CADO//

Playbook

The Ultimate Guide to **Ransomware Incident Response & Forensics**

Table of Contents

Introduction

Conducting a thorough forensics investigation post breach is critical to identifying root cause and preventing future breaches. As we've seen, ransomware operators are known to execute repeat-ransomware attacks where they target the same victim twice using the knowledge they gained or the tools they left behind from the initial intrusion. Further, as outlined in our former analysis of the HelloKitty ransomware, ransomware operators often disappear and resurface with new branding, so it's extremely important to understand how these attackers operate across all stages of the attack lifecycle to ensure future detections are investigated thoroughly before they escalate.

In this guide, we've outlined some guidance on investigating ransomware, post breach.

Kicking off a Ransomware Investigation

Generally it's a good idea to switch off or hibernate the infected system. If you do so quickly, it's possible that the ransomware hasn't finished encrypting the files on disk. If it's a Virtual Machine, take a snapshot.

Many ransomware variants encrypt files on network shares, or spread within networks. If you are unable to turn off the system, isolate the host from the network. You can do this remotely, or simply disconnect it from the network if you have physical access to the machine.

Understanding the Type of Ransomware You’re Dealing With

It’s important to identify if you are dealing with common opportunistic ransomware, or something more targeted as soon as possible. Historically, ransomware was deployed through malicious emails. These normally don’t provide the attacker with interactive access to your network. Today, more commonly seen in cloud environments, opportunistic ransomware includes worm-like functionalities that enable the attackers to spread through the network quickly.

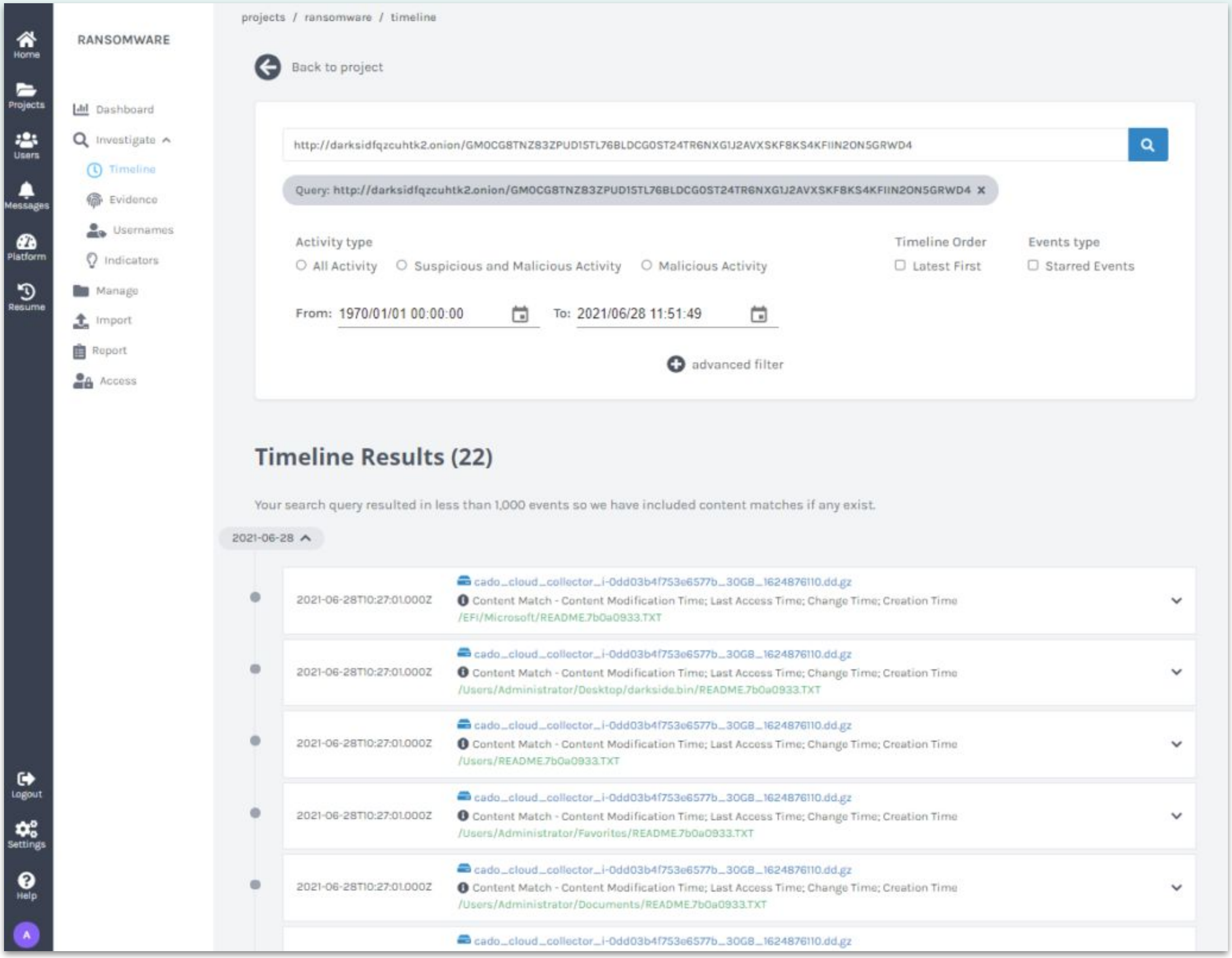
Most of the ransomware that makes the news today, such as DarkSide, are deployed manually by an attacker as part of a classic intrusion. The attacker will then likely spread to multiple systems, and maintain access until they are removed.

