The Data Dilemma

The Value of Secure Transaction Solutions

THE AEGENIS GROUP

6410 N Business Park Loop Rd
Suite E
Park City, UT 84098
435-615-6711
www.aegenis.com

By Chris Mark, CPISA, CISSP, CIPP

Contents

Executive Summary

The current economic environment, coupled with the increasing sophistication and motivation of data thieves, has put companies at a disadvantage in their efforts to protect sensitive data. Companies are being forced to secure increasingly complex networks to protect data that, if compromised, could result in huge financial liabilities for the organization and significant brand damage. In response to the growing number of compromises, various state governments have passed breach notification laws, and the Payment Card Brands have instituted a number of security requirements with which companies must comply. Adherence to the requirements is an often monumental task that some argue does not appreciably reduce the risk to sensitive data. A trend is emerging in which companies are developing alternative methods of addressing compliance with the PCI DSS and various state laws by removing the need to retain sensitive data. Within the last several years, organizations have begun marketing solutions that address the root of the problem - namely the transmission and retention of sensitive data. By removing the data from the equation, companies are able to significantly reduce their risk exposure and achieve compliance with the PCI DSS and other regulations in a cost effective and efficient manner.

Solutions such as those described above emerged in early 2004 as technologies designed to remove the need to store sensitive data. Over the years, the solutions have become increasingly sophisticated. The current generation of products, referred to as 3rd Generation or *Encrypted Magnetic Stripe Reader with Secure Virtual Terminal,* provide merchants with a level of protection not previously available. Products such as ProPay Inc.'s ProtectPay™ coupled with the MicroSecure™ swipe device enable merchants to accept payment cards while ensuring the transmission and storage of payment card data is carried out securely. ProtectPay and the MicroSecure Card Reader represent the pinnacle of the latest generation of secure, alternative solutions to traditional unsecured transaction processing and PCI DSS compliance.

Data Compromise Trends

Companies today face an ever increasing number of sophisticated attacks designed specifically to compromise sensitive personal data. A quick read through a national newspaper or a search on a major search engine will reveal numerous data compromises. In spite of efforts by the major Payment Card Brands and state and federal governments, data compromises continue to increase in frequency and severity. Companies that handle payment card data, such as merchants and service providers, appear to be at particular risk of data compromise.

- ☑ *Verizon Business Risk's analysis of over 500 compromise investigations found that payment card data was compromised in 84% of cases. 32% of compromises included other forms of Personally Identifiable Information (PII) such as bank account numbers, social security numbers, and other data.*[1]

[1] Verizon Business 2008 Data Breach Investigations Report; http://securityblog.verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/

Since 2003, the methods of compromise have continued to evolve despite the advent of data breach notification laws and the Payment Card Industry Data Security Standard (PCI DSS). In 2003, many compromises were the result of simple network layer attacks exploiting misconfigured firewalls or the absence of encryption technology. Since 2005, data thieves have begun to employ more sophisticated, targeted methods to obtain sensitive data. Wireless attacks and malicious software, such as trojans, have begun to take center stage in the compromise of data within the payment card industry. Contrary to what many surveys suggest, evidence supports the fact that the vast majority of data compromises within the payment card industry are the result of external attacks.

☑ *Verizon's analysis identified external sources as being responsible for 73% of breaches with 31% resulting, in part, through malicious software.*

A relevant example of the dangers of malicious software and the perpetrators of data theft can be seen in the recent *Information Week* article regarding the Sinowal Trojan. The Sinowal Trojan is thought to have originated with the Russian Business Network (RBN), an infamous Russian hacking and data theft network. According to RSA researchers who discovered the trojan, Sinowal had been quietly collecting stolen login credentials from approximately 300,000 online bank accounts. A similar number of credit and debit cards were also compromised by the trojan.

