Lessons Learned From 6 LAPSUS$ Incident (Responses)

Disclamer: Opinions are our own and do not express the views or opinions of our employer.

SANTIAGO ABASTANTE

- Threat Intel Leader
- First talk in Virus Bulletin
- Cloud Incident Responder

GABRIELA NICOLAO

- Threat Intel Leader
- Fifth talk in Virus Bulletin
- Malware Analysis

PRESENTATION CONTENT

01 LAPSUS$ PROFILE

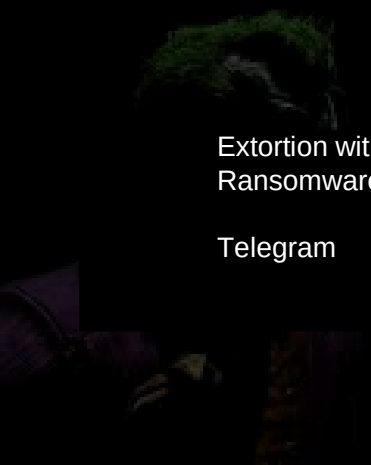
02 IR INSIGHTS

03 LESSONS LEARNED

LAPSUS$ PROFILE

Lapsus$ Profile

Caracteristics



Financial

"Watch the world burn"

Extortion without Ransomware

Telegram

2021-2022

17 year old in England aka "White" or "Breachbase" → Doxxed
7 people between 16 and 21 In England (released)
Teenager residing in Brazil

Lapsus$ Profile

Doxxing

Let me introduce you to [redacted] aka White / Breachbase. Originally starting his internet presence being obsessed with Minecraft servers and fantasizing about being the next big hacker to walk the RIU streetz, he later become friends with Miku & other young people that were involved in the selling/trading private 0day community. [redacted] slowly began making money to further expand his exploit collection. After a few years his net worth accumulated to well over 300BTC (Close to 14 MIL USD). Of course things don't always go to plan, and he gambled a large amount to impress like-minded idiots. The rest was left open in an RDP which was compromised, twice. [redacted] previously co-founded a group with Miku called 'Infinity Recursion' (Early 2021). He is currently involved with a newly formed ransomware group, with the name of 'Lapsus$' (https://vile.sh/white/IziGz.png)

[redacted] is currently 16 (at the time of posting) years old, still living with his parents & loves fishing with his uncle! Despite his family having no idea of his huge net worth, he has the brain of a 8 year old with severe autism.

Doxbin was briefly owned by White, when he bought it from kt & Brenton in November 2021. In the matter of 3 months, he completely destroyed any reputation the site had, along with breaking many functions that made Doxbin great. kt & Brenton decided to buy the website back (for 20% of the cost previously). After the deal, White knew he made a mistake; he decided to lock the registrar account & steal the Discord vanity in an attempt to get on kt's nerve. Which ultimately failed, as we got the vanity back within 2 hours. He then attempted to publicly advertise a bounty of $100,000 for kt's dox on the main Doxbin Twitter (https://vile.sh/white/lSeSS.png). 5 hours later, kt gains access to the Twitter account to start mocking White on his very awful internet security & opsec skills (https://vile.sh/white/AMynI.png). Due to kt not having the ability to change the email/password on the account, the only option left was to forcefully suspend the account.

» [D] Email: admin@leaks.direct / Rocketreach
» [D] Creation Date: 2021-02-08 17:04:48 / Twitter
» [D] <3 [] Github
» [D] Status: Active \ Discord
» [D] Relevancy: Common \

https://doxbin.com/upload/White

Lapsus$ Profile

Timeline

2021

MAY, 2021
Financial, Consumer
AR

JUNE, 2021
Technology, Media and Telecommunications
US

SEPTEMBER, 2021
Consumer
AR

OCTOBER, 2021
Technology, Media and Telecommunications
AR

DECEMBER, 2021
Leaks, show off
Public Sector BR
Public Sector, TMT BR

2022

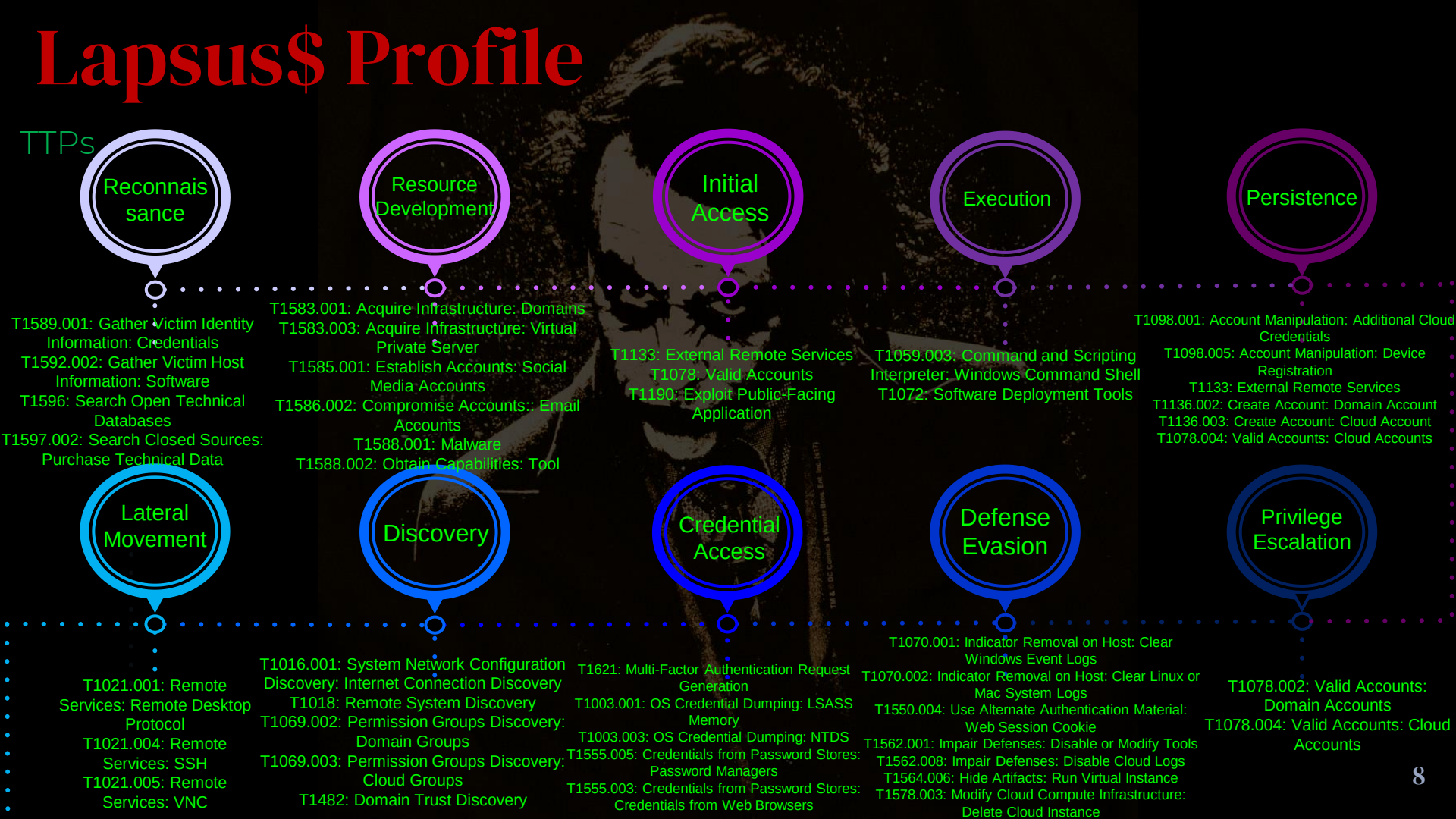
JANUARY, 2022
Doxxing
TMT, Consumer
PR,US,BR
Technology, Media and Telecommunications
AR

