

Extrusion (*)

אף אחד לא רץ לספר לחבר'יה

זליגה של מידע רגיש ויקר ערך מהארגון (*) **Extrusion, n.**

Boasting , *Modern Hebrew slang.* רץ לספר לחבר'יה

“Dick Cheney told me this... and Condoleeza told me that...”

Extrusion Prevention you'll need it when you outsource.

כוח הרגולטור וכורח המציאות של מיקור חוץ

CISO Meeting

December 29, 2004

© 2004 Open Solutions www.software.co.il

The information contained herein is subject to change without notice



Agenda

- Introduction
- Four deadly myths
- Live examples
- Solution
- Future

Introduction

- Why is extrusion a threat when you Outsource?
 - Employees lose their loyalty
 - Assets start disappearing
 - Digital asset protection is usually *not a clause* in the outsourcing contract
 - Firms have no way to *enforce* non-disclosure
 - Everyone wants to save money – *internal security is not a priority* for the outsourcing vendor.
 - *The priority is operations not asset protection*
- Examples
 - We will show several examples from a real network

The four deadly myths

1. Authorized channels are not a threat
2. Authenticated users are not a threat
3. Authorized systems are not at risk
4. Firewall and url filtering protect sensitive digital assets

Extrusion threats

- Trusted insider theft
- Human error in operation or systems
- System vulnerabilities
- Intruders: usually spy-ware
- Extrusion can happen on any channel
 - Mail, http, ftp, telnet, Web proxies, IM
 - The outsourcing vendor is looking at external security not internal security and content monitoring.
 - Maintain status-quo at lowest cost

Modern I.T operations

- Rich in information assets
- Many different kinds of users (employees, contractors, partners, customers)
- Many internal system implementations
- Many interfaces
- I.T Outsourcing focuses on operations and cost reduction, not asset protection.

Outsourcing – you the last one to know?



© UFS, Inc.

Dilbert – Dec 28, 2004

Assets at risk

- Customer personal/billing records
 - Credit cards
 - Pre-paid codes
 - EIS/Data mining, e.g pricing
 - Marketing packages
 - Software source code
-and many more*

True life examples - Customer billing

https://137.0.55.173/l.cgi?sid=20356A6D756C6F0E747E767B6E76&id=t1096384496p8143c12&cmd=selstat&panel=PacketTable.panel&flt=event_id%3d53766 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://137.0.55.173/l.cgi?sid=20356A6D756C6F0E747E767B6E76&id=t1096384496p8143c12&cmd=selstat&panel=PacketTable.panel&flt=event_id%3d53766 Go Links >>

Search Favorites Media

Hotmail Messenger

FIDELIS CommandPost Radar Summary Stats 1 Hour 24 Hrs 7 Days Forensics Reports

Last updated on Tue Sep 28 11:15:02 2004 User **admin** logged on Tue Sep 28 10:36:09 2004 - config - passwd -

Current Status

Last Network Alert
11:14 AM - 9/28
IP fragment overlap
[Protocol violation]
Sensor: ds

Alerts in the past 7 Days

Database Totals

Sensors	1
Alerts	89811

Alerts by Protocols

Version 1.14.1

Alert Details

Alert	P	#	Type	Time	Session
		53766	Potential information leak	2004-09-27 16:04:23	recorded

Sensor ds

Message Suspected transfer of sensitive info: K0088200409271601.csv

Attributes

Decoding Path	Score
: : SMTP[1]: MIME: multipart[3]: MIME(K0088200409271601.csv): base64	10

MCP2

type
Name_SSN

SMTP

Client	Server	From	To
		<info@...>	<josh@travelcell.com>

Mail

From	To	Subject
=?iso-8859-1?Q?Interface Server Production?=<info@...>	ymadl josh@travelcell.com	=?iso-8859-1?Q?Interface Server Production?=<info@...>

Protocol TCP

Source 137.0.1.48 = k

Source Port 4874 = 4874

Destination

Dest Port 25 = smtp

Data Size 32767

Forensic Data "ACCOUNT NUMBER", "PHONE NUMBER", "START TIME", "START DATE", "ORIG. NUMBER", "DESTINATION", "DURATION", "AMOUNT".