You can identify the type of ransomware you’re dealing with by:

- **Researching the ransomware note using a search engine or uploading to ID ransomware;**
- **Identifying the ransomware executable; and**
- **Identifying the initial infection vector**

Researching the Ransomware Note

Ransomware notes are normally easy to find, as the ransomware author wants you to find them. But you can also search for it by running keyword searches or yara rules for common phrases found in ransomware notes. This search may also yield the ransomware executable itself.



http://darksidfqzcuhtk2.onion/GM0CG8TNZ83ZPUD1STL76BLDCG0ST24TR6NXG1J2AVXSKF8KS4KFIIN2ON5GRWD4

Query: http://darksidfqzcuhtk2.onion/GM0CG8TNZ83ZPUD1STL76BLDCG0ST24TR6NXG1J2AVXSKF8KS4KFIIN2ON5GRWD4 ×

Activity type
○ All Activity ○ Suspicious and Malicious Activity ○ Malicious Activity

Timeline Order
□ Latest First

Events type
□ Starred Events

From: 1970/01/01 00:00:00 To: 2021/06/28 11:51:49

Timeline Results (22)

Your search query resulted in less than 1,000 events so we have included content matches if any exist.

2021-06-28

2021-06-28T10:27:01.000Z
cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
Content Match - Content Modification Time; Last Access Time; Change Time; Creation Time
/EFI/Microsoft/README.7b0a0933.TXT

2021-06-28T10:27:01.000Z
cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
Content Match - Content Modification Time; Last Access Time; Change Time; Creation Time
/Users/Administrator/Desktop/darkside.bin/README.7b0a0933.TXT

2021-06-28T10:27:01.000Z
cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
Content Match - Content Modification Time; Last Access Time; Change Time; Creation Time
/Users/README.7b0a0933.TXT

2021-06-28T10:27:01.000Z
cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
Content Match - Content Modification Time; Last Access Time; Change Time; Creation Time
/Users/Administrator/Favorites/README.7b0a0933.TXT

