Malware Attacks Targeting POS Integrators/Resellers

Integrators have become the #1 attack vector in payment card breaches. Attackers realize that targeting a single integrator could reveal the usernames and passwords for dozens, if not hundreds, of individual businesses.

Background

In today's business world, owners are concerned about data breaches, and many take steps to prevent them. Because of this, hackers are now working harder to attack businesses while remaining undetected.

The Sikich forensic investigation team has seen a drastic increase in breaches where attackers are hacking integrators to harvest the passwords that allow them to break into multiple businesses simultaneously.

A successful integrator is a busy organization. In some cases, one employee might provide technical support for hundreds, perhaps thousands, of different hotels and restaurants across an entire metro area. During a weekend's on-call shift, this employee may singlehandedly respond to dozens of emails, text messages and cell phone calls because of point of sale (POS) issues.

What the attackers are doing

Attackers realize that the POS integrator is over worked, which may result in certain corners being cut. For example, the integrator might use the same username and password to provide remote support for the thousands of their merchant customers, despite this being a violation of Payment Card Industry Data Security Standard (PCI DSS) requirements. What's more, the remote access tool involved may only use single-factor authentication (another violation of the PCI DSS).

Once the attacker gets those remote access credentials, the goal is to quickly deploy crimeware/malware at as many merchant locations as possible. After they have infiltrated all of the merchants, the attacker steals cards from just a few merchants at a time, which has become one of the best ways for attackers to evade detection.

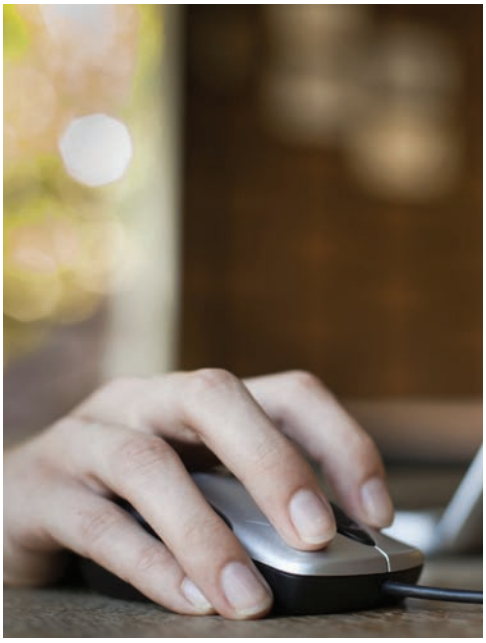
As a PCI Forensic Investigator (PFI), Sikich has been involved in many cases that mimic this behavior. Our PFI statistics from 2015 show that it can take less than 40 seconds for attackers to install their malware at one integrator merchant customer and move onto the next. The malware installed is capable of stealing payment card numbers in real time. To the consumer end user, the transaction seems normal. In reality, the malware allows the attacker to simultaneously send the payment card information to the attacker's server.

> "it can take **less than 40 seconds** for attackers to **install their malware** at one integrator merchant customer and move onto the next"

While 40 seconds does not seem long, 1,000 merchants would take the attacker a little over 11 hours to victimize. In some cases, Sikich found that attackers dedicated themselves to working during night hours. In fact, one attack group intentionally works only between midnight and 5:00 a.m. in hopes that the business owner does not see the mouse cursor moving on the POS screen. While it may take three nights to complete the attack across the integrator's customers, the increased likelihood of avoiding detection makes it worth the attacker's patience.

What needs to change immediately

How do you stop these attacks? Where do you begin? The simple answer starts with increasing employee awareness and focusing on meeting PCI DSS requirements.

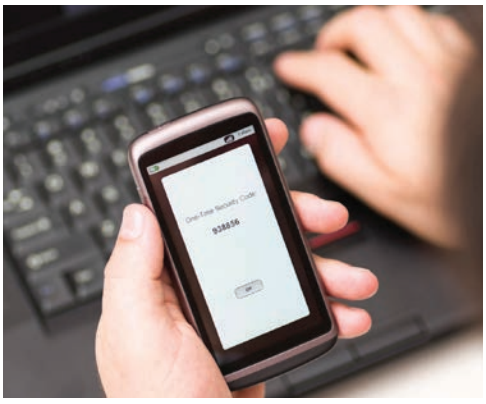


1. Don't click the link

Most of these attacks begin with phishing. The attacker sends a malicious email, oftentimes including an attachment, to the integrator that is intended to look legitimate. This attachment may appear to be a Word document, a PDF or even a ZIP file. In reality, this attachment contains malware. Once opened, the attacker can steal the integrator's "master password" in less than a second.

Attackers don't just target the technical staff. Owners and executives of the POS integrators are just as likely to make the mistake of clicking on a malicious file or link. Attackers not only know the names of the POS integrator companies, but they also know the email addresses of the employees. Using their knowledge, an attacker may pretend to be a restaurant owner in the integrator's area and will tailor the email to look like it is coming from an existing customer of the integrator.

Users can stop these attacks by simply not opening unexpected attachments. As an extra level of security to identify and perhaps stop these attacks (and to meet PCI DSS requirements), owners should make sure that they are actively running up-to-date anti-virus/anti-malware programs. That way, should a user end up clicking a malicious link, there is still a chance for the organization to avoid harm.



2. Use two-factor authentication

When it comes to authenticating to system components, users can be asked to supply something they know (e.g., a passphrase), have (e.g., a token device) or "are" (e.g., a fingerprint). To enhance security for access areas of higher risk, an organization may require two of the methods in order to allow access (i.e., two-factor authentication).

Many remote control tools, such as LogMeIn and TeamViewer, have made it easy to enable two-factor authentication. Industry best practices recommend, and the PCI DSS requires, that you require two-factor authentication immediately for ALL of your technicians and merchant customers. Without this second factor, an attacker could gain access just by brute forcing the password over time.

3. Enable remote access only when needed

Having remote support enabled at all hours is not only a violation of PCI DSS requirements, but also just too dangerous in today's world. Businesses should ONLY turn on remote support when they are expecting the technician to perform work. Remote support should immediately be turned off once that work is completed. Approach enabling and disabling remote access in the same way you would locking and unlocking the doors to your home.

4. Require passwords to be strong and unique

Many integrators create passwords that are unique but use part of the merchant customer's name, address or store number. Practices such as this should be changed immediately. In the past year, hundreds of businesses have been breached because an attacker figured out the pattern used by an integrator to create passwords.

Other integrators store their merchant customers' passwords in the "notes/comments" field of the remote access tool. This practice should also be avoided. Remember, once the attacker has the credentials to your remote control tool, they could see all of your merchant customer notes.

To best protect the environment of the integrator and its merchant customers, passwords need to be both complex and unique.

What this means to your merchant customers

Making these changes will mean a change of habits for your merchant customers, but the alternative (i.e., being breached) is much worse. While business owners may not like having to remember complex passwords, they certainly don't want to be troubled with repairing or replacing systems, combatting negative publicity or something worse.

We hope that making these four changes above helps protect you and your merchant customers.

Questions?

If you or your merchant customers have any questions or believe you have been breached, please contact us at forensics@sikich.com or call 877.403.5227.

About Sikich Security & Compliance

Sikich's Security & Compliance practice is dedicated to assisting our clients with information security consulting, fraud management, risk mitigation and vulnerability detection and prevention. Our experts specialize in performing compliance audits, penetration tests, computer security assessments and computer forensic investigations.