FEBRUARY, 2022
TMT
PR,US

MARCH, 2022
Look for insiders
Suspects caught
TMT, Consumer US, KR, AR
TMT, ERI AR

SEPTEMBER, 2022
Suspect caught
TMT, Consumer
US

Lapsus$ Profile



TTPs

Reconnaissance

T1589.001: Gather Victim Identity Information: Credentials
T1592.002: Gather Victim Host Information: Software
T1596: Search Open Technical Databases
T1597.002: Search Closed Sources: Purchase Technical Data

Resource Development

T1583.001: Acquire Infrastructure: Domains
T1583.003: Acquire Infrastructure: Virtual Private Server
T1585.001: Establish Accounts: Social Media Accounts
T1586.002: Compromise Accounts:: Email Accounts
T1588.001: Malware
T1588.002: Obtain Capabilities: Tool

Initial Access

T1133: External Remote Services
T1078: Valid Accounts
T1190: Exploit Public-Facing Application

Execution

T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1072: Software Deployment Tools

Persistence

T1098.001: Account Manipulation: Additional Cloud Credentials
T1098.005: Account Manipulation: Device Registration
T1133: External Remote Services
T1136.002: Create Account: Domain Account
T1136.003: Create Account: Cloud Account
T1078.004: Valid Accounts: Cloud Accounts

Lateral Movement

T1021.001: Remote Services: Remote Desktop Protocol
T1021.004: Remote Services: SSH
T1021.005: Remote Services: VNC

Discovery

T1016.001: System Network Configuration Discovery: Internet Connection Discovery
T1018: Remote System Discovery
T1069.002: Permission Groups Discovery: Domain Groups
T1069.003: Permission Groups Discovery: Cloud Groups
T1482: Domain Trust Discovery

Credential Access

T1621: Multi-Factor Authentication Request Generation
T1003.001: OS Credential Dumping: LSASS Memory
T1003.003: OS Credential Dumping: NTDS
T1555.005: Credentials from Password Stores: Password Managers
T1555.003: Credentials from Password Stores: Credentials from Web Browsers

Defense Evasion

T1070.001: Indicator Removal on Host: Clear Windows Event Logs
T1070.002: Indicator Removal on Host: Clear Linux or Mac System Logs
T1550.004: Use Alternate Authentication Material: Web Session Cookie
T1562.001: Impair Defenses: Disable or Modify Tools
T1562.008: Impair Defenses: Disable Cloud Logs
T1564.006: Hide Artifacts: Run Virtual Instance
T1578.003: Modify Cloud Compute Infrastructure: Delete Cloud Instance

Privilege Escalation

T1078.002: Valid Accounts: Domain Accounts
T1078.004: Valid Accounts: Cloud Accounts

Lapsus$ Profile

TTPs

Collection

T1005: Data from Local System
T1039: Data from Network Shared Drive
T1114.003: Email Collection: Email Forwarding Rule
T1213.001: Data from Information Repositories: Confluence
T1213.002: Data from Information Repositories: Sharepoint
T1213.003: Data from Information Repositories: Code Repositories
T1530: Data from Cloud Storage Object
T1560.001: Archive Collected Data: Archive via Utility

Command and Control

T1090.002: Proxy: External Proxy
T1105: Ingress Tool Transfer
T1219: Remote Access Software

Exfiltration

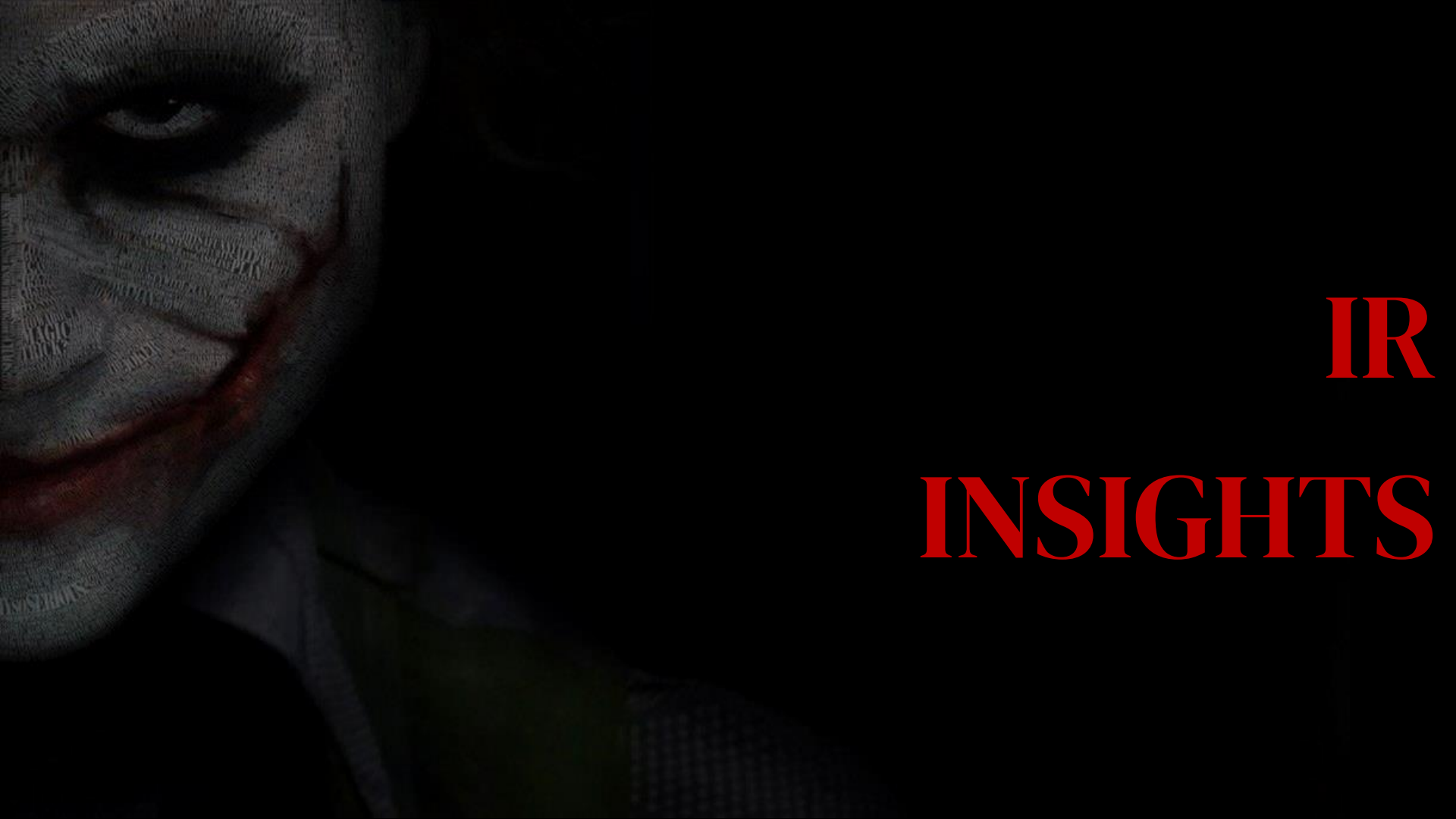
T1567.001: Exfiltration Over Web Service: Exfiltration to Code Repository
T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage

Impact

T1485: Data Destruction
T1489: Service Stop
T1490: Inhibit System Recovery
T1491.002: External Defacement
T1529: System Shutdown/Reboot
T1531: Account Access Removal

Software

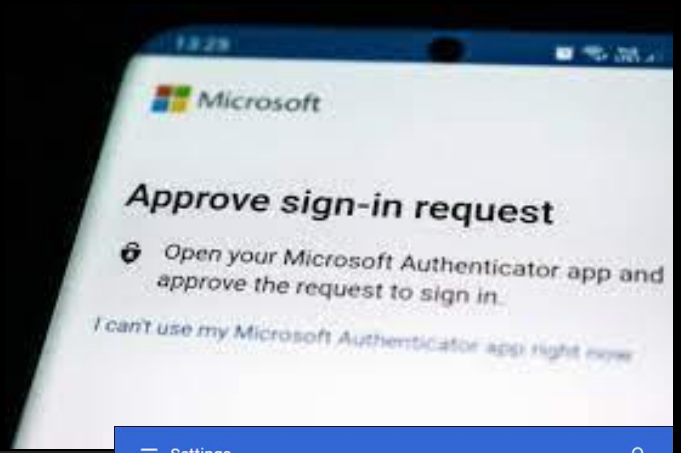
S0002:Mimikatz
S0508: Ngrok
S0106: cmd
Redline
ADExplorer
DCSync
S3Browser

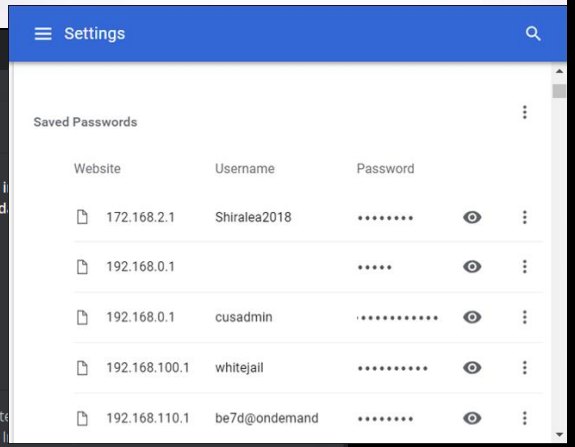

IR
INSIGHTS

IR Insights

Initial Access

- MFA Fatigue
- Cracked Software
- Redline Stealer
- Accessing Chrome Creds
- Raw MFA registration





General | Actors 1 | Events 6 | Indicators 6 | TTPs 13

Redline

Tool's First seen date: February, 2020
Tool's Sandbox time: 301

Tool's creation date i
Tool's modification d

☐ Report as generic in avclass ☑ Malicious

Community identifiers

Redline | Redlinesteal | Redlinestealer | Reline | Relinestealer | Obsidiumstealer | Obsidium

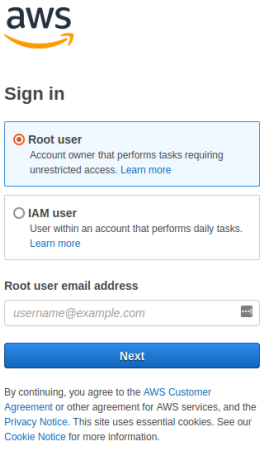
Description

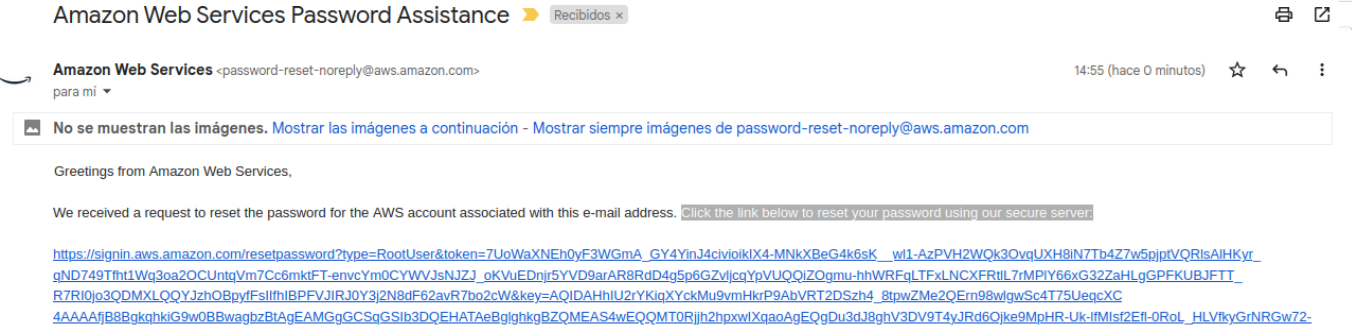
RedLine is an infostealer written in C # that was first available for sale on a Russian underground forum. Its goal is to ste
such as login, autocomplete data, passwords, cryptocurrency wallet information, Discord tokens, and credit card data. I
from Telegram chats, Steam, and VPN services such as NordVPN, OpenVPN, and ProtonVPN. RedLine supports all browsers based on Chromium and based on Gecko.

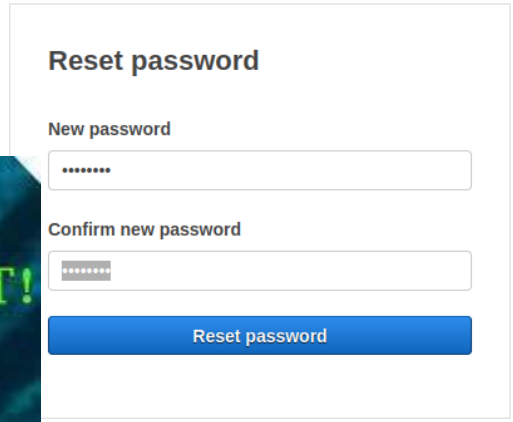
IR Insights

Exchange Takeover for root control and... Nuke!

