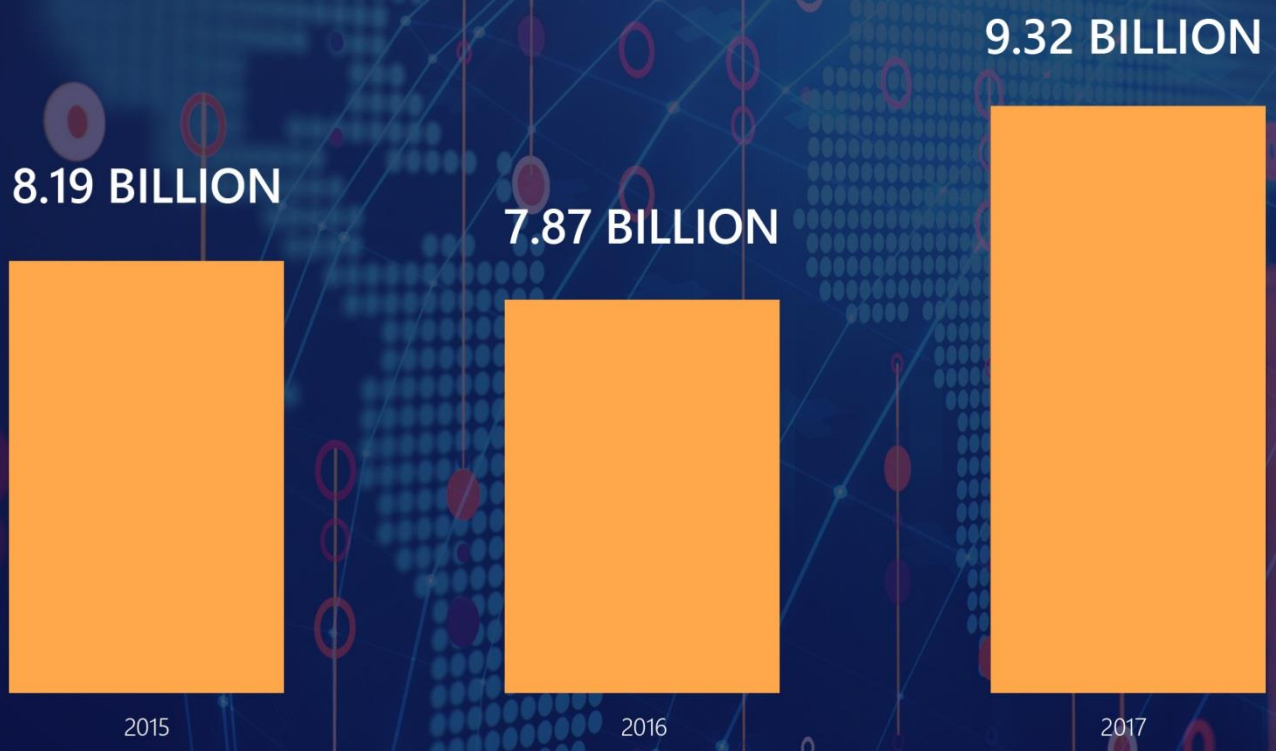
THE TACTICS HAVE CHANGED IN THE CYBER WAR OF 2018

PEGAS
TECHNOLOGY SOLUTIONS LLC

The Tactics Have Changed in the Cyber War of 2018

We're in a war against cybercrime. No business is safe, especially small to mid-sized businesses (SMBs). The statistics are frightening. In 2015 there were over 8.19 Billion attacks. In 2016 they decreased to 7.87 Billion. But in 2017, they skyrocketed to an alarming 9.32 Billion. To ward off these attacks in 2018 requires a plan that is proven to work. The problem is, these threats are evolving and changing.



The Fight Against Ransomware Has Never Been Harder

The way you fought cybercrime two years ago, isn't enough today. There's been a 101.2% rise in new ransomware weapons.

Today there are over 2,900 types of ransomware and more than 12,500 new CVEs (Common Vulnerabilities and Exposures) of which over three quarters are targeted against computer networks.

The criminals are changing their attack strategies. With Ransom32, a type of Ransomware-as-a-Service that provides criminals without any technical knowledge the ability to create their own form of ransomware, these "mercenaries" are creating cyber weapons that can be used against computers that run Windows, Mac OS X, and Linux.

We're caught in the middle of a cyber arms race that must be dealt with head-on with persistence, commitment, and the right defenses.

The Battle Against Encryption

Ransomware's main weapon is encryption technology. Ransomware attacks are on the increase, and as hackers use more sophisticated technology, the threat is constantly evolving.

According to malware security firm Barkly, a company is hit with a ransomware attack every 40 seconds. They also identified ransomware as the most prevalent form of malware, with "4.3x new ransomware variants in Q1 2017 than in Q1 2016."

