Two Shields Investments plc

("TSI", or the "Company")

Brandshield Update

Two Shields Investments plc, the AIM quoted investment company with a strategy to build a high-quality portfolio of investments in fast growing and scalable digital and technology enabled businesses, is pleased to reproduce the following announcement issued by Brandshield, in which it currently has an 11.34% shareholding and a Convertible Loan Note subscription of $1.8m.

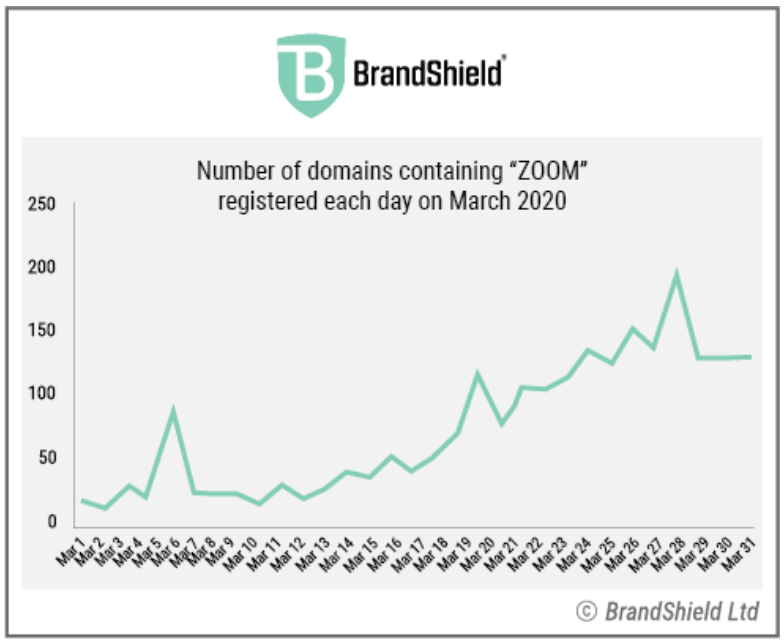
BRANDSHIELD REPORTS THOUSANDS OF POTENTIAL PHISHING SITES CREATED TO TARGET ZOOM USERS AS USAGE SOARS

2,200 new domain names with the word 'Zoom' set up in March 2020 alone with around one-third activating a mail server which is potential evidence of a phishing site

2 April 2020: BrandShield, a leading provider of cyber solutions from brand protection to online threat hunting, has today warned that cybercriminals are increasingly targeting Zoom users.

With COVID-19 forcing millions of employees to work remotely, usage of the popular video conferencing software has soared, with some reports estimating daily users have quadrupled as a result of the crisis. In response, cybercriminals are targeting the ever-growing number of Zoom users through sophisticated schemes. These schemes include the use of social phishing and fraudulent websites set up to steal money from Zoom users who believe they buy a subscription from Zoom directly. Criminals are also trying to steal Zoom user details to compromise accounts or infiltrate sensitive calls.

BrandShield's online threat hunting system has detected the registration of over 3,300 new domain names containing the word "Zoom" since the beginning of 2020. Of these, over 2200 were registered in March alone. This increase coincided with the spread of the virus, and the move to remote working. Over 30% of these new websites have activated an email server which is an indication of these sites being used to process phishing attacks.



Here are a few examples of suspicious websites detected by BrandShield:

- www.zoomnow.net
- www.zoomus.top
- www.zoomus.net
- www.zoomus.org
- www.zoomus.cn
- www.zoomcallonline.com (possible malware)
- www.zoomroom.link (possible malware)

As well as targeting companies through Zoom, cybercriminals are trying other scams to trick companies. These scams include impersonation on social media platforms or phishing emails. The scams are aimed at tricking employees into giving money away, provide the credentials to cloud-based applications, or pay fake invoices. This increase in online fraud is a significant threat that most companies are not prepared for.

Yoav Keren, CEO, BrandShield, said: "With global businesses big and small become increasingly reliant on video conferencing facilities like Zoom, sadly, cybercriminals are trying to capitalise. Businesses need to educate their employees quickly about the risks they may face, and what to look out for. The cost of successful phishing attacks is bad for a Company's balance sheet in the best of times, but at the moment it could be fatal."

"BrandShield protects some of the biggest corporations in the world and we takedown thousands of threats across websites and social media. We are getting companies approaching us all the time asking for our help. This problem is only going to get bigger as people spend more time transacting and interacting online".

Since the crisis began, BrandShield's online threat detection system has revealed a surge in fraudulent online activity, with key sectors being targeted including pharmaceuticals, medical supplies, banking, foreign exchange, loan providers, entertainment, online gaming and delivery companies. Some of the biggest threats are cybercriminals who are trying to capitalise on fears around the disease, and in many cases using the identities of known companies or brands to trick worried consumers. Attacks have included phishing sites, social phishing, fraudulent ecommerce sites, and fake medicine.

BrandShield has outlined the following simple steps companies and employees should take when to handle the growing online threat:

- Monitor – always monitor the digital sphere to find any fraud related to your company or brands, quickly
- Enforce fast – make sure you respond fast and effectively to take down fake sites and fake social media users or posts.
- Educate and warn your employees and customers – proactively communicate to highlight the dangers.
- Manage and control – manage a complete online threat intelligence map, prioritize the potential threats, control reactions and monitor their results.
- Proactiveness – Finding vulnerabilities and securing your weak spots. For example, remove old company websites that might be used for fraud.

Notes to Editors: Yoav Keren, Brandshield CEO, is available for interview via video link to discuss these issues. Please contact Robin Tozer (robin.tozer@newgatecomms.com) or Jamie Williams jamie.williams@newgatecomms.com)

For further information please visit https://twoshields.co.uk/ or contact:

Andrew Lawley	**Two Shields Investments plc**	Tel: +44 (0)20 3143 8300
Neil Baldwin / Andrew Emmott	**Spark Advisory Partners Limited** (Nominated Adviser)	+44 (0) 20 3368 3554
Andy Thacker	**Turner Pope Investments (TPI) Ltd** (Brokers)	+44 (0) 20 3621 4120

Notes to Editors:

Two Shields Investments plc, the AIM quoted investment company with a strategy to build a portfolio of high-quality investments in fast growing, scalable digital and technology enabled businesses, including those in the cyber security, e-commerce services and consumer sectors. The Company has appointed an experienced Board of Directors with a proven pedigree in the origination, acquisition, development & sale of projects and creating value for shareholders. The investment mandate covers unquoted and quoted businesses, as well as direct project investment. Where appropriate the Board will apply its extensive combined experience to directly support investee businesses achieve their growth potential.