☑ *"The criminals behind Sinowal have not only created highly advanced and malicious crimeware, but have also maintained one of the most hidden and reliable communication infrastructures. This infrastructure has been designed to keep Sinowal collecting and transmitting information for almost 3 years."*[2]

While many believe that hacking and data thefts are the sole realm of organized crime and highly technical criminals, recent developments in technology have brought the ability to steal data into the hands of less sophisticated criminals. Tools like Turkojan and Pinch 2 PRO (screenshots in Appendix A) allow even relatively novice hackers to create sophisticated trojans that can be used to capture sensitive data.

Turkojan lists a warranty on their website that allows those who purchase the product to have assurance that the malicious software created will not be detectable by anti-virus. Support for Turkojan ranges from $99 US to $249 US. The warranty states:

☑ *"...6 months (unlimited) or 9 months (maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)"*[3]

It is suggested that one of the primary reasons that malicious software is being increasingly employed by hackers and data thieves is that it exploits perceived gaps in the PCI DSS. As an example, the PCI DSS does not require encryption for data being transmitted over the internal network. This leaves data being transmitted from POS terminals to the POS server or processor

[2] RSA Blog; One Sinowal Trojan + One Gang....http://www.rsa.com/blog/blog_entry.aspx?id=1378
[3] http://www.turkojan.com/eng/

vulnerable to capture. This transaction information also contains the sensitive authentication data so highly valued by data thieves.

Two of the more prominent data compromises in history were the direct result of malicious software. In 2006, MasterCard International released the following statement after the compromise of a large payment processor:

- ☑ *"The data security breach, possibly the largest to date, happened because intruders were able to exploit software security vulnerabilities to install a rogue program on the network of (Company), MasterCard International spokeswoman Jessica Antle said. The program captured credit card data, she said."*[4]

In 2008, a major supermarket chain experienced a data compromise. A report after the compromise stated:

- ☑ *"The malicious software was used to intercept the payment card data as the information was being transmitted from (Company's) point-of-sale systems to authorize transactions."*[5]

In summary, targeted attacks against organizations that possess valuable personal data are increasing in both volume and sophistication. Companies continue to struggle to stay ahead of the data thieves, while organized hacker groups are bringing technologies to the masses that enable less sophisticated criminals to perpetrate data theft.

State of the Industry: PCI DSS

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed originally as Visa's Cardholder Information Security Program (CISP) in 2001 and later adopted as an international standard. The PCI DSS consists of 12 high-level requirements and approximately 220 sub-requirements. The stated objective of the PCI DSS is to "...encourage and enhance cardholder data security..." It is not, nor was it ever intended to provide an absolute statement on security. As stated on page 2 of the Preface section of PCI DSS v1.2:

- ☑ *"The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally."*[6]

An unfortunate and growing trend within the Payment Card Industry is the ubiquitous belief that compliance with the PCI DSS, or any other standard, equates to sufficient information security or

[4] More Details Emerge on Credit Card Break In; http://m.zdnet.com.au/139198118.htm
[5] Card Numbers Were Sent Overseas...http://tortus.com/news/hannafords_breach_isent_over_your_site
[6] PCI DSS; https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

adequate risk management. It is clear from reading Myth 4 (shown below) of the *10 Myths to PCI Compliance* that the PCI SSC does not consider the PCI DSS the final word on security.

> ☑ *Myth 4 - PCI Will Make Us Secure*
> *Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.*[7]

Companies that pursue compliance with the PCI DSS as the sole means to protect cardholder data are exposing their organizations to risk of compromise from unidentified threats. As stated previously, data thieves intentionally target areas where perceived weaknesses in the standard exist. It is extremely difficult to detect custom developed malicious software and as the PCI DSS does not require encryption on the internal network, installation of a trojan such as Sinowal poses a high risk of sensitive authentication data compromise. Organizations need to be aware of the intent of the PCI DSS and the limitations of complying with any static security standard. It is critical that organizations take a more comprehensive approach to risk management.

Fines, Fees, and Penalties:

Non-compliance with the PCI DSS can result in fines being levied from the Card Brands to the acquiring banks. The acquiring banks may then pass these fines to the merchants or service providers, as appropriate. Fines can range from $2,000 to $25,000 per month for Visa Level 1 Merchants and up to $5,000 per month for Level 2, 3, and 4 merchants. While non-compliance penalties are severe, they pale in comparison to the potential financial liability associated with a compromise of Cardholder Data.