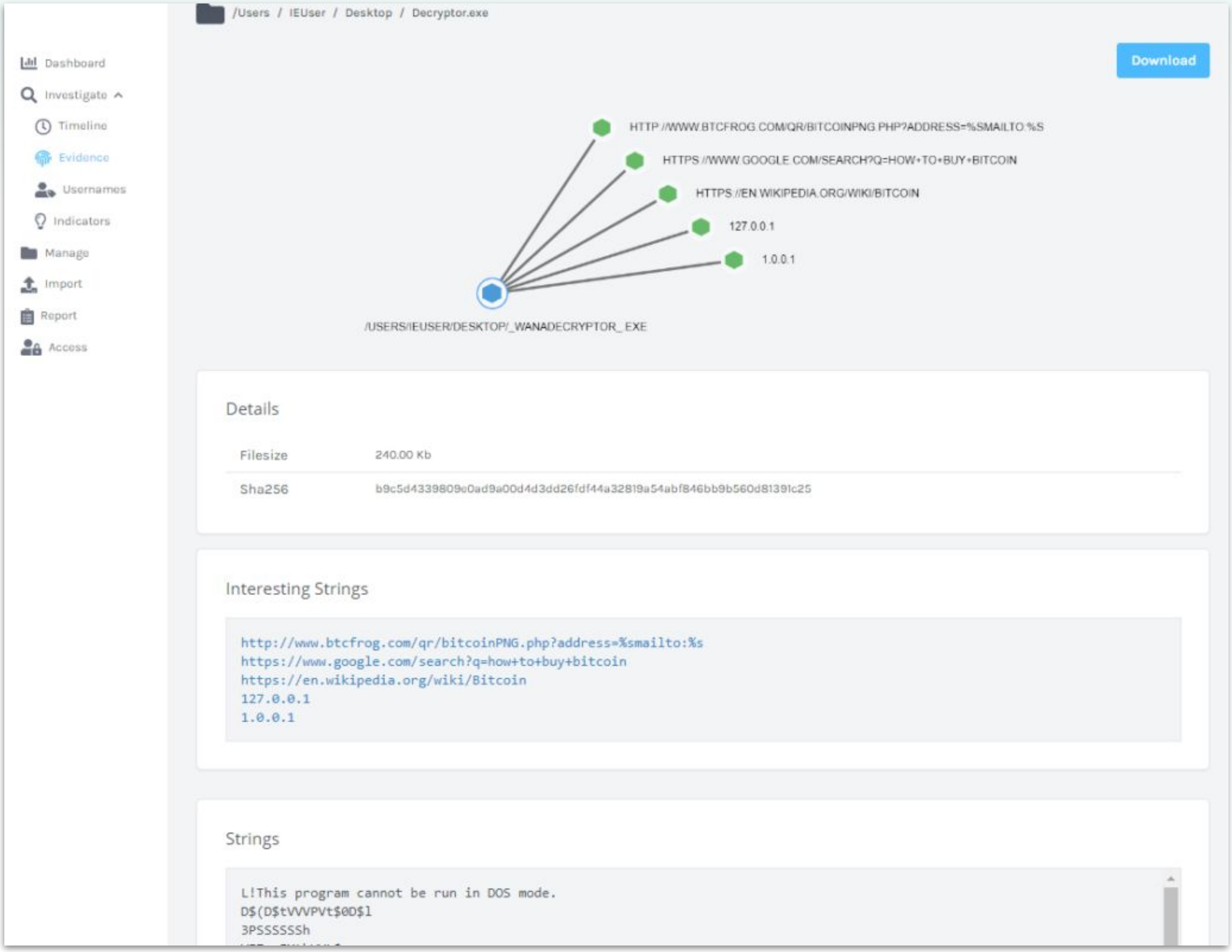
2021-06-28T10:27:01.000Z
cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
Content Match - Content Modification Time; Last Access Time; Change Time; Creation Time
/Users/Administrator/Documents/README.7b0a0933.TXT

cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz

The ransomware note from DarkSide ransomware displayed in Cado Response

Identifying the Ransomware Executable

Normally the ransomware executable is easy to find using timeline analysis. Look for the creation of executables surrounding the first encrypted files, or the initial compromise. Alternatively, most ransomware is well detected by both Anti-Virus signatures and Yara rules.


/Users / IEUser / Desktop / Decryptor.exe
Download
Dashboard
Investigate
Timeline
Evidence
Usernames
Indicators
Manage
Import
Report
Access
HTTP //WWW BTCFROG COM/QR/BITCOINPNG PHP?ADDRESS=%SMAILTO %S
HTTPS //WWW GOOGLE COM/SEARCH?Q=HOW+TO+BUY+BITCOIN
HTTPS //EN WIKIPEDIA ORG/WIKI/BITCOIN
127.0.0.1
1.0.0.1
/USERS/IEUSER/DESKTOP/_WANADECRYPTOR_ EXE

Details

Filesize	240.00 Kb
Sha256	b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Interesting Strings

```
http://www.btcfrog.com/qr/bitcoinPNG.php?address=%smailto:%s
https://www.google.com/search?q=how+to+buy+bitcoin
https://en.wikipedia.org/wiki/Bitcoin
127.0.0.1
1.0.0.1
```

Strings

```
L!This program cannot be run in DOS mode.
D$(D$tVVVPVt$0D$1
3PSSSSSSh
```

The classic WannaCry executable presented in Cado Response

Identifying the Initial Compromise

Identifying the initial compromise is required to protect other systems that could be vulnerable too. You can do so by following the below steps:

1. Identify how the ransomware was distributed within your environment. Typically this would have been initiated from a central management server such as a File Server or Domain Controller

2. Identify the accounts and systems that were used by the ransomware threat actors to gain access to the end servers

3. Follow the trail back and investigate all servers and workstations that were leveraged by the ransomware threat actors to identify patient0 and therefore, the method of exploitation the attackers used to gain initial access

4. Examine the netflow/network traffic to identify signs of data exfiltration

5. It's also important to analyse the TTPs used at the initial point of entry so you can search for and prevent additional entry across your environment

6. The attackers may have exploited a public facing web application. Depending on the application, you may have both web-server logs and application logs to review. Look for web-shells and other signs of post compromise.