Malicious payloads of SSL/TLS encryption were used against businesses more than in previous years. According to SonicWall Capture Labs, on average, 60 file-based malware propagation attempts are made each day. Without the ability to leverage resources like next-generation firewall protection, the average business would have missed over 900 attacks per year.

Mobile Ransomware is Another Threat

It's estimated that 6 billion mobile devices will be in use by 2020. With such a large audience, this is an ideal target. And mobile devices are being used to mine currency for attackers. These are prevalent in Windows and Android devices, and they're already at work.

Memory-Based Attacks Are Something New

It was only last year, in 2017, that processor vulnerabilities were detected. By then chip-based attacks were already in the works. These attack vectors use encryption methods that can't be decrypted. It's more important than ever to use enterprise-based cloud solutions and back up your data, so it's secure and easily recoverable. It's predicted that memory-based attacks will be a large threat to contend with for the foreseeable future.

The Internet of Things Is a Huge Risk

The IoT was a big target last year and will be bigger this year because this kind of smart technology isn't updated regularly. And as more of us are using IoT devices, the criminals have discovered ways to breach them. Mirai, the first IoT open-source botnet will take advantage of devices that are hidden in hard-to-reach places like in cars, machinery, appliances, and medical and manufacturing devices. Mirai is an IoT malware that can be used to launch gigabit-plus DDoS (Distributed Denial of Service) attacks. It uses common factory default usernames and passwords to gain access to connected devices and infect them with malicious code.

Artificial Intelligence Is Being Used Against Us

With the increased use of Artificial Intelligence and robotic workforces, cybercriminals now have additional targets of opportunity. With the invention of smart trucks and cars just now in the testing mode, external bad actors have already invented their own ways of taking control of the wheel.

PDF and Microsoft Office Threats Require New Forms of Protection

The next, new attack vector cybercriminals are leveraging are against PDFs and Microsoft Office programs. Many older legacy firewalls and anti-virus solutions can't identify and mitigate these threats.

Modern malware uses advanced techniques like custom encryption, obfuscation, packing, and sandboxing to hide malicious activity within memory. It hides sophisticated weaponry that's impossible to analyze in real-time using static detection techniques. To find and mitigate it requires a Real-Time Deep Packet Inspection Solution.

Data Grabbers

Many of today's critical threats use malware that steals information from computer devices. Some have political motivations and target defense personnel in specific areas. User data will continue to be a valuable commodity for hackers.

According to SonicWall president and CEO Bill Conner:

"Governments, enterprises, and individuals are in the crosshairs of a global cyber arms race. The risks to business, privacy, and related data grow by the day — so much so that cybersecurity is outranking some of the more traditional business risks and concerns."

His belief is also supported by the 2018 World Economic Forum (WEF) Global Risks Report, which found that many of the unexpected costs from 2017 came from cyberattacks.

"The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 were related to ransomware attacks, which accounted for 64 percent of all malicious emails."

Encrypted traffic is a growing weapon for cybercriminals. To survive the 2018 cyber war, your business must leverage the latest cybersecurity tools and solutions. What worked last year, and the year before won't be sufficient. They are already considered outdated.

What is Deep Packet Inspection?

Ransomware and encryption attacks will continue to be a threat during 2018 and beyond. Yet many aren't aware of the need to inspect SSL and TSL traffic, and the need to do so with solutions that utilize deep packet inspections.

Deep packet inspection (DPI), also known as complete packet inspection and information extraction is a form of filtering that is used to inspect data packets that are sent from one computer to another over a network. It is a very sophisticated form of packet filtering that operates at the application layer. It allows Technology Solution Providers to hunt down, identify, categorize, and reroute or block harmful packets with malicious code.

Normal packet filtering only inspects the packet headers. DPI goes deep to inspect the packet's data to find intrusions, spam, or viruses. With DPI, you can arm yourself with the weapons you need to fight today's malicious threats without a large investment in network technologies.

DPI combines the features of an intrusion prevention system (IPS) and an intrusion detection system (IDS) with a conventional firewall. Your Technology Solutions Provider can use it to manage network traffic and protect your business. With it, they control network traffic by allocating valuable network resources to high-priority messages and data packets.

DPI is being used by the U.S. government and others to monitor and protect cyber boundaries. It's an efficient, cost-effective method to protect your organization's cyber boundaries and a must-have defense tactic in the Cyberwar of 2018.

Contact us for more information about Deep Packet, SSL/TLS Inspection Controls and how they can protect your organization.

PEGAS
TECHNOLOGY SOLUTIONS LLC

Contact Pegas Technology Solutions at 207-835-4053 or sales@pegas.io