RICHEY MAY Technology Solutions

Discover / Develop / Deliver

Security Implication of ‘Work from Home’: The Year of Breaches

RICHEY MAY
TECHNOLOGY SOLUTIONS

About Me:

in linkedin.com/in/mwylie

twitter.com/TheMikeWylie

Michael Wylie, TPN, MBA, CISSP

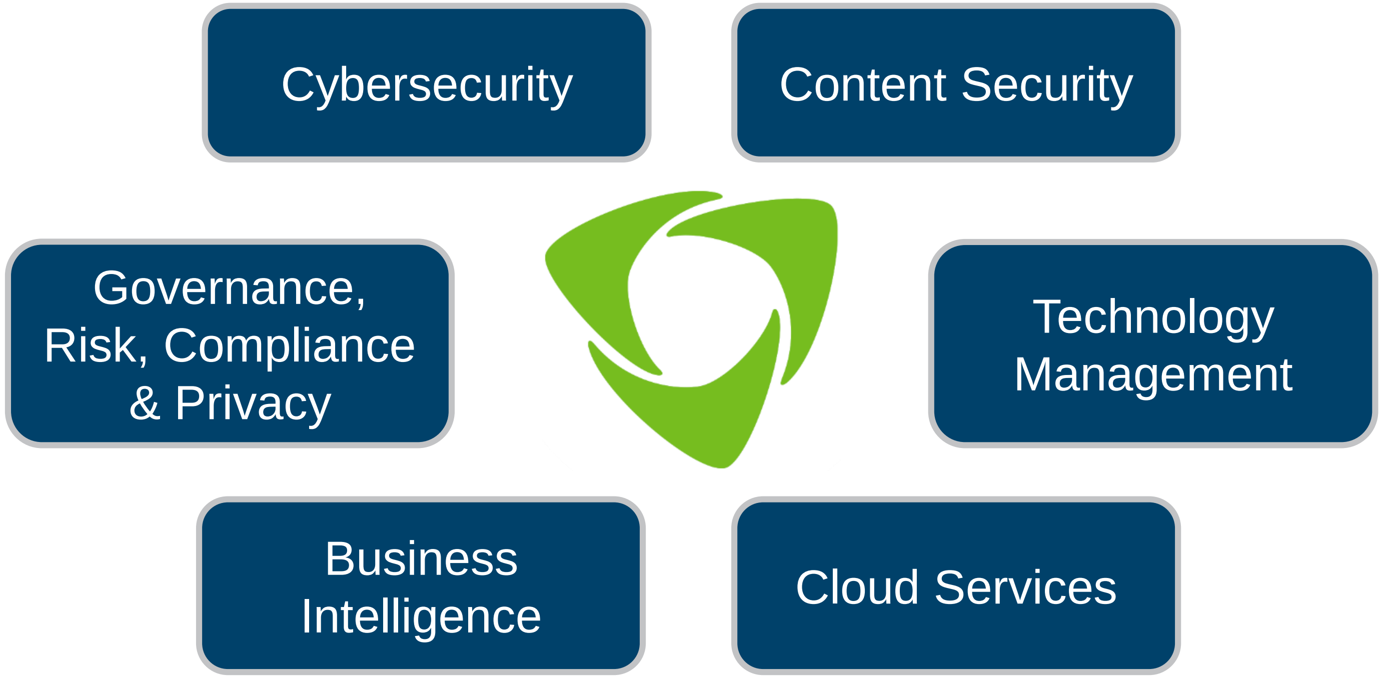
Director, Cybersecurity Services

RICHEY MAY TECHNOLOGY SOLUTIONS

Additional	Certifications
GPEN	CCNA R&S
GMON	CCNA CyberOps
Pentest+	Pentest+
Project+	CHPA
Security+	Splunk User
CEH & CEI	SumoLogic Security

About Richey May Technology Solutions

- Cloud Workflow Integration
- TPN Assessments & Readiness
- Vulnerability Scanning & Penetration Testing
- Content Protection Workflow Design



Cybersecurity

Content Security

Governance, Risk, Compliance & Privacy

Technology Management

Business Intelligence

Cloud Services

RICHEY MAY
TECHNOLOGY SOLUTIONS

What’s the industry’s biggest security concerns?