- Microsoft Exchange RCE
- Only to get an email account
- Request for AWS Root user password reset







IR Insights

Credential Access

- Exposed Vulnerable Jenkins Box
- Leaks.direct
- AWS Credentials Access
- Access Keys / Instance Metadata
- AWS Enumeration and Data dump
- Account Takeover

```
ubuntu@ip-172-31-62-12:~$ curl http://169.254.169.254/latest/meta-data/identity-credentials/
ec2/security-credentials/ec2-instance
{
  "Code" : "Success",
  "LastUpdated" : "2020-04-19T13:51:17Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIA5A6IYBDLML7NRBWR",
  "SecretAccessKey" : "gXjV8iCeW0dh                                    ",
  "Token" : "IQoJb3JpZ2luX2VjENb//////////wEaCXVzLWVhc3QtMSJHMEUCIQCeiGuxRxhzxr1bi12gLAdxHia
WYwxwHSUez03TQ9w2tAIgWEYARJxFYOcpT4CCCtbQpzj4EhZpbMjDtUJbpLPOtOEqyAMI7//////////ARABGgw4OTU
zODQ4MTU4MzAiDOYRJac6nkrEs+8LdyqcAyuL65EQO7+Gd2SEaAdgPqcuqbzw/ChEyWgh4leqol2DXALiC/mOiRPXBNq
PyczNZRZAbqjmsQ/FumNJC4KqZuQYpxrH7UU4OXhPBmHZd6q2wbx8yWlPAEJ0K05ckfqhTGZGIfkAZN+jcsxO6dxmcJG
GR6nnCQ2sPz/MvVE5kkNKw2mNvOUbaDGgKzQwoKDOctyp70fU+sw0Ei29Vt2JJxfmEsEEY2adeiFlX5u9fLrSYXo1JXy
vWMyE1ITBeicR3tnRnaxLG/JUJB8bJtq9QPs7K5DGKNj88ICVVnMoDZcrcAqdevkOO4LlJmePuRP8PxaVVX1+ZWUHVm+
OW16E9EundUwQgv948o3m9KpSE/KiHbVRwEw/U5CHb6Qe2i4UgTi/Kejc+HoCa8OV6E/ZStV0rl0+VZmwkK1hW4LLsxC
                                                                                
                                                                                
                                                                                
6lhRei+3l4cQRX3eTD1stwSMivZwAvAiLhDN55MSmwYq9/FowJ4ePGdxhZ1exsbPILo2khikgFzk=",
  "Expiration" : "2020-04-19T20:21:54Z"
```

```
santiago@thinkpad:~$ cat .aws/credentials
[default]
aws_access_key_id = aws_access_key
aws_secret_access_key = aws_secret_key(SECRET KEY!!)
```

Event name	AWS region	Source IP addr	User agent
ListBuckets	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
ListDistributions	us-east-1	104.199.41.42	S3 Browser/9.9.7 (https://s3browser.com)
GetBucketLogging	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
GetBucketLocation	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
ListDistributions	us-east-1	104.199.41.42	S3 Browser/9.9.7 (https://s3browser.com)
GetBucketVersioning	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
GetBucketRequestPayment	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
GetBucketReplication	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
GetAccelerateConfiguration	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
GetBucketLocation	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]
ListBuckets	us-east-1	104.199.41.42	[S3 Browser/9.9.7 (https://s3browser.com)]

```
santiago@thinkpad:~$ dig leaks.direct

; <<>> DiG 9.16.1-Ubuntu <<>> leaks.direct
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28413
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;leaks.direct.                  IN      A

;; ANSWER SECTION:
leaks.direct.           300     IN      A       104.194.10.104

;; Query time: 388 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 23 14:50:21 -03 2022
;; MSG SIZE  rcvd: 57
```

IR Insights

Exfiltration and Impact

- Nuclear Launch Detected - AWS Nuke
- Github / Gitlab data leaks
- Ngrok / FileZilla exfiltration
- Dropbox data and takeover

README.md

aws-nuke

Golang CI passing | license MIT | release v2.19.0 | docker pulls 353k

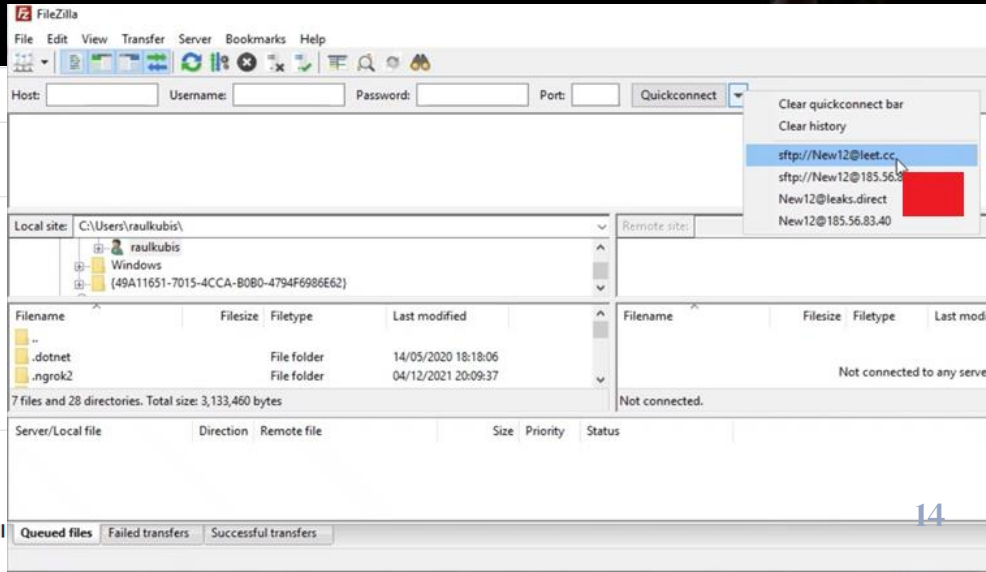
Remove all resources from an AWS account.

> **Development Status** *aws-nuke* is stable, but it is likely that not all AWS resources are covered by it. Be encouraged to add missing resources and create a Pull Request or to create an Issue.

Caution!

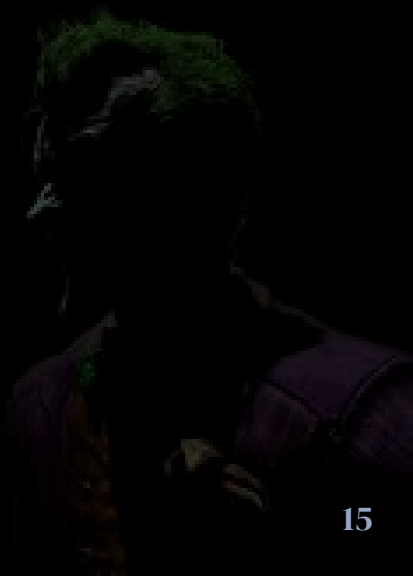
Be aware that *aws-nuke* is a very destructive tool, hence you have to be very careful while using it. Otherwise you might delete production data.

