CYBERSECURITY

365 ARCHITECHS

Information Sheet

Network Threats

Tags: Cybersecurity, Attack Vectors, Threats

Network threats are attack vectors that involve an attack on the network itself. Other types of threats include host threats, application threats and social engineering.

This information sheet considers the different types of network threats that threat actors use to gain access to systems to steal information, harm reputations or disrupt operations.

Once inside a network, threat actors are able to slowly or swiftly move around the network laterally, looking for hosts to compromise by exploiting vulnerabilities. They can also use a network as a stepping stone to another network, such as a customer or suppliers system.

Compromised networks can go undetected for long periods of time, allowing threat actors to attack systems repeatedly. The average amount of time taken to identify and contain a breach is 279 days[1].

Man in the Middle Attacks

A man in the middle (MITM) attack involves threat actors intercepting traffic, either between a target network and external sites or within the network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.

MITM attacks typically rely on spoofing, that is, the act of disguising a communication from an unknown source as being from a known, trusted source. Different things can be spoofed, such as:

IP	ARP	HTTP	DNS

All computers connected to the internet have an IP address. Threat actors can pretend to send or receive communications from another device by masquerading with their IP address.

Address Resolution Protocol (ARP) is a method computers used to translate IP addresses to physical MAC addresses also used to identify specific devices for communications.

HTTP Spoofing involves threat actors creating very similar looking domains to those of the target websites. They might register an SSL certificate with the fake domain to make it look safe. Users are tricked into visiting fake websites by a range of methods, including receiving false links in email attachments.

The **Domain Name System** (DNS) is a component of networks that translate URLs and email addresses to IP addresses. DNS Spoofing can cause a legitimate URL to be redirected to a fake one.

Sniffing and Eavesdropping

When data is transmitted across a network, it isn't usually encrypted. This enables threat actors to intercept information in a similar way to the tapping of phone lines.

[1] IBM Security: Cost of a Data Breach Report 2019

About us
365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.
(07) 3393 1186 | www.365a.com.au | sales@365a.com.au

Disclaimer
These Information Sheets are designed to provide general information only. They should not be relied upon without consulting professional advice on your specific circumstances. 365 Architechs will not be held liable for any acts or reliance upon the information provided contained within.