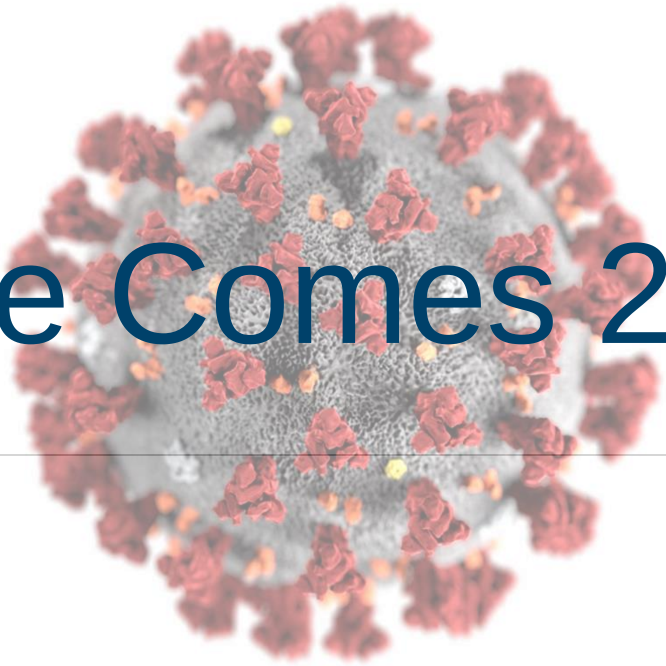
- Piracy
- Leaks
- Spoilers
- Ransomware

How We Protect The Creative Process

- Security guards
- ID badges
- Door access control
- Wired air gapped networks
- Perimeter firewalls
- CCTV
- IDS/IPS
- Secure file transfer

RICHEY MAY
TECHNOLOGY SOLUTIONS

Here Comes 2020



How We Protect The Creative

- Security guards
- ID badges
- Door access control
- Wired air gapped networks
- Perimeter firewall
- CCTV
- IDS/IPS

