Royal Canadian Mounted Police
Criminal Intelligence Program
emerging.trends@rcmp-grc.gc.ca

Reference: EW 2011 05

Early Warning Assessment

Purpose: To provide forward-looking intelligence and analytical judgment on events and developments that will affect criminality and the criminal environment in Canada

Internet Protocol version 6 (IPv6)

December 2011

Summary:

- The current Internet addressing system, Internet Protocol version 4 (IPv4), is nearing exhaustion and a new expanded numbering system, Internet Protocol version 6 (IPv6), has been created. The switch to IPv6 will require a transition period of several years and transition mechanisms in order to give everyone access to the entire Internet. (U)
- This transition period presents vulnerabilities for criminal exploitation because it creates numerous security gaps. (U)
-
- It is assessed with high confidence that cyber criminals will use the transition mechanisms of IPv6 to carry out their illicit activities until computer security measures are reconfigured to block them. In addition to connectivity, the pending shift to IPv6 will warrant better public education as to how governments, businesses and individuals can gain protection against unwelcome intrusions. (A)

s.16(1)(c)
s.15(2)

PROTECTED A

IPv6 transition mechanisms will make combating cyber crime more challenging as criminals continue to exploit the vulnerabilities created by those mechanisms.

IPv6

Just as new telephone area codes are implemented to serve growing populations, an expanded addressing system is needed to accommodate the increasing number of devices connected to the Internet. Under the current system, known as Internet Protocol version 4 (IPv4), the pool of available addresses is nearing exhaustion. The last IPv4 addresses (the numbers that allow machines to identify each other on the Internet) are expected to be assigned in North America by early 2012. In Asia[1] the last block of addresses was released in the spring of 2011 and in Britain[2] the last addresses are currently being allocated. (U)

In response to this pending address depletion, Internet Protocol version 6 (IPv6) has been created, which uses an expanded numbering system to allow for 340 undecillion (10^{36}) new devices to be connected to the Internet, ranging from home computers and smart phones to TVs, fridges and home heating.

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32 bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366,920,938,463,463,374,607,431,768,211,456

http://news.cnet.com/8301-30685_3-20030482-264.html

The switch to IPv6 cannot happen overnight. It will likely be years before it will be used exclusively, meaning transition mechanisms must be implemented to allow it to operate alongside the current IPv4 system and to give users access to the entire Internet. It is this transition period that presents the greatest vulnerabilities for criminal exploitation because the tools used to assist the conversion to IPv6, in effect, give cyber criminals more avenues for attack. (U)

The following assessment will look at how the transition to IPv6 will impact Canadian law enforcement's ability to police cyber crime in the next 12-24 months and how criminals can exploit these transition mechanisms to further their illicit activities. (U)

Current Situation

Cyber criminals[1] succeed, in part, because Canadians let them into their systems through their own failure to fully understand the potential severity of, and protect against, attacks. Cyber crime is most often silent. Victims aren't aware of what has happened to them and even when they are, they presume attacks are nothing more than a nuisance and they do not equate them with having serious consequences for themselves or their organization.[4] There are various types of cyber crime. Some exploit existing vulnerabilities in software and hardware. Others can trick people into infecting their computers with malicious software, known as malware, or take advantage of people who do not change their passwords frequently.[5](U)

Some types of cyber crime, such as botnets, are believed to be linked to organized crime.[6] A botnet is a network of personal computers (PCs) that has been infected with malicious programs. The criminals essentially hijack the PCs to send spam, attack and shut down web sites with floods of traffic and steal personal data such as banking information and passwords.[7] Botnets are increasingly a problem for law enforcement as they have not only become more prevalent in the last 12 months, but they are resource intensive to investigate and international in scope. (U)

It is not yet known what impact the transition to IPv6 will have on criminal activity and how law enforcement can best respond. This is in large part because there are three different transition options, each with its own vulnerabilities or challenges, and much will depend on the option chosen by each Internet Service Provider (ISP). Several of the large telecommunications companies operating in Canada have indicated they are able to "support" IPv6, however it is not clear what exactly that means. (U)

The three types of transition options are:

- Dual Stack Configuration: Allows IPv6 hosts and routers to be implemented in such a way that they can co-exist with IPv4 hosts and routers. (U)
- Tunneling: Allows IPv6 hosts and routers to connect with other IPv6 hosts and routers over the existing IPv4 Internet. (U)
- Translation: Various methods of translation (NAT, NAT64, NAT-PT) are needed to allow IPv6 hosts to communicate with IPv4 servers and hosts. (U)

In Canada, there has been no criminal activity linked to IPv6 as the protocol is not yet operating on its own (without IPv4). However, RCMP cyber crime investigators share many of the same concerns expressed by their British and American colleagues. (U)

[1] The term "cyber criminal" includes hackers, spammers, hacktivists and anyone else using the cyber world to perpetrate illicit activity.

