Before the Breach

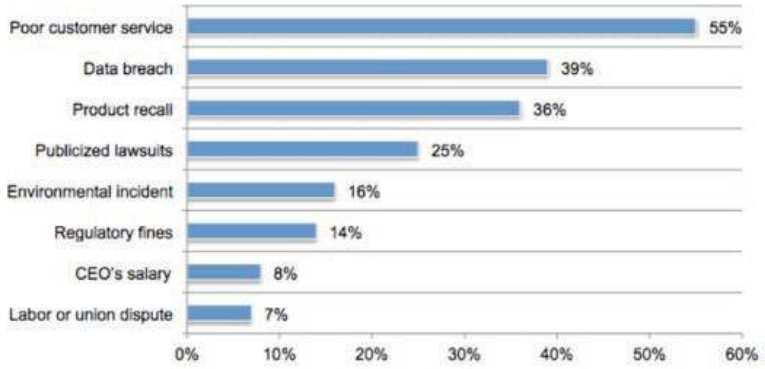
Protect Private Information from Key-Loggers and Cyber Thieves

Presented by Secure Identity Systems

Corporate data theft and data breaches are making headlines every day. Hackers and cyber criminals look to steal usernames and login password credentials from employees, steal bank account and payroll information, customer information, intellectual property, sensitive corporate secrets, etc., the list goes on and on..

Ponemon Institute's Third Annual Data Breach Study found that "data breach" ranked as the second highest issue that would have the greatest impact on an organization's reputation.

Figure 4. Which of the following issues would have the greatest impact on your organization's reputation?
Two responses permitted



To combat these threats and stressors, we need to stop relying on technology that does not fully protect individuals and organizations from a data breach. For example, antivirus and anti-spyware cannot stop a keyboard level attack.

In 2014, key-logging malware made up 90% of all cyber attacks and 63% of all reported data loss. Recent data breaches caused by key-loggers include:
Anthem, 79 million impacted
Target, 70 million impacted
Home Depot, 56 million impacted
CareFirst Blue Cross Blue Shield, 1.1 million impacted

And, so many more — to the point that the average American was in 3.1 breaches in 2015.

Key-Logging Malware

With more than 12,000 key-loggers in distribution, the malware is successful in stealing keystrokes 98% of the time, and more than 93% of passwords worldwide were stolen due to key-loggers.

What is a Key-Logger?
A key-logger is a piece of malicious software (or "malware") that records every keystroke you make on a keyboard. Key-loggers are inexpensive and effective. They can be embedded in emails, videos and music files, software downloads and even legitimate websites.

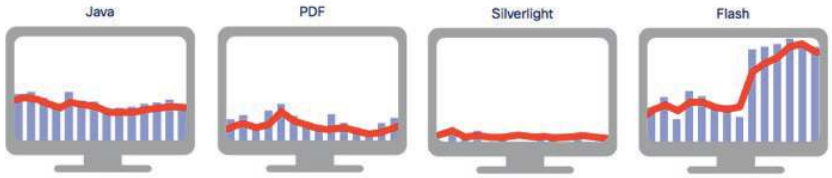
What Happens If a Key-Logger is On My Computer?
Key-loggers are designed to steal your keystrokes when you work, bank, shop and access email and personal or business information online or even over your office intranet. The corporate, personal and financial information that you enter both off and online is exactly what the identity thief is after.

What About My Antivirus Programs?
Eighty-percent of all key-loggers are not detectable by antivirus software, anti-spyware software or firewalls. Antivirus programs can only stop and detect against “known” and already “catalogued” viruses — they cannot protect you against new viruses.

Most antivirus software requires a frequently updated database of threats. However, this update process can take anywhere from several months up to a full year to build a “fix” for a single virus. It is estimated that there are currently thousands of new viruses introduced on the Internet on a daily basis. It is an impossible task to immediately identify a new virus and protect against it.

Figure 18. Most Common Malware Vectors

Share the report



Source: Cisco Security Research

Figure 18 shows the log volume of Java, PDF, and Flash exploits for the first half of 2015. PDF exploits vary on a month-to-month basis, but in general, are not as common as Flash exploits. Flash is a favored tool of developers of exploit kits, so its presence in the log volume chart above may be directly tied to outbreaks of criminal activity involving exploit kits such as Angler (see page 10). In addition, the volume of Silverlight exploits is very small compared with the number of exploits based on Flash, PDF, and Java.

Massively Distributed Malware in APT-Style Attacks

More and more frequently, hackers are using massively distributed malware in APT-style attacks. These advanced persistent threat (APT) attacks are a form of cyber-espionage that uses mass distribution techniques to infect as many computers as possible to steal intellectual property and access corporate data and resources. By hooking into the keyboard APIs or obtaining root access to the kernel, massively distributed APTs use key-logging malware to record users’ keystrokes and transmit them to the command-and-control server.

