The Security Skeptic

The Security Skeptic blogs about all matters related to Internet Security, from domain name and network security to phishing and malware.

Internet Address Hijacking, Spoofing and Squatting Attacks

Dave Piscitello, dave@corecom.com

Some of the prominent Internet routing attacks are not attacks against the routing system at all. The purpose of this set of attacks is not to disrupt the routing system itself but to (i) use the routing system to make addresses that criminals use for spam or other malicious activities known and reachable and thus (ii) allow malicious traffic to originate from these addresses and be delivered to recipients across the Internet.

This series of blog articles explores attacks that exploit the Internet's routing system in this manner. In particular, I'll consider attacks that exploit the Border Gateway Protocol (RFC 1771), a routing protocol that is used to exchange network reachability information among autonomous systems (AS, defined as one or more IP networks that operate under a single routing policy). BGP is a ripe target for exploit attacks. BGP has no mechanisms to protect against attacks that modify, delete, forge, or replay data, any of which has the potential to disrupt overall network routing behavior (RFC 4272) and studies and events show BGP to be vulnerable to monitoring, insertion and other man-in-the-middle attacks. Such BGP exploits are discussed in Revealed: The Internet's Biggest Security Hole.

This series describes the motives for such attacks, classifies the attacks based on certain distinguishing characteristics, and suggests measures that can be taken to mitigate attacks of these kinds. Since the objective of this paper is to describe how and why attackers target specific addressing resources, the paper does not describe how attacks are executed in detail but instead treats them all as insertion attacks.

Criminals Need IP Addresses

Criminals use hosts connected to the Internet to act as traffic sources, proxies or application servers for spam, phishing, or other criminal activities. These hosts are typically infected with some form of malware and are often elements of a botnet. Irrespective of the intended use by criminals, these hosts need public Internet addresses and in fact have IP addresses assigned to them by public or private network administrators. However, measures to identify and block the IP addresses of infected hosts are now sufficiently effective that criminals have altered their tactics in response.

Consider direct-to-MX spam (Note: A summary of this and other spam techniques can be found at Spam Transmission Methods Explained). Criminals use this technique to send spam directly from infected hosts they control to mail servers whose IP addresses are identified in mail exchange (MX) records in the DNS. The source IP addresses that appear in direct-to-MX spam messages are quickly added to block lists such as the Composite or Exploits Block Lists (CBL, XBL). Investigators use this and other information and work in cooperation with law enforcement and justice systems to disrupt or dismantle spam botnet. Such activities threaten the spammers' livelihoods, so these criminals have altered their tactics to provide greater agility and stealth to their activities.

Rather than relying on the IP addresses assigned to infected hosts by network administrators, criminals have turned to using "someone else's IP addresses". Specifically, they take control over blocks of IP addresses, worm their way into the Internet routing system to announce these IP blocks as reachable from an injection point of their choosing, and spam from hosts to which they've assigned addresses from these IP blocks. Once they've completed a spam campaign, they cease spamming from this insertion point, stop announcing the IP addresses into the routing system, and effectively "disappear".

Criminals Obtain and Use IP addresses in Several Ways

The phrase *AS hijacking* is liberally applied to scenarios where criminals obtain and use someone else's IP addresses in this manner. *AS* refers to *Autonomous System*, a number that is in the Internet routing system to identify a group of IP networks that operate under a single routing policy. In certain scenarios, the routing information attackers insert does include an Autonomous System number (ASN) and in such cases, the attackers do impersonate an AS. Labeling all unauthorized route insertion attacks as AS hijacks, however, is inaccurate. In some scenarios, routing information that is inserted identifies destination networks that can be reached via an ASN. Such destinations are represented as IP Prefixes, also known as a CIDR blocks. In all cases, the attacker's objective is to put the IP addresses where he intends to host criminal activities on the routing "map".

