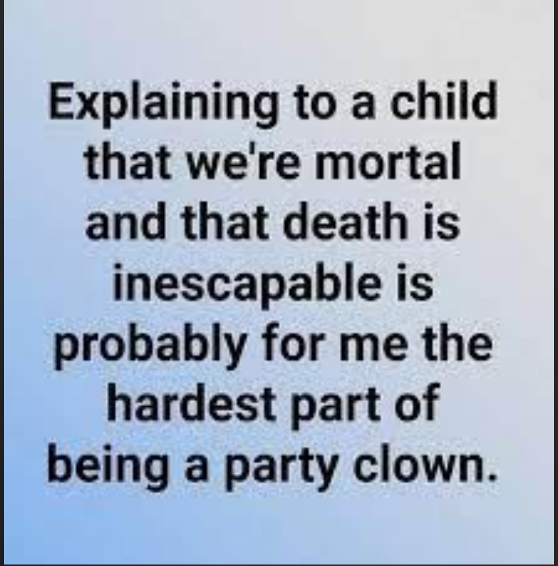
I Hate Ransomware.

And, you should too!

John Strand

What We Are Covering

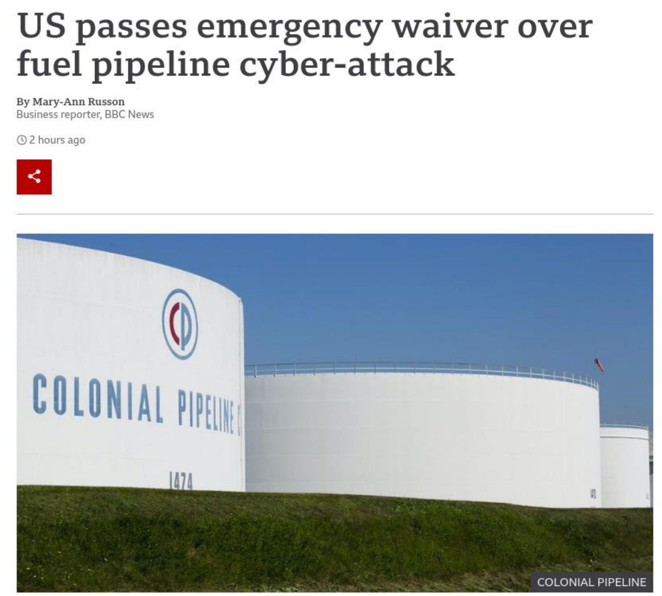
- Recent attacks
- Deception… Again.
- Beacons…. Again.
- Third type of ransomware
- Raccine
- Windows Settings



Explaining to a child that we're mortal and that death is inescapable is probably for me the hardest part of being a party clown.

No point of this.. I just miss Jack Handy on SNL.

Recent Attacks

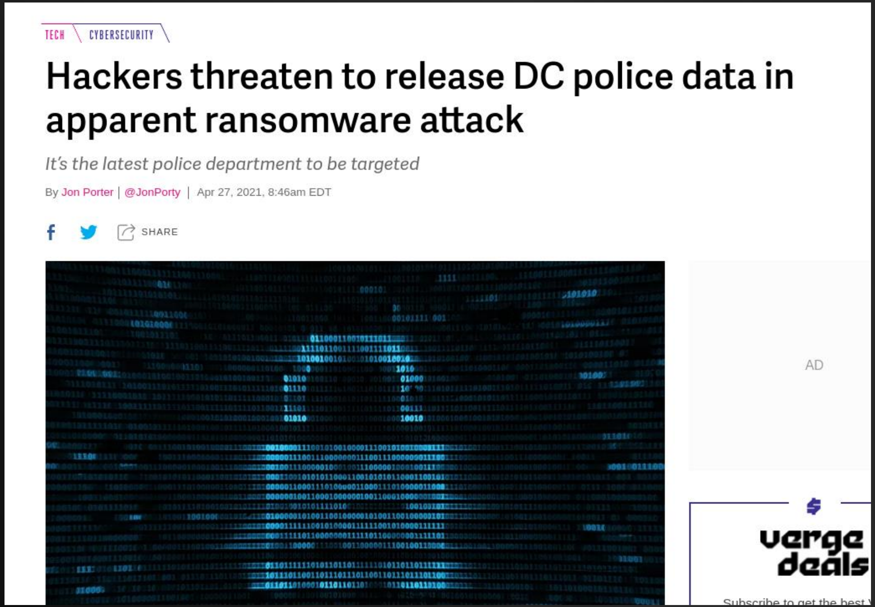


US passes emergency waiver over fuel pipeline cyber-attack

By Mary-Ann Russon
Business reporter, BBC News

2 hours ago

COLONIAL PIPELINE



TECH \ CYBERSECURITY \

Hackers threaten to release DC police data in apparent ransomware attack

It's the latest police department to be targeted

By Jon Porter | @JonPorty | Apr 27, 2021, 8:46am EDT

SHARE

AD

verge deals

Subscribe to get the best

Cookies....

So... Deception.

- Let's hash this out
- Deception is no longer a "nice to have"
- Deception is no longer a "neat thing"
- It is core
- It is essential
- Fight me.

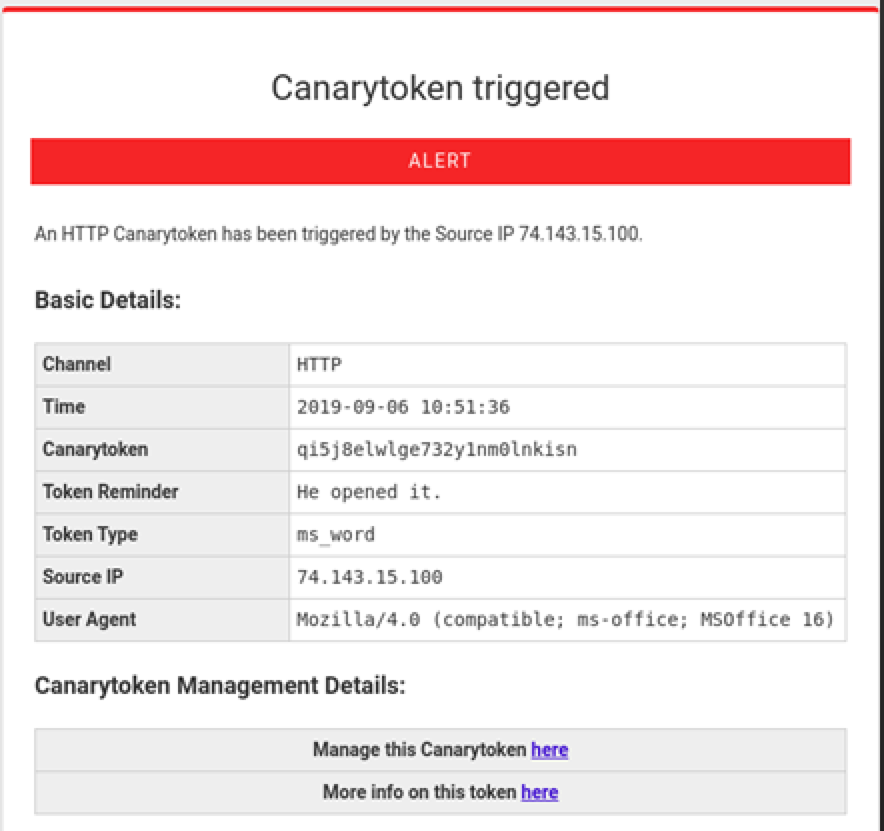
"Let's Dance!"

Word Docs!!!

- Word docs are great because we can put them on:
  - Shares
  - Compromised systems
  - Websites (Robots.txt)
  - Email to spammers!
- When an attacker pivots... Give them something

Would you run it from a share?
Would you run it from a chair?
Would you run it for TOR?
If the FBI comes should you open the door?

Yes! CanaryTokens!



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 74.143.15.100.

