Initial Results from an IPv6 Darknet

Matthew Ford
BT Group plc
matthew.ford@bt.com

Jonathan Stevens
BT Group plc
jonathan.2.stevens@bt.com

John Ronan
TSSG/WIT
jronan@tssg.org

Abstract

A darknet is an advertised and routed portion of Internet address space that contains no advertised services. Any traffic observed on a darknet is therefore illegitimate and darknets are useful tools for observing the level of background 'noise' on a larger network. Darknets have been used in existing IPv4 networks to help to identify malicious traffic, malware trends, or the consequences of misconfiguration. We have created what may be the world's first IPv6 darknet to help us observe the 'noise' present on the IPv6 Internet and to see how this differs from the IPv4 Internet. Initial results suggest that the level of undirected malicious software active on the IPv6 Internet is currently minimal and there is no apparent undirected port-scanning activity. We suspect this is partially a (predicted) consequence of the larger IPv6 address space and also an indication of the immaturity of the IPv6 Internet at the present time.

1. Introduction and motivation

A darknet is simply an advertised and routed portion of Internet address space that contains no advertised services. Any traffic observed on a darknet is therefore abnormal and darknets are useful tools for observing the level of background 'noise' on a larger network. Darknets have been and are used in existing networks to help to identify the types and sources of malicious traffic present on the larger network of which they form a part [1]. The benefit of a darknet is that there is typically very little legitimate traffic present (network mapping projects may generate legitimate traffic to a darknet) which makes the process of identifying illegitimate traffic extremely simple. Traffic typically observed on a darknet is either the result of malware scanning for hosts to infect, the result of misconfiguration, or backscatter from hosts under attack.

IPv4 darknets can see huge amounts of traffic for even small amounts of address space, e.g. average traffic levels of 541.8kbps in a single /24 of darkspace [2]. IPv4 darknets are characterised by relatively constant receipt of traffic to the darkspace. This is not surprising given the widespread and indiscriminate nature of IPv4 malware 'deployed' on the Internet today.

The IPv6 Internet has now achieved global proportions, although it does not offer the same level of quality, in terms of route efficiency and link bandwidth, as the IPv4 Internet [3]. As part of our ongoing work to support and develop the IPv6 Internet through the operation of the UK6x Internet Exchange [4], we considered that it would be instructive to establish and monitor an IPv6 darknet to assess the level of malicious activity present on the IPv6 Internet, and also to verify the predicted lack of undirected port-scanning activity on the IPv6 Internet as a consequence of the much larger address space [6]. We consider that this may also become a great resource for a longitudinal study of malware in the IPv6 Internet.

Section 2 below briefly indicates related work in the area. Section 3 details the design of the deployed darknet. Section 4 presents our initial results while Section 5 provides brief details of some recent activity undertaken to extend the scope of our darknet experiments. Finally, Section 6 draws some conclusions from the results and suggests directions for further research.

2. Related work

The idea of a darknet (or network telescope as the technique is also known) is certainly not new and there are several important papers in the academic literature relating to previous work observing activity on the IPv4 Internet. [8][9][10][11][12] There has also been some recent activity (although as yet unpublished) relating specifically to IPv6 Internet Background Radiation. [13]

3. IPv6 darknet design

This section provides basic details of the design and configuration of our IPv6 darknet.

3.1. Network configuration

Design of the IPv6 darknet was kept deliberately simple. A darknet server was installed at our IPv6 PoP in London, UK, with two Ethernet connections. One of these was cabled to the PoP LAN to provide a management interface to the darknet server. The other interface was linked directly to a spare port on a core router. A darknet prefix was chosen from our larger IPv6 aggregate and the router configured to route this prefix to the darknet server over the dedicated link. A /48 prefix was used for the darknet. This is $1/2^{48}$ of the entire IPv6 address space and $1/2^{31}$ of allocated IPv6 address space (see Section 6 below for elaboration on this point). Figure 1 illustrates the configuration.