The term *hijacking* is also used too generously. Hijacking means that a commodity is taken from a legitimate, authorized owner or registrant by an attacker, and the legitimate party is consequently unable to use that commodity. In certain scenarios, an AS or IP Prefix hijacking does indeed occur. However, the term hijacking is used in circumstances where spoofing more accurately describes the attack. The distinction is important because in the case of spoofing, the legitimate user may be advertising routes and the attacker may be advertising conflicting routes at the same time; in the hijacking case, the legitimate user may not be advertising at all, or the hijack attack may prevent from doing advertising legitimate routing information entirely.

Hijacking is also incorrectly used when an attacker makes use of ASNs or IP Prefixes that are not assigned (not registered through a Regional Internet Registry, RIR) or that are assigned but dormant (not in use by the registered party). Such attacks are more characteristically like squatting than spoofing or hijacking.

Attacks that exploit ASNs

I classify attacks that exploit ASNs for malicious activities as hijacking, spoofing, or squatting attacks in several articles that follow. The goal in defining this taxonomy is to call attention to the distinguishing characteristics of each kind of attack and identify measures to possibly mitigate them.

ASN Squatting attacks

There are two forms of ASN squatting attacks. In the first scenario, the attacker determines that an ASN is not registered at an RIR. The attacker ignores the customary registration channels and uses this ASN to announce IP Prefix it intends to use for malicious purposes. The victim is thus the RIR, whose resource is used without authorization. No registrant is victimized.

In the second scenario, a criminal does research in search of a dormant ASN, i.e., the resource has a registrant but the resource is not in use (no advertisements currently inserted into the Internet routing system). The criminal uses some form of the registrant's point of contact information to impersonate the registrant and requests that the RIR reset or allow access to the account through which the target ASN is managed and thus gains control of the ASN. Here, the registrant and the RIR are victims.

In circumstances where RIRs will accept requests from point-of-contact (POC) email addresses, the criminal looks for a dormant AS that has a POC email address that is assigned from an available domain name (specifically, a domain name that was once registered by the organization that "owns" this ASN, according to the RIR's registration data). He registers the domain name, creates the POC email address, and uses this to impersonate the AS registrant of record. Alternatively, the criminal could attempt to hijack the domain name registration account to gain control of the domain in which the POC email address is assigned.

In circumstances where RIRs require other/additional forms of verification before granting access to the RIR account, the criminal can resort to social engineering of RIR staff or would use other fraudulently produced credentials in the impersonation attempt.

Once in control, the criminal has a veil of legitimacy and can go to an ISP and ask to have its resource advertised. There are several ways the attacker may "use" the ASN following either form of squatting attack:

1. Insert advertisements directly into the global routing system by establishing a BGP connection and peering with a network operator that he has monitored and targeted for the insertion. Prior to the insertion, the attacker has observed that the operator is lax with respect to screening advertisements and so expects to avoid detection by the autonomous system he's peered with while the routing information propagates through the global routing system.

2. Convince an access or transit provider to connect with the attacker as a BGP peer through social engineering or coercion. Here, the access or transit provider becomes an unwitting or unwilling participant when it propagates advertisements it receives from the attacker into the global routing system.

   (1) and (2) are illustrated in Figure 1. The color red is depicts the criminal actor and fraudulent information and green depicts unwitting participants:

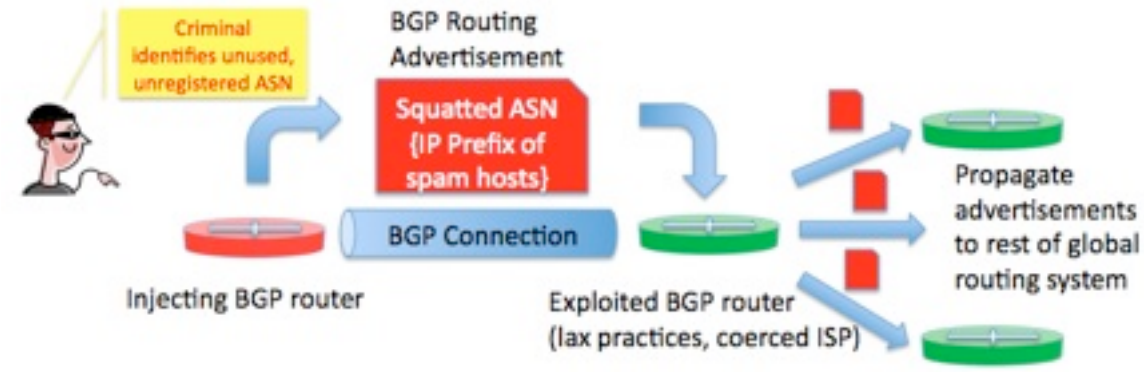

Figure 1. ASN Squatting via unwitting parties

3. Convince an access or transit provider to connect with the attacker as a BGP peer BGP peer through collaboration or bribery. Here, the access or transit provider is a willing and likely a profiting participant. This is illustrated In Figure 2. The color red depicts the criminal actor and willing participants and green again depicts unwitting participants:

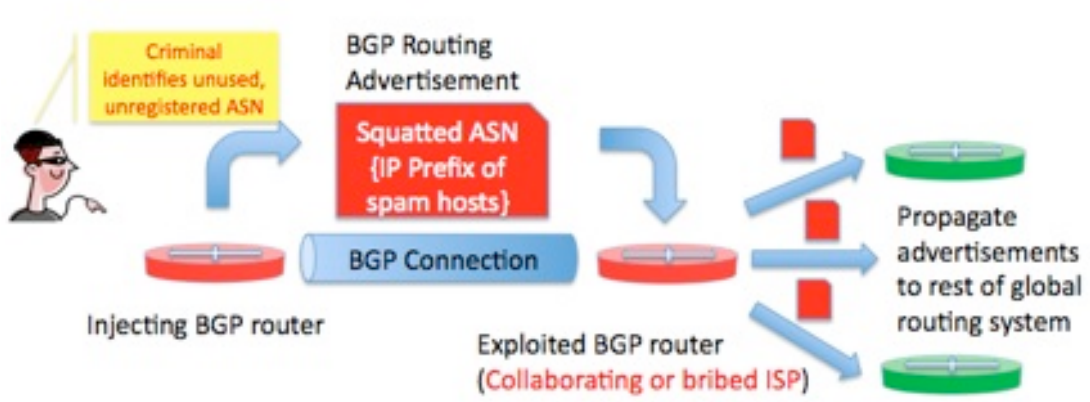

Figure 2. ASN Squatting via willing parties.

ASN Hijacking Attacks

As is the case in the domain name registration world (SAC007), an ASN hijacking is an attack against an RIR registration service that results in the attacker seizing control over of a registration account and thus all the resources managed through this account. The attacker may use social engineering to convince an RIR employee to grant access to the account, or may gain control of or impersonate the legitimate registrant's email to request account access (e.g., a password reset), or he may attempt to exploit a web application vulnerability at the RIR to seize an account.

This scenario is distinguished from ASN squatting because here, the attacker seizes control of an ASN that is registered and actively used by the registered party (registrant). The registrant is thus the victim since, in normal circumstances, an authorized, registered party uses the ASN and other autonomous systems routinely see BGP advertisements mentioning this ASN in the routing system.

If the attacker is successful, he is able to impersonate the authorized registrant by representing his own information using this ASN. Specifically, the attacker's BGP advertisements will replace the authorized party's BGP advertisement, and, rather than announcing the IP Prefixes that should be associated with the authorized party's ASN, the attacker's advertisements will announce IP Prefix(es) the attacker intends to use for malicious purposes.