Egregious data compromise cases involving full magnetic stripe data can result in fines of up to $500,000 from Visa, and similar fines from the other major card brands. In addition to the fines, merchants and service providers may also be held accountable by their acquirers for reimbursing the card issuers for fraudulent transactions as well as the costs associated with account monitoring and card re-issuance. In some cases re-issuance can be as high as $25 per card. It is easy to see how one major merchant in 2005 was fined $880,000, yet had additional fees that they had to settle amounting to $41 million for Visa and $24 million for MasterCard.

Case Study: (Supermarket Chain)

In one of the more recent data compromises, a company that had been validated as being compliant with the PCI DSS had a large theft of cardholder and sensitive authentication data.

This begs the question: how can a company that is adhering to the PCI DSS have a theft of cardholder data?

[7] 10 Common Myths; https://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf

The answer demonstrates the limitations of the PCI DSS, or any other security standard. Quite simply, compliance with a standard does not ensure or suggest that the company is adequately protected. In the referenced case, the company was found to have been compromised, at least in part, through malicious software, such as the trojans listed previously. Many in the industry argued that this fact alone should have precluded compliance with the PCI DSS. Additionally, the Qualified Security Assessors (QSA) has been blamed for either not being sufficiently comprehensive or making a mistake in their assessment.

Unfortunately for the critics, neither one of these suppositions is correct. The issue lies with the standard.

PCI DSS Requirement 5 states:

Requirement 5: *Use and regularly update anti-virus software or programs*

> ***5.1*** *Deploy anti-virus software on systems commonly affected by viruses.*
>
> > ***5.1.1*** *Ensure that all anti-virus programs are capable of detecting, removing and protecting against all known types of malicious software.*
>
> ***5.2*** *Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*

It is important to note that PCI DSS Requirement 5 applies to the installation, configuration, and maintenance of the anti-virus solution. The requirement does not state that the QSA is responsible for ensuring that no malicious software is present on the system, nor does it require that organizations that must comply be certain that malicious software is not present. In short, the company could have been fully compliant and still been the victim of a malicious software infection that resulted in data compromise.

Challenges with Security Standards

While the development of security standards designed to increase the protection of cardholder and other sensitive data is laudable, compliance with the requirements outlined in such standards is not sufficient to ensure the security of sensitive data. The primary challenge associated with most security standards is that they are, by nature, static while the risks to organizations and their data are fluid and dynamic. A company can be fully compliant with PCI DSS, while still exposed to significant residual risks. This is demonstrated in the aforementioned case study, and Myth-4 of the PCI DSS detailed on page 4 of this document. It is further supported by PCI DSS Requirement 12.1.2 which states that companies must: "... (undergo an) annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment." Compliance with any given standard does not and cannot offer protections against risks that the standard is not designed to address. The supermarket case study referenced above provides ample illustration of just such a paradox - a compliant company that becomes the victim of a data compromise.

Alternative Solutions

Challenges with achieving compliance with the PCI DSS and maintaining the security of data against increasingly sophisticated and determined data thieves have led numerous companies in the United States to begin developing secure alternative solutions to contemporaneously address security and compliance. Instead of attempting to build and maintain hugely complex security infrastructures, these secure solutions attempt to remove the value of the data and thus remove the risk of data compromise. It should be noted that these solutions are not without precedent. In the Asia Pacific region, the major Card Brands are supporting end-to-end encryption of transaction data. Currently, the entire country of Malaysia encrypts transaction data from the point of sale through the transaction process. Thailand and Australia are working toward the same goal in 2009. To understand these solutions it is important to have a working understanding of Cardholder Data.