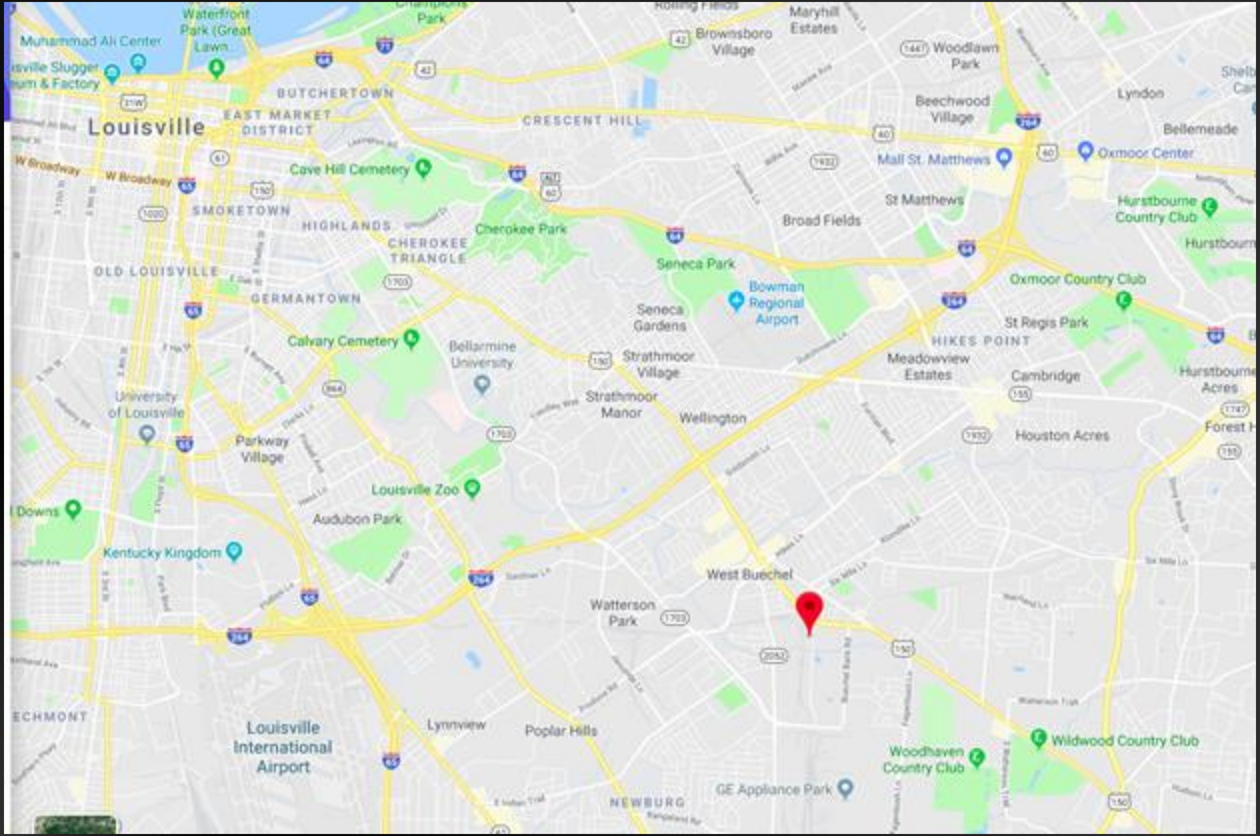
Basic Details:

Channel	HTTP
Time	2019-09-06 10:51:36
Canarytoken	qi5j8elwlge732y1nm0lnkisn
Token Reminder	He opened it.
Token Type	ms_word
Source IP	74.143.15.100
User Agent	Mozilla/4.0 (compatible; ms-office; MSOffice 16)

Canarytoken Management Details:

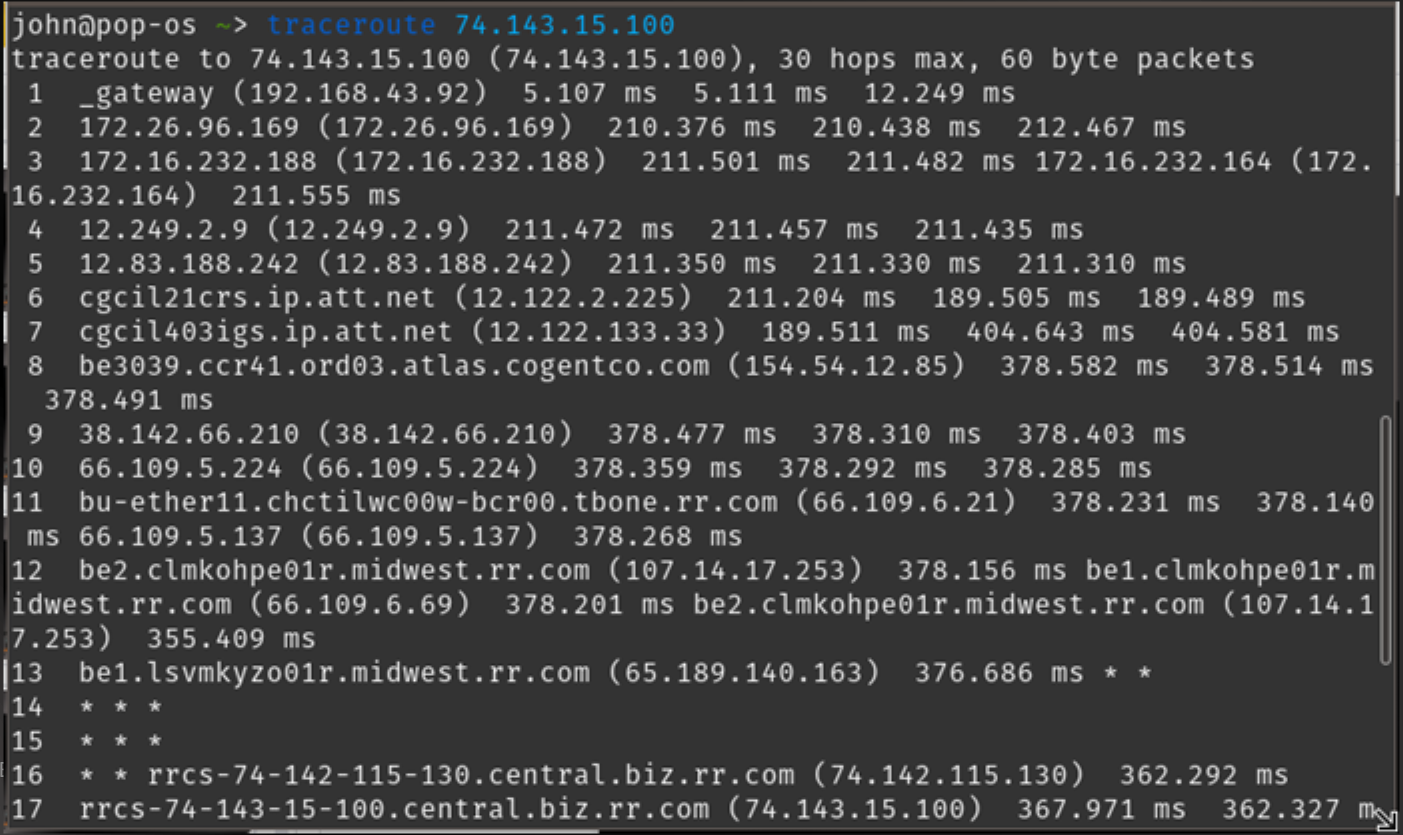
Manage this Canarytoken here
More info on this token here

Not bad..