An IBM Security Intelligence blog found that an average of 24 in 100 machines in the U.S. are infected with massively distributed APT malware at any point in time. This mass infiltration means that by providing a simple configuration update, hackers can take advantage of already infected endpoints to find a way to infiltrate a new target.

The New York Times http://nyti.ms/1AB11C4

WORLD

Bank Hackers Steal Millions via Malware

By DAVID E. SANGER and NICOLE PERLROTH FEB. 14, 2015

PALO ALTO, Calif. — In late 2013, an A.T.M. in Kiev started dispensing cash at seemingly random times of day. No one had put in a card or touched a button. Cameras showed that the piles of money had been swept up by customers who appeared lucky to be there at the right moment.

How Hackers Infiltrated Banks

Since late 2013, an unknown group of hackers reportedly stole $300 million — possibly as much as triple that amount — from banks across the world, with the majority of the victims in Russia. The attacks continue, all using roughly the same method:

1. Hackers send email containing a malware program called Carbanak to hundreds of bank employees, hoping to infect a bank’s administrative computer.
2. Programs installed by the malware record keystrokes and take screenshots of the bank’s computers, so that hackers can learn bank procedures. They also enable hackers to control the bank’s computers remotely.

Keystroke Encryption Software

Keystroke encryption software stops malicious key-logging programs by encrypting every keystroke at the point of typing, and rerouting those encrypted keystrokes directly to your browser through its own unique path. Encryption is a process that scrambles information into a format that unauthorized parties cannot decode or utilize.

Most anti-spyware tools find hidden software after they have already been installed on the victim’s computer and their important information is already in the hands of an identity thief. Keystroke encryption software actually stops the transfer of personal and sensitive information before it can get into the thief’s hands.

Keystrokes are encrypted when:
Keying in user names and passwords
Browsing the Internet through most browsers
Using online banking
Using online bill-pay
Shopping online
E-mailing through Web-based email
Keying into Internet applications and registrations
Arranging online travel
Clicking on Web pages
Even when using programs like Excel, Word or PowerPoint

It is imperative that individual and company cyber security measures include encryption at the keyboard level as that is the only way to stop this form of attack.

"We need systems in place that can protect data from the computer terminals inside your office as well as the independent contractor who connects to your network from a coffee shop."

Mobile Hacking

Keystroke encryption software can also go a long way to prevent mobile hacking. Kaspersky Lab's 2015 Global IT Security Risks Survey found that 54% of respondents are much more concerned about the security of mobile devices than they were a year ago, and 18% of the workforce use smartphones to conduct business on the move with the help of mobile data.

Android devices are the most likely to be breached. According to Verizon's 2015 Data Breach Investigations Report, 96% of mobile malware targeted the Android platform, and more than 5 billion downloaded Android apps are vulnerable to remote attacks.

For our modern workforce, we need systems in place that can protect data from the computer terminals inside your office as well as the independent contractor who connects to your network from a coffee shop.

Industry Spotlight: Financial Services

It is an unfortunate reality that banks are currently more likely to spend their IT budgets on reactive measures than preventative measures. Kaspersky Lab's 2015 Global IT Security Risks Survey found that 48% of financial institutions' IT security measures are designed to mitigate rather than solve the problem, and 29% of financial institutions thought it was cheaper and more effective to deal with online fraud issues as they arrive, rather than try to prevent them from happening in the first place.

This reactive approach is short-sighed, as the same report found that 72% of businesses look at a bank's security track record before deciding whether or not to approach them, and 90% of enterprise businesses would pay for greater security if it meant more secure financial transactions.

Conclusion

According to Kaspersky Lab's 2015 Global IT Security Risks Survey, 60% of businesses that suffered a data breach found their ability to function afterwards severely reduced. Of the compromised businesses, 57% had to pay significant additional costs, and 56% of data loss events led the business to suffer damage to its image and reputation.

Given these high costs and consequences, companies need to pay close attention to key-loggers, which are the biggest source of cyber-attacks and identity theft breaches. With more than 12,000 key-loggers in distribution, antivirus and anti-spyware aren't enough to protect onlineactivity from identity thieves. By installing keystroke encryption software, individuals and companies can be protected from even the most tenacious online identity thieves.

About Secure Identity Systems
Secure Identity Systems was initially created to mitigate the risk for financial institutions by identifying growing security threats. By 2006, Secure Identity Systems held three North American Patent Rights for ID Theft prevention and authentication. By the time the regulatory "Joint Release Red Flag Rule" was handed down, SIS was the only company in the U.S. to have a complete end-to-end solution already in place. Today, SIS serves financial institutions, businesses and families with the most robust products and services available.

For more information on Secure Identity Systems, please call 877.304.3349 or visit SecureIdentitySystems.com. Follow Secure Identity System on Facebook and Twitter for security updates and special offers.

Secure Identity™
615.732.7100 | secureidentitysystems.com