Cardholder Data Defined

Cardholder Data as defined by the PCI DSS includes, at a minimum, the Primary Account Number (PAN). Cardholder Name, Expiration Date, and Service Code are also defined as Cardholder Data if any or all of the elements are retained in conjunction with the PAN. It is clear from the PCI DSS and related documents that Cardholder Data exists only if PAN is present.

The PCI DSS states that encrypted Cardholder Data is still considered Cardholder Data and therefore subject to the requirements of the PCI DSS. Many mistakenly believe this statement was included because the security of the algorithm is suspect. This statement was added because the potential weakness with the approved encryption solutions lay in the key management and not with the algorithm. This is supported within the PCI DSS standard. Requirement 3 specifically states:

- ☑ *"If any intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person."*[8]

The intent of the above statement is clear. Specifically, that in the absence of a mechanism for merchants to decrypt appropriately encrypted data, the encrypted data is not considered Cardholder Data and therefore NOT subject to the PCI DSS requirements. It is this premise on which many of the alternative solutions have been developed.

At this point it is important to interject a brief discussion of service providers and third parties. It is of vital importance to ensure that each third party involved in the transaction process is a "trusted party" and has a demonstrated need to access the data. Just as sound information security principles dictate restricting logical and physical access of employees on a "need to know" basis, it is paramount that merchants apply the same principles to their services providers. If a service provider does not have a demonstrated need to receive or access the sensitive data, then that organization should be removed from the transaction process or have access to the data appropriately restricted. When conducting QSA training, The Aegenis Group differentiates

[8] PCI DSS; https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

between a "business convenience" and a "business need" to access data. An organization without a demonstrated business 'need' to handle data in support of transaction processing or other vital functions simply exposes the data to additional, unnecessary risk. Several organizations are offering encryption and decryption services for merchants. These services are not required to support authorization or settlement of transactions. It is this author's position that allowing a third party, which does not have a demonstrated need to access the data, the ability to decrypt the data is not consistent with the requirements of the PCI DSS and does not represent sound information security.

1st Generation

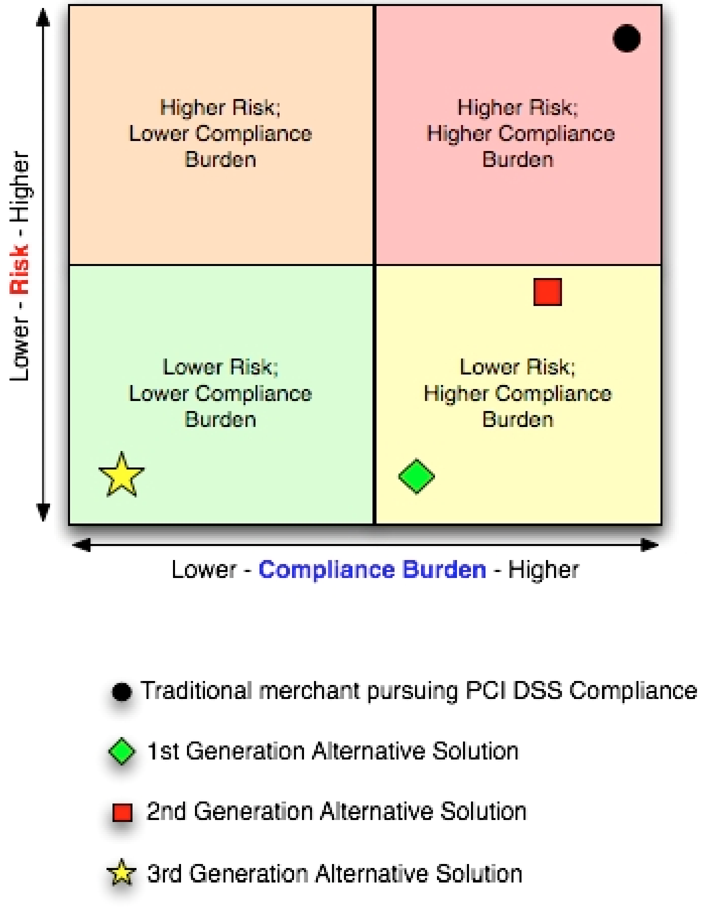
The first generation of solutions can be described as *Transaction Replacement* technology. Transaction Replacement solutions do not encrypt the transaction data being transmitted and only address the storage of Cardholder Data subsequent to receipt of the authorization response. In these solutions Cardholder Data and other transaction data is replaced with an abstract representation of data that is not considered Cardholder Data and therefore not subject to the PCI DSS. Because these solutions do not address the transmission of data, it provides limited value.

