# Companies Exposed As 5 in 6 AntiVirus Solutions Fail To Identify Threats

**Monday 24 March, 2014**

London UK, Monday 24th March 2014 – Businesses across the globe are becoming dangerously exposed to increasing cyber threats as almost 85% of the world's leading AntiVirus solutions are constantly failing to identify emerging threats.

With an increasing level of technological solutions becoming implemented across the everyday operations of businesses everywhere, cyber-crime is quickly becoming the most prevalent risk to companies, their data, assets and customers. With leading AntiVirus vendors providing an inadequate level of protection for both individuals and businesses alike, the risk to company and client data is being left open to compromise on a daily basis.

In addition to more sophisticated IT systems and cloud based computing, the huge increase in personal devices being used in the workplace means the potential for malicious attacks has never been more real. Graeme Batsman, Security Director at EncSec commented:

“Working in the cyber security niche means I experience first hand how destructive malicious cyber attacks can be. We're constantly reminding clients that identifying vulnerabilities and addressing them now with a suitably robust multi-level approach, is the only way to deal with the developing cyber threat.

Simply installing an AntiVirus software isn't anywhere near sufficient, with recent testing identifying that only 1 in 6 AntiVirus vendors were successfully identifying virus infections. Hacktivism, organised crime, commercial intrusion, data theft and even terrorism are now cyber enabled, so it's no longer an option to rely on conventional all-in-one antivirus solutions, regardless of the brand”.

EncSec staff test out live virus samples many times per month to see how leading antivirus vendors score. Email borne infected attachments are scanned by using 51 antivirus engines. EncSec has seen a decline in detection rates over the last two years because of the increased sophistication of methods used to infiltrate computers and networks.

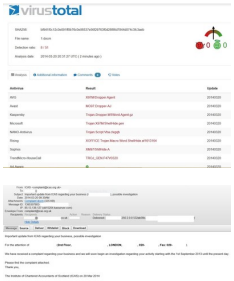
UK telecoms company 'BT' has released recent findings which indicate that 83% of surveyed business leaders do not feel cyber security should be a priority, contributing to the insufficient level of protection and preparedness for the most minatory global threat to emerge in 50 years.

**Notes to editor:**
EncSec is an independent IT security, investigation and digital forensics company based in Central London. They strive to offer private clients and their businesses reassurance and privacy from unwanted intrusion.

Image #1
Attached to the email is a .docm file (part of the Microsoft Word family) and this is uploaded to Virus Total which scans using 51 antivirus engines from 49 vendors. Only eight out of 51 antivirus engines detected the presence of malicious code.

Image #2
An email arrives claiming to be from ICAS (Institute of Chartered Accountants of Scotland). It claims a complaint has been filed against company X and within the email, company specific contacts are listed. All of this makes it more convincing and the recipient fearful of its reputation.

## Media:




## Related Sectors:

Business & Finance :: Computing & Telecoms ::

## Related Keywords:

Virus :: Malware :: Hack :: Hacking :: Cyber :: Crime :: Firewall :: Antivirus ::

## Scan Me:

## Company Contact:

_

**EncSec Ltd**

T. 0207 112 8222
E. info@encsec.com
W. https://www.encsec.com

**Additional Contact(s):**
Main Contact:
Graeme Batsman
07909 474 479

Alternative Contact:
Rob Webster
07545319460

View Online

**Additional Assets:**

**Newsroom:** Visit our Newsroom for all the latest stories:
**https://www.encsec.pressat.co.uk**