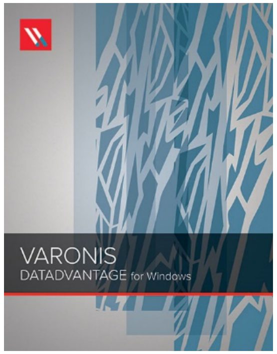
Insider Threats: Malice, Mistakes and Mountains Lions

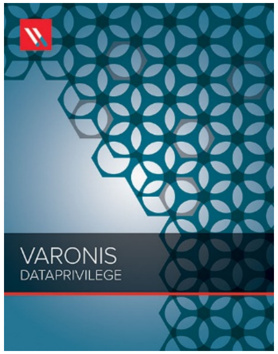
Presented by: Brian Vecci, Technical Evangelist, Varonis Systems, Inc.

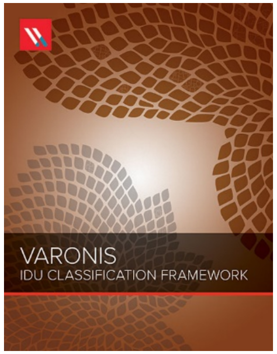
Cybersecurity Essentials – E31

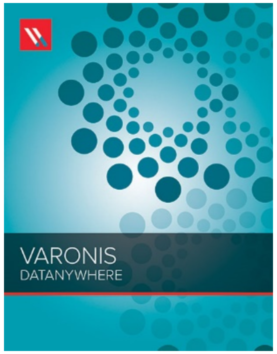
About Varonis

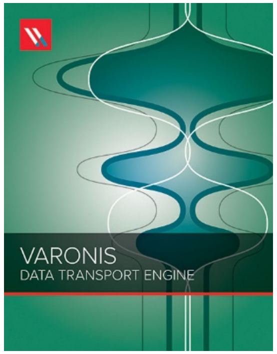
- Started operations in 2005
- Over **3500** Customers
  - (as of March, 2015)
- Software Solutions for Human Generated Data

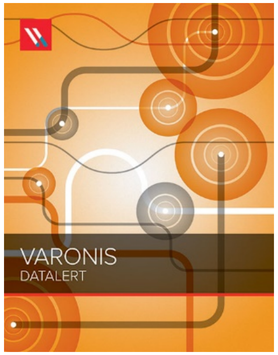


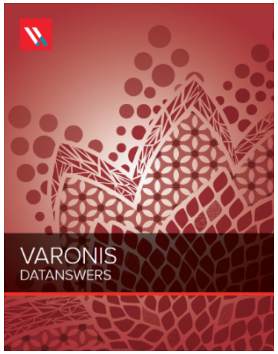












The Varonis Origin Story

Agenda

- The anatomy of insider breaches
- Real world breaches: stats and examples
- Our irrational biases about risk
- 6 tips for mitigating insider threats

INSIDER THREATS: THE ACTORS

THE TURNCLOAK

THE PAWN

THE IMPOSTER

The Script

Get inside (if not there already)

- Usually done by phishing or social engineering

Snoop around

- Enumerate current access; attempt to elevate
- Visa cards anyone?

Exfiltration

- Get the data out without sounding alarms

```
PS C:\Users\eddard> findstr /r "^4[0-9]{12}(?:[0-9]{3})?$"
```

By the Numbers

Figure 43.
Top 10 threat action varieties within Miscellaneous Errors (n=558)