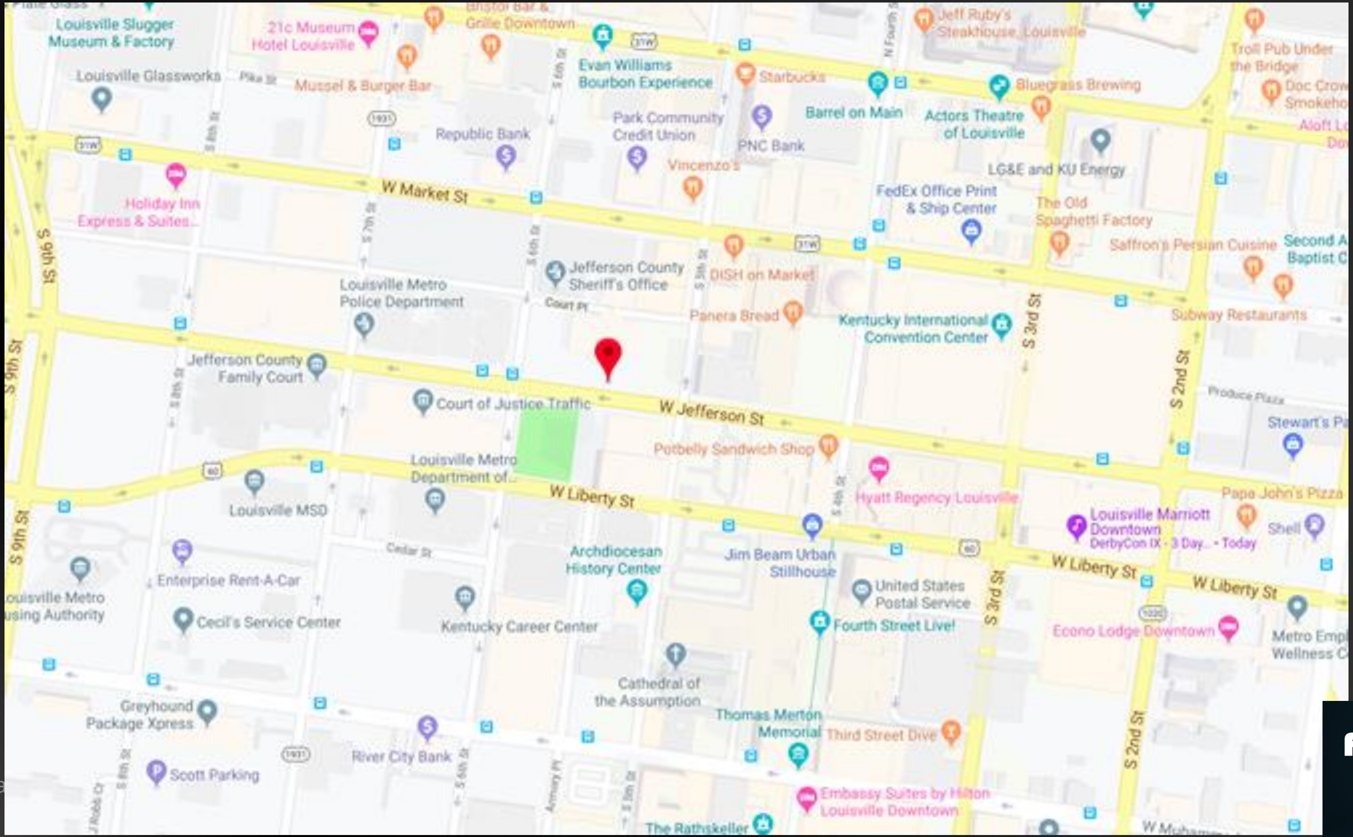
ACTIVE SOC
Powered By: BLACK HILLS | Information Security

But we can do better...



```
john@pop-os ~> traceroute 74.143.15.100
traceroute to 74.143.15.100 (74.143.15.100), 30 hops max, 60 byte packets
 1  _gateway (192.168.43.92)  5.107 ms  5.111 ms  12.249 ms
 2  172.26.96.169 (172.26.96.169)  210.376 ms  210.438 ms  212.467 ms
 3  172.16.232.188 (172.16.232.188)  211.501 ms  211.482 ms 172.16.232.164 (172.
16.232.164)  211.555 ms
 4  12.249.2.9 (12.249.2.9)  211.472 ms  211.457 ms  211.435 ms
 5  12.83.188.242 (12.83.188.242)  211.350 ms  211.330 ms  211.310 ms
 6  cgcil21crs.ip.att.net (12.122.2.225)  211.204 ms  189.505 ms  189.489 ms
 7  cgcil403igs.ip.att.net (12.122.133.33)  189.511 ms  404.643 ms  404.581 ms
 8  be3039.ccr41.ord03.atlas.cogentco.com (154.54.12.85)  378.582 ms  378.514 ms
  378.491 ms
 9  38.142.66.210 (38.142.66.210)  378.477 ms  378.310 ms  378.403 ms
10  66.109.5.224 (66.109.5.224)  378.359 ms  378.292 ms  378.285 ms
11  bu-ether11.chctilwc00w-bcr00.tbone.rr.com (66.109.6.21)  378.231 ms  378.140
 ms 66.109.5.137 (66.109.5.137)  378.268 ms
12  be2.clmkohpe01r.midwest.rr.com (107.14.17.253)  378.156 ms be1.clmkohpe01r.m
idwest.rr.com (66.109.6.69)  378.201 ms be2.clmkohpe01r.midwest.rr.com (107.14.1
7.253)  355.409 ms
13  be1.lsvmkyzo01r.midwest.rr.com (65.189.140.163)  376.686 ms * *
14  * * *
15  * * *
16  * * rrcs-74-142-115-130.central.biz.rr.com (74.142.115.130)  362.292 ms
17  rrcs-74-143-15-100.central.biz.rr.com (74.143.15.100)  367.971 ms  362.327 m
```

Enhance


Louisville Slugger Museum & Factory
21c Museum Hotel Louisville
Bristol Bar & Grille Downtown
Evan Williams Bourbon Experience
Jeff Ruby's Steakhouse, Louisville
Troll Pub Under the Bridge
Louisville Glassworks
Pike St
Mussel & Burger Bar
Starbucks
Barrel on Main
Bluegrass Brewing
Doc Crow's Smokehouse
Aloft Louisville Downtown
Park Community Credit Union
PNC Bank
Actors Theatre of Louisville
Republic Bank
Vincenzo's
LG&E and KU Energy
Holiday Inn Express & Suites...
W Market St
FedEx Office Print & Ship Center
The Old Spaghetti Factory
Saffron's Persian Cuisine
Second Avenue Baptist Church
S 9th St
S 7th St
S 6th St
S 5th St
N Fourth St
Jefferson County Sheriff's Office
DISH on Market
Louisville Metro Police Department
Court Pl
Panera Bread
Kentucky International Convention Center
S 3rd St
Subway Restaurants
S 2nd St
S 9th St
S 8th St
Jefferson County Family Court
Court of Justice Traffic
W Jefferson St
Produce Plaza
Stewart's Pa
Potbelly Sandwich Shop
Louisville Metro Department of...
Hyatt Regency Louisville
Papa John's Pizza
W Liberty St
Louisville MSD
Louisville Marriott Downtown
DerbyCon IX - 3 Day... • Today
Shell
Cedar St
Archdiocesan History Center
Jim Beam Urban Stillhouse
W Liberty St
W Liberty St
S 9th St
Louisville Metro Housing Authority
Enterprise Rent-A-Car
United States Postal Service
S 3rd St
Cecil's Service Center
Kentucky Career Center
Fourth Street Live!
Econo Lodge Downtown
Metro Employee Wellness C
Cathedral of the Assumption
Greyhound Package Xpress
Thomas Merton Memorial
Third Street Dive
S 2nd St
River City Bank
Scott Parking
Embassy Suites by Hilton Louisville Downtown
The Rathskeller
W Muhammad
31W
60
150