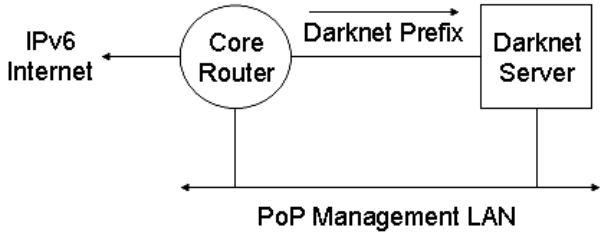

Figure 1. Network configuration for the IPv6 darknet installed at UK6x, Telehouse, London, UK. The *Core Router* is configured to route the *Darknet Prefix* to the *Darknet Server* over a dedicated point-to-point link. The *Darknet Server* is also accessible via the *PoP Management LAN* to enable management operations to be undertaken without polluting the darknet packet capture operation

3.2. Darknet server configuration

The darknet server configuration was based on a minimal subset of the information contained in [1]. The server is running the FreeBSD OS. We have configured it to run ntp to ensure relatively accurate timestamps on the logged packets. A blackhole route is installed for the darknet prefix to ensure that it isn't possible for the darknet server to respond to any traffic sent to the darknet prefix. The pf packet filter is used to block all traffic in and out of the darknet interface thereby ensuring none of the running processes on the darknet server can be affected by traffic to the darknet prefix. Finally, pflogd is enabled to capture all packets arriving on the darknet interface and log them to a file for later analysis using tcpdump. It is also possible to view packets arriving in real time by executing tcpdump on the pflog0 virtual interface.

3.3. Router interface configuration

In addition to the configuration necessary to enable the point-to-point link to the darknet server and to route the darknet prefix over the correct interface, it is also worth noting two additional aspects of the router configuration specific to the darknet.

- Router Advertisement messages are suppressed on the point-to-point link as they are not desirable on a statically configured interface and would only serve to pollute the darknet with extraneous packets.
- A static entry is configured in the router's Neighbour Cache with the MAC address of the darknet server NIC. This is necessary because the darknet server will filter Neighbour Solicitation messages by design, rendering the Neighbour Discovery protocol inoperative [5].

4. Initial results

The darknet was installed at the beginning of December 2004 and in the period until March 2006 a total of 12 packets were observed. The following traffic has been observed (in the analysis below, our darknet prefix has been deliberately obscured):

```
2004-12-18 18:10:03.861642
xxxx:xxxx:Axxx::51f3:10ee >
xxxx:xxxx:Bxxx::51f3:10ee: icmp6:
echo request seq 1

.

.

2004-12-18 18:10:11.860203
xxxx:xxxx:Axxx::51f3:10ee >
xxxx:xxxx:Bxxx::51f3:10ee: icmp6:
echo request seq 9
```

– ICMP echo requests where mistyped destination address can be inferred from the fact that the destination address prefix is only one digit altered from the source address prefix (i.e. A = B + 1)

```
2005-04-22 18:27:59.463636
xxxx:xxxx:Axxx::d995:72c2 >
xxxx:xxxx:Bxxx:9ccf::d995:72c2:
icmp6: echo request seq 1
```

– Probably another typo, although in this case the destination prefix is less similar to the source prefix.

```
2005-06-07 18:01:39.316524
2001:618:400::1 >
xxxx:xxxx:xxxx:29aa::35: [|icmp6]
```

– ICMPv6 Destination Unreachable Message (communication with destination administratively prohibited) indicating source address of the original packet was within the darkspace. The original packet was either deliberately or accidentally using a false source address. The presence of only a single such packet suggests accidental misconfiguration that was quickly remedied.

```
2005-06-15 15:40:51.566615
2001:7f8:2:c021::2 >
xxxx:xxxx:xxxx:ffff:af5f:8e7c:fc6b
:eca6: [|icmp6]
```

– ICMPv6 Destination Unreachable Message (no route to destination) indicating source address of the original packet was within the darkspace. The original packet was either deliberately or accidentally using a false source address. As above, the fact that there is only a single such packet suggests accidental misconfiguration that was quickly remedied.

