Advanced Cyber Security Corp.

EndpointLock™

Keystroke Encryption

Don't let cybercriminals steal
your organization's sensitive data

Important Stats:

- Experts believe that 76% of successful attacks on an organization's endpoints were zero-day. [1}
- Over 80% of enterprises now allow employees to use personal devices (BYOD) to connect to corporate networks. [2]
- 85% of data breaches can be traced back to phishing links. This includes clicking on bad links that download keyloggers. [3]
- 72% of malware cannot be detected by antivirus. [4]
- 97% of malware now employs polymorphic techniques to change their form and evade antivirus. [5]

The Problem:

Traditional security solutions leave organizations vulnerable to zero-day keyloggers, a type of malware that steals your keystrokes including your passwords. These keyloggers can bypass even the most advanced security systems, putting your sensitive data at risk.

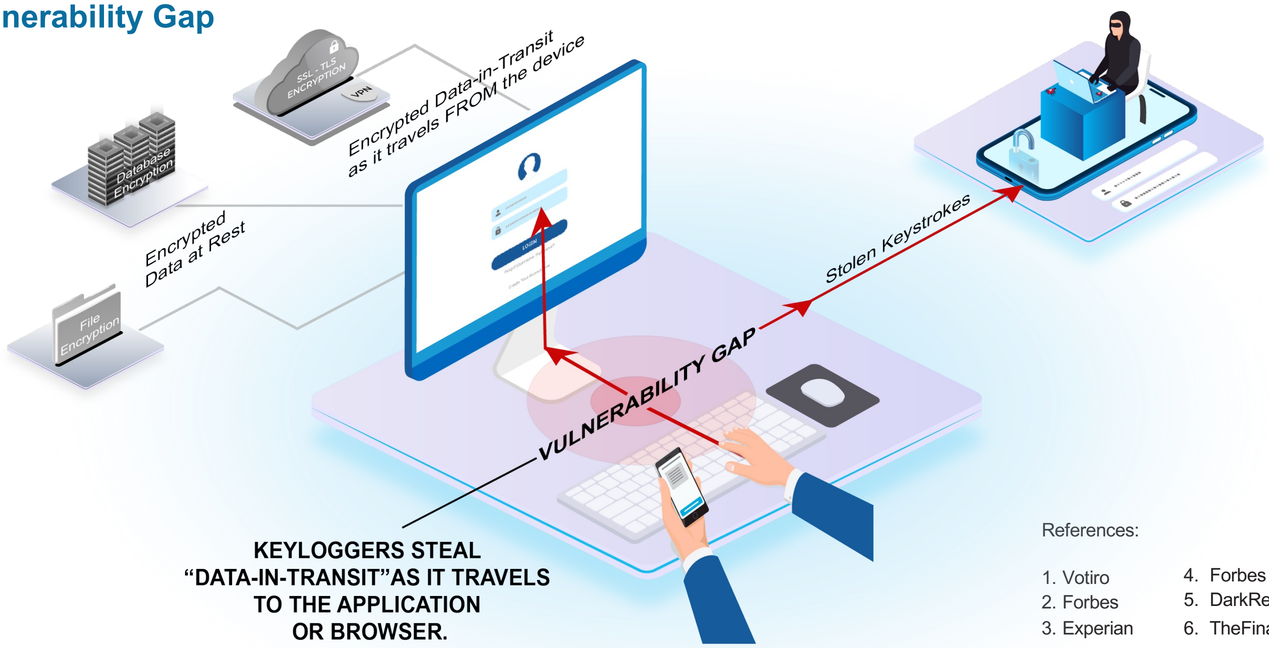
Keyloggers can record every keystroke you make, putting your data at risk. They're often used in the early stages of a data breach to steal passwords and other credentials that grant access to a network. Many keyloggers are difficult to detect because they can change their form, even in environments designed to be highly secure.

The Vulnerability Gap in Endpoint Security:

The zero-day keylogger installs low in the OS (Operating System), evades antivirus and captures the keystrokes as they pass through the stack on their way to the browser or application. This vulnerable area is often unprotected from a zero-day keylogger.

Figure 1:

The Vulnerability Gap


SSL · TLS ENCRYPTION
VPN
Encrypted Data-in-Transit as it travels FROM the device
Database Encryption
Encrypted Data at Rest
File Encryption
VULNERABILITY GAP
Stolen Keystrokes
KEYLOGGERS STEAL "DATA-IN-TRANSIT"AS IT TRAVELS TO THE APPLICATION OR BROWSER.