2nd Generation

In 2005, the second generation of solutions was promoted. These can be described as *Transaction Replacement with Application Layer Transmission Encryption*. These solutions build upon first generation solutions and incorporate another layer of security by encrypting data within the application resident on the Point of Sale (POS) solution. These solutions took great strides toward reducing the risk to data but did not appreciably reduce the compliance burden as the data is encrypted at the application and not the hardware device. This resulted in the POS system requiring protection, as it could be potentially circumvented to compromise data.

3rd Generation

The third generation of alternative solutions, released in 2007, continued to build upon the previous technologies. These newer solutions are a convergence of two technologies that provide a significant increase in both the security of data as well as a reduction in the PCI DSS compliance burden. Third generation solutions can be referred to as *Encrypted Magnetic Stripe Reader with Secure Virtual Terminal.* Third generation solutions encrypt data at the point of swipe using specially designed swipe terminals that encrypt data at the magnetic stripe reader head. These solutions employ asymmetric key management techniques such as Derived Unique Key Per Transaction (DUKPT) where the decryption keys are managed at a trusted third party such as a gateway or processor and not at the merchant. Once received for authorization, the trusted third party retains the data in a secure environment allowing the merchant to log-in through a secure website to research transactions, initiate chargebacks and provide other services. The merchants are restricted in their ability to see, or otherwise compromise sensitive data or circumvent the security of the data. More importantly, third generation solutions render data unreadable and not subject to the PCI DSS removing the burden of compliance from merchants while simultaneously reducing the risk to sensitive data.


Higher Risk; Lower Compliance Burden
Higher Risk; Higher Compliance Burden
Lower Risk; Lower Compliance Burden
Lower Risk; Higher Compliance Burden
Lower - Risk - Higher
Lower - Compliance Burden - Higher
● Traditional merchant pursuing PCI DSS Compliance
◆ 1st Generation Alternative Solution
■ 2nd Generation Alternative Solution
☆ 3rd Generation Alternative Solution

Evaluation of ProtectPay and MicroSecure Card Reader:

ProPay Inc. developed the 3rd Generation ProtectPay and MicroSecure technologies specifically to reduce the risk to Cardholder Data and reduce the PCI DSS compliance burden of their clients. Each solution will be discussed briefly.

ProtectPay

ProPay's ProtectPay forms the foundation of their secure solutions designed to support merchants and service providers within the Payment Card Industry. ProtectPay is a secure data repository and secure virtual terminal that enables merchants and service providers to securely store their data with a trusted third party. As a payment processor and payment gateway, ProPay has a demonstrated need to access and handle client transaction and other data. ProPay ensures that they maintain PCI DSS compliance and maintain strict information security controls beyond those required by the PCI DSS. By removing the storage of data from their own environment, merchants and service providers are greatly reducing their risk of data compromise and may greatly reduce their PCI and other regulatory compliance obligations.

MicroSecure Card Reader

ProPay's MicroSecure Card Reader provides the second vital component to the complete 3rd Generation solution. MicroSecure is an encrypted magnetic stripe reader that operates in both an online and offline capacity allowing merchants to securely swipe payment cards and retain the data securely until such a time in which they are able to connect to the Internet to transmit the transaction data. MicroSecure employs a secure encryption protocol that leverages DUKPT key management and robust authentication of the MicroSecure device. This provides assurance that theft of the device will provide no useable data and further ensures that a data thief cannot steal the device and use for another account or replace the device and use an insecure device. Since the data is encrypted at the device level and is never in an unencrypted format within the merchant environment, it removes the merchant environment from scope of the PCI DSS requirements.