2020’s Greatest Threat

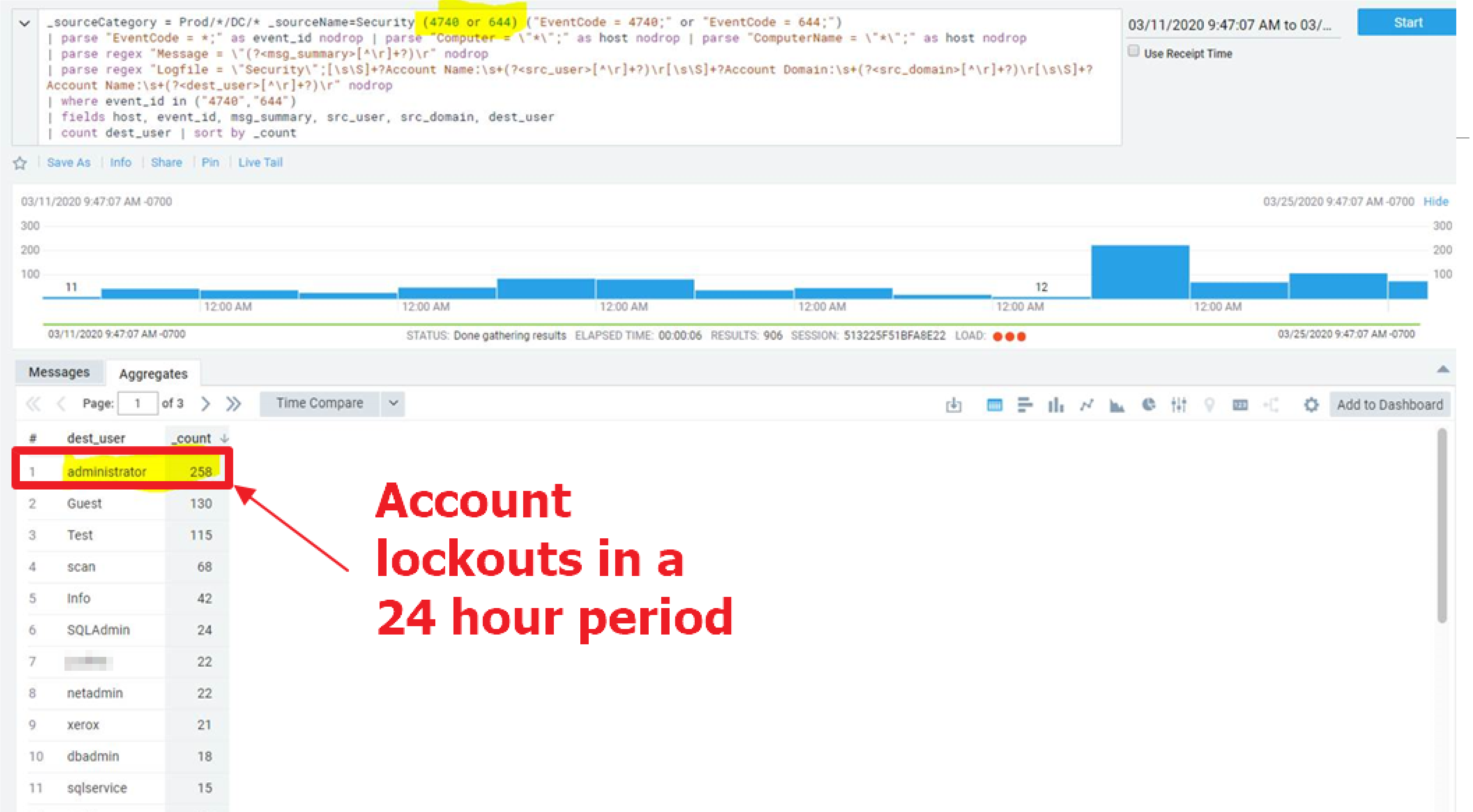
Work From Home

2020 Highlights

- Businesses needed to activate their BCP overnight
- Industries like M&E implemented new remote workflows
- Computers moved from secure facilities to employee's dinning room tables
- NFL opted for a remote draft
- Thousands of COVID-19 domains registered daily
- Mass phishing campaigns reek havoc

2020 Brings New Risk

- WFH with roommates and kids
- Insecure WiFi networks
- No network firewalls
- No IDS/IPS
- No central logging
- VPN and remote desktop usage at an all-time high
- Sensitive conversations and screen sharing over Zoom



```
_sourceCategory = Prod/*/DC/* _sourceName=Security (4740 or 644) ("EventCode = 4740;" or "EventCode = 644;")
| parse "EventCode = *;" as event_id nodrop | parse "Computer = \"*\";" as host nodrop | parse "ComputerName = \"*\";" as host nodrop
| parse regex "Message = \"(?<msg_summary>[^\r]+?)\r" nodrop
| parse regex "Logfile = \"Security\";[\s\S]+?Account Name:\s+(?<src_user>[^\r]+?)\r[\s\S]+?Account Domain:\s+(?<src_domain>[^\r]+?)\r[\s\S]+?
Account Name:\s+(?<dest_user>[^\r]+?)\r" nodrop
| where event_id in ("4740","644")
| fields host, event_id, msg_summary, src_user, src_domain, dest_user
| count dest_user | sort by _count
```