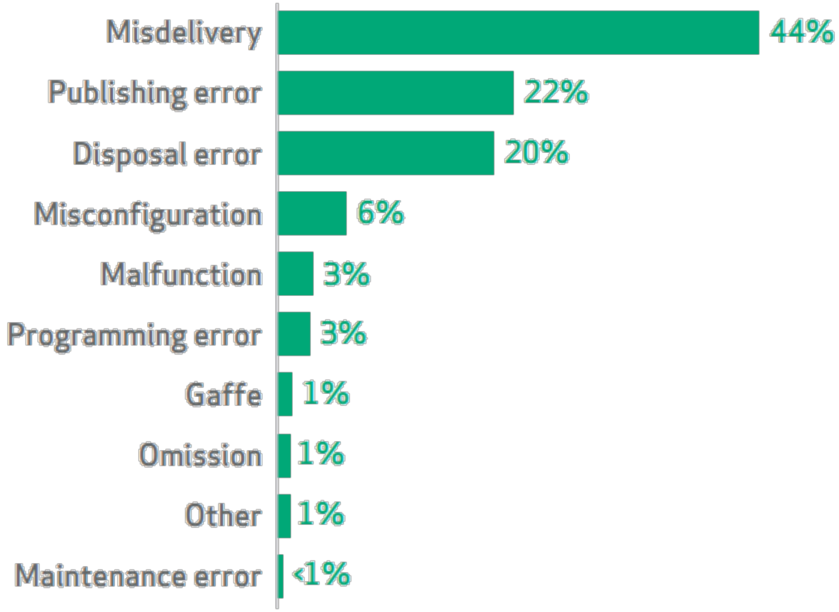
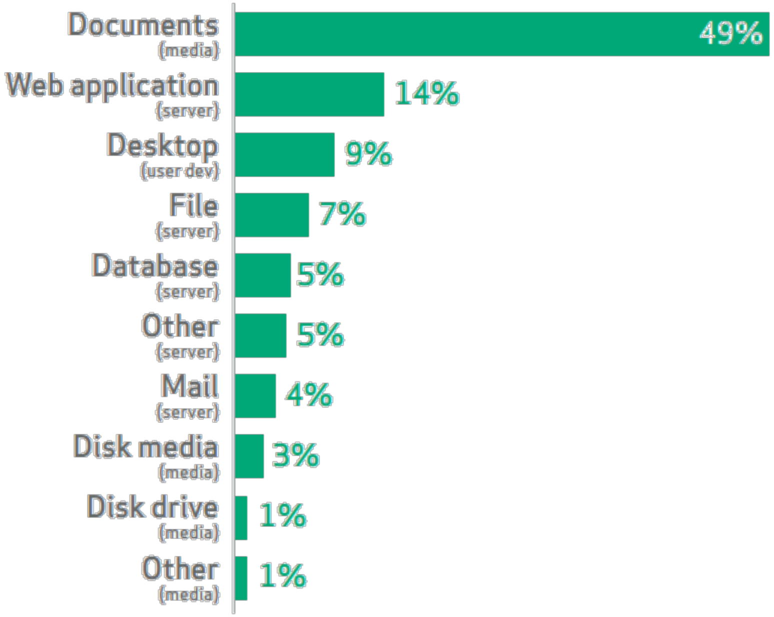
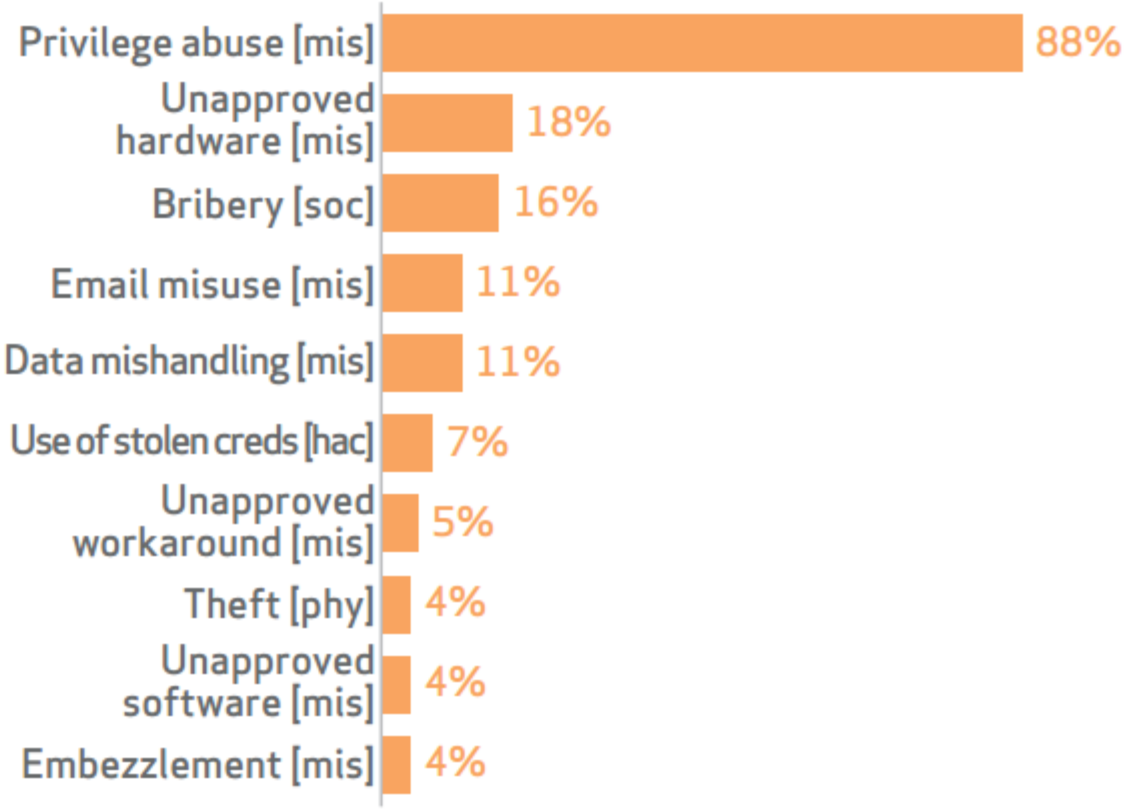


Figure 44.
Top 10 assets affected within Miscellaneous Errors (n=546)

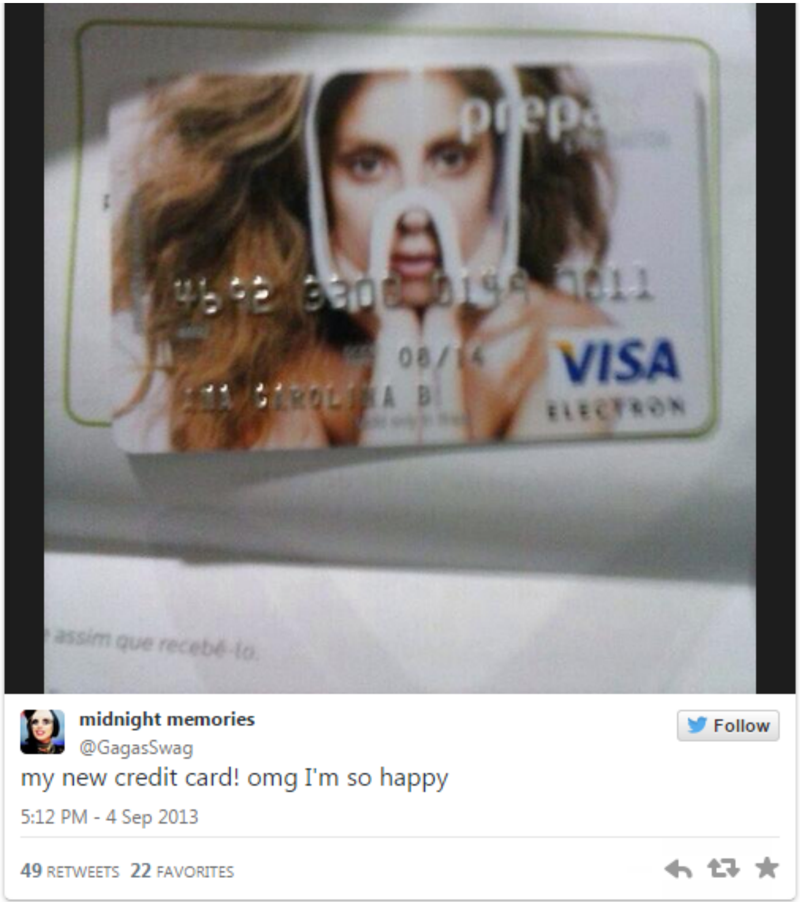


Privilege Abuse

Figure 30.
Top 10 threat action varieties within Insider Misuse (n=153)



Our Own Worst Enemy



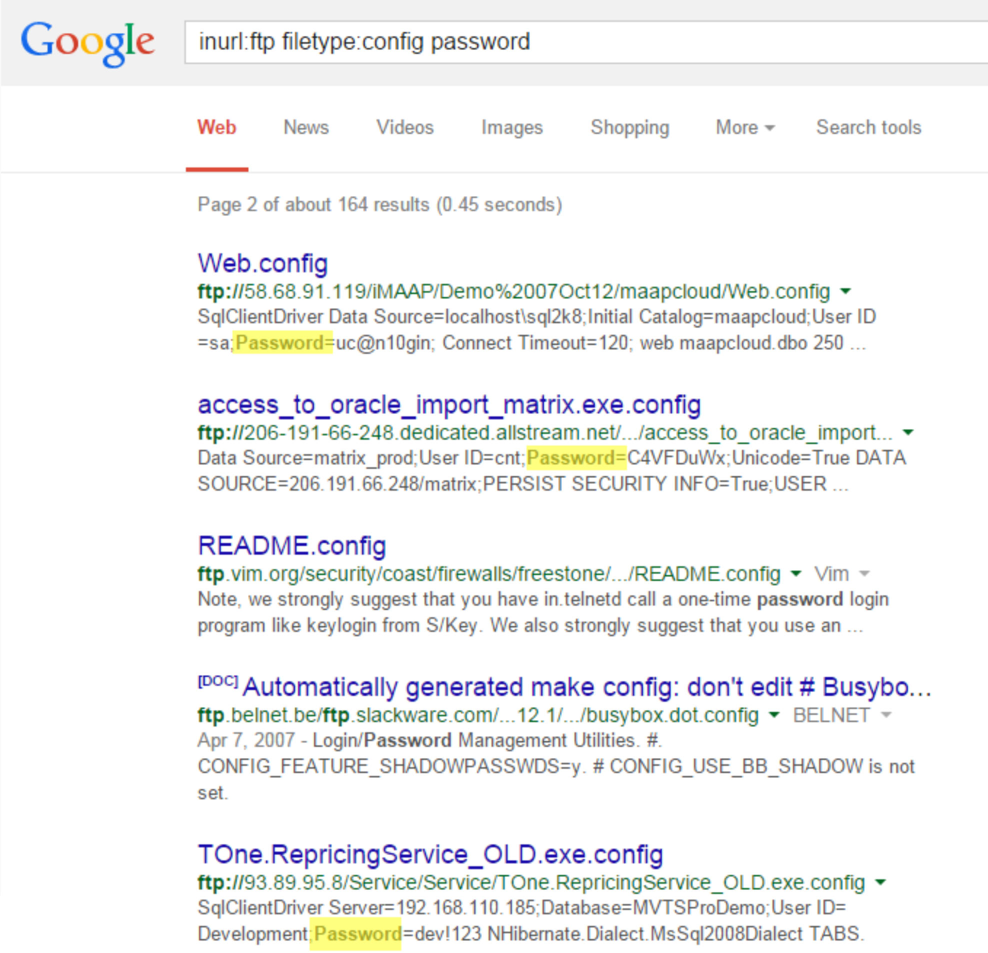
midnight memories @GagasSwag

Follow

my new credit card! omg I'm so happy

5:12 PM - 4 Sep 2013

49 RETWEETS 22 FAVORITES



inurl:ftp filetype:config password

Page 2 of about 164 results (0.45 seconds)

Web.config
ftp://58.68.91.119/iMAAP/Demo%2007Oct12/maapcloud/Web.config
SqlClientDriver Data Source=localhost\sql2k8;Initial Catalog=maapcloud;User ID =sa;Password=uc@n10gin; Connect Timeout=120; web maapcloud.dbo 250 ...

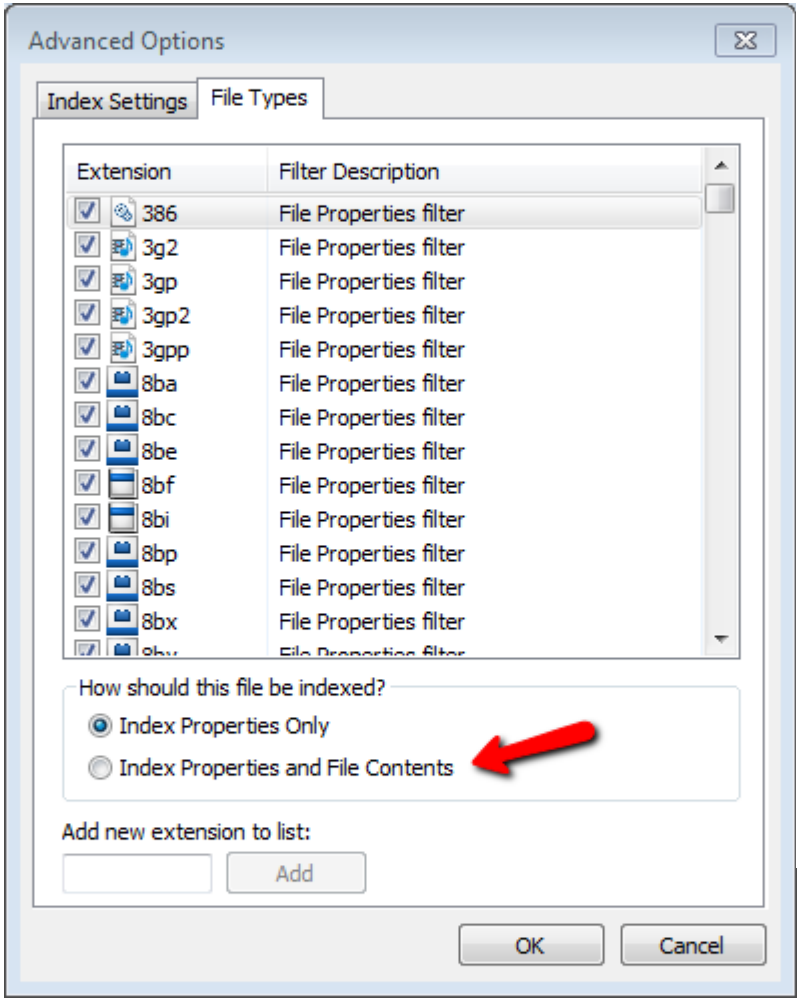
access_to_oracle_import_matrix.exe.config
ftp://206-191-66-248.dedicated.allstream.net/.../access_to_oracle_import...
Data Source=matrix_prod;User ID=cnt;Password=C4VFDuWx;Unicode=True DATA SOURCE=206.191.66.248/matrix;PERSIST SECURITY INFO=True;USER ...

README.config
ftp.vim.org/security/coast/firewalls/freestone/.../README.config Vim
Note, we strongly suggest that you have in.telnetd call a one-time **password** login program like keylogin from S/Key. We also strongly suggest that you use an ...

[DOC] Automatically generated make config: don't edit # Busybo...
ftp.belnet.be/ftp.slackware.com/...12.1/.../busybox.dot.config BELNET
Apr 7, 2007 - Login/**Password** Management Utilities. #. CONFIG_FEATURE_SHADOWPASSWDS=y. # CONFIG_USE_BB_SHADOW is not set.

TOne.RepricingService_OLD.exe.config
ftp://93.89.95.8/Service/Service/TOne.RepricingService_OLD.exe.config
SqlClientDriver Server=192.168.110.185;Database=MVTSProDemo;User ID= Development;Password=dev!123 NHibernate.Dialect.MsSql2008Dialect TABS.

Snooping Behind the Firewall



Advanced Options

Index Settings | File Types

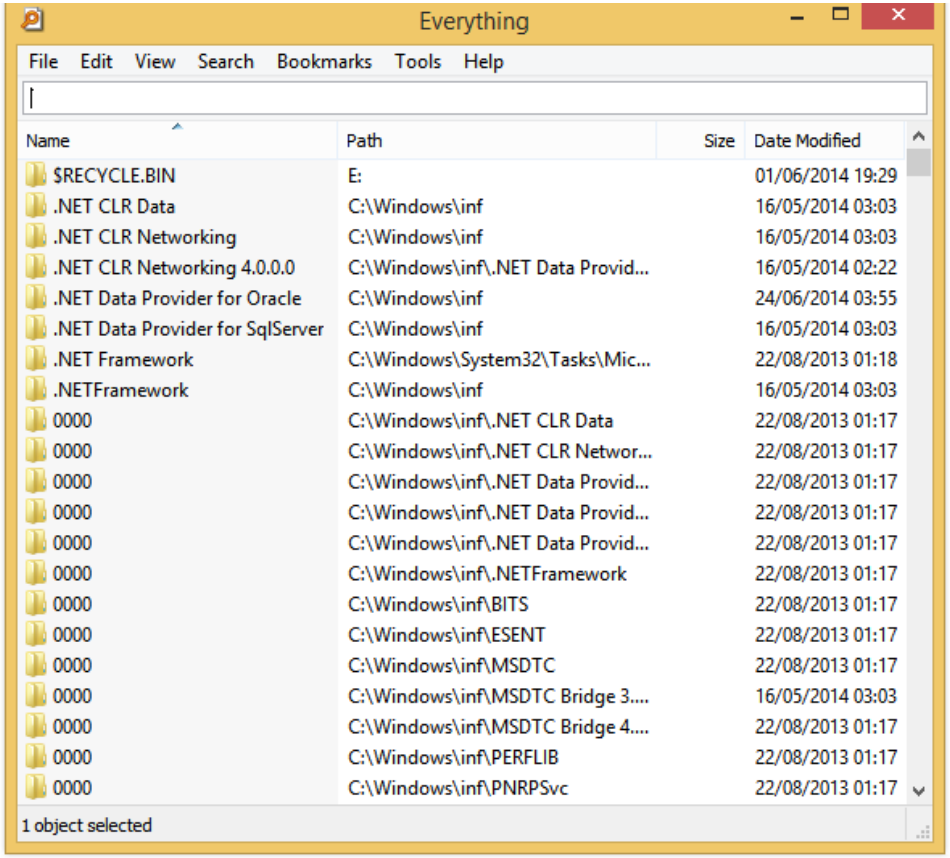
Extension	Filter Description
☑ 386	File Properties filter
☑ 3g2	File Properties filter
☑ 3gp	File Properties filter
☑ 3gp2	File Properties filter
☑ 3gpp	File Properties filter
☑ 8ba	File Properties filter
☑ 8bc	File Properties filter
☑ 8be	File Properties filter
☑ 8bf	File Properties filter
☑ 8bi	File Properties filter
☑ 8bp	File Properties filter
☑ 8bs	File Properties filter
☑ 8bx	File Properties filter

How should this file be indexed?

● Index Properties Only

○ Index Properties and File Contents

Add new extension to list:



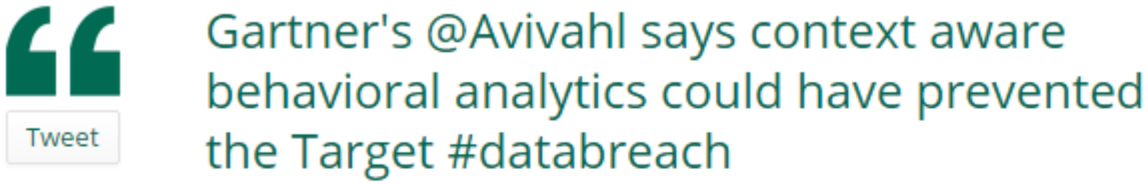
Everything

Name	Path	Size	Date Modified
$RECYCLE.BIN	E:		01/06/2014 19:29
.NET CLR Data	C:\Windows\inf		16/05/2014 03:03
.NET CLR Networking	C:\Windows\inf		16/05/2014 03:03
.NET CLR Networking 4.0.0.0	C:\Windows\inf\.NET Data Provid...		16/05/2014 02:22
.NET Data Provider for Oracle	C:\Windows\inf		24/06/2014 03:55
.NET Data Provider for SqlServer	C:\Windows\inf		16/05/2014 03:03
.NET Framework	C:\Windows\System32\Tasks\Mic...		22/08/2013 01:18
.NETFramework	C:\Windows\inf		16/05/2014 03:03
0000	C:\Windows\inf\.NET CLR Data		22/08/2013 01:17
0000	C:\Windows\inf\.NET CLR Networ...		22/08/2013 01:17
0000	C:\Windows\inf\.NET Data Provid...		22/08/2013 01:17
0000	C:\Windows\inf\.NET Data Provid...		22/08/2013 01:17
0000	C:\Windows\inf\.NET Data Provid...		22/08/2013 01:17
0000	C:\Windows\inf\.NETFramework		22/08/2013 01:17
0000	C:\Windows\inf\BITS		22/08/2013 01:17
0000	C:\Windows\inf\ESENT		22/08/2013 01:17
0000	C:\Windows\inf\MSDTC		22/08/2013 01:17
0000	C:\Windows\inf\MSDTC Bridge 3....		16/05/2014 03:03
0000	C:\Windows\inf\MSDTC Bridge 4....		22/08/2013 01:17
0000	C:\Windows\inf\PERFLIB		22/08/2013 01:17
0000	C:\Windows\inf\PNRPSvc		22/08/2013 01:17

1 object selected

Target as a Target

- **$162 million breach**
- Lots of fancy tools watching the perimeter (candy bar syndrome)
- "[…] spokeswoman, Molly Snyder, says the intruders had gained access to the system by using stolen credentials from a third-party

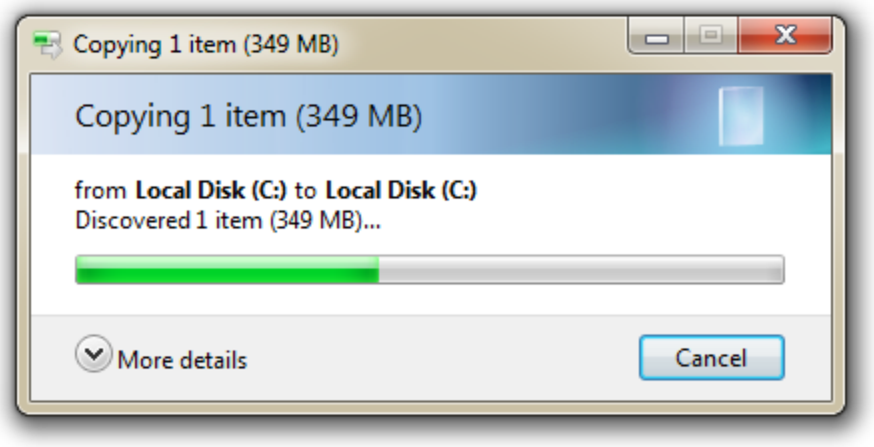


Gartner's @Avivahl says context aware behavioral analytics could have prevented the Target #databreach

Risk and Irrational Biases

Fear and Frequency

- Large university
- 146,000 student records, including SSNs, exposed
- Cause? **Copy/paste**

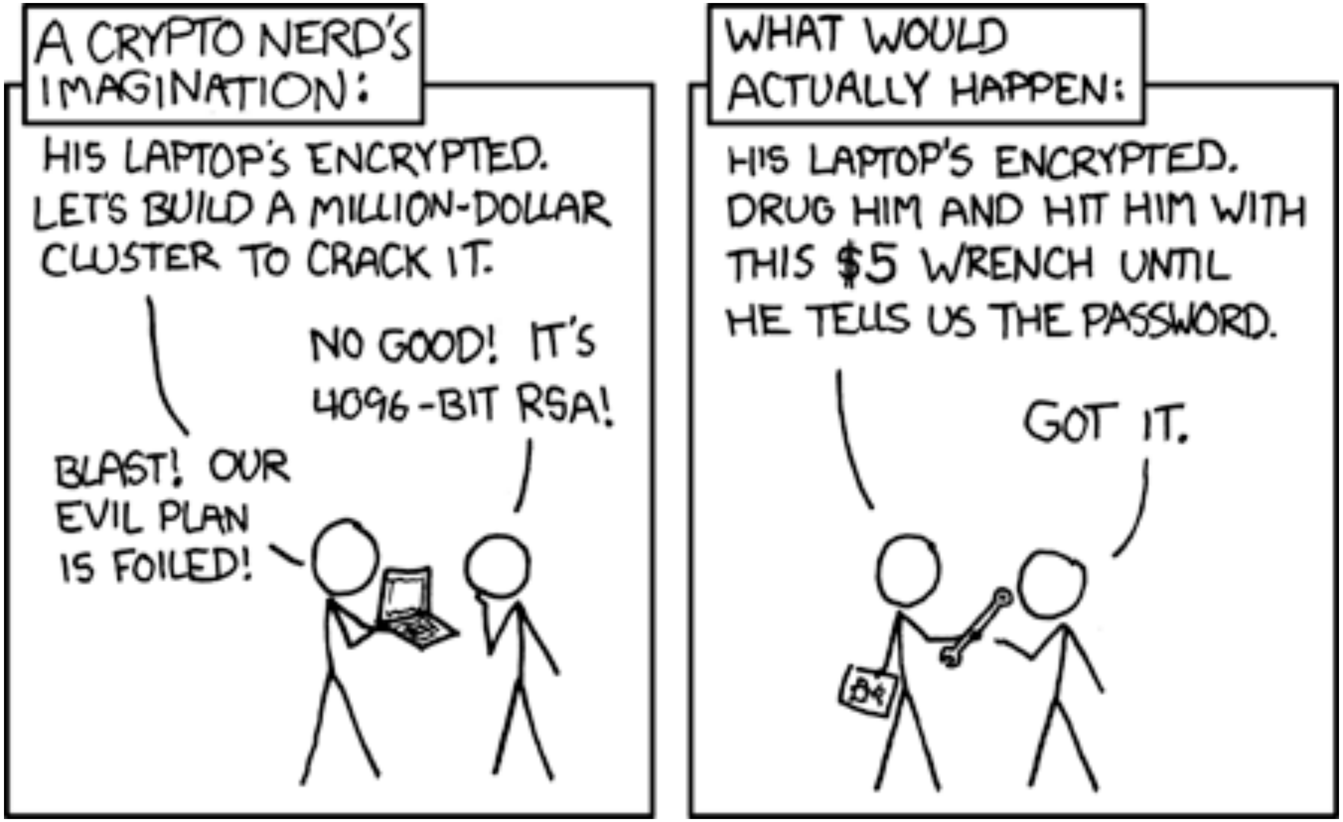


Copying 1 item (349 MB)

Copying 1 item (349 MB)

from **Local Disk (C:)** to **Local Disk (C:)**
Discovered 1 item (349 MB)...

A Story About Trees


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

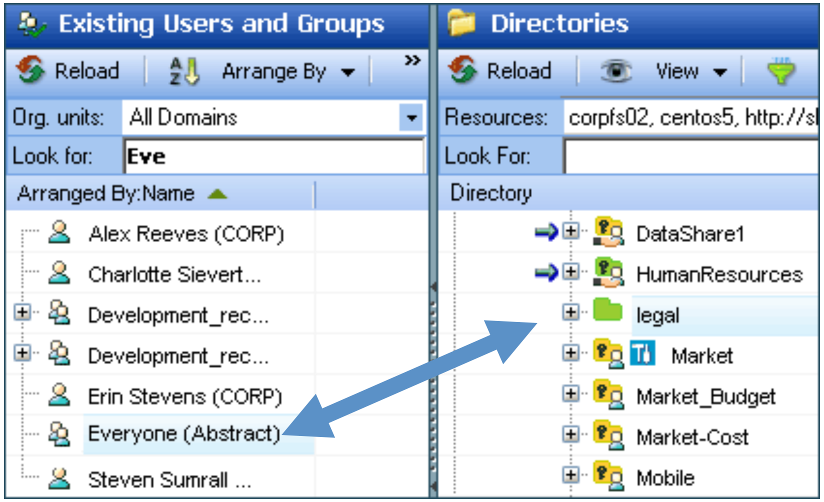
They’re in—now what?

6 Mitigation Tips

1. Eliminate Global Access
2. Eliminate Excessive Permissions
3. Alert on Privilege Escalations
4. Alert on Behavioral Deviations
5. Setup Honeypots
6. Closely Monitor High-Risk People and Data

Tip #1: Eliminate Global Access

- Locate groups like “Everyone” and “Authenticated Users” and replace them with tighter security groups
- How do I avoid cutting off legitimate access?



Org. units: All Domains

Look for: Eve

Arranged By:Name

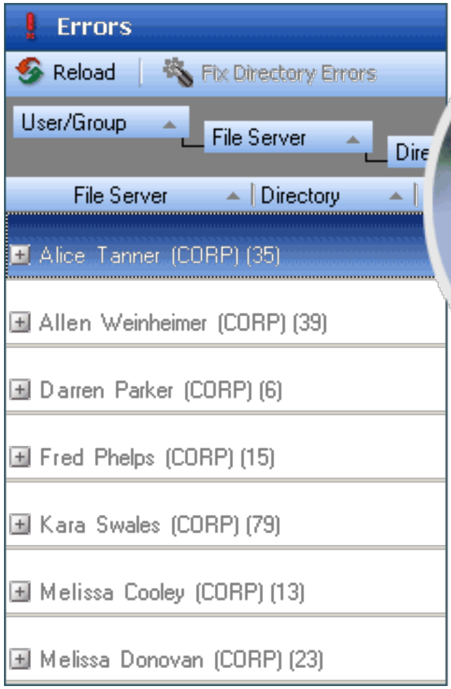
Alex Reeves (CORP)
Charlotte Sievert...
Development_rec...
Development_rec...
Erin Stevens (CORP)
Everyone (Abstract)
Steven Sumrall ...

Resources: corpfs02, centos5, http://s

Look For:

Directory

DataShare1
HumanResources
legal
Market
Market_Budget
Market-Cost
Mobile

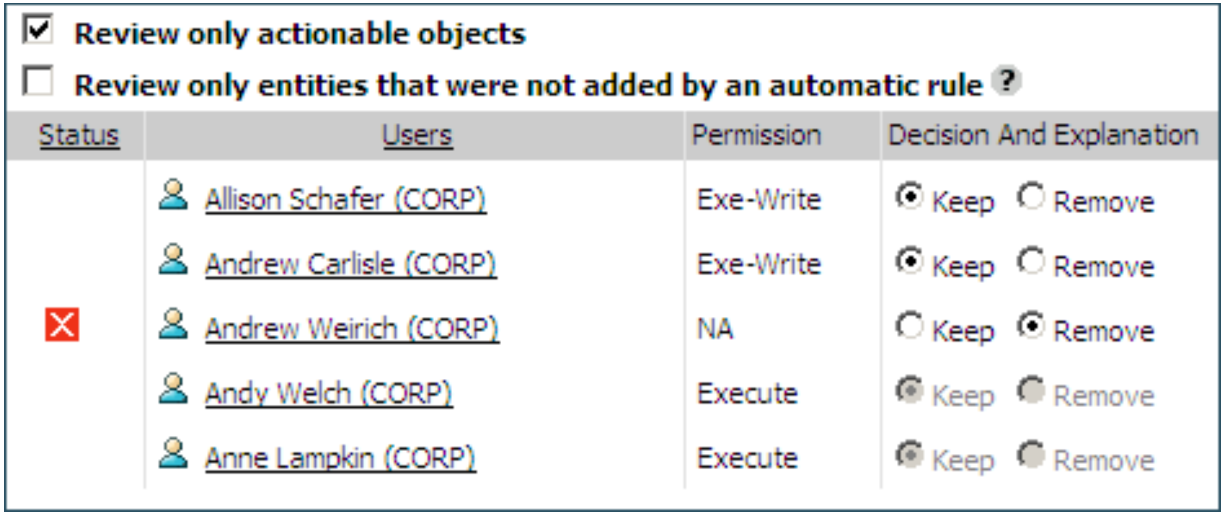


Alice Tanner (CORP) (35)
Allen Weinheimer (CORP) (39)
Darren Parker (CORP) (6)
Fred Phelps (CORP) (15)
Kara Swales (CORP) (79)
Melissa Cooley (CORP) (13)
Melissa Donovan (CORP) (23)

Alice Tanner will lose access to data she has been using!

Tip #2: Eliminate Excessive Permissions

- People *and* software!
- Figure out what people have access to but *shouldn't*
  - Amazon-like recommendations
- Auto-expire temporary access
- Periodically review entitlements



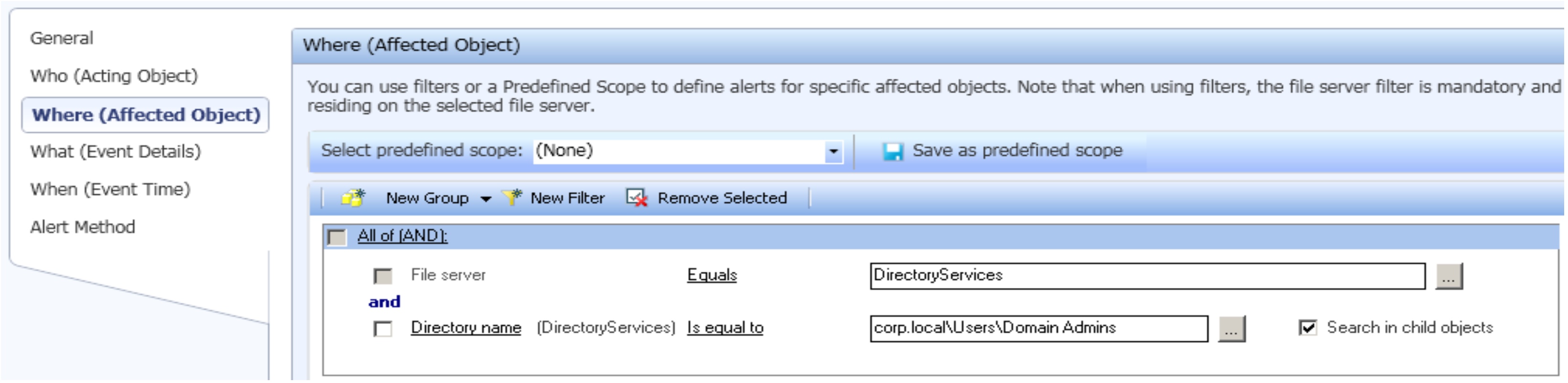
☑ Review only actionable objects

☐ Review only entities that were not added by an automatic rule ?

Status	Users	Permission	Decision And Explanation
	Allison Schafer (CORP)	Exe-Write	● Keep ○ Remove
	Andrew Carlisle (CORP)	Exe-Write	● Keep ○ Remove
☒	Andrew Weirich (CORP)	NA	○ Keep ● Remove
	Andy Welch (CORP)	Execute	● Keep ○ Remove
	Anne Lampkin (CORP)	Execute	● Keep ○ Remove

Tip #3: Alert on Privilege Escalations

- Do you know when someone gets root access?



Where (Affected Object)

You can use filters or a Predefined Scope to define alerts for specific affected objects. Note that when using filters, the file server filter is mandatory and residing on the selected file server.

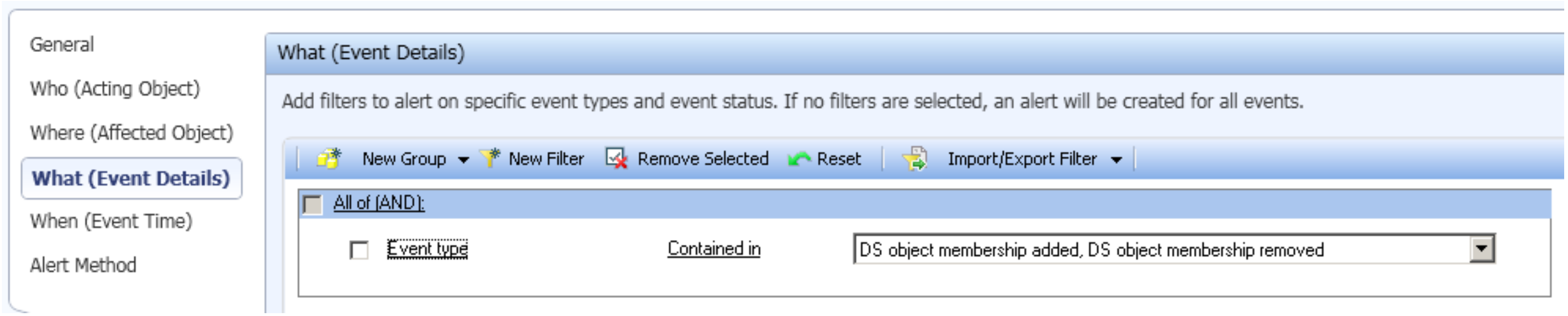
Select predefined scope: (None)

□ All of (AND):

□ File server Equals DirectoryServices

and

□ Directory name (DirectoryServices) Is equal to corp.local\Users\Domain Admins ☑ Search in child objects



What (Event Details)