BLACK HILLS Information Security
CELEBRATING 10 YEARS
• 2008-2018 •

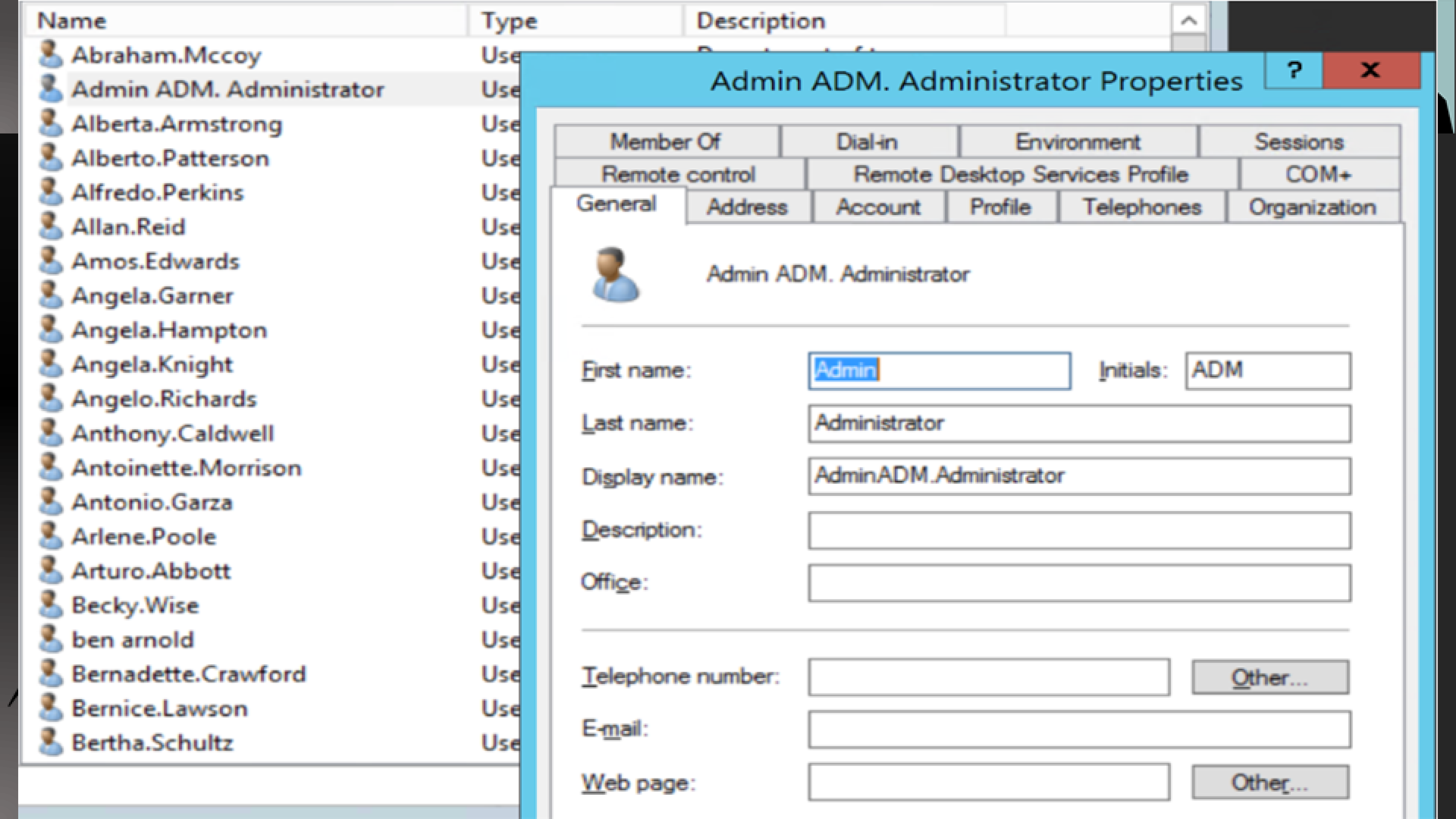
© Bla

ACTIVE SOC
Powered By: BLACK HILLS | Information Security

Applicability

- Attacker pops a box
- They try to pivot by finding docs with passwords in them
- They open a honeydoc
- You get an alert
- You shut them down
- You don't end up in the news
- Everyone likes that...

"Let's Dance!"



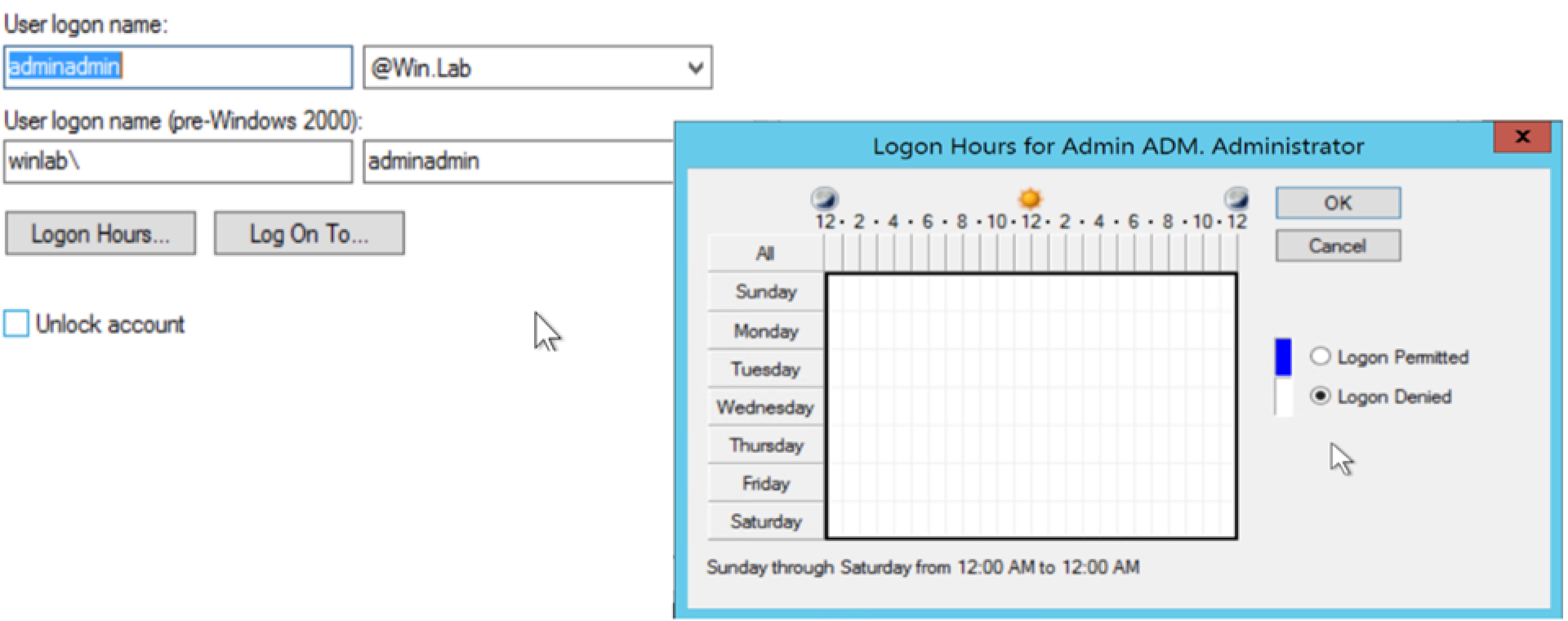
Name	Type	Description
Abraham.Mccoy	Use	
Admin ADM. Administrator	Use	
Alberta.Armstrong	Use	
Alberto.Patterson	Use	
Alfredo.Perkins	Use	
Allan.Reid	Use	
Amos.Edwards	Use	
Angela.Garner	Use	
Angela.Hampton	Use	
Angela.Knight	Use	
Angelo.Richards	Use	
Anthony.Caldwell	Use	
Antoinette.Morrison	Use	
Antonio.Garza	Use	
Arlene.Poole	Use	
Arturo.Abbott	Use	
Becky.Wise	Use	
ben arnold	Use	
Bernadette.Crawford	Use	
Bernice.Lawson	Use	
Bertha.Schultz	Use	

Admin ADM. Administrator Properties

Admin ADM. Administrator

First name: Admin
Initials: ADM
Last name: Administrator
Display name: AdminADM.Administrator
Description:
Office:
Telephone number:
E-mail:
Web page:

Important!