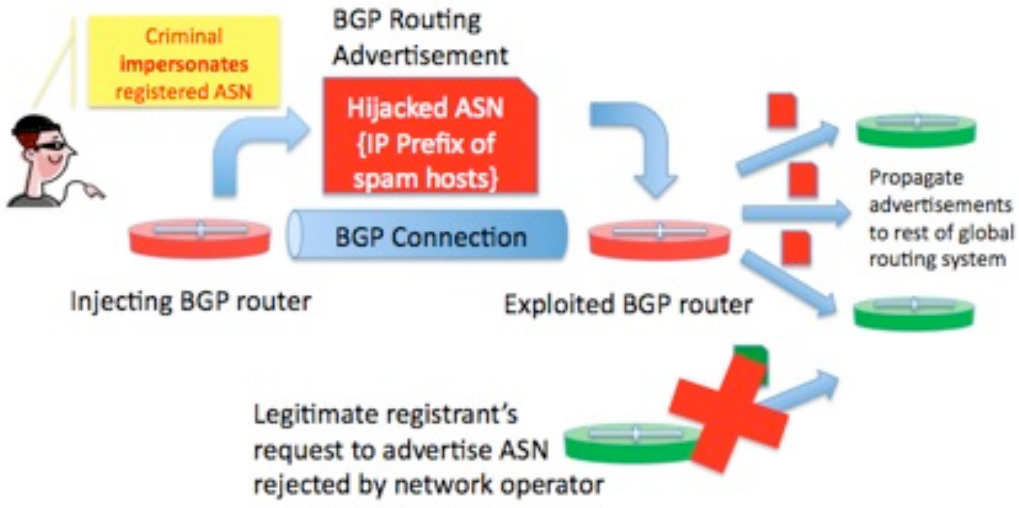

Figure 3. ASN Hijacking

ASN Spoofing Attacks

In this scenario, the attacker does not attack the RIR or attempt to break into a registration account but instead, assumes the use of an AS number that is registered and is actively in use by an authorized, registered party and uses it without regard to whether it is actively in use by the registered party. An important difference between this attack and those previously discussed is that this attack can result in conflicting advertisements: what the attacker inserts into the routing system and where this insertion takes place are different from what the legitimate registrant advertises, and where. In this scenario, the registrant is the victim.

The attacker injects BGP advertisements into the global routing system using one of the same methods described under items (1)-(3) in ASN Squatting Attacks (direct injection through an ISP that's not screening, social engineering/coercion of an ISP, or ISP collaboration/bribery). The attacker expects that routing peers that are duped by the deception will (i) incorporate the updates into their routing database, (ii) forward data from sources enumerated in the AS and (iii) deliver traffic to destinations enumerated in his

AS. However, peers that are not duped may (i) block traffic to/from that AS, or (ii) ignore updates, and use routing advertisements they consider complete and accurate. This is very possibly a noisy, disruptive and a shorter-lived attack than ASN hijacking or ASN squatting attacks. Since the attacker may only need a small window of opportunity to direct a spam campaign, this method does serve the attacker's needs.