Analysis of ProtectPay and MicroSecure

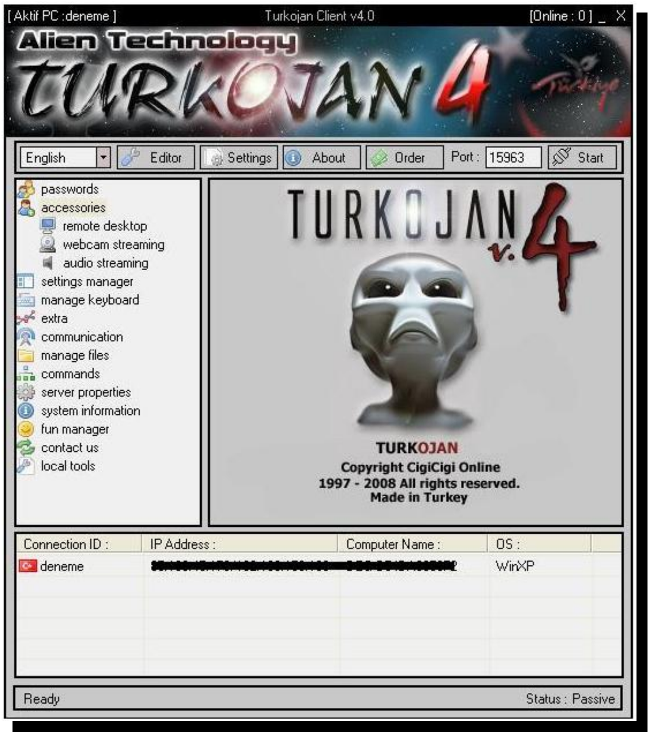
In the experience of this author, ProtectPay and MicroSecure represent the latest and most well-defined products in a new generation of secure payment technologies. While 1st and 2nd generation technologies discussed in this document provided nominal increases in the security of data, the 3rd generation of technologies represents a significant leap forward in terms of both the protection of sensitive data, as well reduction of compliance requirements. As with any technology or service, the experience, and expertise of the developing organization is critical to the security and efficacy of the solution. In addition to providing a new generation of secure, alternative transaction technologies, ProPay has demonstrated an industry leadership position by ensuring continual compliance with the PCI DSS as well as ensuring security remains a core competency of their organization.

Summary

The challenges associated with the protection of data will increase proportionally to the ingenuity of the data thieves committed to stealing that data. For most companies, this represents an obstacle that is increasingly difficult to overcome. Companies are less able to divert scarce resources from their core competency to the protection of sensitive data, particularly in a trying economy. Products such as ProPay's ProtectPay and MicroSecure allow companies to "do the right thing" with respect to the protection of consumer data while also allowing them to focus on their core business. ProtectPay allow companies to store their data with a trusted third party that has demonstrated security expertise. MicroSecure allows merchants to accept payment cards, without the attendant data security concerns. In combination, the two products represent a new paradigm of data protection for the payment card industry.

