PRODUCT SHEET

EndpointLock™

Desktop and Mobile Security

Keystroke Encryption Software

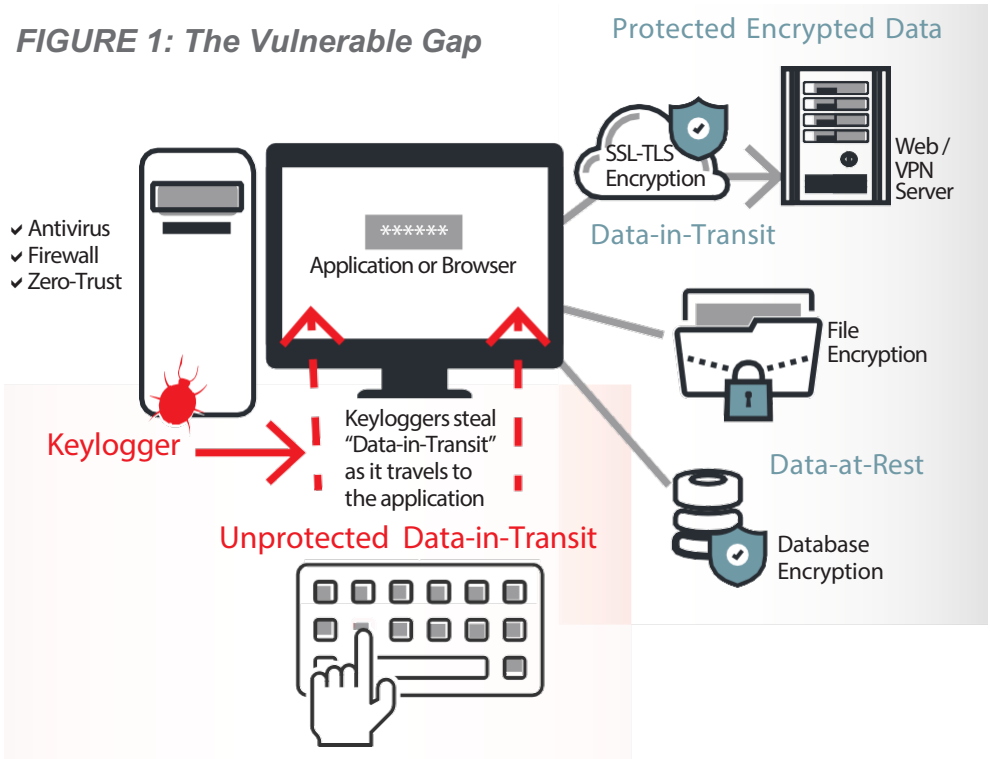
THE PROBLEM: ZERO-DAY KEYLOGGERS

Up until now, enterprises and government agencies have lacked the ability to fully protect their endpoints from a zero-day keylogger, surveillance software that is a primary component of all malware and advanced persistent threats. Keyloggers have the capability to record every keystroke a user makes on their desktop or mobile device and are leveraged in the first stages of a breach to gain access credentials into the network of an organization as well as other sensitive information. Many keyloggers are polymorphic and have the ability to change their form and remain undetected "zero-day", even in a zero-trust environment.

THE VULNERABLE 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. See Figure 1

FIGURE 1: The Vulnerable Gap



IMPORTANT STATS:

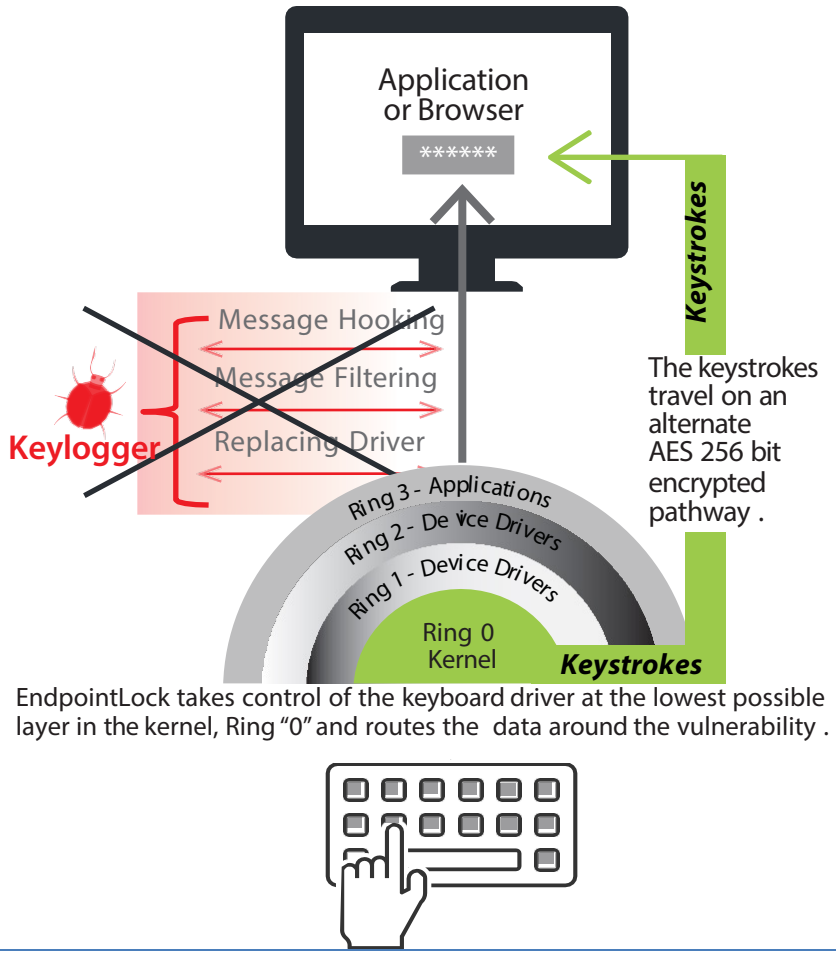
- Experts believe that 76% of successful attacks on an organization's endpoints were zero-day. [1}
- Over 80% of enterprises now allow employees to use personal devices (BYOD) to connect to corporate networks. [2]
- 85% of data breaches can be traced back to phishing links. This includes clicking on 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]
- 67% of organizations had a data breach when an employee used their mobile phone to access the company's data. [6]

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

THE SOLUTION: A PRO-ACTIVE APPROACH TO ZERO-DAY KEYLOGGERS

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 press, before network transmission. The keystrokes travel on a 256bit encrypted pathway and are decrypted into the text box. For optimum protection of 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 2. In addition to Keystroke Encryption, EndpointLock includes built-in Dark Web Scanning. Scan an unlimited number of email addresses at any time to see if your associated accounts have been compromised.

FIGURE 2: KTLS (Keystroke Transport Layer Security)



EndpointLock takes control of the keyboard driver at the lowest possible layer in the kernel, Ring "0" and routes the data around the vulnerability .

KEY FEATURES:

- **Built-In Unlimited Dark Web Email Scanning:** Provides immediate detailed results with steps you can take to protect your accounts.
- **Eliminate Keylogging Capture** wherever EndpointLock is installed including those not yet catalogued by antivirus (zero-day).
- **Secure Access Credentials, BYOD and Remote Login** which can pose the highest threat.
- **Scalable:** Many deployment methods including MS GPO, PowerShell, SCCM, 3rd Party Apps.

Compatible Platforms:

Windows, Mobile (Android and iOS)