Attack: Orchestrating malicious flows with BGP. arXiv:1905.07673 [cs.CR]. arxiv.org/abs/1905.07673