User logon name: adminadmin @Win.Lab

User logon name (pre-Windows 2000): winlab\ adminadmin

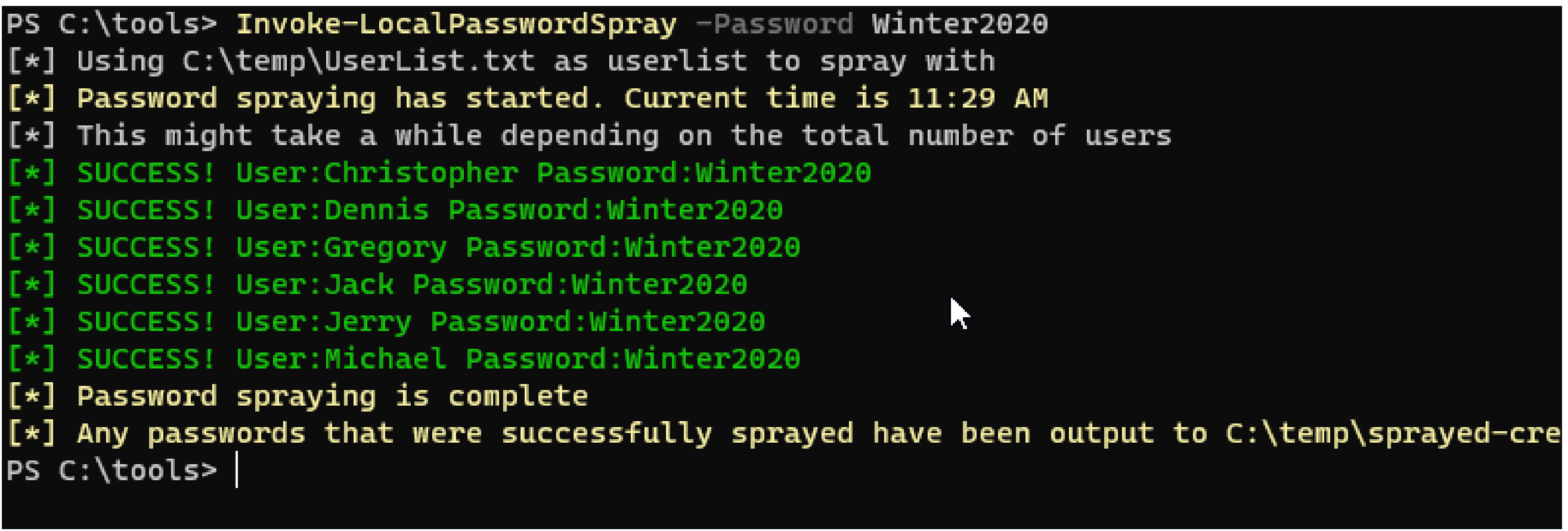
□ Unlock account

Logon Hours for Admin ADM. Administrator

○ Logon Permitted

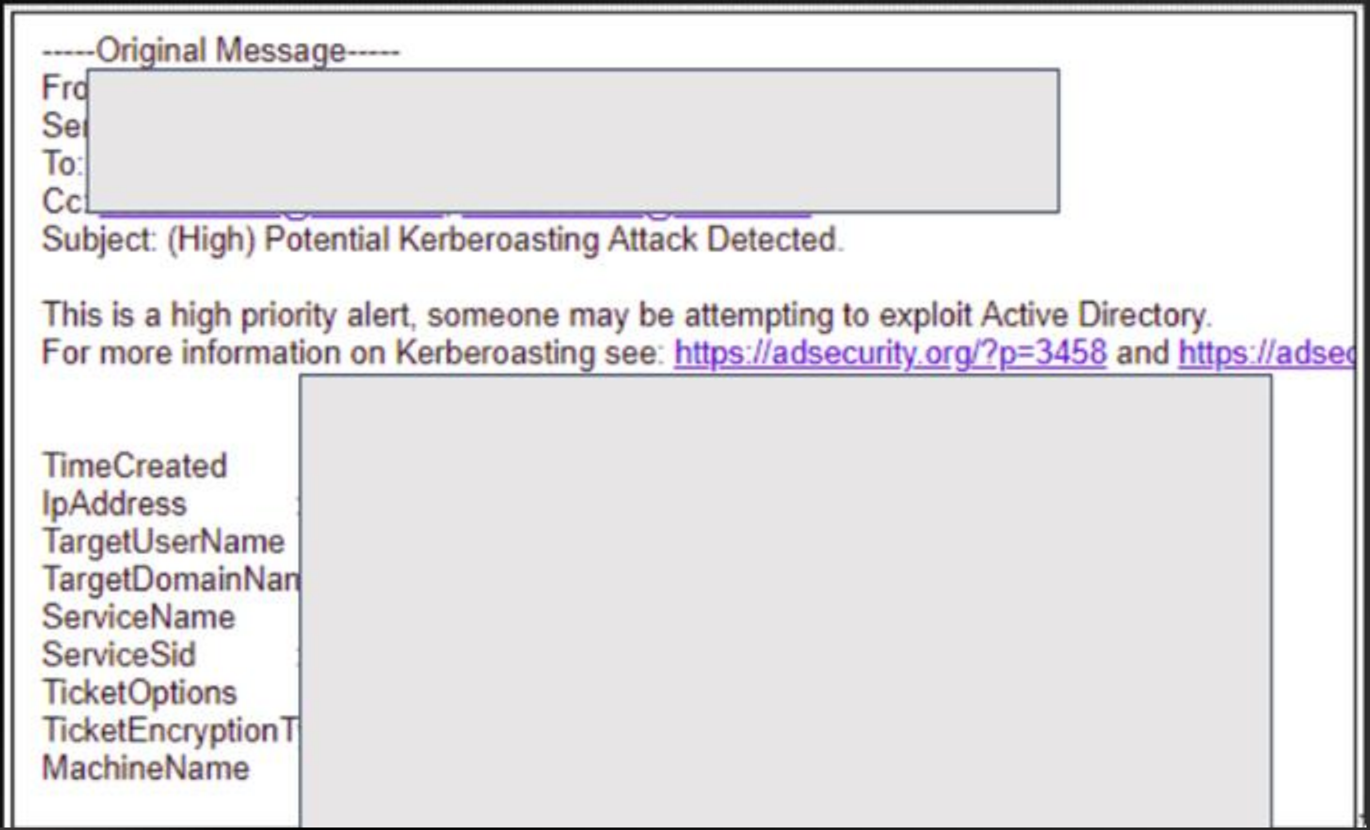
● Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM



```
PS C:\tools> Invoke-LocalPasswordSpray -Password Winter2020
[*] Using C:\temp\UserList.txt as userlist to spray with
[*] Password spraying has started. Current time is 11:29 AM
[*] This might take a while depending on the total number of users
[*] SUCCESS! User:Christopher Password:Winter2020
[*] SUCCESS! User:Dennis Password:Winter2020
[*] SUCCESS! User:Gregory Password:Winter2020
[*] SUCCESS! User:Jack Password:Winter2020
[*] SUCCESS! User:Jerry Password:Winter2020
[*] SUCCESS! User:Michael Password:Winter2020
[*] Password spraying is complete
[*] Any passwords that were successfully sprayed have been output to C:\temp\sprayed-cre
PS C:\tools>
```

Kerberoasting



-----Original Message-----
Fro
Se
To:
Cc: [redacted]
Subject: (High) Potential Kerberoasting Attack Detected.

