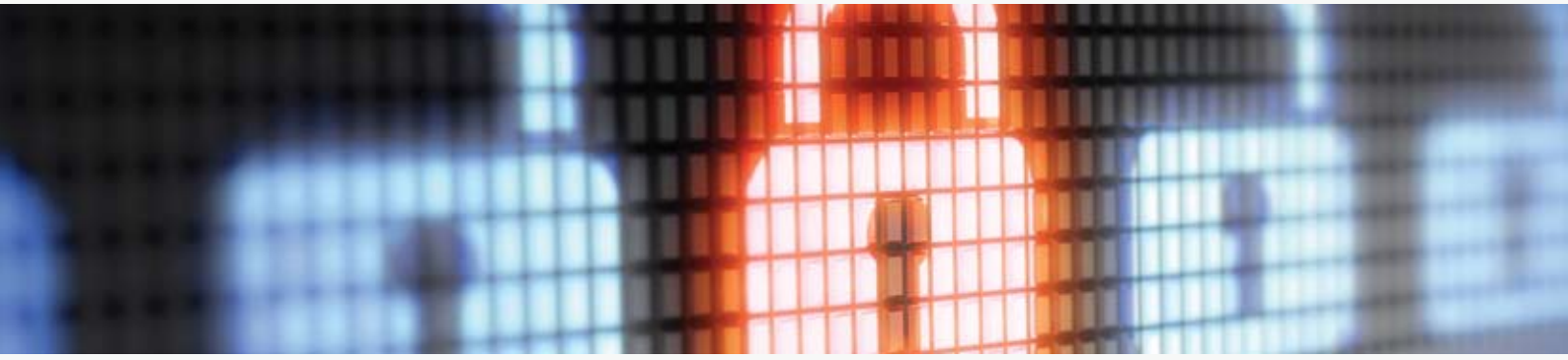
Netintelligence



Our Assesment Process

Netintelligence

Our Assesment Process

There can be little doubt that the internet has had a major impact on our lives. As well as being the world's biggest library, the internet now offers us instant communications, marketing and sales opportunities & ecommerce - all at the click of a button. Yet the internet is not without its perils.

The online world, like the rest of society, is made up of a wide array of people and organisations. The overwhelming majority are decent but a very small minority are intent on causing harm and exploiting the vulnerabilities of others.

In 1998, Netintelligence realised that there would be a downside to internet usage and set about 'mapping the dark side of the web'. This involved a team of people collecting and assessing as many different types of Malware as possible - Malware in this case literally meaning 'bad/harmful software' e.g. hacking, phreaking, credit card generating tools, password crackers and steganography
applications. The objective behind this 'mapping' exercise was to produce a database that could be used to assist commercial organisations, who were just beginning to enter this brave new technological world, in identifying the presence of these threats on their own networks. From these early pioneering days, this database has grown to become one of the worlds largest of its type.

Netintelligence's hosted security and management products are unique in that they constantly communicate with the Security Centre databases receiving the latest updates, anti virus & anti spyware signature files automatically - without any end user intervention/action. The Databases contain inappropriate and harmful web sites & files, anti virus & anti spyware signature files and materials classified as illegal by the Internet Watch Foundation.

Content Assessment & Categorisation Technologies

Netintelligence has developed a proprietary content assessment system which incorporates several differing technologies, the main one being 'Digital Fingerprinting'.

Every day, thousands of files are harvested from a number of sources - the internet, newsgroups and commercially available lists. Each file is gathered using a number of procedures, both automated and manual e.g. all files posted on potentially relevant newsgroups are automatically collected, and materials downloaded from targeted sources. Netintelligence also subscribes to various lists, provided by professional industry bodies, to widen the scope of the collection process.

Using these methods, the database collects approximately 700 000 files per week. Once gathered, the files are put through a process which assigns the "fingerprint" to the file, checking whether that fingerprint is already in the database, and copies any new files to a holding area to await assessment. On average, this process will provide around 300 000 files for assessment per week, indicating that around 57% of files gathered are already fingerprinted within the Netintelligence databases.

Any new fingerprinted files, held within the holding area, are then personally assessed by the team, as belonging to one or more of the undesirable categories held within the databases. The intervention of human assessment reduces false positives and over blocking or preventing access to innocent sites.

Numerically, the vast majority of files presented for assessment involve pornography, nudity, or sexuality, and are assessed as such. However, there is a wide range of alternative subjects available, and the Netintelligence assessors ensure that files are allocated to the correct category.