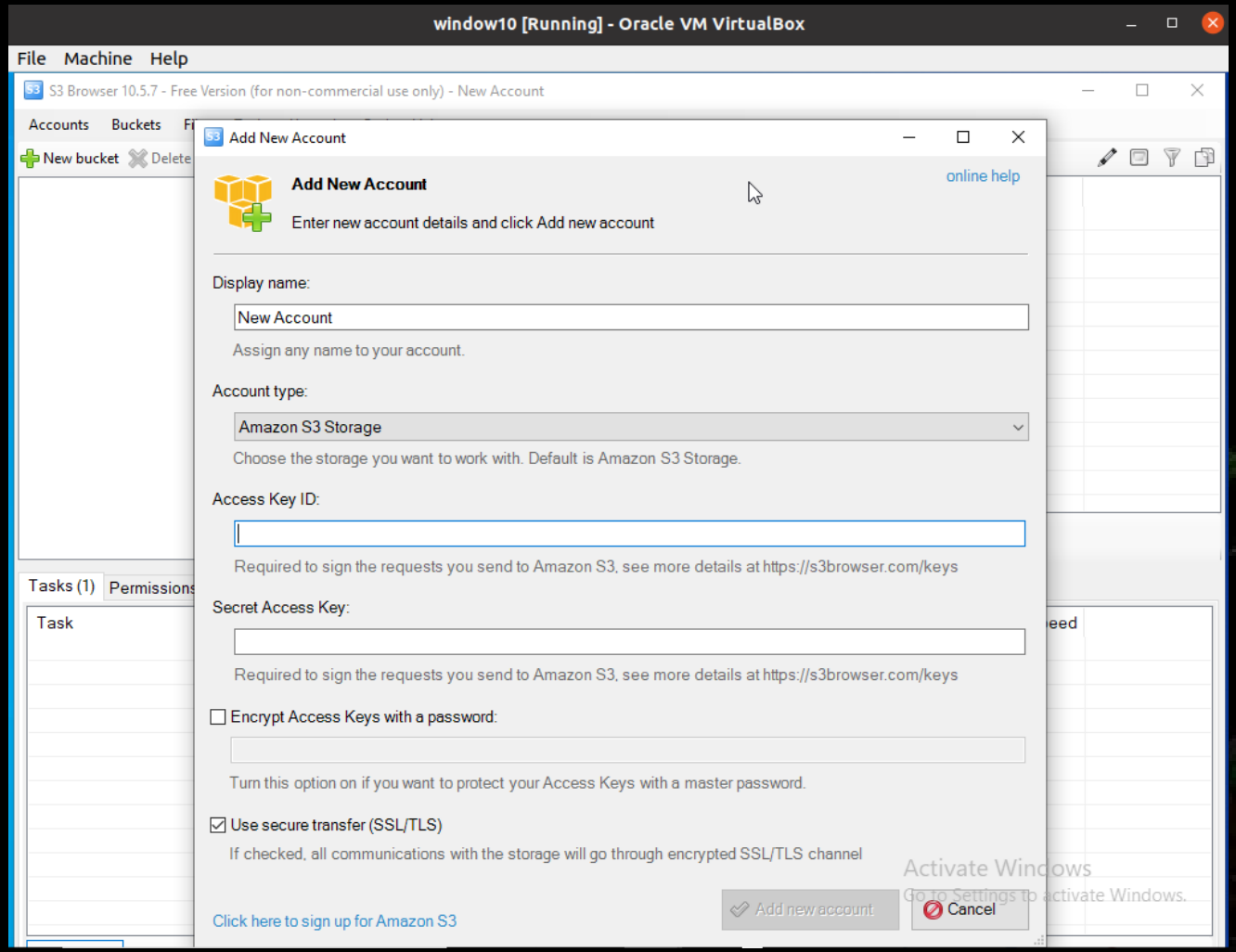
We strongly advise you to not run this application on any AWS account, where you cannot afford to lose all resources.



IR Insights

AWS Attack Demo




window10 [Running] - Oracle VM VirtualBox
File Machine Help
S3 Browser 10.5.7 - Free Version (for non-commercial use only) - New Account
Accounts Buckets
New bucket Delete
Tasks (1) Permissions
Task
Add New Account
Add New Account
online help
Enter new account details and click Add new account
Display name:
New Account
Assign any name to your account.
Account type:
Amazon S3 Storage
Choose the storage you want to work with. Default is Amazon S3 Storage.
Access Key ID:
Required to sign the requests you send to Amazon S3, see more details at https://s3browser.com/keys
Secret Access Key:
Required to sign the requests you send to Amazon S3, see more details at https://s3browser.com/keys
Encrypt Access Keys with a password:
Turn this option on if you want to protect your Access Keys with a master password.
Use secure transfer (SSL/TLS)
If checked, all communications with the storage will go through encrypted SSL/TLS channel
Click here to sign up for Amazon S3
Add new account
Cancel
Activate Windows
Go to Settings to activate Windows.

```
santiago@thinkpad:~/vbdemo$ ./aws-nuke -c  full.yml --profile default --no-dry-run
aws-nuke version v2.18.0.dirty - Thu Apr 28 09:06:07 UTC 2022 - aa877dbc56140d408bef8c64f3a0d34f2172dbbc

Do you really want to nuke the account with the ID 695395027189 and the alias 'vbdemo'?
Do you want to continue? Enter account alias to continue.
> vbdemo

global - IAMInstanceProfileRole - assume_role_ec2_role -> assume_role_ec2_role - [InstanceProfile: "assume_role_ec2_role", InstanceRole: "assume_role_ec2
global - IAMSAMLProvider - arn:aws:iam::695395027189:saml-provider/AWSSSO_11d267b53f5cc61c_DO_NOT_DELETE - would remove
global - IAMInstanceProfile - assume_role_ec2_role - [Name: "assume_role_ec2_role", Path: "/"] - would remove
global - IAMVirtualMFADevice - arn:aws:iam::695395027189:mfa/root-account-mfa-device - Cannot delete root MFA device
global - IAMUser - ghost - [Name: "ghost"] - would remove
global - IAMUser - lambda_test - [Name: "lambda_test"] - would remove
global - IAMUser - terraform_admin - [Name: "terraform_admin"] - would remove
global - IAMUser - vbdemo - [Name: "vbdemo"] - would remove
global - Budget - Test Budget - [AccountID: "695395027189", BudgetType: "COST", Name: "Test Budget"] - would remove
global - IAMLoginProfile - terraform_admin - [UserName: "terraform_admin"] - would remove
global - IAMUserPolicyAttachment - lambda_test -> lambda_List - [PolicyArn: "arn:aws:iam::695395027189:policy/lambda_List", PolicyName: "lambda_List", Us
 would remove
global - IAMUserPolicyAttachment - terraform_admin -> AdministratorAccess - [PolicyArn: "arn:aws:iam::aws:policy/AdministratorAccess", PolicyName: "Admi
e: "terraform_admin"] - would remove
global - IAMUserPolicyAttachment - vbdemo -> AdministratorAccess - [PolicyArn: "arn:aws:iam::aws:policy/AdministratorAccess", PolicyName: "Administrator
o"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/service-role/AWSLambdaBasicExecutionRole-2a28910c-0c8a-4f0d-b9e0-8e8f1dddfcf8 - [ARN: "arn:aws:iam
vice-role/AWSLambdaBasicExecutionRole-2a28910c-0c8a-4f0d-b9e0-8e8f1dddfcf8", Name: "AWSLambdaBasicExecutionRole-2a28910c-0c8a-4f0d-b9e0-8e8f1dddfcf8", P
licyID: "ANPA2D2GGBD24CYTERBSI"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/assume_role_ec2 - [ARN: "arn:aws:iam::695395027189:policy/assume_role_ec2", Name: "assume_role_ec2
ANPA2D2GGBD26Q77LTPYO"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/service-role/AWSLambdaBasicExecutionRole-a18b31d2-6ccb-44c4-8833-8f1e808451d6 - [ARN: "arn:aws:iam
vice-role/AWSLambdaBasicExecutionRole-a18b31d2-6ccb-44c4-8833-8f1e808451d6", Name: "AWSLambdaBasicExecutionRole-a18b31d2-6ccb-44c4-8833-8f1e808451d6", P
licyID: "ANPA2D2GGBD2Q4EQNM3TS"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/service-role/CloudTrailPolicyForCloudWatchLogs_6d8a5058-6361-48aa-a764-34d9f828a461 - [ARN: "arn:a
cy/service-role/CloudTrailPolicyForCloudWatchLogs_6d8a5058-6361-48aa-a764-34d9f828a461", Name: "CloudTrailPolicyForCloudWatchLogs_6d8a5058-6361-48aa-a76
service-role/", PolicyID: "ANPA2D2GGBD2QOHGM3ZDI"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/service-role/AWSLambdaBasicExecutionRole-aaac046f-ac92-449a-908d-844768345808 - [ARN: "arn:aws:iam
vice-role/AWSLambdaBasicExecutionRole-aaac046f-ac92-449a-908d-844768345808", Name: "AWSLambdaBasicExecutionRole-aaac046f-ac92-449a-908d-844768345808", P
licyID: "ANPA2D2GGBD2QUYJBRXWP"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/assume_role_policy - [ARN: "arn:aws:iam::695395027189:policy/assume_role_policy", Name: "assume_ro
licyID: "ANPA2D2GGBD2SRFTXHSKD"] - would remove
global - IAMPolicy - arn:aws:iam::695395027189:policy/lambda_List - [ARN: "arn:aws:iam::695395027189:policy/lambda_List", Name: "lambda_List", Path: "/"
T3IM6C2S6"] - would remove
global - IAMUserAccessKey - ghost -> AKIA2D2GGBD2WBE6ECTX - [AccessKeyID: "AKIA2D2GGBD2WBE6ECTX", UserName: "ghost"] - would remove
global - IAMUserAccessKey - lambda_test -> AKIA2D2GGBD237GU2RXE - [AccessKeyID: "AKIA2D2GGBD237GU2RXE", UserName: "lambda_test"] - would remove
global - IAMUserAccessKey - terraform_admin -> AKIA2D2GGBD2ZL5BF7VS - [AccessKeyID: "AKIA2D2GGBD2ZL5BF7VS", UserName: "terraform_admin"] - would remove
global - IAMUserAccessKey - vbdemo -> AKIA2D2GGBD2RTDDVAMU - [AccessKeyID: "AKIA2D2GGBD2RTDDVAMU", UserName: "vbdemo"] - would remove
global - IAMRole - assume_role_ec2_role - [Name: "assume_role_ec2_role", Path: "/"] - would remove
```