Appendix A: Malware Screenshots

Turkojan4



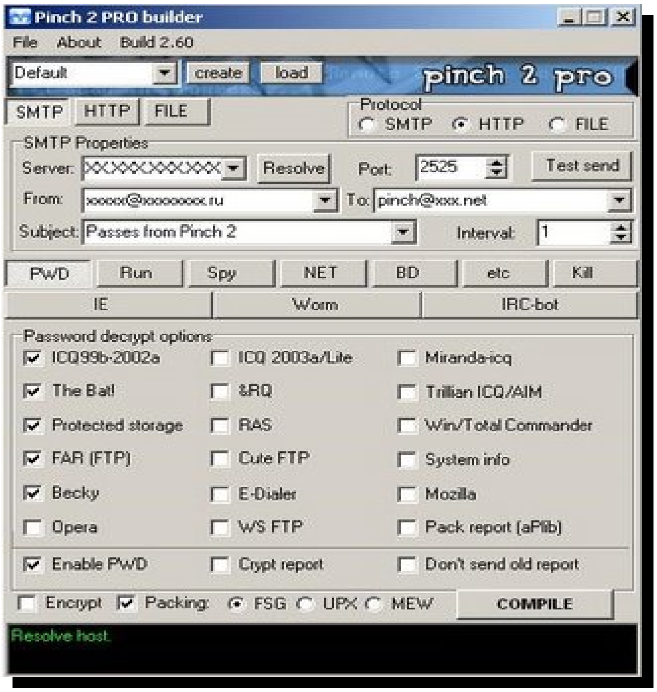
Port : 15963

TURKOJAN
Copyright CigiCigi Online
1997 - 2008 All rights reserved.
Made in Turkey

Connection ID :	IP Address :	Computer Name :	OS :
deneme	[redacted]		WinXP

Ready   Status : Passive

Pinch 2 PRO



Default

Protocol: ○ SMTP ● HTTP ○ FILE

SMTP Properties
Server: XX.XXX.XXX.XXX   Port: 2525
From: xxxxx@xxxxxxxx.ru   To: pinch@xxx.net
Subject: Passes from Pinch 2   Interval: 1

Password decrypt options

☑ ICQ99b-2002a   □ ICQ 2003a/Lite   □ Miranda-icq
☑ The Bat!   □ &RQ   □ Trillian ICQ/AIM
☑ Protected storage   □ RAS   □ Win/Total Commander
☑ FAR (FTP)   □ Cute FTP   □ System info
☑ Becky   □ E-Dialer   □ Mozilla
□ Opera   □ WS FTP   □ Pack report (aPlib)
☑ Enable PWD   □ Crypt report   □ Don't send old report

□ Encrypt ☑ Packing: ● FSG ○ UPX ○ MEW

Resolve host.

About The Author

Chris Mark is the President and CEO of The Aegenis Group. He is an experienced information security professional and recognized payment card industry security expert. The Aegenis Group is the worldwide QSA trainer and contracts with the major card brands to train merchants, service providers and banks on the PCI DSS, and risk management. Prior to founding The Aegenis Group, Chris was the founder and owner of a QSA firm which was subsequently acquired. As a QSA, Chris performed over 100 onsite PCI DSS assessments. Chris has also worked at MasterCard Worldwide and was a founding member of the PCI SSC Technical Working Group. He has also contracted with Visa International and worked with the major card brands on development of their security standards. Chris is a frequent public speaker and has published numerous articles on PCI DSS and data security within the payment card industry. He is also responsible for the founding of the Society of Payment Security Professionals (SPSP) and led the development of the Certified Payment-Card Industry Security Manager (CPISM) and Certified Payment Card-Industry Security Auditor (CPISA) certifications. Chris holds a CISSP, CIPP, CPISA, and numerous technical certifications. He also holds MBA and BA degrees.

About The Aegenis Group, Inc.

The Aegenis Group is dedicated to helping companies navigate the choppy waters of data security, information risk, and privacy regulation. The Aegenis Group believes that the ability to understand not just the regulatory mandates themselves, but their total impact on the business environment can act as a compelling tool for business enablement. From understanding the ways in which your products and services can protect sensitive data to making the right compliance decisions for your business environment, The Aegenis Group can assist your company in facing the risks associated with an increasingly complex landscape of the business world.

Corporate Headquarters:

6410 N Business Park Loop, Suite E
Park City, UT 84098
435-615-6711
www.aegenis.com
info@aegenis.com

The information contained in this document represents the current view of The Aegenis Group, Inc. on the issues discussed herein as of the date of publication. It should not be interpreted as a commitment on the part of The Aegenis Group, Inc and The Aegenis Group, Inc cannot guarantee the accuracy of the information presented after the date of publication. Specifications and content are subject to change without notice. This document is for informational purposes only. THE AEGENIS GROUP, INC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The Aegenis Group is a trademark of The Aegenis Group, Inc. Other product or company names mentioned herein may be the trademarks of their respective owners.