**Intrusion and Data Breach Prevention Hits 21 Billion Mark**

FOR IMMEDIATE RELEASE: May 24, 2016

Oasis Technology, Inc., of Camarillo, California recently announced that their Titan Intrusion and Data Breach Protection system has now detected, prevented, and analyzed over 21 billion Intrusion and Data Breach attempts in less than two years.

This massive number surprises even the cyber-security engineers at Oasis Technology. “The real importance of this volume of attacks is the resultant statistics that this data provides. This massive amount of data provides a statistical awareness of how many unknown data breaches can occur in the realm of generally unprotected networks. This high number would not be occurring if there was no money in it. This large number of attempts indicates that stealth data breaches are lucrative and fertile hunting grounds for the hackers,” said George Baldonado, President and CEO of Oasis Technology, a leading provider of Internet and Network Security and Network Support for businesses.

Analysis of this data indicates the following:

- **Hack attempts are coming in 24x7.**

"This huge number of attacks further confirms our belief that cyber-terrorism, cyber-hacking and data breach attempts are the continuous, silent, hidden, stalking time bombs that threaten all Internet connections 24 hours a day, seven days a week. The attacks are continuous and will continue until an opening or weakness is found," added Baldonado.

- **All external IP addresses are being attacked regardless of the size of the company (big or small).**

It is apparent that hack attempts are being performed on all external/Internet based IP addresses, regardless of the size of the company. The only concern of the hackers is to find an open IP address. The size of the company that owns that IP address is of no concern to the hackers. All they care about is whether they can get into the network. Most hackers are like miners. Once they find a gold nugget (a weak IP address), they sell these IP addresses to big time hackers who use this information to open the Internet connection to obtain as much information as possible. This finding defeats the long held belief that companies will not get hacked because they are not big enough.

These statistics indicate that size does not matter when it comes to hackers.

- **Firewalls cannot provide all the protection needed.**

"While companies have installed popular firewalls, most firewalls really cannot withstand or control the barrage of sophisticated, constantly evolving threats that number in the millions per hour. Unfortunately, most companies do not even know that this is happening,” says Baldonado.

- **Many networks, even those with strong firewall defense systems, are vulnerable. Sooner or later all networks will collapse under the strain.**

At various times, IP addresses and networks are attacked by several thousand attacks per second, such as in the case of DDOS attacks and combined flood attacks. Many times a single IP address is attacked by several hackers at the same time. "As evidenced by this staggering number of attacks from geographically distinct locations, it is apparent that armies of hackers from all over the world are targeting the world's entire cyber-infrastructure, which includes all forms of information and capabilities such as military, data, intellectual property, innovations, our ideas and even our identity information. At their disposal are thousands of foreign computers that churn out thousands of hack attempts per millisecond looking to gain a foothold anywhere they can. Sooner or later the targeted network will most likely fold and open up. Once it opens up, either the network, firewall, operating system or program will crash, allowing the hackers to enter.

- **The attacks are coming from computer software especially designed to do hacking - as well as human attacks.**

Analysis of the attacks show that some attacks are coming from high volume servers or PC's and some attacks are low volume, carefully crafted attacks that are specific to the target.

- **Hack attempts are coming from all over the world, including the US, China, and Eastern Europe.**
- **Hackers are focusing on the millions of weak points on all networks.**

The origination geography of attacks show that the attacks can come from anywhere, even the United States. It appears that, on average, most computers are only 311 milliseconds away from most other computers in the world. This volume indicates that a great number of people are looking to illegally enter the computers -- and geographical location does not matter.

- **Hacking must be a lucrative venture - that is why so much effort is being put into it.**
- **When hackers attack your network they eat up your bandwidth, too.**

When hackers attack, they use up a little bit of your bandwidth. However, when thousands of people and computers attack a single IP address, this can result in a DDOS (Distributed Denial of Service) attack that can crash your servers, provide entry to your network, or severely limit access to or from your network. Sometimes this can be detected; sometimes it cannot be.

- **Stealth hacks are the worst because the victims do not know that they have been hacked -- and the hackers keep coming back to steal more.**

At least in a burglary, the victim knows that someone has broken in and something has been stolen. With stealth attacks, the victim does not know that something is stolen because a copy is made of the data and the original data is still in place. It is important to note that they do not alert you because then they can come back over and over again to obtain more and more information. Once they get in, the sky's the limit. "The frightening part is that most companies, corporations, and agencies don't even know that it has happened to them, that it is continually happening to them, or that they have even been breached," added Baldonado.

- **Network security has become extremely complicated.**

The sophisticated communications software that binds all computers together has become so powerful; yet each revision seems to come bundled with many additional vulnerabilities. This makes it almost impossible for any one individual to manage. As a result, many times the person in charge of network security does not know of the new vulnerabilities and therefore cannot proactively protect their networks. The large volume of attacks numbering in the millions can overwhelm even the most seasoned Cybersecurity manager.

- **Lastly, what is hidden will not be detected and not acted upon.**

With the combination of high volume attacks, increasingly more sophisticated attacks and stealth, the attacks and their results will most likely be hidden from almost all cyber-security experts. As a result, most network managers will falsely assume that their networks are not being attacked or that their networks are impenetrable. That is when the networks are the most vulnerable.

In summary, given the inevitable rise of IoT (the Internet of Things) and the ubiquitous connection to the Internet, everyone who is connected to the Internet -- almost every single person in the world -- needs to put considerably more effort and concentration into protecting their assets. Internet security levels are currently similar to the initial rise of viruses in the 80's. Many people thought that they were not vulnerable, only to find that this belief caused considerable consternation and grief.

In order to provide assistance in this area and to provide additional transparency on cyber-security to their customers and other professionals, Oasis Technology has provided a special web page to allow IT professionals and corporate governance to look into the current real time cyber threat index. This site will provide a glimpse into what is really happening and who the offenders are. The results can be surprising.

The URL for this site is http://www.oasistechnology.com/fightback/

This site is now available to the public.

"Misha Glenny, world renowned cyber-security specialist stated 'There are two types of companies in the world: those that know they've been hacked, and those that don't.' Studies indicate that Misha Glenny is very correct," closed Mr. Baldonado.

Oasis Technology is a leading provider of products and consulting services for information technology and cyber security serving all industries with sensitive data. For more information about Oasis Technology or Titan, visit the company website at www.oasistechnology.com

In addition to preventing intrusions, data breaches and providing instant external PCI compliance, Oasis is now also actively researching and adding technology to prevent social media attacks such as Ransomware and CryptoLocker.

George Baldonado, President and CEO, is responsible for the general direction of the company. He began his career in the computer industry in 1973, holding various technical and management level positions in international corporations such as Pacific Bell, GTE/Verizon, Eli Lilly, and Bank of America.

In 1991, he converted his partnership and founded Oasis Technology, Inc., a California "C" corporation. He holds a B.A. from the University of California, Santa Barbara, 1974, in Mathematics.

References:

http://www.oasistechnology.com/titan/

http://www.oasistechnology.com/fightback/

http://www.oasistechnology.com/juniper-breach-proves-that-titan-works/

www.facebook.com/oasistechnology

www.facebook.com/titanisp

http://usnews.nbcnews.com/_news/2013/02/19/17019005-successful-hacker-attack-could-cripple-us-infrastructure-experts-say?lite

###

Oasis and OASIS TITAN, OASIS Pegasus, OASIS Atlas, OASIS Zeus are trademarks of Oasis Technology, Inc.

Editorial contact:

George Baldonado, president

Oasis Technology, Inc.

Telephone: 805-445-4833

georgeb@oasistechnology.com