References:

1. Votiro
2. Forbes
3. Experian
4. Forbes
5. DarkReading
6. TheFinancialBrand

EndpointLock™

Keystroke Encryption

A Pro-Active Approach to Zero-Day Keyloggers

Key Benefits:

- Eliminate Keylogging Capture wherever EndpointLock is installed.
- EndpointLock blocks even the keyloggers not yet catalogued by antivirus (zero-day).
- Secure Access Credentials, BYOD and Remote Login which can pose the highest threat.
- Scalable: [EndpointLock has been designed with the enterprise in mind. EndpointLock can be easily deployed out across your enterprise using the same methods you currently use for software deployment.

Compatible Platforms:
Windows, Android and iO

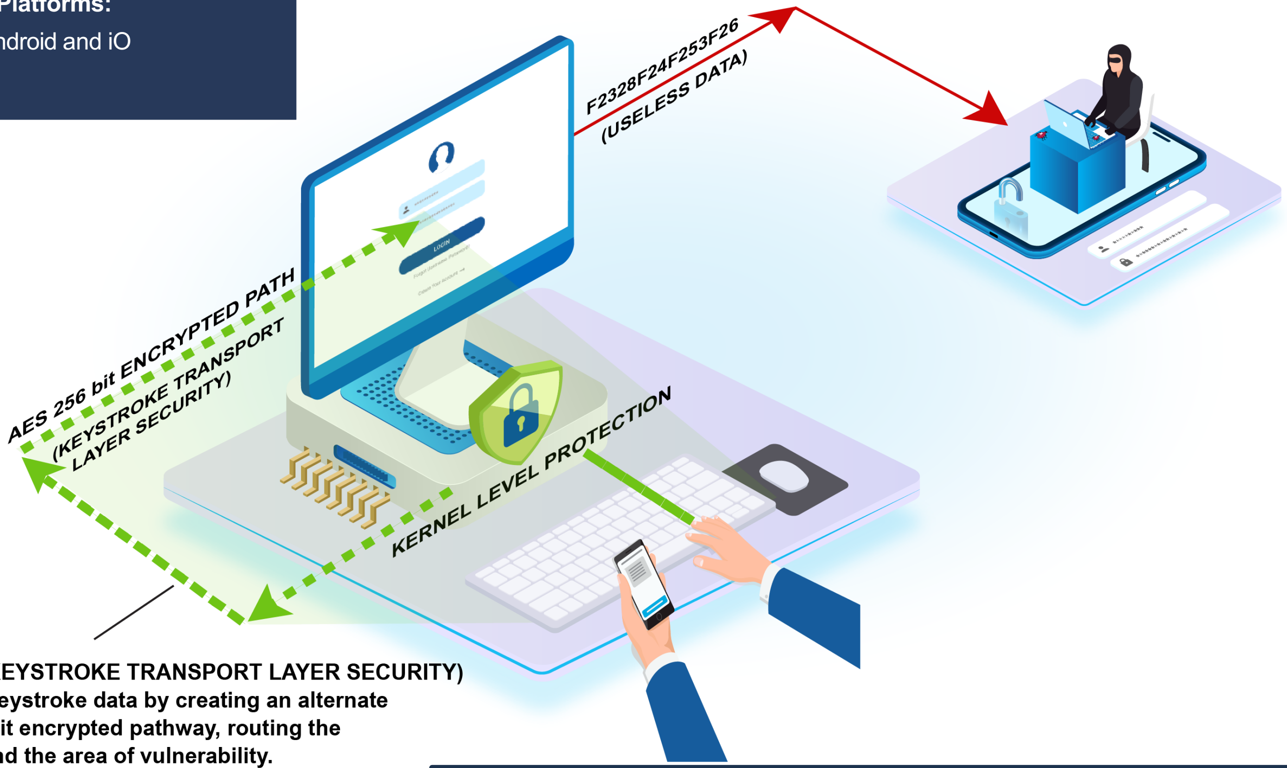
The Solution:

To mitigate input capture via a zero-day keylogger, EndpointLock utilizes KTLS (Keystroke Transport Layer Security) to protect the transport of keystrokes from the point of data entry.

While SSL and TLS enable strong encryption in network transport (Layer 5 of the OSI model), KTLS begins strong encryption from the kernel level at ring 0 within the operating system; KTLS encrypts all keystrokes at the moment of keystroke press, before network transmission. The keystrokes travel on a 256bit encrypted pathway and are decrypted into the text box. For optimum protection of government access credentials and sensitive data, keystroke encryption software should be installed on all connected desktop and mobile devices within an organization to help avert the advancement of a breach. See Figure below.

Figure 1:

Keystroke Transport Layer Security:



KTLS™ (KEYSTROKE TRANSPORT LAYER SECURITY) protects keystroke data by creating an alternate AES 256 bit encrypted pathway, routing the data around the area of vulnerability.

ACS
Advanced Cyber Security Corp.