SecurityFAQ: DoS & DDoS

What is a DoS attack?

A DoS attack is a malicious attempt to make a machine or network unavailable to its intended users. DoS attacks have become highly sophisticated and can target network and application layers. Application layer attacks continue to become increasingly common.

How do DoS attacks work?

The classic DoS attack model involves one attacker attempting to make a computational resource such as CPU, disk, memory or network unavailable to its intended users, taking advantage of the asymmetry between the request and response necessary to perform a determined task.

What is the difference between a DoS attack and a DDoS attack?

Distributed Denial of Service (DDoS) is a type of Denial of Service (DoS) attack. This type of attack involves multiple slave computers in a botnet that act in coordination to attack the target.

Is my financial institution or customer data at risk due to DoS attacks?

No. DoS attacks are not designed to infiltrate systems, but they do affect the availability of our services to end users. Our number one priority during a DoS attack is to fully restore availability of all services without impacting end users. Digital Insight™ Solutions has strong “defense in depth” measures in place to protect all data, even during a DoS attack. During these attacks, our systems and security defense technologies are still fully operational, but the attacks block traffic from accessing our applications.

How does NCR typically combat these attacks?

We combat DoS attacks with a multilayer set of prevention, detection and mitigation capabilities to block application and network-based attacks. In keeping with industry practices and risk management, we cannot explain the specific processes and technology that we employ to detect and mitigate DoS attacks. However, we can assure you that we have several layers of protection in place and understand normal network traffic and systems behavior, which we monitor at all times.

When potentially malicious traffic is detected, we alert our security experts for immediate response and review. Our mitigation response blocks malicious traffic while allowing legitimate traffic to communicate with your financial services in a normal fashion. Our number one priority is to allow zero impact to end users while mitigating nefarious traffic during a DoS attack.

How else does NCR stay on top of trends related to these?

NCR constantly monitors DoS trends, current attack techniques and learn how to detect and mitigate them by working closely with our security partners and industry-leading intelligence sources. We also review all attack patterns we are experiencing. This continual awareness of current, real-world threat trends allows us to ensure that we can respond quickly to attacks and mitigate them with the minimum impact to you and your customers.

Is there anything my financial institution can do to provide additional protection?

If your financial institution does experience a DoS attack, it’s a good idea to review large transactions to ensure they are not fraudulent. DoS attacks are sometimes used to distract from normal business operations.

Will NCR notify our financial institution if a DDoS occurs?

A representative from NCR will contact your financial Institution if a DDoS attack is directed at your site that we manage and it impacts your service level.

Will NCR provide my financial institution with the IP addresses you are blocking so we can mitigate DDoS attacks on our end, too?

No. Sometimes a DDoS seizes control of legitimate computers that have been infected. This means that law abiding citizens or businesses can unintentionally be part of the group of computers used in a DDoS attack. To turn over these IP addresses would violate their privacy. Also, it would not help you permanently prevent DDoS attacks, which often change tactics and the compromised computers they use. In fact, rather than providing any benefit, you could unintentionally block traffic from legitimate end users.

Are these attacks preventable?

While there are steps you can take to defend, you cannot proactively prevent DoS attacks. Preventing them would require blocking legitimate traffic to your site, often due to the fact that DoS attacks utilize legitimate computers that have been compromised. The appropriate mitigation techniques use traffic patterns, signatures and other protocol sometimes combined with IP addresses to block illegitimate traffic, rather than only using an IP address, which would block all traffic from reaching a site. It is possible for a customer, whose computer is participating in an attack, to still access your site while the illegitimate traffic from the same customer's computer is being blocked.

Why can't you tell me early on if we're not the financial institution being attacked?

Due to the ever-changing nature of DDoS attacks, it's not always possible to confirm in real-time which financial institution or group of financial institutions are the target of a specific attack, or if they are the target at all. As soon as we have confirmed the target, we will work to update you. This message would likely say, "We are experiencing a DDoS. You are not the target, but the availability of your digital banking services may be impacted."

What is behind the recent DDoS attacks and are they all related?

The FBI has provided briefings, open to all U.S. financial institutions, on what they know about the recent DDoS attacks. We recommend you contact your local FBI office to ask for more details.