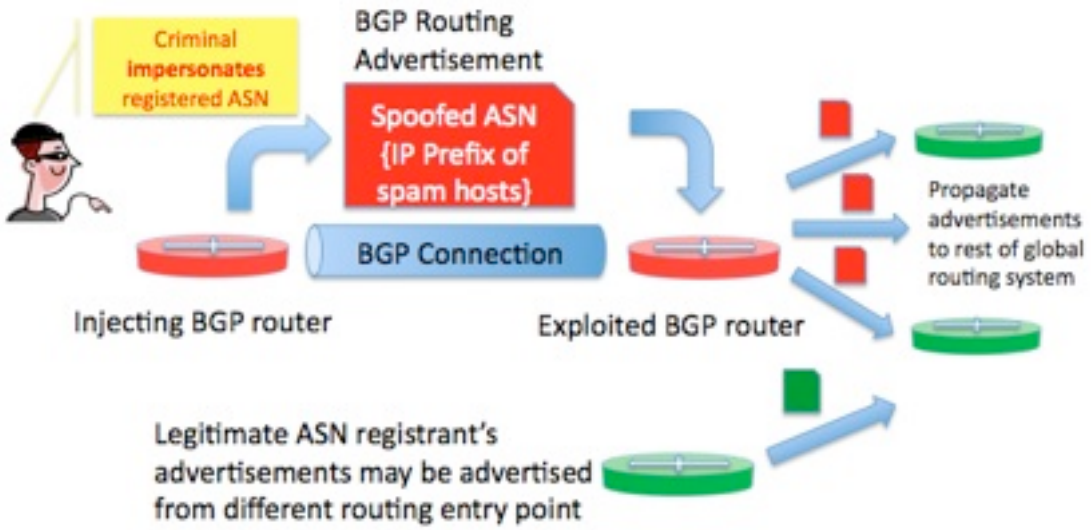

Figure 4. ASN Spoofing

Attacks that exploit IP Prefixes

In the following sections we classify attacks that exploit IP Prefixes for malicious activities as hijacking, spoofing, or squatting attacks, again with the purposes of calling attention to the distinguishing characteristics of each kind of attack and identify measures to possibly mitigate them. The attacks – squatting, hijacking, and spoofing – are very similar to attacks that exploit ASNs, so some of the discussion will feel repetitive. Readers who feel they have a sufficient understanding of the distinguishing characteristics of these attacks may skip to the section Addressing Attack Mitigation. Others may wish to read these sections to understand how the attacks differ when IP Prefixes are the exploited resource.

IP Prefix Squatting Attacks

This is a continuation of Internet Address Hijacking, Spoofing, and Squatting Attacks.

In this scenario, the attacker determines that an IP Prefix is not registered at an RIR, or the registration is dormant. The attack scenarios are similar to AS squatting, and again, the victim is the RIR. Here, the targeted resource is an IP Prefix. In the not registered scenario, the attacker ignores the customary registration channels, squat on the IP Prefix and uses it for malicious purposes. In the dormant scenario, the attacker compromises or socially engineers access to the legitimate registrant's registration account.

The attacker doesn't need to squat on or hijack an AS to announce the IP net block; he must, however, find a way to have the IP prefix advertised as reachable via an autonomous system. He can try any of the following attack vectors:

1. Inject advertisements directly into the global routing system by establishing a BGP connection and peering with an autonomous system that doesn't diligently screen advertisements. The injected routing information announces reachability of the squatted IP Prefix.

2. Through social engineering or coercion, convince an access or transit provider to include the squatted IP Prefix in BGP advertisements. Here, the ISP becomes an unwitting or unwilling participant when it propagates advertisements into the global routing system.

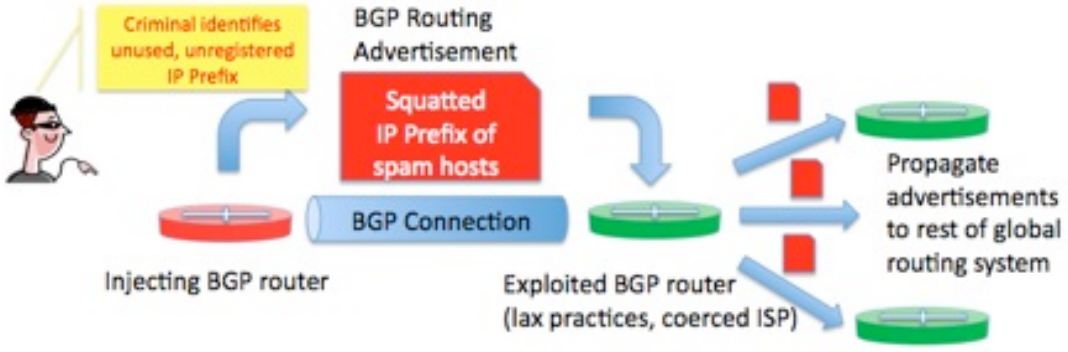

Figure 5. IP Prefix Squatting via unwitting party

3. Through collaboration or bribery, convince an access or transit provider to include the squatted IP Prefix in BGP advertisements. Here, the ISP is a willing participant when it propagates advertisements into the global routing system.

