Your data isn’t safe. And neither is your website or your business.

Hacking has become more prevalent and more sophisticated over the years. But sometimes it’s the least sophisticated method of hacking that threatens the world’s biggest industries. In recent years, hacking has evolved from single-source denial of service (DoS) attacks to Distributed Denial of Services (DDoS) attacks, which strike from thousands of unique IPs. These disturbances can be created cheaply and easily and can take a service offline or shut a business down completely.
DDoS attacks have grown rapidly in scale and frequency, says Gartner research director Jeremy D’Hoinne. In a June 2015 webinar entitled, “The Cyberthreat Landscape,” he discussed the growth of DDoS attacks – from 10 Gbps in 2005, to 100 Gbps in 2010, to 400 Gbps in 2014.

In 2014, PC Mag reported on the explosive trend in volumetric DDoS attacks during the first half of the year in an article entitled, “DDoS Attack Volume Exploded in 2014.” It cited more than 100 events over 100 Gbps and about 5,800 20 Gbps attacks. These 2014 figures were more than double the approximately 2,600 DDoS attacks in 2013.

Mitigation service provider Prolexic recently reported on the industries most frequently targeted by DDoS attacks in its Q1 2015 “State of the Internet Security Report.” The gaming industry – with 35 percent of attacks – was the hardest hit, followed by software and technology (25 percent), Internet and telecom (14 percent), financial services (8.5 percent), and media and entertainment (7.5 percent).

Real-time infrastructure monitoring can provide the first line of detection against DDoS attacks. This is because, although use cases typically center on performance issues, the ability to monitor firewall and load balancer activity can arm network operations and security teams with the advanced warning they need to mitigate a DDoS attack.
There are more than a dozen well-known types of DDoS attacks impacting today's organizations. Some are orchestrated by seasoned hackers, but most are conducted by just a few computers aiming to take down a service or website by sending too many requests.

The most common types of attacks include:

- **SYN Flood attack** – This type of attack exploits the negotiation of a TCP connection, or the three-way handshake. An attacker will send a succession of SYN requests to their target’s system, attempting to consume server resources and rendering the system unresponsive to regular, authentic traffic.

- **UDP Flood attack** – This type of attack can be initiated by sending a large quantity of UDP packets to random ports on a remote host. From there, the host will check for the application listening to that port and learn no application is listening. The host will then reply with an ICMP destination unreachable packet. The attacker may also spoof the IP address of the UDP packets, which can render the service or website unreachable to other clients.

- **ICMP Flood attack** – This ping attack overwhelms the resource with large numbers of packets, sending them as fast as possible without waiting for a reply. This type of attack can jeopardize both incoming and outgoing bandwidth, slowing a service or website significantly.

These types of DDoS attacks have occurred at retail giants and big banks, alike in recent years. In July 2015, a DDoS attack caused a 50-minute outage to the Royal Bank of Scotland’s online banking system, affecting customers from RBS, Ulster Bank and NatWest Online Systems. In May 2015, hackers launched a DDoS attack on two of the largest financial institutions in Hong Kong – the Bank of China and the Bank of East Asia.
In July 2015, hackers compromised Planned Parenthood’s website, and New York Magazine’s website after it published the much-anticipated Billy Cosby exposé. Ashley Madison – a self-proclaimed site for extramarital affairs – was compromised as well, putting user databases, financial records and other proprietary information for 37 million customers in jeopardy.

In cases like these, when an attacker initiates a connection-based protocol, he or she might send 50,000 packets a second over the network, leaving connections open and vulnerable. If a company is monitoring their network, they’ll likely see a massive spike in connections from the load balancer, along with an increase in throughput on the firewall and the bandwidth utilization on Internet links.

Large enterprises and organizations are met with DDoS attacks on a daily basis. While a smaller attack may not have much of an impact, a bulk attack could yield or halt the delivery of applications or services.

When service is degraded or stopped altogether, the company’s reputation is impacted. Consider this: would you bank with a large financial institution if its website is slow or always down, or if there’s a high risk that the privacy of your financial information could be compromised?