In the United Kingdom, the Serious Organised Crime Agency (SOCA) assesses that the adoption of IPv6 could lead to a significant increase in cyber crime. Investigations will be more difficult because of the billions of domain names and IP addresses available for use once IPv6 is fully adopted. [9] (U)

At the very least, cyber crime causes inconvenience when people mistakenly link to infected sites or install compromised code on their home computer, causing it to crash. In other cases, personal information such as banking passwords could be compromised resulting in financial loss. In the most serious cases, cyber crime can result in widespread damage: (U)

- A November 2011 Reuters news report about an FBI investigation into last year's cyber attack on the exchange company Nasdaq OMX stated weak security measures made the company an easy target for hackers. While trading systems were adequately protected, some computers had out-of-date software, misconfigured firewalls and uninstalled security patches that could have repaired known bugs hackers could exploit.[10] This incident demonstrates how important it is for companies to ensure their security measures are current and it also highlights the potential risks that exist if financial trading systems are not adequately protected. (U)
- Newly developed software called RCS – Remote Control System – can enter a digital device undetected, bypass the most sophisticated electronic defences and disrupt anything from a railway signaling system to a nuclear power station. While the technology is intended as an investigative tool for law enforcement and security agencies engaged in counter-terrorism and counter-espionage, its existence points to the kind of extensive damage that those wanting to wreak havoc could cause.[11] (U)

Challenges and Opportunities for Law Enforcement

Investigation

Under IPv6 however, all devices in one house will have a separate IP address. The need for individual user names and passwords makes it difficult for someone to deny they were using a computer at the time of an attack. (A)

Criminal Exploitation

IPv6 is not yet in widespread use in Canada but is currently enabled by default on many home and business computers, allowing cyber criminals to monitor communications. This creates vulnerability as firewalls are not yet set up to monitor IPv6, potentially allowing cyber criminals to utilize alternate communication channels that may not be monitored by IPv4 firewalls or Intrusion Detection Systems (IDS).[12] IDS, a more sophisticated method of finding suspicious traffic than firewalls, may also ignore the IPv6 or tunneling from IPv4.[13] The key to preventing malicious attacks is to configure firewalls and IDS to detect and block an intrusion. Cyber criminals count on a lack of vigilance regarding the security of personal and work computers and devices to carry out their illicit activities. (U)

There is also a "privacy extension" option within IPv6 which, when activated by a user, randomly changes the last portion of the IP address (Media Access Control, or MAC, address), so users of a device (such as a smart phone, laptop, personal computer, etc.) can still be connected without part of their IP address being revealed.[15] While the intention is to offer users added privacy protection, it also provides another means to conceal information or launch targeted attacks. This feature makes it difficult for law enforcement to link the same person to several

Looking Forward

The coming year is expected to be a significant one for IPv6 adoption in Canada. Some of the bigger names in the telecommunications industry are currently providing customers with trial access to IPv6 services or plan to in the coming months. Others are making investments in the necessary preparations and infrastructure upgrades to ensure residential customers have no disruption in service. [11] (A)

Barring any significant improvements in security preparedness, cyber criminals will continue to exploit the above-mentioned gaps to carry out their illicit activities. The transition mechanisms between the current protocol and IPv6 are where the new threats and vulnerabilities will emerge.

In addition, law enforcement will need to be cognizant that competitive and financial interests could influence how forthcoming ISPs will be in reporting security issues with the IPv6 transition. A co-operative relationship with these companies will help police determine how criminals are exploiting the transition to IPv6 and develop the most effective countermeasures for crime prevention. (A)

As IPv6 becomes increasingly prevalent, cyber criminals will be able to inflict greater damage due to their ability to hide their IPv6 malicious code by using IPv4 as a tunnel. As the integration to IPv6 increases, more vulnerability will emerge. However, it can be expected that ISPs will also have no choice but to devote more time and financial resources to devising solutions and new ways to detect and protect against criminal misuse of IPv6. The window of opportunity for identifying and rectifying potential problems is before, not after, IPv6 becomes the only option for subscribers and criminals have learned even more sophisticated modes of attack. (A)

It is assessed with high confidence that cyber criminals will use the transition mechanisms of IPv6 to carry out their illicit activities until such time as firewalls and IDS are reconfigured to block them.

governments, businesses and individual users of computers and mobile devices can gain protection against unwelcome intrusions. (A)

[1] http://www.iana.net/internet-coordination/ipv4-exhaustion, last accessed 2011-12-15
[2] http://www.networkworld.com/news/2011/041411 apnic ipv4 gone.html, last accessed 2011 12 15
[3] http://news.bbc.co.uk/2/hi/technology/7220116.stm, last accessed 2011-12-15.
[4] It's All About You: Building Capacity in Cyber Security, Executive Summary, The Conference Board of Canada, National Security and Public Safety. September 2011, Preface.
[5] http://www.publicsafety.gc.ca/prg/ns/cbr/cssi-ecc-eng.aspx, accessed on 2011-12-15
[6] http://gadgetwise.blogs.nytimes.com/2008/08/15/botnets-captured-and-studied-and-the-findings-arent-good/, last accessed 2011-12-15
[7] Ibid
[8] http://www.v3.co.uk/v3-uk/news/2107731/ipv6-lead-huge-jump-cyber-crime, last accessed on 2011-12-15
[9]
[10] http://www.reuters.com/article/2011/11/18/us-nasdaq-cyber-idUSTRE7AG2NU20111118, last accessed 2011-12-15
[11] http://www.canada.com/story_print.html?id=5744140&sponsor=, last accessed 2011-12-16
[12] http://www.wired.com/threatlevel/2008/07/the-ghost-in-ys/, last accessed 2011-12-15
[13] http://www.ultrware.com/blog/?p=592, last accessed 2011-12-15
[14]
[15]
[16] http://www.theglobeandmail.com/news/technology/shaping-the-future/when-the-internet-runs-out-of-addresses/article2117561/, last accessed 2011-12-15