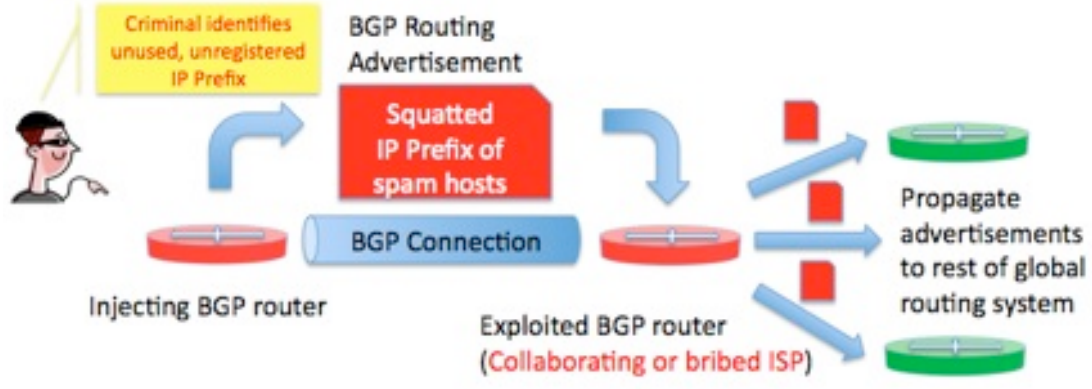

Figure 6. IP Prefix Squatting via willing party

IP Prefix Hijacking Attacks

This scenario is similar to an ASN hijacking attack but in this case, the attacker hijacks the registration of an IP prefix. The IP Prefix registrant is the victim. In order to use the IP net block, the attacker must find a way to have the IP Prefix advertised. He could use any of the methods described under IP Prefix Squatting Attacks. It may be possible that he could also exploit the existing arrangement between the legitimate IP Prefix registrant and his "native" AS. The operator of the AS is unlikely to be aware that the IP net block was hijacked and will advertise it as reachable as part of normal routing operations.

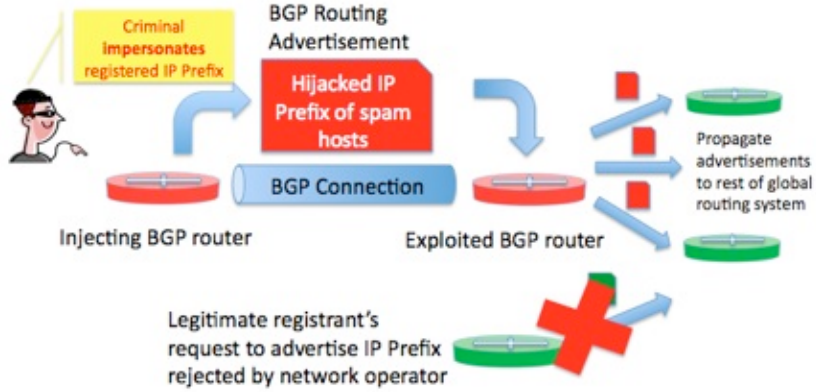

Figure 7. IP Prefix Hijacking

IP Prefix Spoofing Attacks

In this scenario, the attacker does not attack the RIR or registration account but instead, assumes the use of an IP Prefix that is registered and is actively in use by an authorized, registered entity. The attacker contrives to have the spoofed IP Prefix advertised using any of the methods described under IP Prefix Squatting. There is also a scenario where attackers announce smaller IP Prefixes to exploit that BGP follows paths to the shortest matching prefix. The earlier referenced Wired article refers to this as an IP hijack; however, the attack method does not require than the registration be hijacked as I describe here.).

As is the case for AS spoofing, this attack can result in conflicting advertisements: what the attacker injects into the routing system (and where) is different from what the legitimate registrant advertises.