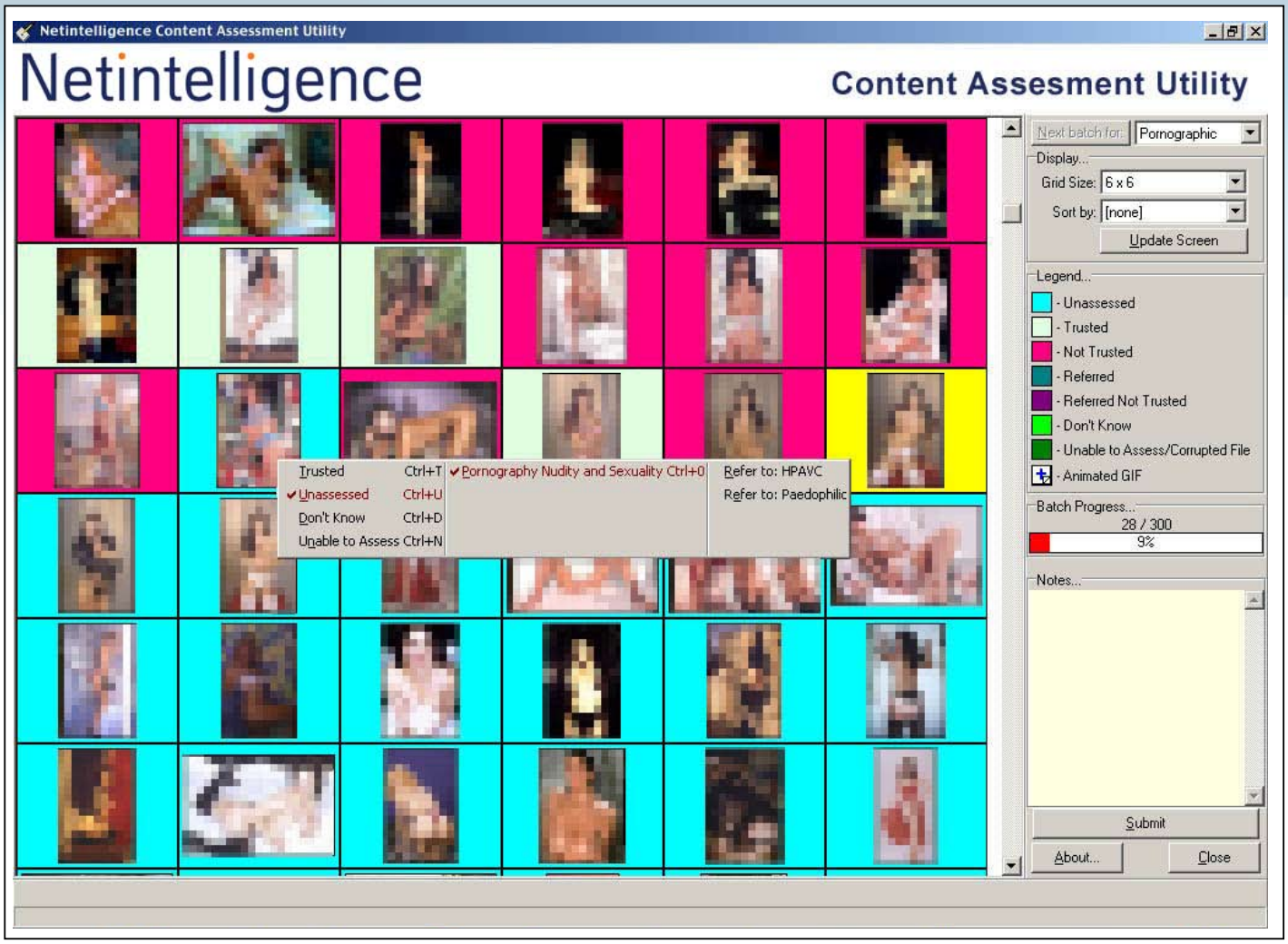
Many files are entirely innocent, and are assessed as such; fingerprints of these files will not appear in the database, but will be retained to avoid future duplicate assessment. This process produces an average of 100 000 new fingerprints of inappropriate files weekly.

After the assessment procedure is complete, the file and the fingerprint become entirely separate entities. Although the fingerprint is unique to that file (the result of a one-way algorithm - ensuring that every file has a different fingerprint) there is now no need to retain the files, and these are then deleted; only the fingerprints appear in the database, not the files themselves.