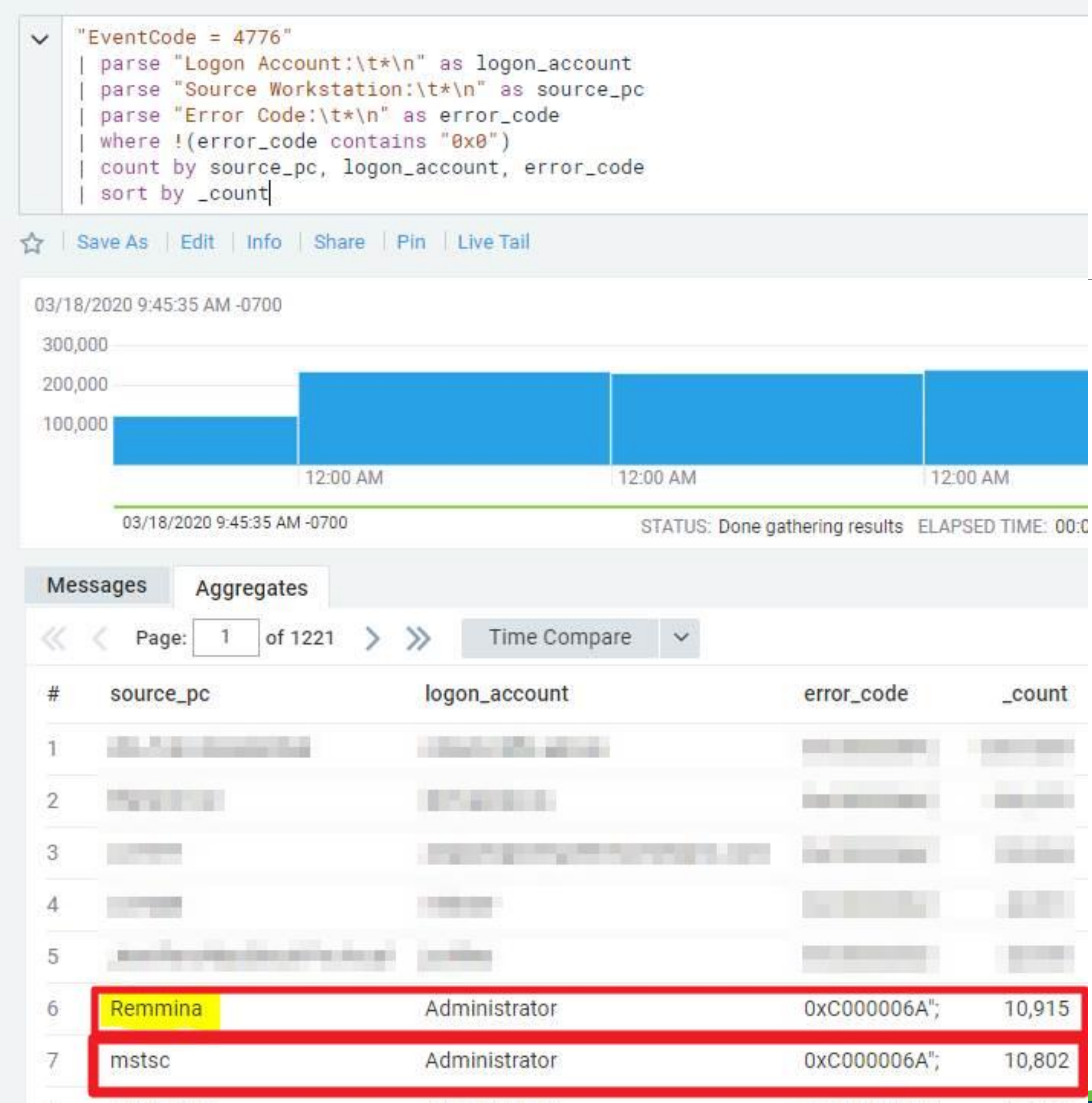
03/11/2020 9:47:07 AM to 03/...

