NEN – The Education Network

Guidance Note: The Dark Web

July 2016

This Guidance Note is based on an original paper written by Paul Mavis @ Netsweeper Inc

What is the Dark Web?

"The Dark Web" as a phrase often conjures the impression of something scary. It can be a scary place, but it isn't necessarily so. Firstly it will probably help to define the term "The Dark Web"; it appears to be an alias of an earlier term "The Deep Web" and seems to be interchangeably utilised. It may be that the term "The Dark Web" has become more popular simply because it conjures a fearful mental picture.

The Deep Web

The term "The Deep Web" was first ascribed to Michael K. Bergman who in the year 2000 said how searching on the Internet can be compared to dragging a net across the surface of the ocean. This led to two analogies, "the surface web" and "the Deep Web". In essence the surface web is that portion of the World Wide Web that can be located and indexed by traditional search engines, whereas the Deep Web is all the content that the search engines cannot reach. Most of this Deep Web content has no special context, it is just data that may reside on a web server but is protected by a login and password.

The Deep/Dark Web & anonymity

There are sections of this Deep Web content that have been subverted and used for illegal activity. For example the TOR network originated from the work of the United States intelligence agencies and the US military. The goal of the TOR network is to anonymise the routing of data packets across the Internet, the intention is to make it incredibly difficult to trace back to the source of a connection. Whilst we might immediately see this as a negative, there are positive uses for such anonymity such as allowing civil liberty to be expressed in an otherwise heavily censured regime. However, TOR has been used for much illegal activity too, possibly the most (in)famous examples relate to illegal drugs, images of child abuse and fraud.

The Deep/Dark Web & protecting children in school

What can we do about this? Well the good news is that a school with a properly managed network environment with a good web filtering solution already has some protections in place.

The Dark Web is not just a web filtering issue, the firewall that protects the boundary of a school's network must also be well configured. The firewall should prevent any attempted connection from client computers to servers on the Internet. Instead client computers should need to go through a controlled proxy server, and/or have explicit permission (firewall rules). This applies to web browser

traffic, but also to other types of traffic such as terminal sessions (telnet, ssh), and remote desktop sessions (RDP, VNC), file exchange protocols (ftp), virtual private networks (VPNs) etc.

Taking the TOR browser as an example, when that application starts, it will also start some background processes that will assist in making network connections. These connections should be denied by the firewall. The TOR browser can also use standard web browser connections to web servers that act as gateways into the TOR network.

A good way to manage and track these web gateways into the TOR network is to ensure that the onion domain is denied by your filtering system deny list.

An entry of onion of type URL will deny access to any server on the .onion domain. Similarly, you should consider denying access to the .exit and .noconnect domains because those 3 domains are strongly connected to the operation of the TOR network.

To help further, a deny entry of tor of type path will further deny access to much of the TOR network's automatic configuration entries. You should probably also consider denying torproject.org of type URL since this will limit the download of the TOR browser, and the supporting information, such as the list of bridges.

It is also worth noting that the developers of the TOR network and its software are aware that controlled networks will attempt to deny access. They have therefore developed methods to utilize other common transport protocols. The most advanced other protocol is SMTP, therefore you will also need to look to your email gateways and firewalls to further protect your users.

There is yet more in this area, the TOR developers have provided a plug-in mechanism that rapidly allows other developers to circumvent your network protections. It is beyond the scope of this document to detail these plug-ins. System administrators beware!

For web browser traffic, the good news is that filtering Groups and Policies will protect you and your users from accessing much of the Dark Web. We would recommend controlling access to social media too. It is believed that most young people are first exposed to the Dark Web and indeed radical idealisms over social networks.

In some scenarios it may be more beneficial to report and/or alert members of staff when certain web sites or categories of web sites are accessed, rather than denying them. Teaching and learning sessions could then follow up as appropriate.

Multiple layers of protection are always recommended by security professionals. Where possible you should prevent your end users from installing or running unauthorized software using workstation or domain policy enforcement.

Other measures might include developing a school policy to encourage any personally owned smartphones and tablets used in school (as part of a Bring Your Own Device or BYOD policy) to connect to the school Wi-Fi network in order to provide a level of filtering, since a Wi-Fi connection is generally preferred by devices over mobile/cellular networks.

The Dark Web is an ever changing, ever developing "place". A final cautionary note is to remind you that web filtering is not the only tool required to keep your users safe when online; see the advice

on the following page and consult your broadband and/or filtering service provider for further support.

Further NEN advice & guidance:

- 10 steps to protect your schools' network http://www.nen.gov.uk/10-steps-to-protect-your-schools-network-a-guide-for-school-leaders/
- E-Security: Managing and maintaining e-security/cyber-security in schools http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
- School e-Security Checklist http://www.nen.gov.uk/school-e-security-checklist/
- Differentiated Filtering for Schools http://www.nen.gov.uk/differentiated-filtering-for-schools/

E-safety guidance from NEN providers:

- London Grid for Learning: online safety & safeguarding https://www.lgfl.net/online-safety/
- South West Grid for Learning: online safety services http://swgfl.org.uk/products-services/esafety
- East of England Broadband Network E2BN: essential online safety http://www.e2bn.org/cms/index.php/e-safety
- Northern Grid for Learning: Digitally Confident http://www.digitallyconfident.org/
- Birmingham City Council Link2ICT: safeguarding http://www.link2ict.org/safeguarding

Filtering & internet security providers:

- Netsweeper http://www.netsweeper.com
- Lightspeed Systems http://www.lightspeedsystems.com/en-uk/
- Smoothwall http://smoothwall.com/
- RM SafetyNet http://www.rm.com/products/online-safety-tools/rm-safetynet
- Kaspersky Web Filter http://www.kaspersky.com/partners/oem/oem-technology-solutions/KWF
- Bloxx https://www.bloxx.com/uk/ & https://www.bloxx.com/uk/news-events/2015/november/akamai-acquires-bloxx/
- OPENHIVEwebshield http://www.openhive.net/openhive-products/openhivewebshield/
- Trend Micro: Going Deeper: Exploring the Deep Web http://www.trendmicro.co.uk/vinfo/uk/security/news/cybercrime-and-digital-threats/exploring-the-deep-web

Please note: the above links to commercial providers are included for information and illustration only; the inclusion of a link in this list does not imply any endorsement by the NEN, nor does exclusion imply the reverse.