What Is an Advanced Persistent Threat (APT)?

If there's one thing that keeps corporate cybersecurity professionals awake at night, it's the thought of an attack employing a range of sophisticated techniques designed to steal the company's valuable information.

As the name "advanced" suggests, an advanced persistent attack (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences.

The Prime Targets

Because of the level of effort needed to carry out such an attack, APTs are usually leveled at high value targets, such as nation states and large corporations, with the ultimate goal of stealing information over a long period of time, rather than simply "dipping in" and leaving quickly, as many black hat hackers do during lower level cyber assaults.

APT is a method of attack that should be on the radar for businesses everywhere. However,

The whole purpose of an APT attack is to gain ongoing access to the system. Hackers achieve this in a series of stages.

Stage One: Gain Access

Like a burglar forcing open a door with a crowbar, cybercriminals usually gain entry through a network, an infected file, junk email, or an app vulnerability to insert malware into a target network.

Stage Two: Establish a Foothold

Cybercriminals implant malware that allows the creation of a network of backdoors and tunnels used to move around in systems undetected. The malware often employs techniques like rewriting code to help hackers cover their tracks.

Stage Three: Deepen Access

Once inside, hackers use techniques such as password cracking to gain access to administrator rights so they can control more of the system and get even greater levels of access.

Stage Four: Move Laterally

Deeper inside the system with administrator rights, hackers can move around at will. They can also attempt to access other servers and other secure parts of the network.

Stage Five: Look, Learn, and Remain

From inside the system, hackers gain a full understanding of how it works and its vulnerabilities, allowing them to harvest the information they want at will.

Hackers can attempt to keep this process running — possibly indefinitely — or withdraw once they accomplish a specific goal. They often leave a back door open to access the system again in the future.

The Human Factor

A Remaining Threat

The major danger of APT attacks is that even when they are discovered and the immediate threat appears to be gone, the hackers may have left multiple backdoors open that allow them to return when they choose. Additionally, many traditional cyber defenses, such as antivirus and firewalls, can't always protect against these types of attacks.

A combination of multiple measures, ranging from sophisticated security solutions like Kaspersky Enterprise Security to a workforce that is trained and aware of social engineering techniques, must be deployed to maximize the chance of a successful ongoing defense.

Featured Articles

4 Common Cryptocurrency Scams and How to Avoid Them

AI and Machine Learning in Cybersecurity — How They Will Shape the Future

Is private browsing and VPN really secure?

What is a QR Code and how do I scan one?

What is Social Engineering?

Get the Power to Protect. Discover how our award-winning security helps protect what matters most to you.

Our FREE security tools and more can help you check all is as it should be... on your PC, Mac or mobile device.

Helping you stay safe is what we're about – so, if you need to contact us, get answers to some FAQs or access our technical support team, click here.

Who We Are

Find out why we're so committed to helping people stay safe... online and beyond.

Get Your Free Trial

Try Before You Buy. In just a few clicks, you can get a FREE trial of one of our products – so you can put our technologies through their paces.

Renew your license

Save up to 30% when you renew your license or upgrade to another Kaspersky product

Stay in Touch

f   🐦   in   ▶   📷

Home Products

Kaspersky Anti-Virus

Kaspersky Android Antivirus

Kaspersky Internet Security

Kaspersky Total Security

Kaspersky Security Cloud

Kaspersky VPN Secure Connection

Free Antivirus

All Products

Small Business Products
(1-50 EMPLOYEES)

Kaspersky Small Office Security

Kaspersky Endpoint Security Cloud

All Products

Medium Business Products
(51-999 EMPLOYEES)

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Business Select

Kaspersky Endpoint Security for Business Advanced

All Products

Enterprise Solutions
(1000+ EMPLOYEES)

All Solutions

Global

Contact Us   •   About Us   •   Partners   •   Blog   •   Resource Center
•   Press Releases   •   Sitemap

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE