



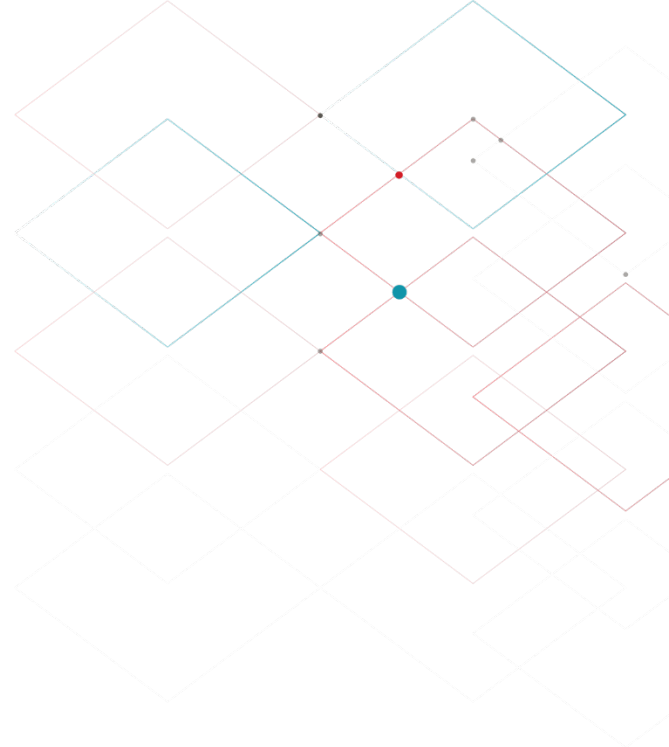
Our mission is to protect data from insider threats and cyberattacks.

The Enemy Within

Understanding Insider Threats

Agenda

- ◆ A few thoughts on ransomware
- ◆ Examples of insider threats
- ◆ Mitigating insider threats



About Me

- ◆ Ben Hui
- ◆ Manager Solution Architects
- ◆ www.varonis.com



The Boston Globe

ING 



MoMA

EMC²



What I know about Ikoyi house where EFCC found over N13 billion – Former PDP Chairman

April 14, 2017 Samuel Ogundipe



N13Billion Ikoyi money

A former chairman of the People's Democratic Party, Adamu Mu'azu on Friday explained his connection to the Lagos property where the anti-graft EFCC found over N13 billion hidden in an apartment.



UCLA
HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER

40 BTC


 VARONIS



UCLA
HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER

\$17,000

 VARONIS



But what's a hospital's data
actually worth?

What are their
services worth?

SCHEDULE OF MEDI-CAL ANCILLARY COSTS

Provider Name:
HOLLYWOOD PRESBYTERIAN MEDICAL CENTER

Fiscal Period Ended:
DECEMBER 31, 2012

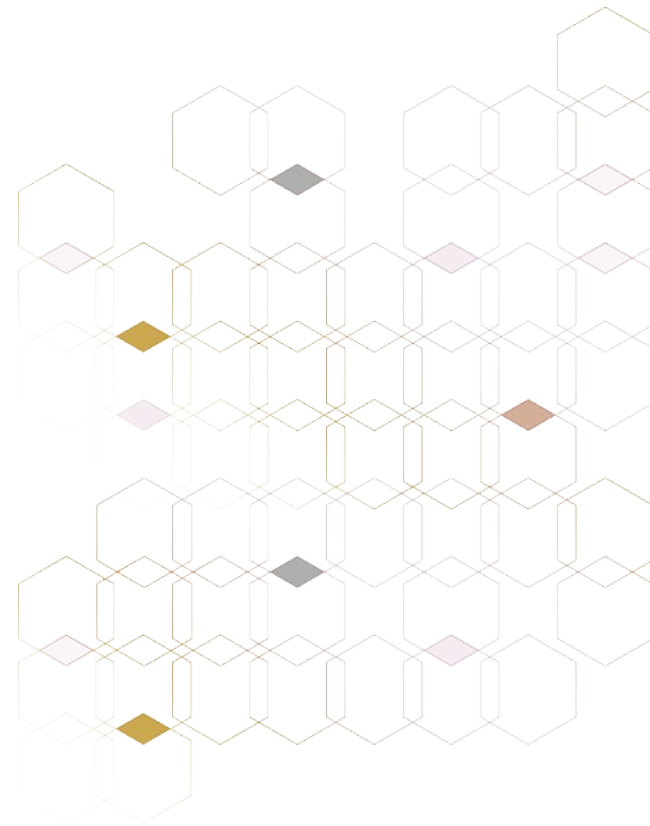
Provider NPI:
1922033547

		TOTAL ANCILLARY COST *	TOTAL ANCILLARY CHARGES (Adj)	RATIO COST TO CHARGES	MEDI-CAL CHARGES (From Schedule 6)	MEDI-CAL COST
ANCILLARY COST CENTERS						
50.00	Operating Room	\$ 9,028,033	\$ 52,526,135	0.171877	\$ 0	\$ 0
51.00	Recovery Room	2,320,630	38,463,066	0.060334	0	0
52.00	Labor Room and Delivery Room	10,690,393	19,893,113	0.537392	0	0
53.00	Anesthesiology	102,463	8,983,402	0.011406	0	0
54.00	Radiology-Diagnostic	4,238,445	23,400,390	0.181127	21,248	3,849
55.00	Radiology-Therapeutic	3,758,828	24,879,197	0.151083	0	0
56.00	Radioisotope	1,580,397	4,672,251	0.338252	200	68
57.00	CT Scan	1,679,398	41,541,854	0.040427	0	0
58.00	Magnetic Resonance Imaging (MRI)	1,002,291	11,215,016	0.089370	0	0
59.00	Cardiac Catheterization	2,271,938	17,755,163	0.127959	0	0
60.00	Laboratory	10,315,623	54,670,364	0.188688	75,110	14,172
61.00	PBP Clinical Laboratory Services-Program Only	0	0	0.000000	0	0
62.00	Whole Blood & Packed Red Blood Cells	0	0	0.000000	0	0
63.00	Blood Storing, Processing, & Transfusion	1,798,944	3,328,273	0.540504	0	0
64.00	Intravenous Therapy	0	0	0.000000	0	0
65.00	Respiratory Therapy	10,473,538	146,614,591	0.071436	0	0
66.00	Physical Therapy	3,660,298	13,750,674	0.266190	59,810	15,921
67.00	Occupational Therapy	147,028	6,918,015	0.021380	12,487	288

“

I am seeing around 4,000
new infections per hour,
or approximately
100,000 new infections
per day.

”



– Kevin Beaumont, Malware Analyst

Why is Ransomware so dangerous when it becomes an insider?

Insiders have a lot of access

62%

of end users say they have access to company data they probably shouldn't see

29%

of IT respondents say their companies fully enforce a strict least privilege model



Very few watch what insiders are doing

35%

of organizations have no searchable records of file system activity

38%

do not monitor any file and email activity.



Insiders are beyond the perimeter security





The Pawn

The canary in the coal mine: Malware Molly

1 Payment Declined -- Update Required Immediately!

2 From: **ApplePay Support** <customer_support_ref_@apple.com>

3 Dear Apple User,

4 It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

5 <https://www.applepay.com/subscriptions/payment-update>
6 <http://944.535.32/index/apple.html>

7 **If you do not update your payment information in the next 24 hours, your account will be deactivated.**

8 Regards
9 ApplePay Support

Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

9  apple-invoice.zip [Download](#)

1 Sense of urgency Fear tactics	2 Imitating known brand Fake email address	3 Impersonal	4 Urgency Punctuation and grammar mistakes	5 Rollover shows malicious link
6 Scare tactics	7 Impersonal Not real customer service	8 Copyright date is incorrect Location is incorrect	9 ZIP file	