This is a high priority alert, someone may be attempting to exploit Active Directory.
For more information on Kerberoasting see: https://adsecurity.org/?p=3458 and https://adsec

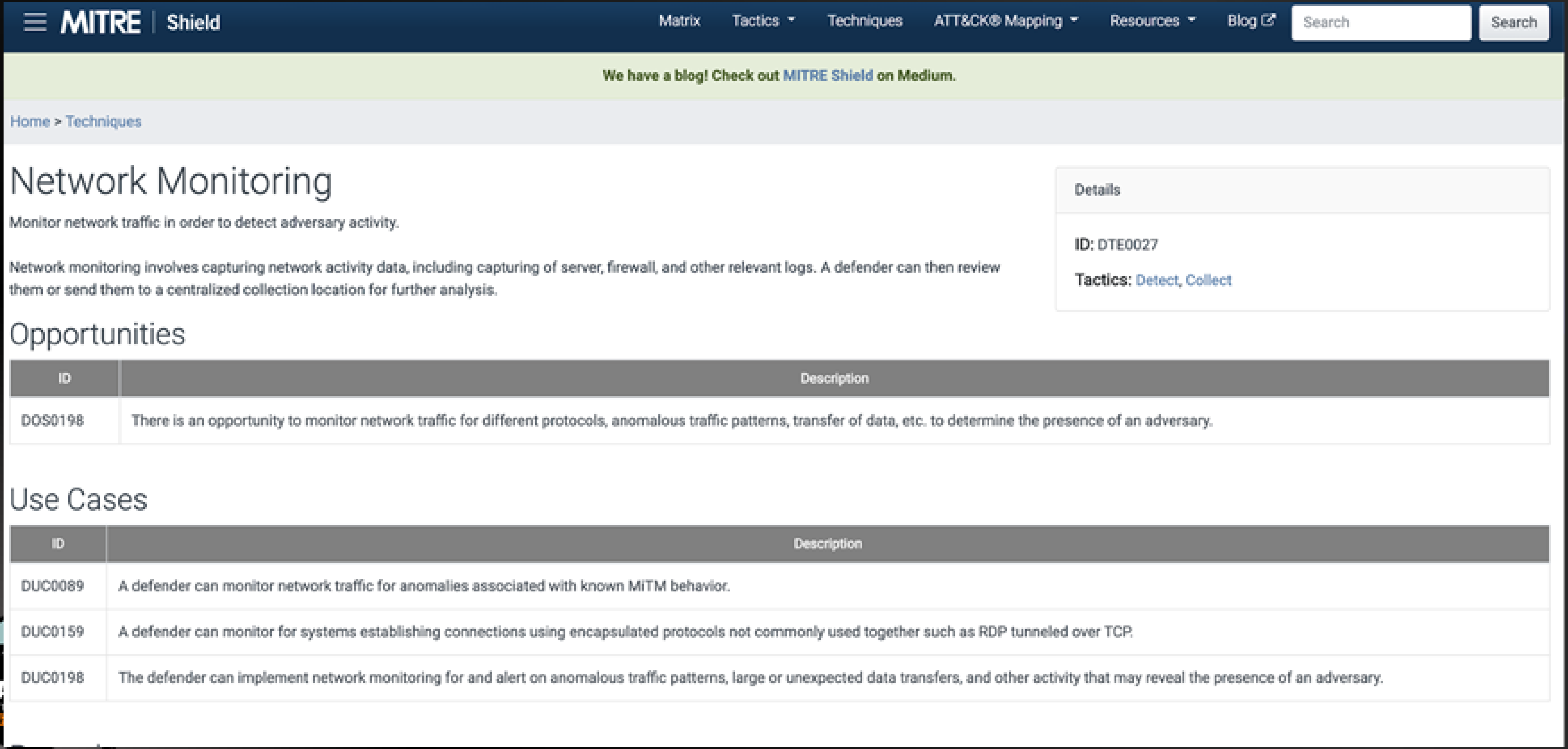
TimeCreated
IpAddress
TargetUserName
TargetDomainNam
ServiceName
ServiceSid
TicketOptions
TicketEncryptionT
MachineName
[redacted]

Applicability

- Attacker pops a box
- They try to pivot by password spraying or Kerberoasting
- You detect it immediately
- You shut them down
- Your CEO does not throw you under the bus before congress
- It was a good day.

"Let's Dance!"

Network Analysis



We have a blog! Check out MITRE Shield on Medium.

Home > Techniques

Network Monitoring

Monitor network traffic in order to detect adversary activity.

Network monitoring involves capturing network activity data, including capturing of server, firewall, and other relevant logs. A defender can then review them or send them to a centralized collection location for further analysis.

Details

ID: DTE0027

Tactics: Detect, Collect

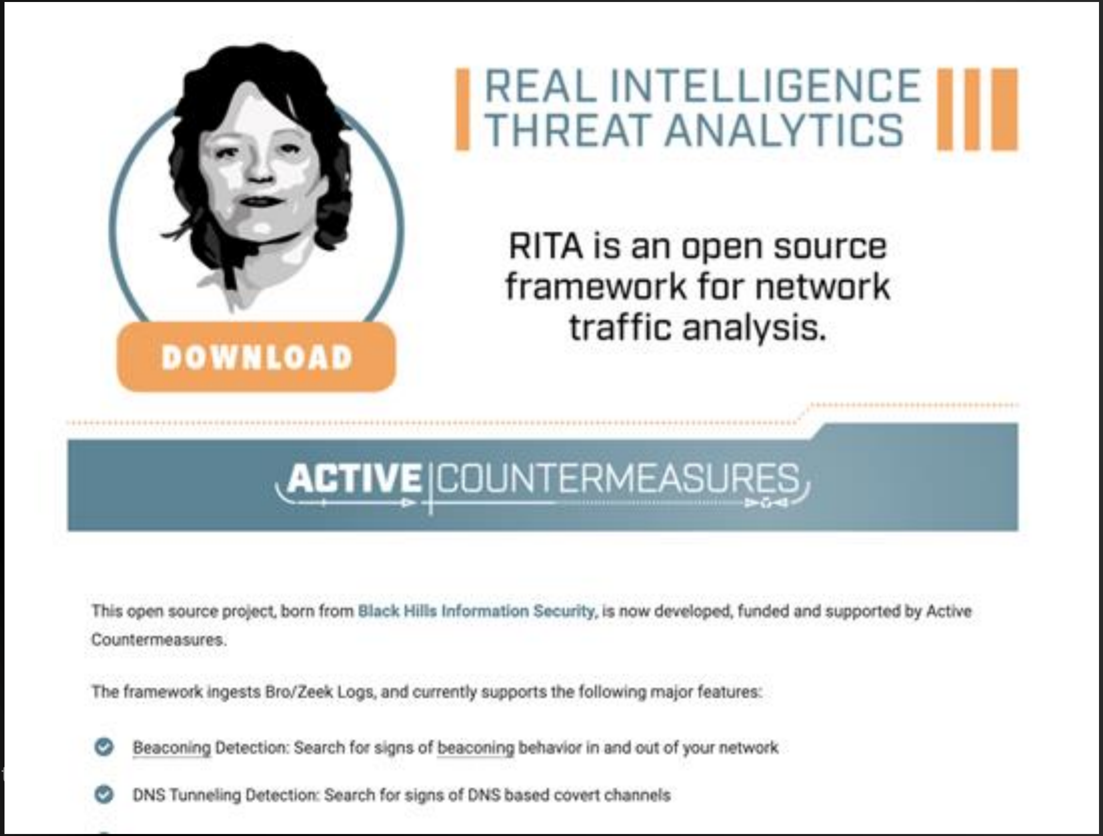
Opportunities

ID	Description
DOS0198	There is an opportunity to monitor network traffic for different protocols, anomalous traffic patterns, transfer of data, etc. to determine the presence of an adversary.

Use Cases

ID	Description
DUC0089	A defender can monitor network traffic for anomalies associated with known MiTM behavior.
DUC0159	A defender can monitor for systems establishing connections using encapsulated protocols not commonly used together such as RDP tunneled over TCP.
DUC0198	The defender can implement network monitoring for and alert on anomalous traffic patterns, large or unexpected data transfers, and other activity that may reveal the presence of an adversary.

https://www.activecountermeasures.com/free-tools/rita/



REAL INTELLIGENCE THREAT ANALYTICS

RITA is an open source framework for network traffic analysis.

This open source project, born from Black Hills Information Security, is now developed, funded and supported by Active Countermeasures.

