Zero-Click Attack

sanskritiias.com/pt-cards/zero-click-attack-39

- A zero-click attack **helps spyware like Pegasus gain control over a device without human interaction or human error.** So all awareness about how to avoid a phishing attack or which links not to click are pointless if the target is the system itself.
- Most of these attacks exploit software which receive data even before it can determine whether what is coming in is trustworthy or not, like an email client.
- Zero-click attacks are hard to detect given their nature and hence even harder to prevent. **Detection becomes even harder in encrypted environments where there is no visibility on the data packets being sent or received.** One of the things users can do is to ensure all operating systems and software are up to date so that they would have the patches for at least vulnerabilities that have been spotted.
- **Pegasus is a spy tool developed by an Israeli firm the NSO group,** which is sold to the governments of many countries of the world. **Under this an 'exploit link' is sent to a user's phone, when the user clicks on that link 'Malware' code is installed, through which the attacker takes control of the 'target' user's device.**
- One of the worrying aspects of the Pegasus spyware is how it has evolved from its earlier spear-phishing methods using text links or messages to ‘zero-click’ attacks which do not require any action from the phone’s user.

IAS / PCS
Online Video Course
सामान्य अध्ययन
+
वैकल्पिक विषय
(इतिहास एवं भूगोल)
Online
Learning
Programme
संस्कृति IAS
JOIN NOW
15% Discount for
Next 500 Students

IAS / PCS
Pendrive Course
सामान्य अध्ययन
+
वैकल्पिक विषय
(इतिहास एवं भूगोल)
15% Discount for Next
500 Students