1
2
3
4
2



1

Not a legitimate
Apple website
address

2

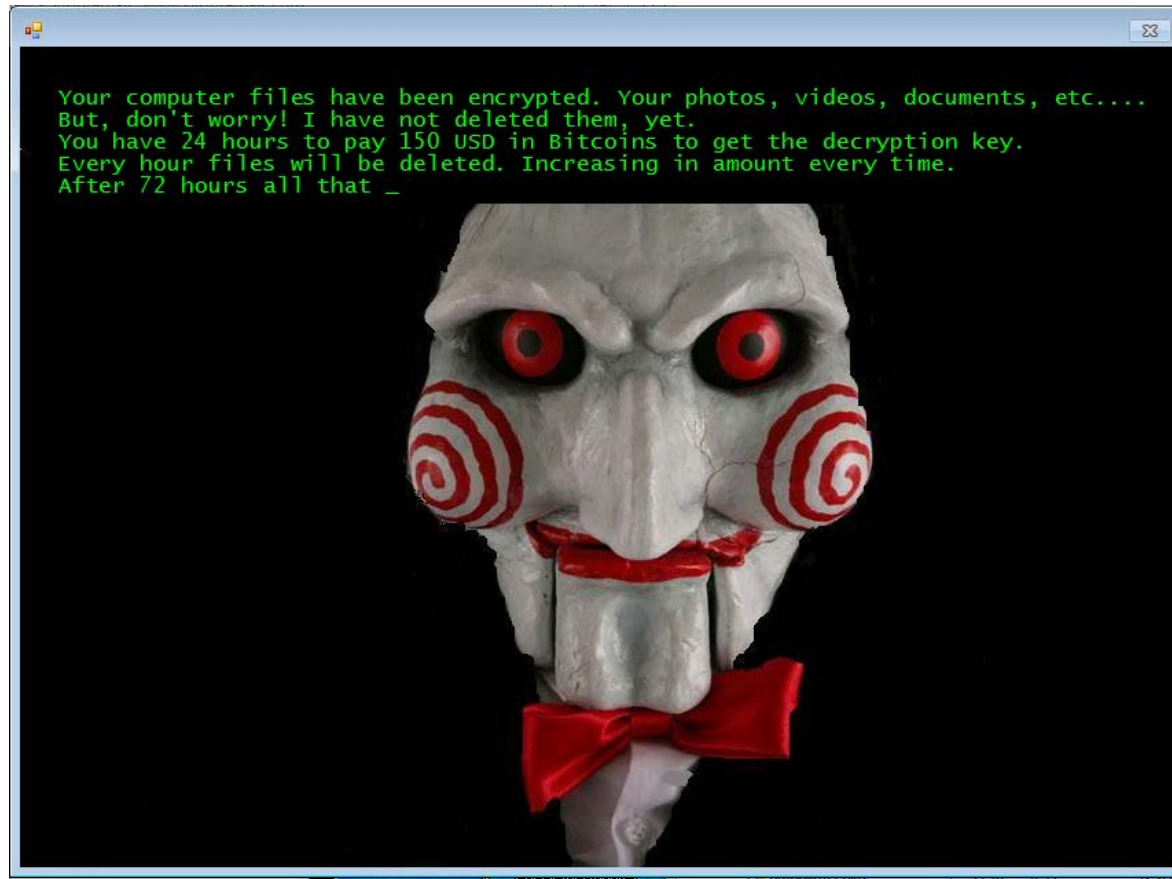
Missing
navigation bar
and footer

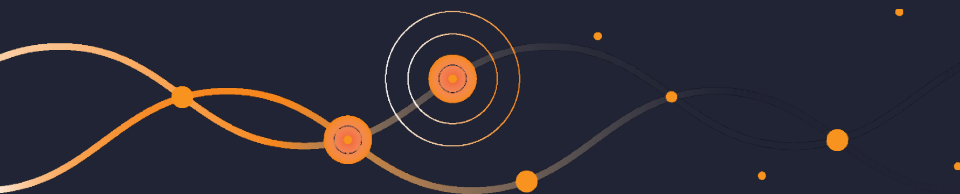
3

"Apple Pay"
is misspelled

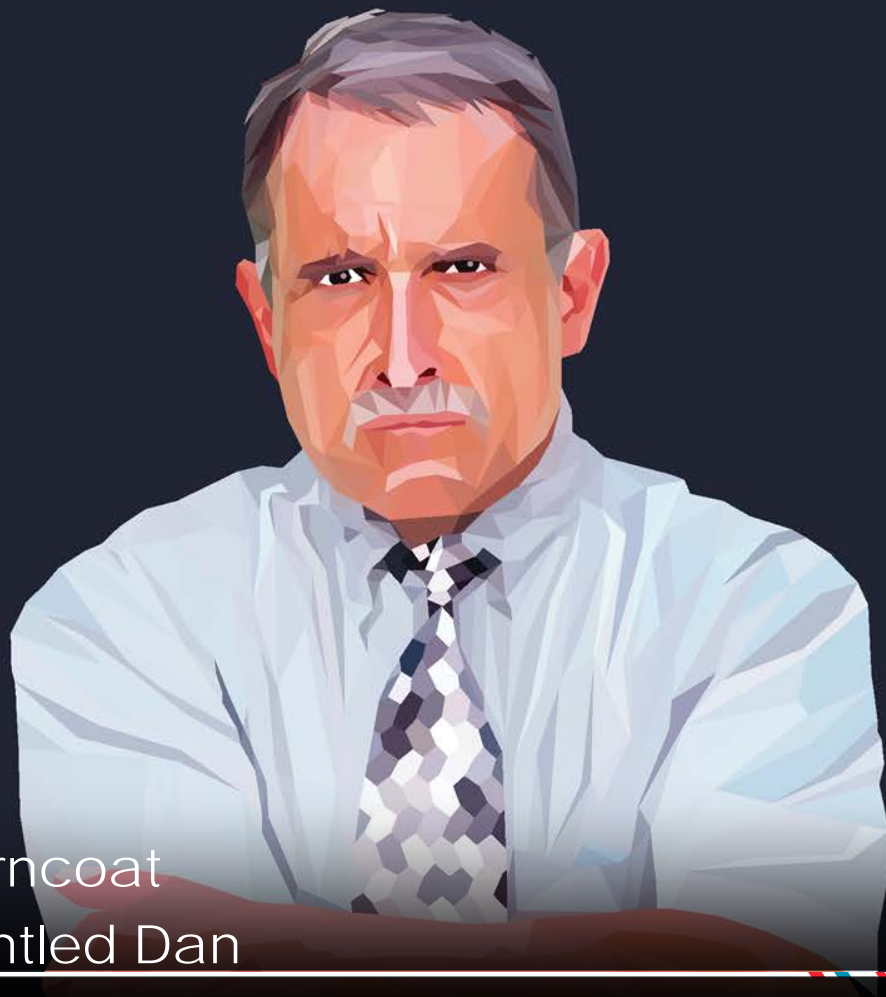
4

Apple ID
homepage doesn't
require password





Let's Meet The Other
Insider Threats



The Turncoat
Disgruntled Dan











The Impostor
Abusive Admin Andy

Retiring Sysadmin Fakes Cyber-Attack to Get Away with Data Theft

news.softpedia.com/news/retiring-sysadmin-fakes-cyber-attack-to-get-away-with-data-theft-50799

SOFTPEDIA® DESKTOP MOBILE WEB NEW

Softpedia > News > Security > Incidents

Retiring Sysadmin Fakes Cyber-Attack to Get Away with Data Theft

He did it because he wanted a house in a seaside town

Sep 6, 2016 02:05 GMT · By Catalin Cimpanu · Share:   

A system administrator for an unnamed company was caught defacing the firm's website to hide the theft of company data, which he planned to steal and then retire to a seaside town abroad.

The system administrator, who, due to non-disclosure agreements signed in such incidents, cannot be named at this point in time, had worked for his company for 1 year and had earned the trust of his colleagues.

The employee had always wanted to buy a house in a seaside town abroad when it was time to retire. Unfortunately, he wasn't able to gather all the money to follow through with his dreams.