The sources for all the observed traffic are within one or other of our prefix allocations from RIPE. We have not seen any inter-provider traffic reach our darknet.

5. Recent activity

In an effort to obtain more data from our IPv6 darknet experiment, we have added a second /48 darknet prefix sourced from within the pool of addresses used for our tunnel-broker service. This pool is relatively densely populated with hosts and may therefore result in a higher level of observable activity.

We have also recently sought to verify our findings by establishing a second darknet at another location. To date, these activities to extend the darknet work have not yielded any additional results.

6. Conclusions and recommendations for further research

It is clear from the initial results detailed above that we have observed no darknet traffic that we can attribute to malware or port-scanning activity of any kind. The very low level of darknet traffic detected seems to be entirely attributable to misconfiguration. This is perhaps not surprising when we consider the theoretical implications of IPv6 for TCP and UDP port-scanning [6]. In addition, the IPv6 Internet is relatively small and under-utilised at the present time and consequently the incentives for malware authors to make their code IPv6 capable are not great. It will be very interesting to track the level of darknet activity over the coming years as IPv6 deployment and utilization escalates.

The prefix allocated for our IPv6 darknet has a prefix-length of /48. Allocating a larger prefix may yield more data as the amount of darkspace encompassed would be commensurately greater. Indeed, a /48 is a tiny proportion of the already allocated IPv6 address space. The RIPE NCC IPv6 Allocations page [7] shows a total of 2,954,600,515 /48s allocated on 2006-03-29, which means that a single /48 is approximately equivalent to something between an IPv4 /31 and a /32, in terms of the proportion of allocated address space encompassed. Allocating a much larger darknet prefix is one area for further research. Similar activity to that reported in this paper, but utilising an IPv6 /32 has seen low-level regular scanning activity. [13]

As the level of background traffic increases, research could progress to developing automatic techniques to separate the benign traffic (network mapping, misconfiguration) from the truly malicious.

An IPv6 honeynet would also be an obvious direction for future research as levels of observed background traffic increase.

7. References

[1] The Team Cymru Darknet Project, http://www.cymru.com/Darknet/

[2] Darknet Incoming Traffic Stats (2005-08-24), DARK06 (ARIN) Average Traffic 541.8 kbps, Dark Space /24 x 1, http://www.cymru.com/Reach/darknet.html

[3] Zhou, X., and P. Van Mieghem, "Hopcount and E2E Delay: IPv6 Versus IPv4", PAM2005, Boston, USA, March 2005

[4] UK6x.com – IPv6 Internet Exchange for the UK, http://www.uk6x.com

[5] Narten, T., E. Nordmark and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC2461, December 1998, http://www.ietf.org/rfc/rfc2461.txt

[6] Chown, T., "IPv6 Implications for TCP/UDP Port Scanning", Internet Draft submitted to IETF IPv6 Operations Working Group, http://www.watersprings.org/pub/id/draft-chown-v6ops-port-scanning-implications-01.txt

[7] RIPE NCC IPv6 Allocations, http://www.ripe.net/rs/ipv6/stats/

[8] K. Thompson, G. Miller, and R. Wilder. Wide area Internet traffic patterns and characteritics. IEEE Network, 11(6):10–23, November 1997.

[9] V. Yegneswaran, P. Barford, and D. Plonka. On the design and use of internet sinks for network abuse monitoring. In Proceedings of Recent Advances in Intrusion Detection, 2004.

[10] V. Yegneswaran, P. Barford, and J. Ullrich. Internet intrusions: Global characteristics and prevalence. In Proceedings of ACM SIGMETRICS, June 2003.

[11] D. Moore. Network telescopes: Observing small or distant security events. Invited Presentation at the 11th USENIX Security Symposium, 2002.

[12] http://www.caida.org/analysis/security/telescope/
[13] D. Pemberton, Internet Background Radiation, presentation to NZNOG Conference 2006, 24-03-2006, http://www.nznog.org