☐ Use Receipt Time

STATUS: Done gathering results ELAPSED TIME: 00:00:06 RESULTS: 906 SESSION: 513225F51BFA8E22 LOAD: ●●●

#	dest_user	_count
1	administrator	258
2	Guest	130
3	Test	115
4	scan	68
5	Info	42
6	SQLAdmin	24
7	[redacted]	22
8	netadmin	22
9	xerox	21
10	dbadmin	18
11	sqlservice	15

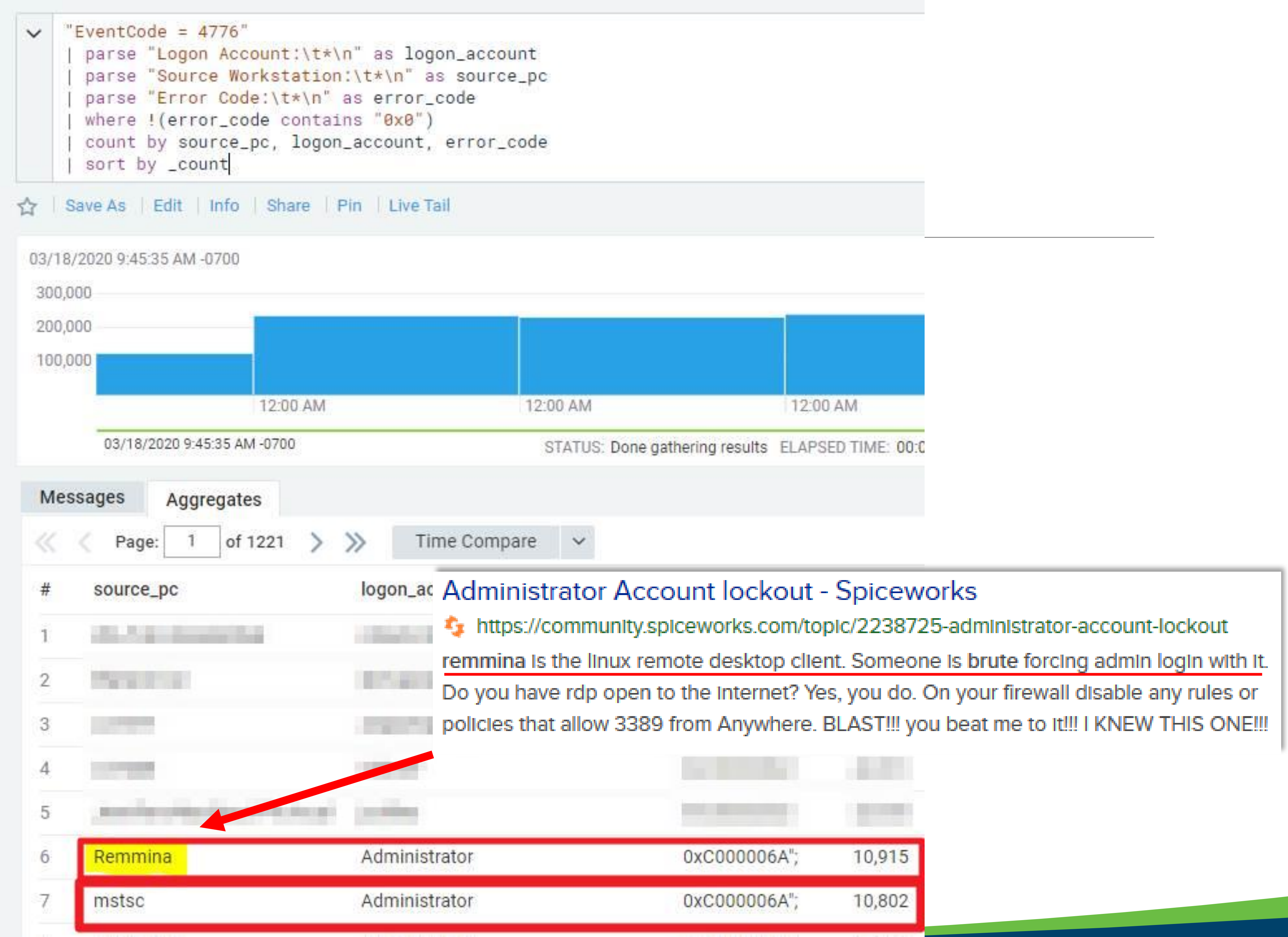
Account lockouts in a 24 hour period



```
"EventCode = 4776"
| parse "Logon Account:\t*\n" as logon_account
| parse "Source Workstation:\t*\n" as source_pc
| parse "Error Code:\t*\n" as error_code
| where !(error_code contains "0x0")
| count by source_pc, logon_account, error_code
| sort by _count
```