IR Insights

AWS Attack Demo (Logs)

Event record Info

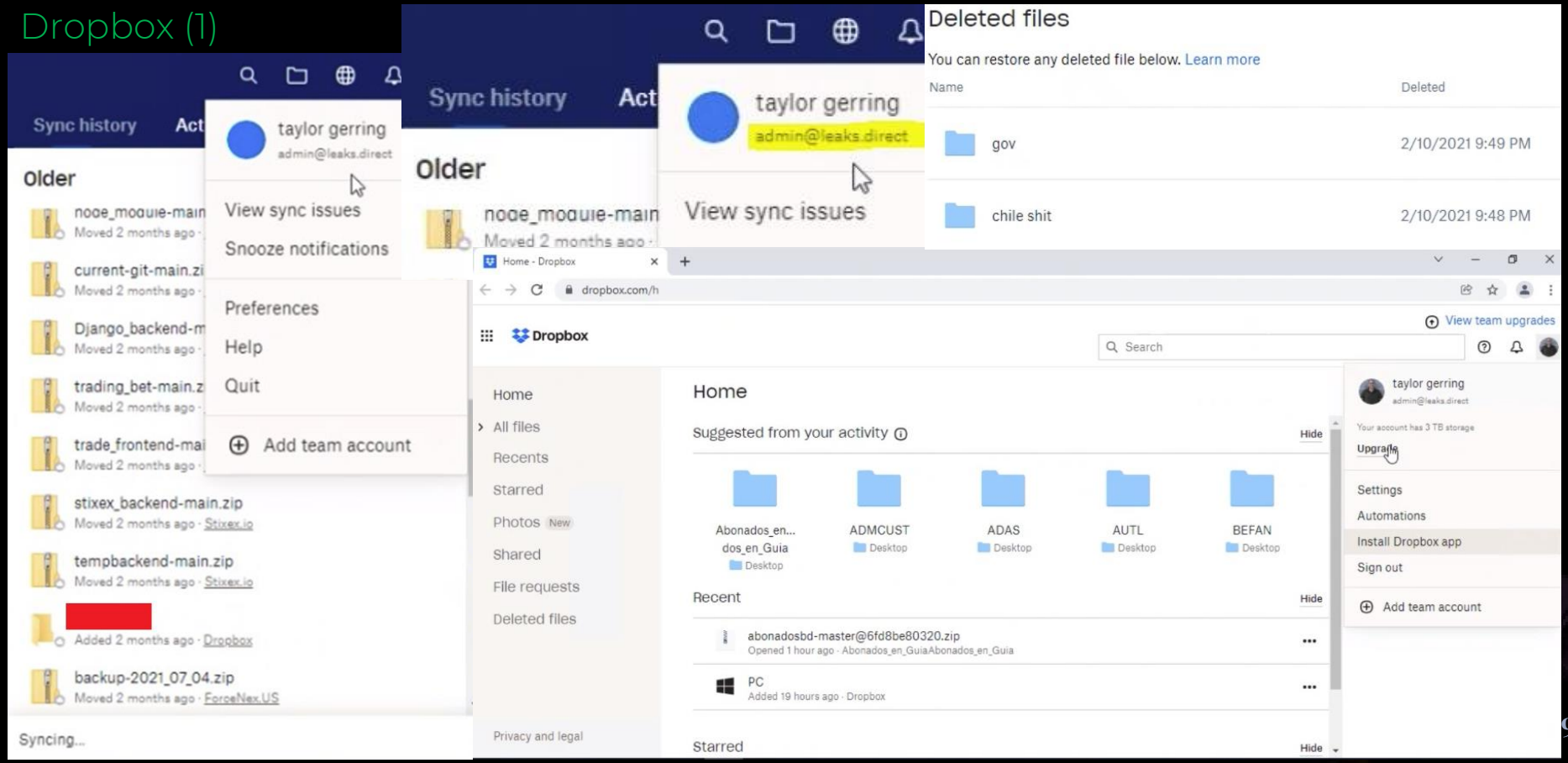

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA2D2GGBD2QIMEPMIAM",
        "arn": "arn:aws:iam::695395027189:user/vbd
        "accountId": "695395027189",
        "accessKeyId": "AKIA2D2GGBD2RTDDVAMU",
        "userName": "vbdemo"
    },
    "eventTime": "2022-09-29T16:53:01Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "CreateBucket",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "82.142.85.165",
    "userAgent": "[S3 Browser/10.5.7 (https://s3br
    "requestParameters": {
        "bucketName": "aws-logs-for-vbdemo",
        "Host": "aws-logs-for-vbdemo.s3.us-east-1.
    },
    "responseElements": null
```