The framework ingests Bro/Zeek Logs, and currently supports the following major features:

- ✓ Beaconing Detection: Search for signs of beaconing behavior in and out of your network
- ✓ DNS Tunneling Detection: Search for signs of DNS based covert channels

And now…
A very special note from Chris Brenton.

Hey dude,

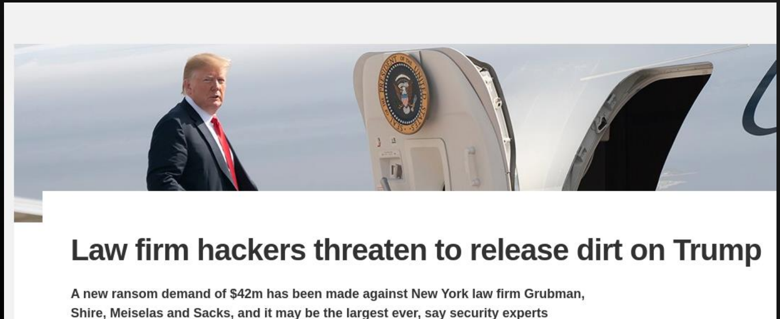
One data point you may want to convey tomorrow is that ransomware is skewing the dwell time numbers between initial compromise and detection. The sites that are reporting that we are getting better than 6 months at detection are including ransomware in their calculations. IMHO, that shouldn't count as it's the attacker revealing themselves, not an actual "detection". When you separate ransomware and APT, we're still at a 6-month dwell time for APT.

HTH,

C

GOOD NEWS EVERYONE
THERE IS NO GOOD NEWS
memegenerator.net

Ransomware of the third kind

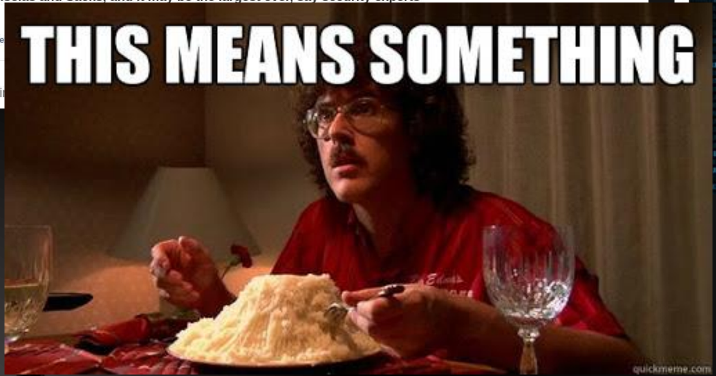


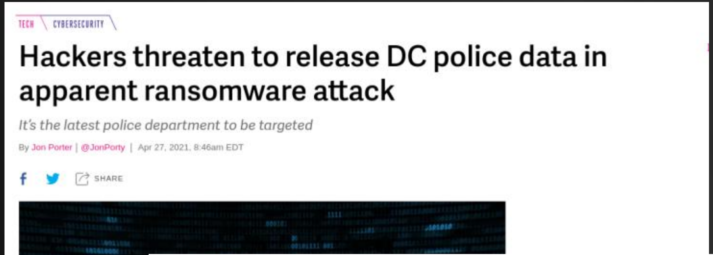
Law firm hackers threaten to release dirt on Trump

A new ransom demand of $42m has been made against New York law firm Grubman, Shire, Meiselas and Sacks, and it may be the largest ever, say security experts

By Ale

The cyber crimi





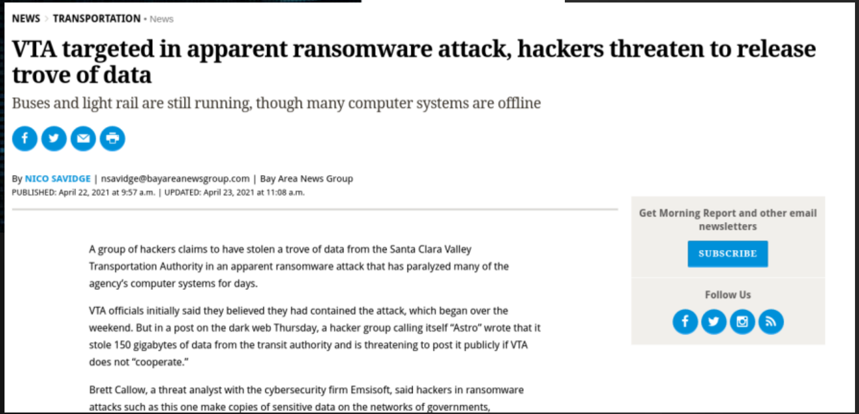
TECH \ CYBERSECURITY

Hackers threaten to release DC police data in apparent ransomware attack

It's the latest police department to be targeted

By Jon Porter | @JonPorty | Apr 27, 2021, 8:46am EDT

SHARE



NEWS › TRANSPORTATION • News

VTA targeted in apparent ransomware attack, hackers threaten to release trove of data

Buses and light rail are still running, though many computer systems are offline

By NICO SAVIDGE | nsavidge@bayareanewsgroup.com | Bay Area News Group
PUBLISHED: April 22, 2021 at 9:57 a.m. | UPDATED: April 23, 2021 at 11:08 a.m.

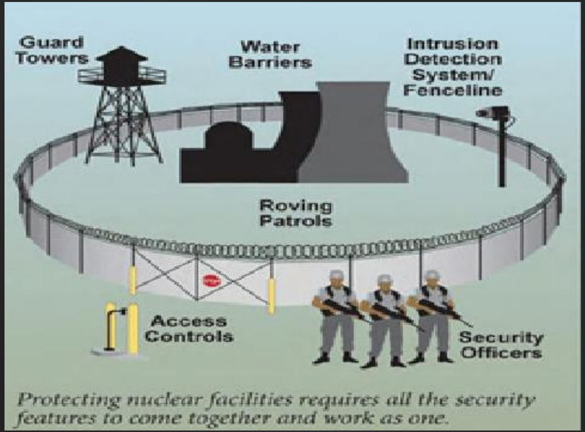
A group of hackers claims to have stolen a trove of data from the Santa Clara Valley Transportation Authority in an apparent ransomware attack that has paralyzed many of the agency's computer systems for days.

VTA officials initially said they believed they had contained the attack, which began over the weekend. But in a post on the dark web Thursday, a hacker group calling itself "Astro" wrote that it stole 150 gigabytes of data from the transit authority and is threatening to post it publicly if VTA does not "cooperate."

Brett Callow, a threat analyst with the cybersecurity firm Emsisoft, said hackers in ransomware attacks such as this one make copies of sensitive data on the networks of governments,

ACTIVE COUNTERMEASURES

A quick note..



Protecting nuclear facilities requires all the security features to come together and work as one.

The power grid is a special security case. We need segmentation and to keep legacy systems running for years. If we don't do this correctly... People can die.

Another note..

Medical is a special security case. We need segmentation and to keep legacy systems running for years. If we don't do this correctly... People can die.

ACTIVE COUNTERMEASURES

Another note..

Financial is a special security case. We need segmentation and to keep legacy systems running for years. If we don't do this correctly... People can die.

ACTIVE COUNTERMEASURES

Another note..

```
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE
CARDS AGAINST HUMANITY
GLOBAL THERMONUCLEAR WAR
```

Defense is a special security case. We need segmentation and to keep legacy systems running for years. If we don't do this correctly... People can die.

ACTIVE COUNTERMEASURES

They are all correct..

- This needs to stop
- Belief that a market vertical is "unique" helps create excuses for not doing the "right" thing
- I know I am preaching to the choir
- One powerful question... "When?"

ACTIVE COUNTERMEASURES

If we don't get it.. It's OK.

These folks will teach us the error of our ways.

Anndd....

