TOKIO MARINE KILN

Cyber threat landscape Jargon buster

Your business faces many cyber security threats and the multitude of technical terms used to describe them can be bewildering. Below is a useful guide to the key threats you should be aware of:

APT

Advanced Persistent Threat. A very sophisticated attack that is carried out over an extended period of time and in different stages. After gaining initial access to your computer network, an APT will look to gain administrator rights and move laterally across the system in order to steal as much data as possible. Unlike the 'smash and grab' nature of a ransomware attack, an APT will try to remain undetected for as long as possible.

Botnet

A combination of 'Robot' and 'Network'. A botnet is a group of hijacked computers which has been infected by malware and is under the control of a malicious actor. Botnets can be used to launch DDoS attacks against your business. Your computer network can also be hijacked to form part of a botnet.

Credential stuffing

If your employees have been caught up in a third-party data breach, their compromised username and password credentials may be used to gain access to your computer network. Malicious actors use automated software to 'stuff' your network access login page with thousands if not millions of username and password combinations until they gain access.

Crypto-jacking

Cryptocurrency markets such as Bitcoin require large amounts of processing power to operate. Individuals can make money by volunteering their computers to carry out the complex mathematical processing required ('crypto-mining'). Crypto-jacking is where your computer network is hijacked by a malicious actor to run crypto-mining software which can dramatically slow down and potentially shutdown your computer systems.

Dark Web

Websites that exist on an encrypted network and cannot be accessed using traditional web browsers. The Dark Web is not indexed by regular search engines. If your business suffers a data breach, your stolen confidential information may end up for sale on the Dark Web. Malicious actors can also purchase tools on the Dark Web to target your business (e.g. ransomware, DDoS-as-a-service).

DDoS

Distributed Denial of Service attack. The use of a botnet to flood your network with electronic traffic in an attempt to overload your systems and prevent them from operating. DDoS attacks are particularly concerning for businesses reliant upon ecommerce as they prevent legitimate customers from accessing your site and buying your goods and services.

Malware

A blend of 'malicious' and 'software'. Malware is a programme or piece of code injected into a computer system for malicious purposes, such as stealing data, corrupting files or allowing unauthorised access. A computer virus is a type of malware. Criminals will target your business with malware in an attempt to make money, e.g. by deploying ransomware.

Ransomware

A specific type of malware that encrypts the data stored on your computer network and demands that a ransom be paid to gain access to the decryption keys. Recent ransomware outbreaks have crippled many large, sophisticated businesses networks. WannaCry, notPetya and LockerGoga are all strains of ransomware.

Social engineering

Social engineering relies on using confidence tricks as opposed to technical computer skills to lure your employees into releasing confidential information, visiting malicious websites or downloading malware. The most common example is phishing, of which spear-phishing is the most serious threat to your business.

Spear-phishing

Regular phishing is a non-personalised form of social engineering that attempts to trick your employees into taking action that threatens your network security. Spear-phishing attacks target a specific employee with emails purporting to come from a trusted source that they are familiar with and often include personal information. Given the level of personalisation, spear-phishing is more difficult to identify than large-scale phishing attacks.

Vulnerability

A vulnerability is a flaw or weakness in a computer system that leaves it susceptible to an attack from a malicious actor. You can minimise your exposure to known vulnerabilities by regularly patching your computer systems with the latest security updates. This will not work in the event of a zero day exploit, however.

Zero day exploit

An attack on your computer system that exploits a vulnerability before developers have released a security update allowing the vulnerability to be patched. In other words, the bad guys exploit the vulnerability before the good guys have had a chance to fix it.

About Tokio Marine Kiln

Tokio Marine Kiln is a leading international insurer with a reputation for underwriting excellence, great people and innovative products. As part of one of the largest insurance groups in the world, our underwriters are empowered to assess each individual risk, to make on-the-spot decisions and to find the right solutions for our clients' needs.

The ability to settle valid claims quickly and fairly in a human way is central to our business philosophy, and our adjusters are empowered to exercise their professional judgement to deliver an exceptional customer service.

If you want to find out more about our cyber product or other product lines, please contact us at hello@tokiomarinekiln.com

Empowered Expertise

www.tokiomarinekiln.com
T +44 (0)20 7886 9000

47949/05/20

To Be a ***Good Company***

Tokio Marine Kiln
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Firm Reference Number: 204909. Registered office is located at 20 Fenchurch Street, London EC3M 3BY Registered Number: 729671. Tokio Marine Kiln is a trading name.