```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA2D2GGBD2QIMEPMIAM",
        "arn": "arn:aws:iam::695395027189:user/vbdemo",
        "accountId": "695395027189",
        "accessKeyId": "AKIA2D2GGBD2RTDDVAMU",
        "userName": "vbdemo"
    },
    "eventTime": "2022-09-29T10:02:37Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "DeleteBucketPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "82.142.85.169",
    "userAgent": "[aws-sdk-go/1.42.45 (go1.17.9; linux; amd64)]",
    "requestParameters": {
        "bucketName": "vb-test-s3-bucket-5",
        "Host": "vb-test-s3-bucket-5.s3.amazonaws.com",
        "policy": ""
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "Pwm4J0XPEG1GkrLXqthKnzWtjOHNQllgBuL+IG56cS/mCzu6tz4stQZ3IYNM8KFMBJ7puCDMg50=",
        "bytesTransferredOut": 0
    },
```

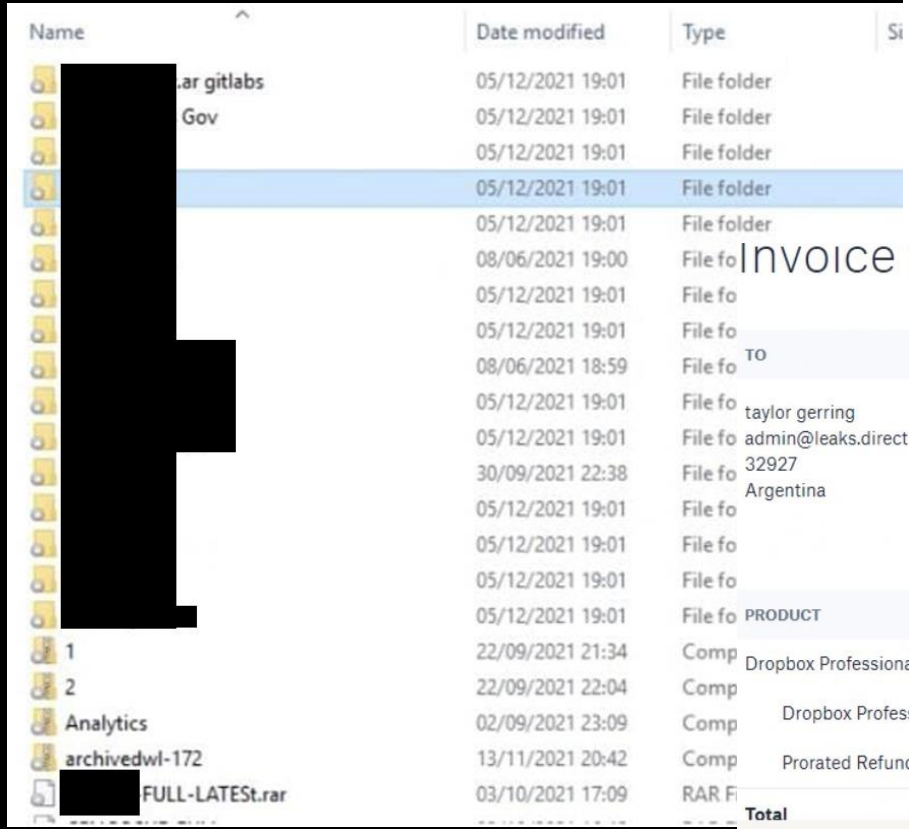
IR Insights

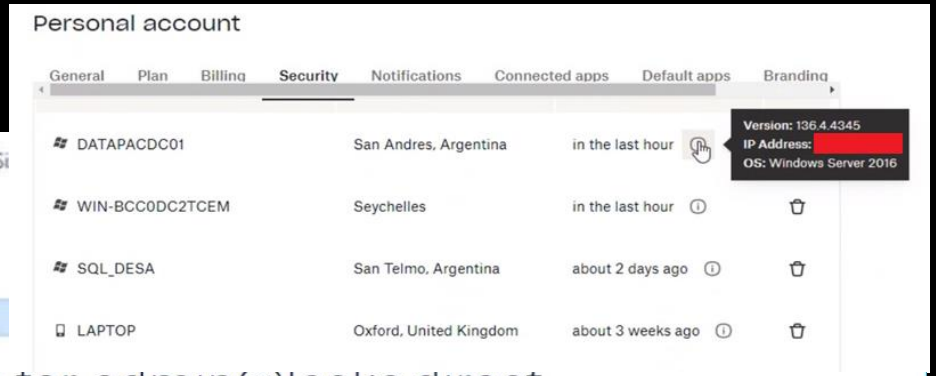
Dropbox (1)



IR Insights

Dropbox (2)





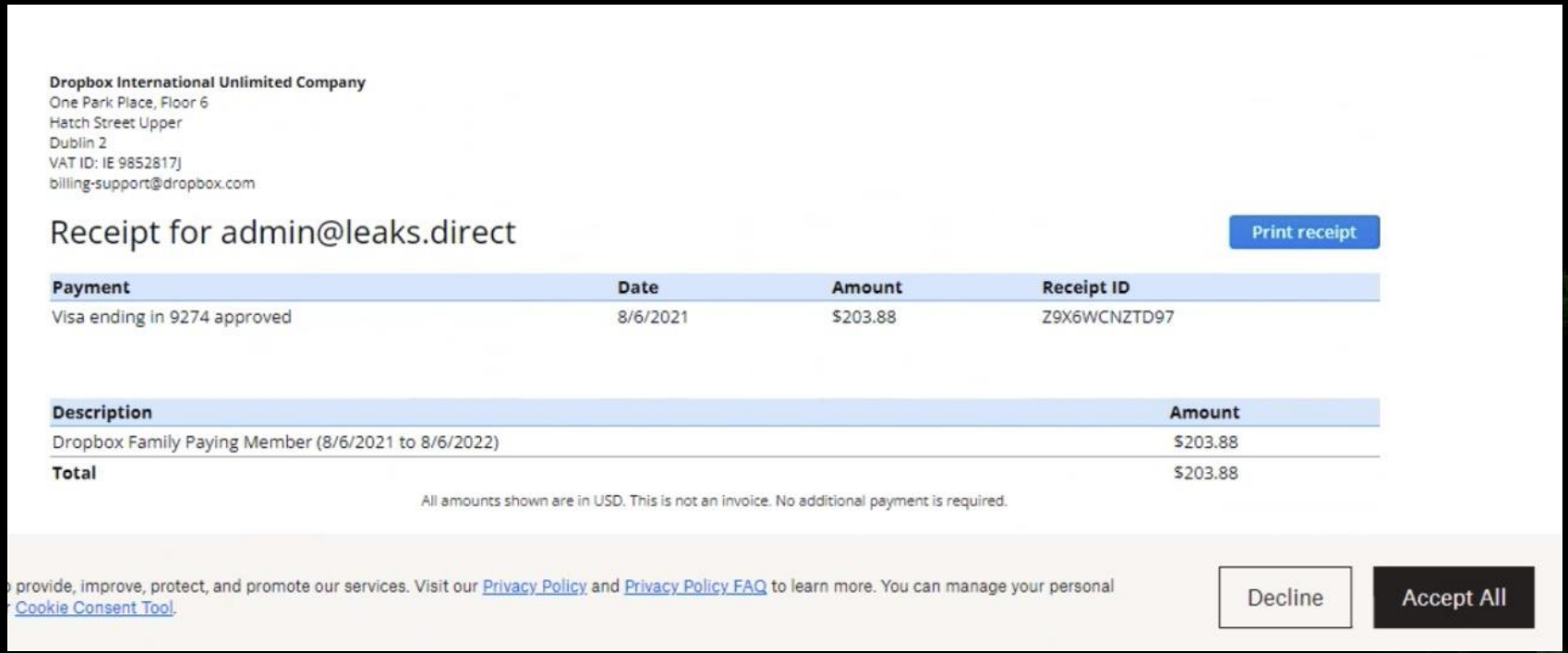
Invoice for admin@leaks.direct

TO	DATE	INVOICE ID
taylor gerring admin@leaks.direct 32927 Argentina	October 3, 2021 12:53 AM GMT	H1GGSVM2N5QM

PRODUCT	AMOUNT