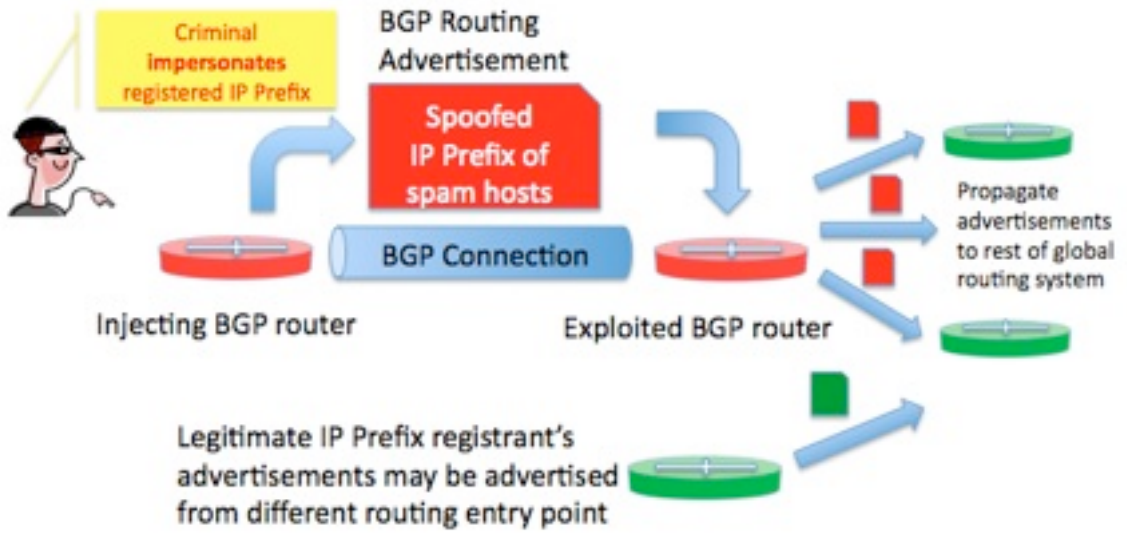

Figure 8. IP Prefix Spoofing

Addressing Attack Mitigation

Measures that could reduce attacks of these kinds include the following:

- Network operators who participate in BGP routing: filter or block routing advertisements that contain ASNs or IP Prefixes that are not registered.

- RIRs: implement measures to protect registrant accounts against hijacking or misuse; in particular, certain measures recommended to protect domain name registration accounts against attack or misuse (SAC040) may be of equal use to RIRs.

- RIRs: to combat squatting or hijacking, insist on strong proof of registration before providing access to registration accounts; in particular, do not rely on correspondence from a point of contact email address as sufficient demonstration that the sender is the legitimate registrant. Alternatively, implement a secure email (non-repudiation, authentication) capability so that registrants must digitally sign correspondence and thus provide verification of sender.

- Community effort: to combat dormant registration squatting, RIRs, ICANN, and TLD registries could share information regarding changes to domain name registrations of domain names from which POC email addresses in AS or IP Prefix registrations. Use a change in registration of such a domain name as an alert to a possible squatting attack (clearly, other factors must be considered to

avoid a false positive).

- Community effort: identify and share information regarding network operators who are victims of or seemingly complicit in advertising spoofed, hijacked, or squatted ASNs or IP Prefixes. Assist victimized network operators in implementing filtering/blocking fraudulent advertisements either through direct dialog or a dissemination of best practices. Bring allegedly complicit network operators to the attention of law enforcement.

Address Attacks: Conclusions

Criminals or miscreants need public IP addresses for the compromised hosts they use to conduct a variety of criminal or activities such as spam, phishing, or denials of service. Historically, spoofing IP addresses served these bad actors well. Techniques to detect and thwart address spoofing have improved, and attackers have responded by using various methods to obtain and misuse legitimate public addresses. Classifying these methods serves to show how criminals target and victimize Regional Internet Registries or their customer-registrants. By distinguishing the attacks as well as the victims using the taxonomy described in this paper, we can better identify protective measures RIRs, registrants, and IP network operators can implement to reduce the threat of IP address attacks.