MCP found customer files being sent periodically to a josh@travelcell.com and an employee who no longer has "need to know"

Password file extrusion

https://137.0.55.173/l.cgi?sid=20356A6D756C6F0E747E767B6E76&panel=PacketTable.panel&id=t1096386 - Microsoft Internet Explorer

Address: https://137.0.55.173/l.cgi?sid=20356A6D756C6F0E747E767B6E76&panel=PacketTable.panel&id=t1096386537p11818c12&cmd=selsat&flt=event_id%3d259

CommandPost
Radar Summary Stats 1 Hour 24 Hrs 7 Days Forensics Reports

Current Status
Last updated on Tue Sep 28 11:49:40 2004 User admin logged on Tue Sep 28 10:36:09 2004 - con

Last Network Alert
11:49 AM - 9/28
IP fragment overlap
[Protocol violation]
Sensor: ds

Alerts in the past 7 Days

Database Totals
Sensors: 1
Alerts: 89949

Alerts by Protocols

- TCP (42%)
- UDP (21%)
- ICMP (25%)
- ARP (< 1%)
- other (12%)

Version: 1.14.1

Fidelis CommandPost — ©2003,2004 Fidelis Security Systems, Inc. All rights reserved.

Alert Details

Alert	P	#	Type	Time	Session
259	Potential information leak	2004-09-26 13:02:04	records		

Sensor: ds

Message: suspicious file: passwords.xls

Attributes: Decoding Path: : : HTTP : multipart[12] : MIME(passwords)

Match #1: Expression: \.xls

Protocol: TCP

Source: 137.0.59.11 = nmcc12.

Source Port: 2595 = 2595

Destination: .net.il

Dest Port: 80 = www

The production server passwords was stored in a file in "MyDocuments" on a NOC PC. One click and it was extruded. Good example of how human error can threaten a production environment.

The solution

1. Require the outsourcing vendor to comply and enforce internal security
2. Require real-time network audit for compliance
 - Independent of perimeter controls and permissions
 - Independent of network administrators
 - No software installations
 - No systems integration work needed to start working
3. Mitigate all 4 extrusion threats
4. Protect assets directly

Fidelis Extrusion Prevention Appliance

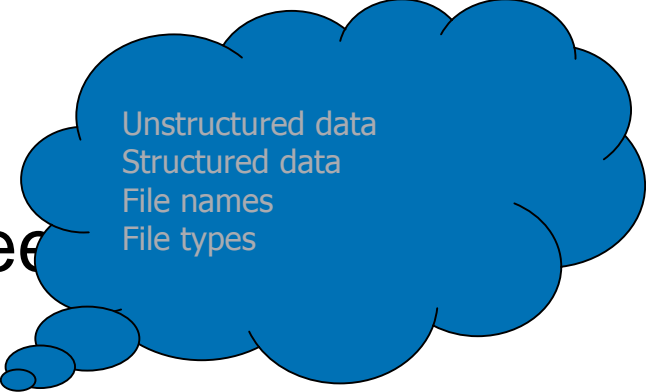
Real Time Network Audit and Investigation Appliance



- Detects flow of profiled digital assets to suspicious / forbidden destinations
- Real-time reporting
- Complete forensics + session snapshots
- Commodity Intel hardware – IBM x335
- Hardened Linux
 - Passive network tap
 - ***Can kill sessions in active mode***
 - 1Gbit full duplex wire-speed
 - Deploy in DMZ or on backbone

Features

1. Scans all channels
2. Works at internal network speed
3. Multi-modal content analysis
4. Extrusion prevention
5. Extrusion & Intrusion in one box
6. Solves event flood problem
7. Digital asset-oriented, not file-oriented
8. No software installations



Unstructured data
Structured data
File names
File types

תהיות על הצפוי לנו בעידן של חוק נתוני אשראי ומיקור חוץ רבתי
- כוח הרגולטור וכורח המציאות



- We're playing last year's game:
Bank of Israel, Dept of Justice employ consultants
 - The consultants copy and paste from 357
 - Is any one thinking ahead?
- Consumer identity theft is a HUGE issue:
 - The No. 1 consumer threat in U.S
 - Cardholders at mercy of consumer credit firms
 - Concern in Knesset Economic committee

Will Identify Theft become Israel's No. 1 problem in 2006?

Open Solutions - Specialists in Open Source software security

<http://www.software.co.il>

Thank you.