STATUS: Done gathering results ELAPSED TIME: 00:0

#	source_pc	logon_account	error_code	_count
1	[redacted]	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]	[redacted]
6	Remmina	Administrator	0xC000006A";	10,915
7	mstsc	Administrator	0xC000006A";	10,802



```
"EventCode = 4776"
| parse "Logon Account:\t*\n" as logon_account
| parse "Source Workstation:\t*\n" as source_pc
| parse "Error Code:\t*\n" as error_code
| where !(error_code contains "0x0")
| count by source_pc, logon_account, error_code
| sort by _count
```

STATUS: Done gathering results ELAPSED TIME: 00:0

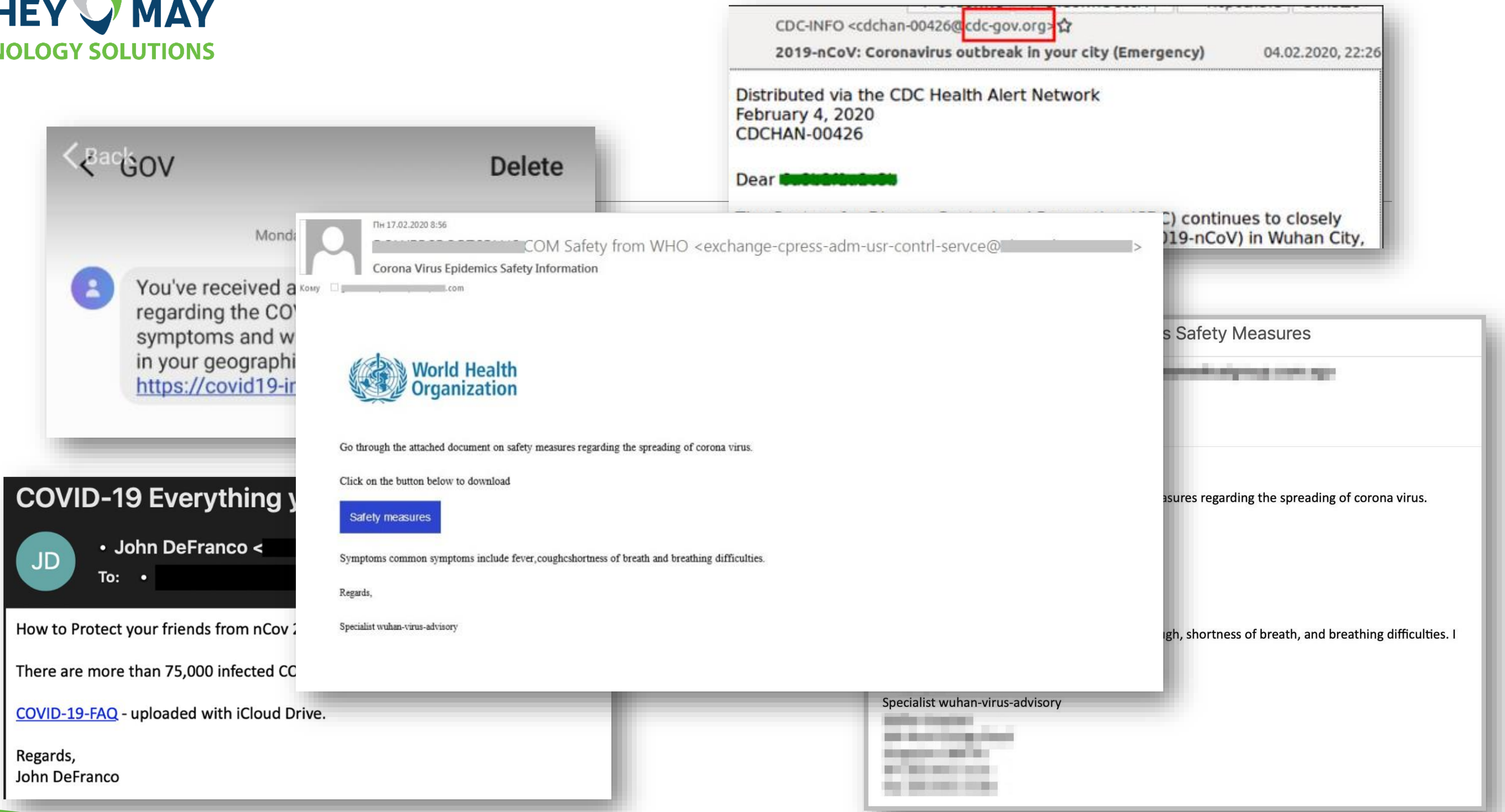
#	source_pc	logon_ac		
1	[redacted]	[redacted]		
2	[redacted]	[redacted]		
3	[redacted]	[redacted]		
4	[redacted]	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]	[redacted]
6	Remmina	Administrator	0xC000006A";	10,915
7	mstsc	Administrator	0xC000006A";	10,802