Dropbox Professional + Prorated Refund (3/10/2021 to 8/6/2022)	
Dropbox Professional	$135.76
Prorated Refund	($139.09)
Total	($3.33)

IR Insights

Dropbox (3)



Dropbox International Unlimited Company
One Park Place, Floor 6
Hatch Street Upper
Dublin 2
VAT ID: IE 9852817J
billing-support@dropbox.com

Receipt for admin@leaks.direct

Print receipt

Payment	Date	Amount	Receipt ID
Visa ending in 9274 approved	8/6/2021	$203.88	Z9X6WCNZTD97

Description	Amount
Dropbox Family Paying Member (8/6/2021 to 8/6/2022)	$203.88
Total	$203.88

All amounts shown are in USD. This is not an invoice. No additional payment is required.

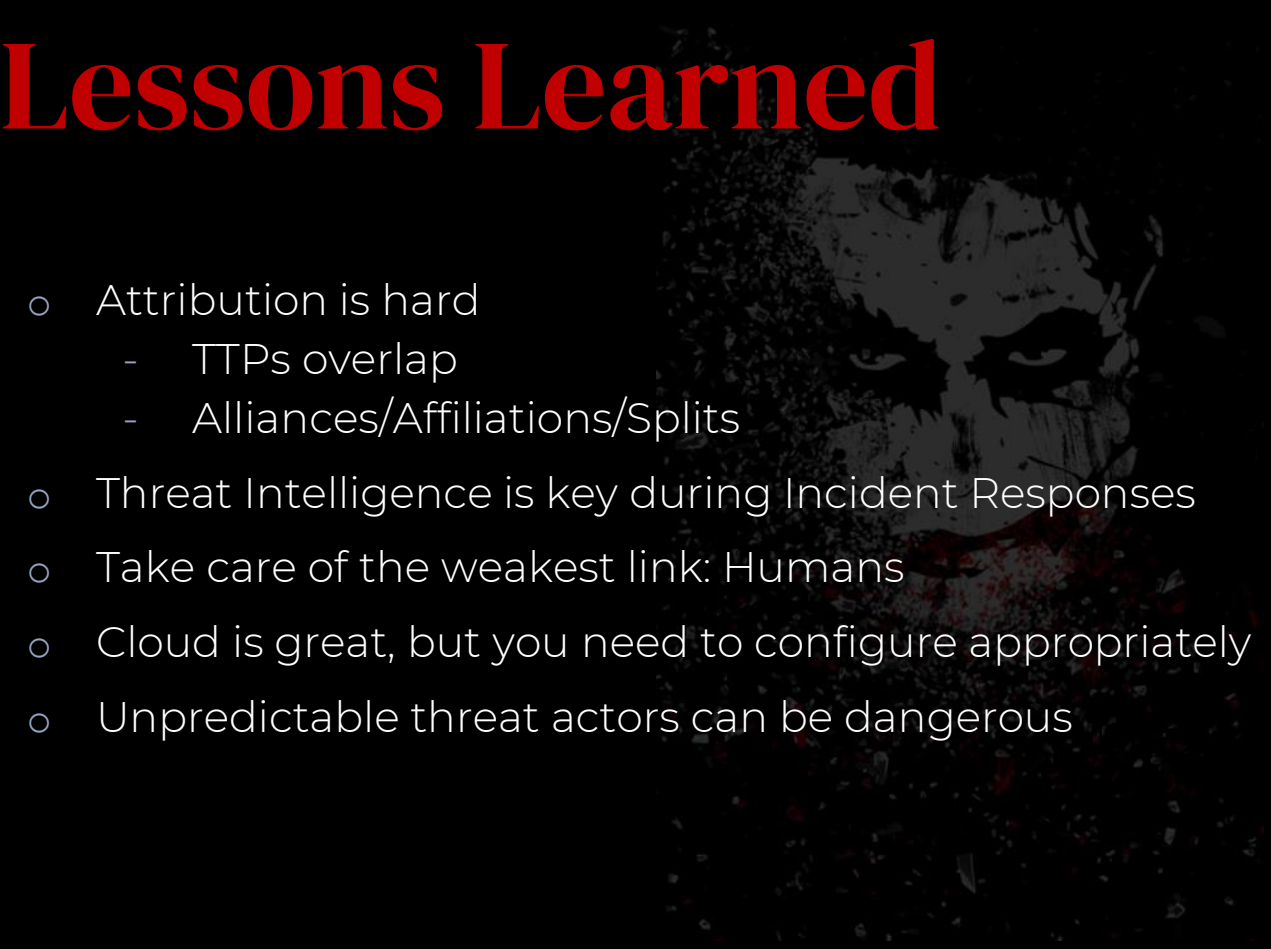
provide, improve, protect, and promote our services. Visit our Privacy Policy and Privacy Policy FAQ to learn more. You can manage your personal Cookie Consent Tool.

Decline

Accept All

Lessons Learned

Lessons Learned



- Attribution is hard
  - TTPs overlap
  - Alliances/Affiliations/Splits
- Threat Intelligence is key during Incident Responses
- Take care of the weakest link: Humans
- Cloud is great, but you need to configure appropriately
- Unpredictable threat actors can be dangerous


Thank you!