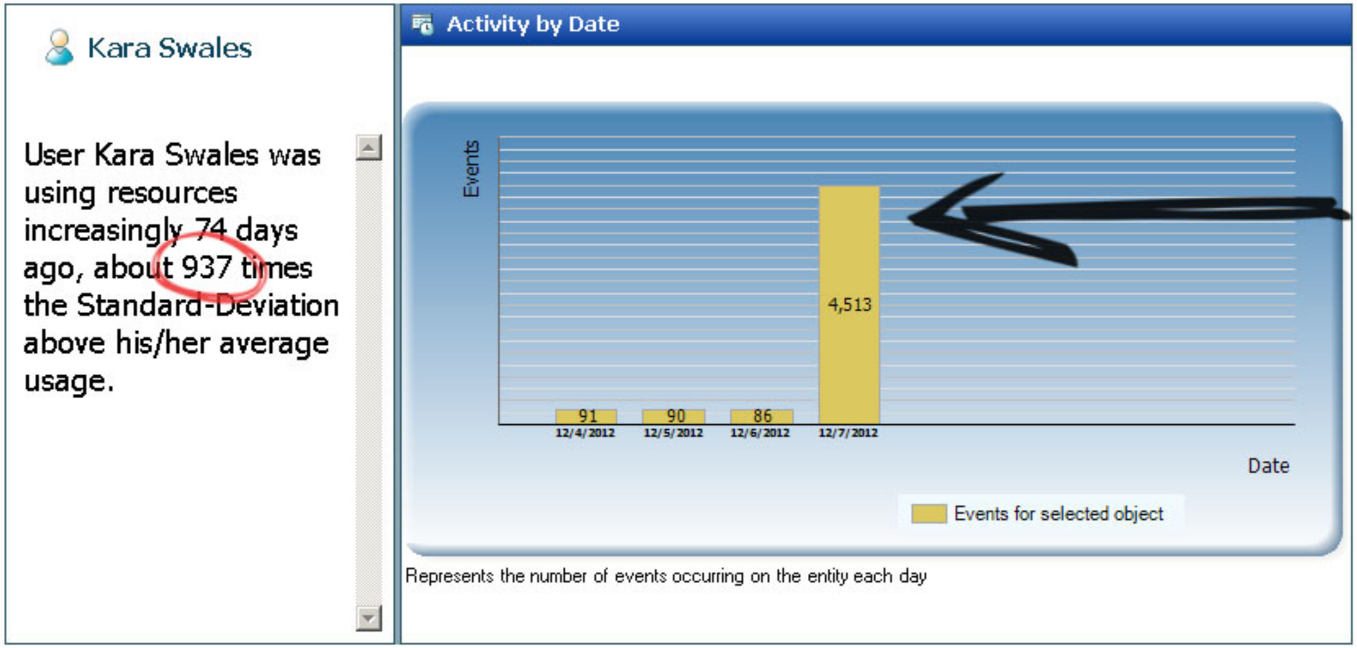
Add filters to alert on specific event types and event status. If no filters are selected, an alert will be created for all events.

□ All of (AND):

□ Event type Contained in DS object membership added, DS object membership removed

Tip #4: Alert on Behavioral Deviations

- Behavioral activity spikes (email, files, access denied)
- Monitor activity outside of normal business hours



Kara Swales

User Kara Swales was using resources increasingly 74 days ago, about 937 times the Standard-Deviation above his/her average usage.

Represents the number of events occurring on the entity each day

Alert on anomalous behavior.

Detecting CryptoLocker

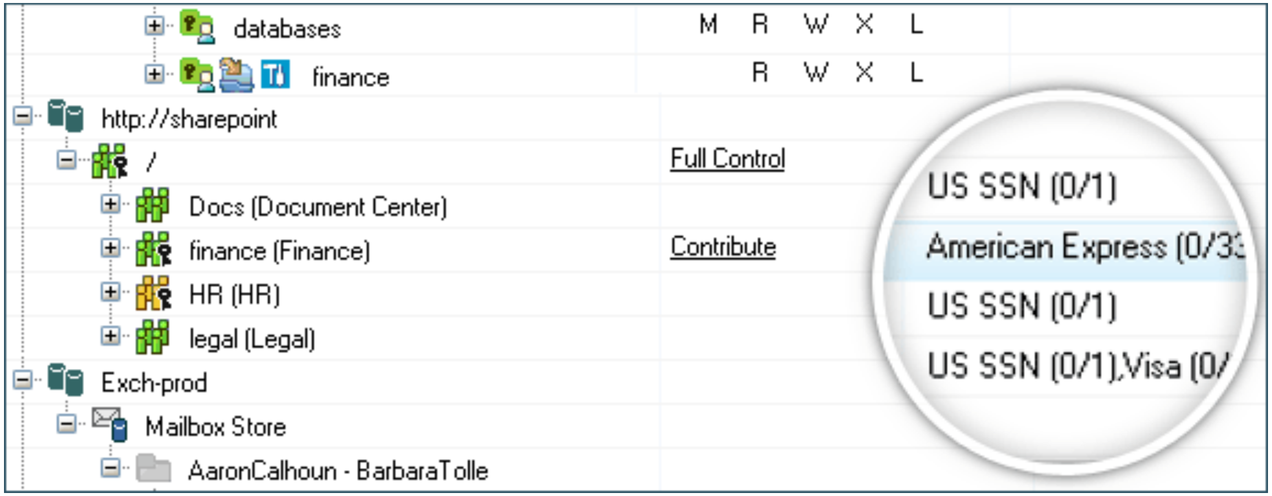
- Alert on more than 100 file modify events from a single user in under a minute
- Alert triggers an action to:
  - Notify IT admins
  - Grab the username and machine
  - Check the machine's registry for key/value that CryptoLocker creates
    - `Get-Item HKCU:\Software\CryptoLocker\Files).GetValueNames()`
  - If value exists, disable user automatically:
    - `Disable-ADAccount -Identity $actingObject`

Tip #5: Setup Honeypots

- Setup a shared folder that is open to everyone
  - X:\Share\Payroll
  - X:\Share\Confidential
  - X:\Share\CEO
- See who abuses it

Tip #6: Monitor High Risk People and Data

- Alert or auto-quarantine sensitive data when it shows up in a public place
- Watch what root/domain admins are doing
- Watch what contractors are doing



databases	M R W X L	
finance	R W X L	
http://sharepoint		
/	Full Control	
Docs (Document Center)		
finance (Finance)	Contribute	
HR (HR)		
legal (Legal)		
Exch-prod		
Mailbox Store		
AaronCalhoun - BarbaraTolle		

US SSN (0/1)
American Express (0/3
US SSN (0/1)
US SSN (0/1),Visa (0/

FREE THREAT ASSESSMENT

HTTP://BIT.LY/THREATCHECK

THANK YOU!