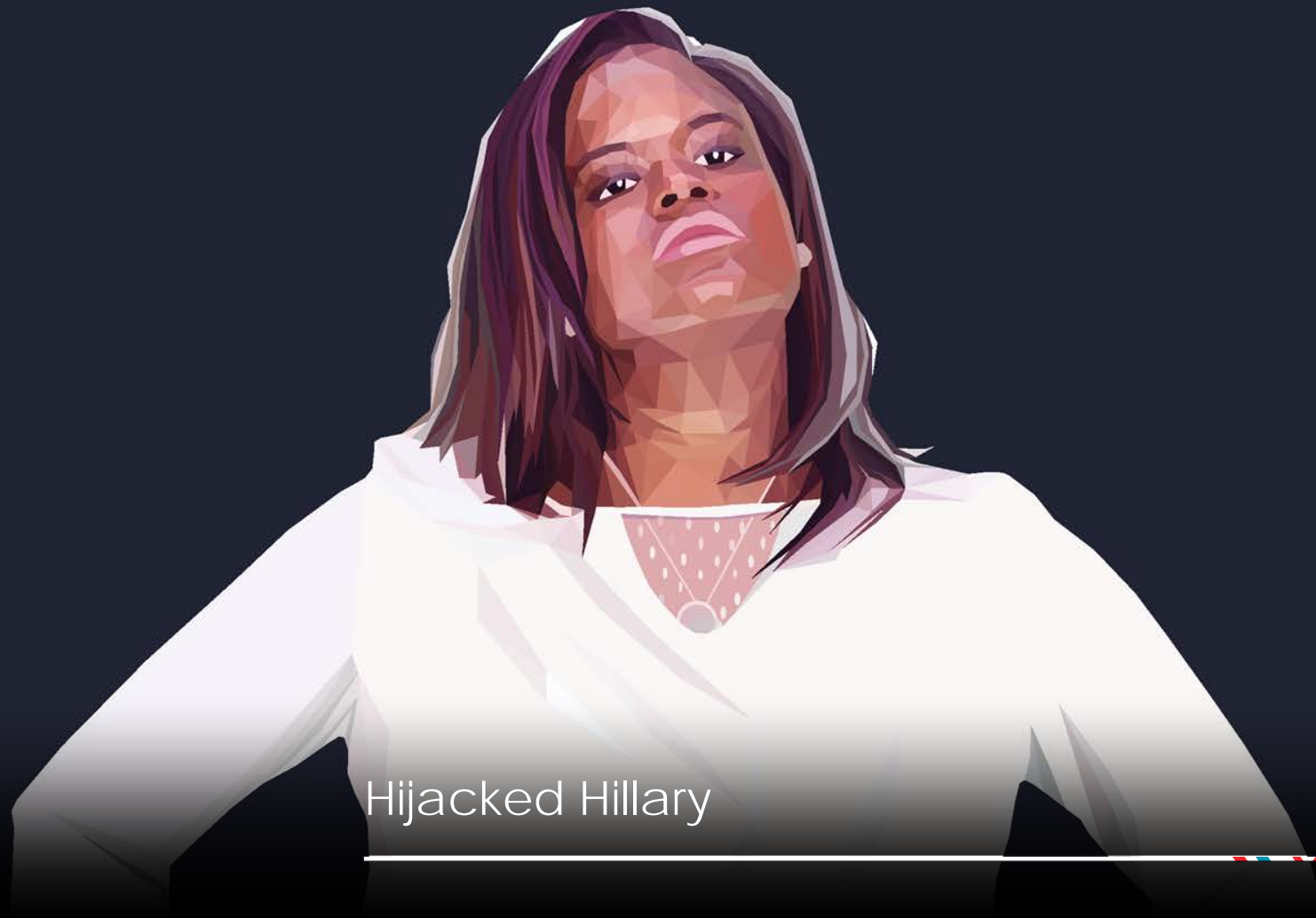
This site uses cookies to offer you a complete experience. [Find out more](#) or [CLOSE](#) ✕ this notification

“

As he was getting near retirement, the system administrator received an offer to sell corporate data, which would have allowed him to purchase the house of his dreams and retire as he always wanted.

”





Hijacked Hillary



Stealing White

How a corporate spy swiped plans for DuPont's billion-dollar color formula





UNIVERSITY OF CALGARY

2500 University Drive NW

Service Sells Access to Fortune 500 Firms

Advertisement

Enterprise-level two-factor authentication now at the push of a button.

LOGIN?

Information panel

Service Stats

Servers available: 16811 (450)
Number of people: 1584 (0)
Online: 15/126/418

Statistics Checker

Completed audits: 305192 running 2/0 in queue

Contact Service

The main support h
main in dedicated
Support (Replaceme
technical issues Em

News Buy a server

To pick up the server with Mask IP (000.000.000): 64.102. Find

ID	Seller (rating)	Country	City	Region	Opera...	Processor
281	lopster (12154)	United States	San Jose	California	Vin2003	Intel(R) Xeon(R) CPU

Note from the seller: Poker - no | Paypal - No | Amazon - No | Daring - No | Admin rights - Yes | Uptime - 7 days, 23:06:08

22 Service Sells Access to Fortune 500 Firms

OCT 12

An increasing number of services offered in the cybercrime underground allow miscreants to purchase access to hacked computers at specific organizations. For just a few dollars, services offer the ability to buy your way inside of Fortune 500 company networks.

