Solution Brief

EndpointLock™
Desktop and Mobile Security

FINANCIAL INSTITUTIONS
A big target for cybercrime

PROBLEM:

KEYLOGGING SPYWARE is a main component in malware, used to advance an attack.

Banks and financial institutions fall victim to cyber attacks 300 times more frequently than businesses in other indutries. Keylogging spyware, used to steal everything typed into a desktop or mobile device is often leveraged in the initial stages of a breach in order to steal credentials and other sensitive data from an unsuspecting bank employee. Once access is obtained, hackers can either exfiltrate sensitive data, transfer funds or install ransomware to lock down the system and hold it for ransom.

Keyloggers are unknowingly downloaded to a desktop or mobile device after an employee clicks on an infected link inside an email, text, social media and web page. The practice of tricking unsuspecting victims into clicking on links that look legitimate is called “phishing”. According to recent reports, phishing was found in 90% of breaches and 95% of all phishing attempts that led to a breach, were followed by software installation, including keyloggers.

Despite major advances in cyber security, news outlets consistently report on data breaches to the financial sector. Keyloggers have played a significant role in many of these breaches. Unfortunately, this spyware is difficult to detect by traditional antivirus and firewalls, even when these programs are kept up-to-date. Research has found over 97% of malware now employs polymorphic techniques to change their form once catalogued by anti-malware programs. For this reason, keyloggers can remain on a device undetected for months and sometimes years.

ALARMING STATISTICS:

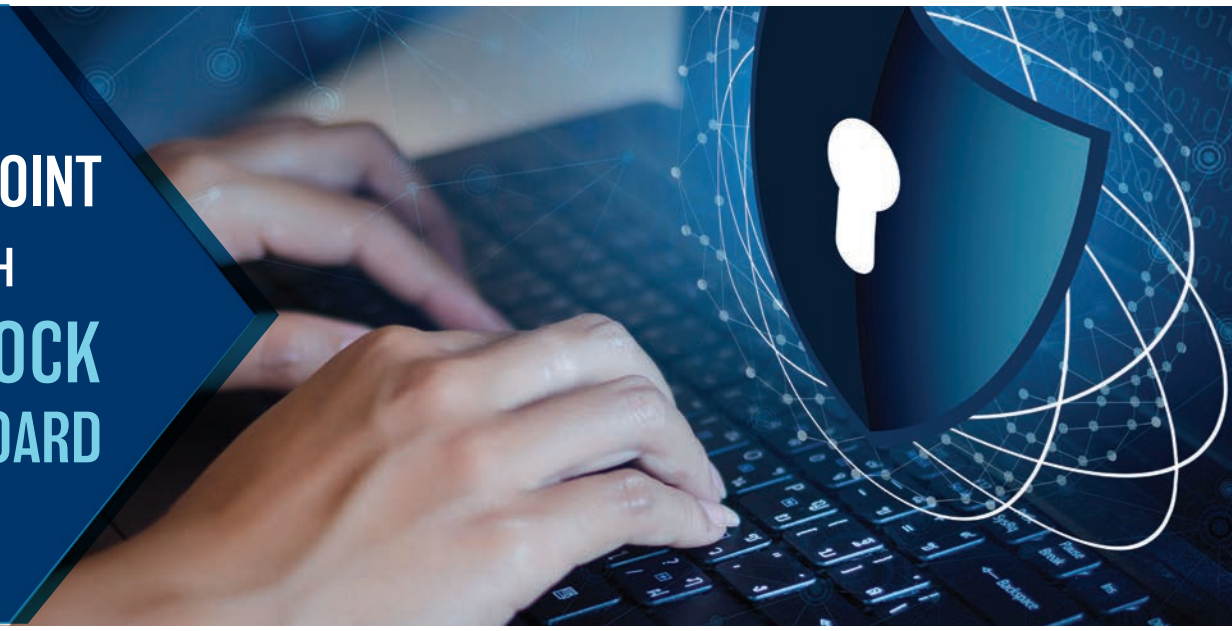
- Cyberattacks cost financial services firms 50% more than any other industry.
- The rate of breaches or theft of sensitive data in the financial services industry has tripled over the last five years.
- Cyber Bank robberies contributed to $1 Trillion in Cybercrime losses last year.
- Account takeovers tripled in the last year.
- 80% of businesses have adopted BYOD (Bring Your Own Device)
- 59% of companies have experienced a data breach caused by one of their vendors or third party partners.
- Hackers use stolen login credentials in 81% all of significant data breaches.

The growing attack surface:
A recent study of financial institutions worldwide, found that one of their biggest security challenges was, “Not being able to control the security of all of the networked devices, systems and applications that interact within their technology ecosystem.” resulting in a much broader “attack surface”. Current research has found that 59% of companies have experienced a data breach caused by one of their vendors or third party partners. In addition, 80% of businesses have adopted BYOD (Bring Your Own Device) and over 50% of employees are working remotely for at least half of their work week.

Solution Brief

EndpointLock™
Desktop and Mobile Security

STEP UP ENDPOINT SECURITY WITH ENDPOINTLOCK SECURE KEYBOARD



SOLUTION:

Stop keylogging spyware that is used to advance an attack.

ACS EndpointLock Keystroke Encryption eliminates the ability of keylogging spyware to capture keystrokes and steal access credentials as they are typed on an employee's desktop or mobile device. Hackers will always find new ways to trick users into downloading a keylogger, but with EndpointLock installed, the spyware is rendered useless. By eliminating this threat, financial institutions are better able to protect their business assets as well as access to valuable customer data. EndpointLock blocks keyloggers even if they have already been downloaded to the device and are able to evade anti-virus.

EndpointLock is simple to install and works on its own in the background with no interaction or technical knowledge needed by the employee. Install at every endpoints and all connected devices, including employee's who work remotely using personal devices, (BYOD) Bring your own device to work, third party partners, subsidiaries, branches, contractors and temporary workers.
By doing so, financial institutions can help strengthen the first link in the security chain by protecting their passwords and other credentials against keyloggers.

EndpointLock™ BENEFITS:

- **Blocks keylogging spyware.**
- **Blocks screen scraping and clickjacking.**
- **Monitors the kernel and alerts of a compromise.**
- **Protects the vulnerable gap found at the point of data entry.**
- **Runs in the background, no employee training needed.**

References:
1. https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#135036406e90
2. https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
3. https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware
4. https://www.apnews.com/556444d2cc114ea9a8ceda8f747b329c
5. https://www.forbes.com/sites/elenakvochko/2015/08/14/has-byod-become-inevitable/#173c44b43998
6. https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html
7. https://www.cso.com.au/mediareleases/29642/hacked-passwords-cause-81-of-data-breaches/

EndpointLock should be the first link in the security chain for ALL industries handling sensitive financial customer information including:

- Commercial Banks
- Credit Unions
- Financial Advisory / Brokerage Firms
- Credit Card Processing
- Credit Card Companies
- Wealth Management / Investment Banks
- CPA Firms
- Mutual Funds
- Insurance Companies
- Mortgage and Loan Brokers