There are three main groups DDoS attacks originate from. The most advanced group is highly complex, and sometimes stems from terrorist organizations. The next level is state-sponsored. The third tier is high school students, who are testing the waters, but typically don’t have the infrastructure or sophistication to launch a massive attack.

In addition to their sophistication and global reach, these hackers are strategic in their approach. On a Monday, they use one signature to infiltrate a network, before being kicked out. By Tuesday, they’ve got a new plan to attack a different organization or orchestrate a varied attack.
While it is difficult to predict where the next DDoS attack will originate from, it helps to be ready for anything. Deploying a real-time infrastructure monitoring platform provides the information needed to act at the first sign of an attack, by providing the IT department with a granular, but full picture of their digital infrastructure.

Monitoring provides a dashboard view across various components of the Internet-facing infrastructure, enabling users to identify the start of an attack in real-time. Users can be alerted when random ports are flooded with packets, or when spoofed requests from a variety of sources attack a target server. This agility helps them identify debilitating attacks before resources are exhausted and the server is forced to go offline.

From the dashboard, when alerted of an attack in real-time, users can drill down to the log data to see what IP address the attack is coming from. They can then work to take action and block traffic from that location.

Proactively monitoring F5’s BIG-IP® system alerts IT teams immediately when a spike in attack packets received occurs.
When considering infrastructure monitoring platforms, it’s important that IT departments choose one that marries performance metrics to log data. That’s because metrics will alert users if and when there is an issue, but the log data will identify the nature of the attack and where it’s coming from.

Reviewing up to a year’s worth of historical data allows users to set up accurate thresholds for questionable network traffic, like: when a specific number of packets come through in two seconds or less, automatically block this traffic. In this way, users are able to limit the number of DDoS attacks on the infrastructure.

According to Gartner’s D’Hoinne continuous monitoring and analytics, can transform organizations from a retrospective and detective mindset to a predictive and preventative one. He believes organizations fall into two different camps when it comes to predicting and preventing DDoS attacks: those who identify the breach themselves and those who learn of it from a third party.

Users who can explain the breach and show they did everything to block and prevent it are on the right track. He believes that how quickly the organization responds to the breach directly determines how much money is spent on mitigating the problem. Currently, according D’Hoinne, 67 percent of organizations that have experienced a breach reported that they learned of the attack from a third party vendor.

However, with the right infrastructure monitoring in place, organizations don’t need to fear learning about a DDoS attack from a third party. Monitoring provides insight into the attack before it’s too late.
A top five global investment bank utilizes an advanced infrastructure monitoring platform to add a layer of security and visibility into its data, applications and website.

Since deploying infrastructure monitoring, one employee said, the organization detected all but two DDoS attacks as they kicked off and had about five to 10 minutes before any services were impacted.

With monitoring in place, the company adopted procedural changes. In a six-month time span, employees prevented at least 12 DDoS attacks thanks to proactive detection. In this same timeframe, employees triaged about three DDoS incidents per week. By discovering the DDoS attacks at the first sign of a problem, the organization was able to spend less to mitigate the issue.
CONCLUSION.

With the threat of global DDoS attacks daily, it’s crucial to know what’s going on in company networks. Infrastructure monitoring provides the visibility and assurance needed to be prepared for a DDoS attack.

While not an absolutely preventative measure, infrastructure monitoring can help detect incoming attacks and prepare employees – who now have a full picture of their network – to handle an attack quickly and efficiently, lessening the harm to users and customers.

By deploying a platform that integrates metrics, flows and logs, employees of the world’s largest enterprises and financial services organizations can be assured they have as much data as possible to see, predict, prevent and address a DDoS attack.

About SevOne.

SevOne provides the world’s most scalable infrastructure performance monitoring platform to the world’s most connected companies. The patented SevOne Cluster™ architecture leverages distributed computing to scale infinitely and collect millions of objects. It provides real-time reporting down to the second and provides the insight needed to prevent outages. SevOne customers include seven of today’s 13 largest banks, enterprises, CSPs, MSPs and MSOs. SevOne is backed by Bain Capital Ventures. More information can be found at www.sevone.com. Follow SevOne on Twitter at @SevOneInc.