Administrator Account lockout - Spiceworks

https://community.spiceworks.com/topic/2238725-administrator-account-lockout

remmina is the linux remote desktop client. Someone is brute forcing admin login with it. Do you have rdp open to the internet? Yes, you do. On your firewall disable any rules or policies that allow 3389 from Anywhere. BLAST!!! you beat me to it!!! I KNEW THIS ONE!!!

Arris TM722 Modem



CDC-INFO <cdchan-00426@cdc-gov.org>

2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

C) continues to closely
019-nCoV) in Wuhan City,

Back GOV Delete

Monda

You've received a
regarding the CO
symptoms and w
in your geographi
https://covid19-ir

Пн 17.02.2020 8:56

[redacted]COM Safety from WHO <exchange-cpress-adm-usr-contrl-servce@[redacted]>

Corona Virus Epidemics Safety Information

Кому [redacted].com

World Health Organization

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Specialist wuhan-virus-advisory

s Safety Measures

[redacted]

asures regarding the spreading of corona virus.

gh, shortness of breath, and breathing difficulties. I

Specialist wuhan-virus-advisory
[redacted]

COVID-19 Everything y

JD • John DeFranco <[redacted]
To: • [redacted]

How to Protect your friends from nCov 2

There are more than 75,000 infected CO

COVID-19-FAQ - uploaded with iCloud Drive.

Regards,
John DeFranco

RICHEY MAY
TECHNOLOGY SOLUTIONS

Securing Creative in the Year of Breaches

Next Steps

- Prevention is ideal, detection is a must
- Secure the endpoint as a new perimeter
- Develop a COVID-19 exit strategy
  - Sheep dip computers
  - Threat hunting
  - Evaluate CCTV effectiveness with masks
- Improve your remote security architecture (DS-3.2)
- Keep current with the latest COVID-19 related threats

RICHEY MAY
TECHNOLOGY SOLUTIONS

Know The Enemy

COVID-19 Real-Time IOC Tracker:
https://bit.ly/RMTS-COVID19

- 78,559 Unique URLs
- 15,685 Unique IP Addresses
- 33,845 Unique Domain Names
- 113 Unique Email Addresses

Know Yourself

- Review policies and procedures
- Endpoint Detection and Response (EDR)
- Continue to deploy and test security awareness training
- Attend an event to learn more about securing the creative
  - RMTS Hollywood Cybersecurity (Virtual) Roundtable
  - Securely Connecting a Stay at Home Workforce (webinar)
  - Developing a COVID-19 Exit Strategy (webinar)
- Consult with an RMTS Certified TPN Security Consultant

RICHEY MAY
TECHNOLOGY SOLUTIONS

Thank You!

MICHAEL WYLIE

TWITTER: @THEMIKEWYLIE
LINKEDIN: LINKEDIN.COM/IN/MWYLIE

WWW.RICHEYMAYTECH.COM