The 'digital fingerprint' ensures that it has captured the file's original 'DNA' and it will not matter if this file is renamed or hosted on a different web site - it remains assessed and captured in the database.

Netintelligence

Our Assesment Process



Content assessment utility - one of the tools used by Netintelligence to capture, identify and classify inappropriate images.

SECURITY CENTRE MAIN CATEGORY DEFINITIONS

- **Adult** – Pornography, nudity, sexuality, art nudes, naturism, adult goods, dating & personals, adult games etc
- **Drugs** – Advocacy, instructional, supply sites and associated literature
- **Hate** – Aggressive, violence, terrorism, gore, promotion of hate, intolerance, prejudice or lawlessness
- **Hacking & Other Threats** – Hacking, cracking, phishing, proxies and redirectors, virus creation, warez etc.
- **Gambling** – Commercial sites, tipping/information sites, casinos, bookmakers etc.
- **Games** – Coin-op , online, video, game-playing groups, puzzles, gaming resources, role-playing etc.
- **Recreation** – Non sport or music related Hobbies & Pastimes, "time-wasting" and joke/humour sites.
- **Caution** – Domains that host thousands of personal and small business web pages e.g. Geocities.com or Angelfire.com. Although such domains are not in themselves untrustworthy, much of their content may be of a harmful nature. Individual web pages are therefore assessed.
- **Alcohol** – Advocacy, supply, manufacture, and associated literature
- **Tobacco** – Advocacy, supply, manufacture, and associated literature
- **Weapons** – Advocacy, supply, instructional and use
- **Web Mail** – Major web mail sites
- **Sports** – participation, spectator and "fan sites".
- **Music** – Music subject matter, recorded music, music tuition, music fan sites, musical instruments, music business etc.
- **Shopping** – Major e-commerce sites, auctions sites, high street stores

Netintelligence

Our Assesment Process

The Internet Watch Foundation (IWF) was formed in 1996 following an agreement between the UK Government, Law Enforcement agencies and the internet service provider industry that a partnership approach was needed to tackle the distribution of child abuse images (often referred to as child pornography) online. The remit of the IWF is to minimise the availability of potentially illegal internet content specifically:

- Images of child abuse* hosted anywhere in the world.
- Criminally obscene content hosted in the UK.
- Criminally racist content hosted in the UK.

Netintelligence is a member of the IWF and obtains a data feed of web sites that have been assessed and classified as illegal by the IWF. This feed directly enters the Security Centre databases.

Netintelligence's unique relationship with Kaspersky, one of the World's leading Anti Virus vendors, ensures that all users of our service are constantly updated and protected, against viruses and spyware, without the need for any intervention at all. Over the past 19 years, Kaspersky has become a technology leader and acknowledged expert in the fields of anti virus and malicious programs.

Kaspersky Lab is the leader in the percentage of viruses, Trojans, backdoors and other malware detected.

#1 in Detection Rates - August 2005

99.88% - Kaspersky ✓
99.41% - Symantec
98.19% - McAfee
95.28% - Frisk Software
91.25% - Trend Micro
89.12% - Sophos
87.44% - GriSoft/AVG

source: www.av-comparatives.org

#1 for the frequency of released, working, unique, automatic anti-virus definition updates (Jan 2005)

573 - Kaspersky ✓
83 - Sophos
54 - Bitdefender
30 - Trend Micro
22 - Fortinet
7 - McAfee
6 - Symantec

Source: AV-Test.org Research Group, Magdeburg University

#1 For response time (response time to a series of incidents Jan 2004)

2h:34m:28secs - Kaspersky ✓
7h:16m:47secs - Sophos
8h:18m:24secs - GriSoft/AVG
8h:42m:51secs - Trend Micro
12h:54m:06secs - McAfee
14h:00m:11secs - Symantec

Source: AV-Test GmbH

HOW THE NETINTELLIGENCE SECURITY CENTRE DATABASES KEEP YOU SAFE AND SECURE

- Over 30 million harmful files and web sites assessed and digitally fingerprinted
- Team of Human Assessors to prevent False Positives
- An average of 100,000 new files added each week
- Automatic Anti Virus & Anti Spyware signature updates from Kaspersky
- Automatic illegal file updates from the Internet Watch Foundation
- Database created in 1998 and has been updated 24 x 7 ever since

Netintelligence

For further details: www.netintelligence.com or email: info@netintelligence.com. Tel: 44 (0)370 050 0121