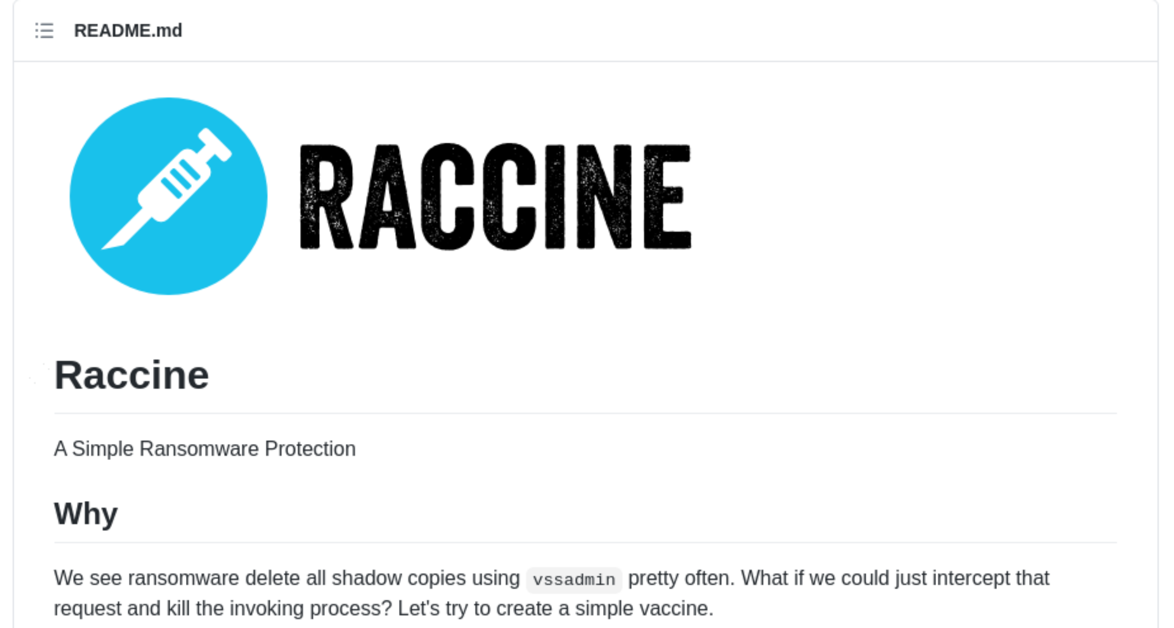
These folks will "fix" the error of our ways....

© Henning Schacht/Getty Images
© Geoff Pugh/AFP/Getty Images
© Carlos Barria/AFP/Getty Images

Let's Think

"Think about how ransomware works Mark! THINK!"

Raccine



README.md

RACCINE

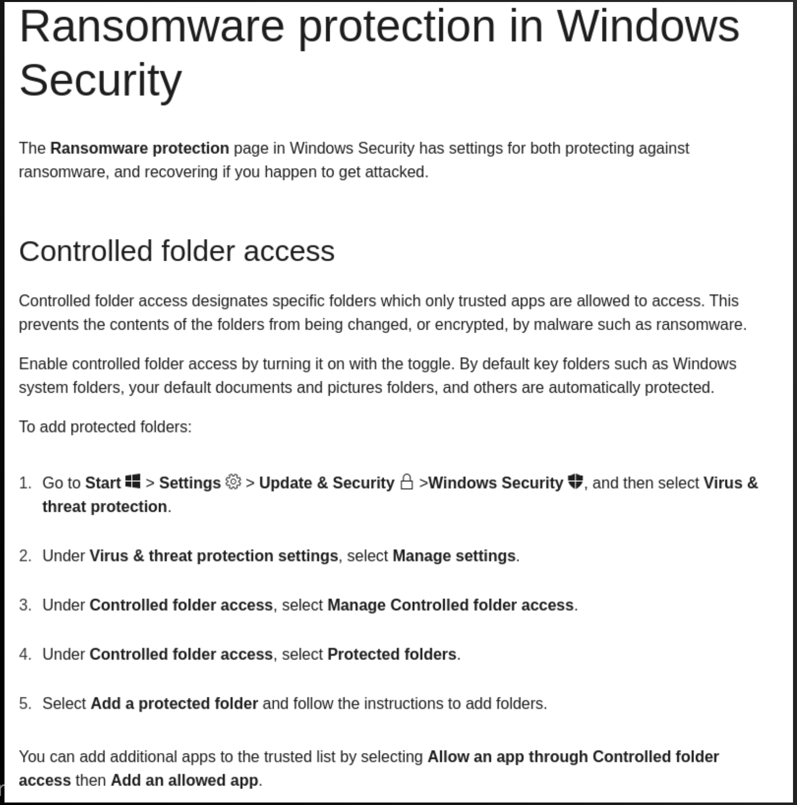
Raccine

A Simple Ransomware Protection

Why

We see ransomware delete all shadow copies using `vssadmin` pretty often. What if we could just intercept that request and kill the invoking process? Let's try to create a simple vaccine.

File and Folder Protection



Ransomware protection in Windows Security

The **Ransomware protection** page in Windows Security has settings for both protecting against ransomware, and recovering if you happen to get attacked.

Controlled folder access

Controlled folder access designates specific folders which only trusted apps are allowed to access. This prevents the contents of the folders from being changed, or encrypted, by malware such as ransomware.

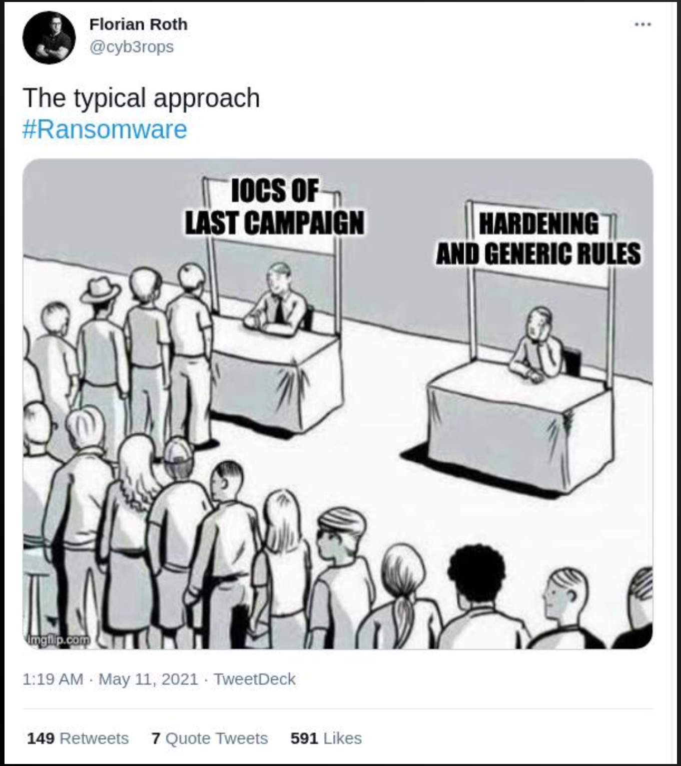
Enable controlled folder access by turning it on with the toggle. By default key folders such as Windows system folders, your default documents and pictures folders, and others are automatically protected.

To add protected folders:

1. Go to **Start** ⊞ > **Settings** ⚙ > **Update & Security** 🔒 >**Windows Security** 🛡, and then select **Virus & threat protection**.
2. Under **Virus & threat protection settings**, select **Manage settings**.
3. Under **Controlled folder access**, select **Manage Controlled folder access**.
4. Under **Controlled folder access**, select **Protected folders**.
5. Select **Add a protected folder** and follow the instructions to add folders.

You can add additional apps to the trusted list by selecting **Allow an app through Controlled folder access** then **Add an allowed app**.

One more thing...



Florian Roth
@cyb3rops

The typical approach
#Ransomware

1:19 AM · May 11, 2021 · TweetDeck

149 Retweets 7 Quote Tweets 591 Likes

Thanks!

- Thanks for hanging out
- John Strand
- @strandjs

Here is a bunny...
Hope it makes up for the Government slide earlier...
Sorry.

Questions?

BLACK HILLS
Information Security
• 2008 •

ACTIVE SOC
Powered By: BLACK HILLS | Information Security

ACTIVE | COUNTERMEASURES