The service I examined for this post currently is renting access to nearly 17,000 computers worldwide, although almost



“

“The service I examined for this post currently is renting access to nearly 17,000 computers worldwide”

”

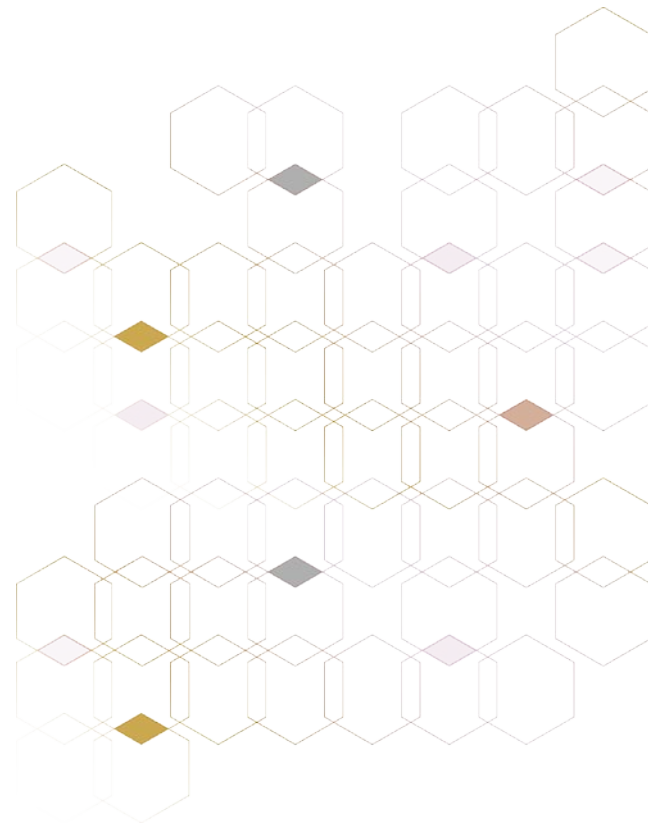


What data is most
vulnerable to insider threats?

“

Data volume is set to grow 800% over the next 5 years and 80% of it will reside as **unstructured data**.

”



— Gartner, 2015

“

The attackers primarily focused on utilizing SMB commands to **map network file shares of OPM users** who had administrator access or were knowledgeable of OPM's PIPS system. The attacker would create a shopping list of the available documents contained on the **network file shares**.

”

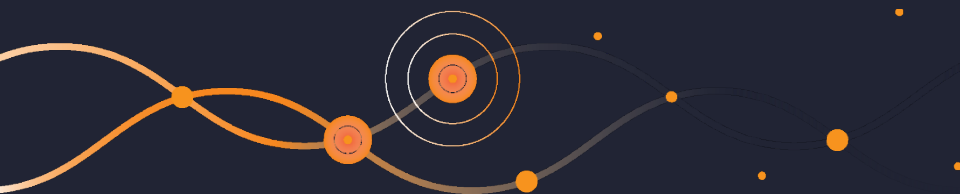
– Jeff Wagner, OPM's Director of Security Operations

LOST CAT

REWARD: \$20,000



CONTACT: 310-299-7905



What can you do?



DETECT

insider threats by analyzing data, account activity, and user behavior.



PREVENT

disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.



SUSTAIN

a secure state by automating authorizations, migrations, & disposition.

DETECT



Map directory services,
permissions, file systems



Discover sensitive
and stale data



Automatically identify
administrators, service
accounts, and executives



Audit all file system
and email activity



Baseline what normal
behavior looks like



Detect suspicious behavior

- Crypto intrusion and other malware infections
- Privilege escalations
- Abnormal access to sensitive data



Prioritize where sensitive
data is overexposed
and at-risk

PREVENT



Lock down sensitive
and stale data



Fix Active Directory and
file system issues



Eliminate global groups



Simplify permissions
structure



Identify Data
Owners outside of IT



Prune unnecessary access



Data Owners perform
entitlement reviews

SUSTAIN



Continuously monitor all user & file system activity



Automatically catch and correct deviations from policy and trusted state



Automate quarantining of sensitive data



Automate archival or disposal of stale data



Automate authorization workflows and entitlement reviews



Automate revocation of access

Summary

- ◆ Ransomware are dumpster divers wanting to collect a quick nickel
- ◆ Its existence, persistence and “success” illustrate how soft our “insides” are
- ◆ Other insider threats are more dangerous
- ◆ Files and emails are frequent targets
- ◆ The approach: Detect, Prevent, Sustain

Free Data Risk Assessment – <http://bit.ly/threatcheck>





Thank You

Ben Hui

bhui@varonis.com

www.varonis.com