7. Today it's very common for ransomware attacks to start with a malicious email. You can parse Outlook web archives (PST files) using forensic tools such as Encase or pffexport (included with SIFT). You can also review attachments if you have access to the mail system itself. Once extracted, attachments can be analysed using Yara and Anti-virus, or by hand.

8. Lastly, you can also review Outlooks temporary archive, and Temporary Internet Files for web-mail. In addition to reviewing attachments, you may also want to extract any URLs from messages and check to see if they are malicious.

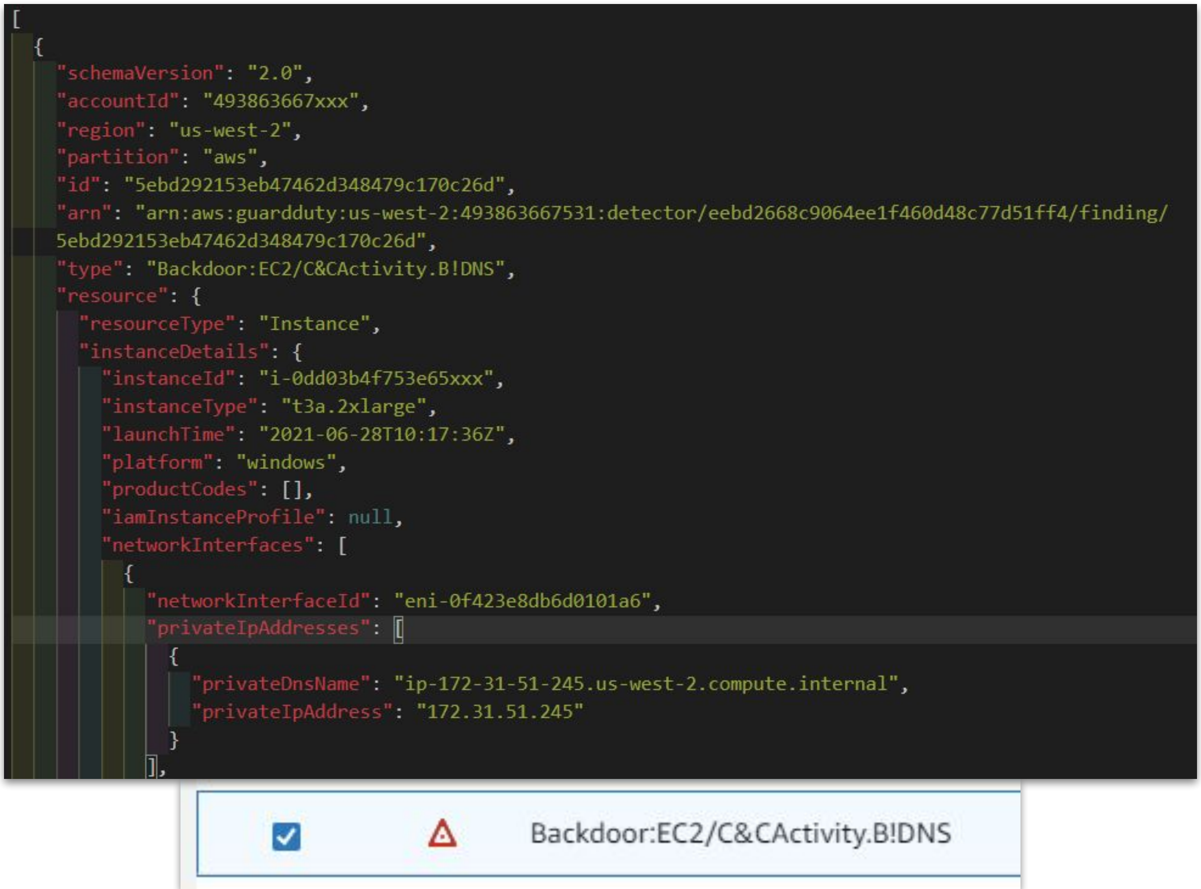
Once you have identified the initial access point, review event logs to identify any potential lateral movement from the infected system.

File Recovery

It’s critical that you have a sound backup and recovery process in place. With backups, it’s important to ensure you have true offline copies, as some attackers will target how your backup systems function. Further, some incremental backups rely on there being a known good state of a system, so it is important that you also consider if you need a full backup vs incremental. Depending on the variant of ransomware, it will normally overwrite original files, and look to delete volume shadow backups. As such, forensic recovery of files is usually met with limited success.

Ransomware in the Cloud

If the ransomware attack also targets cloud assets, Amazon GuardDuty does provide detection of well-known ransomware samples. For example, as you can see below, we executed DarkSide ransomware in our sandbox environment and it was successfully detected:

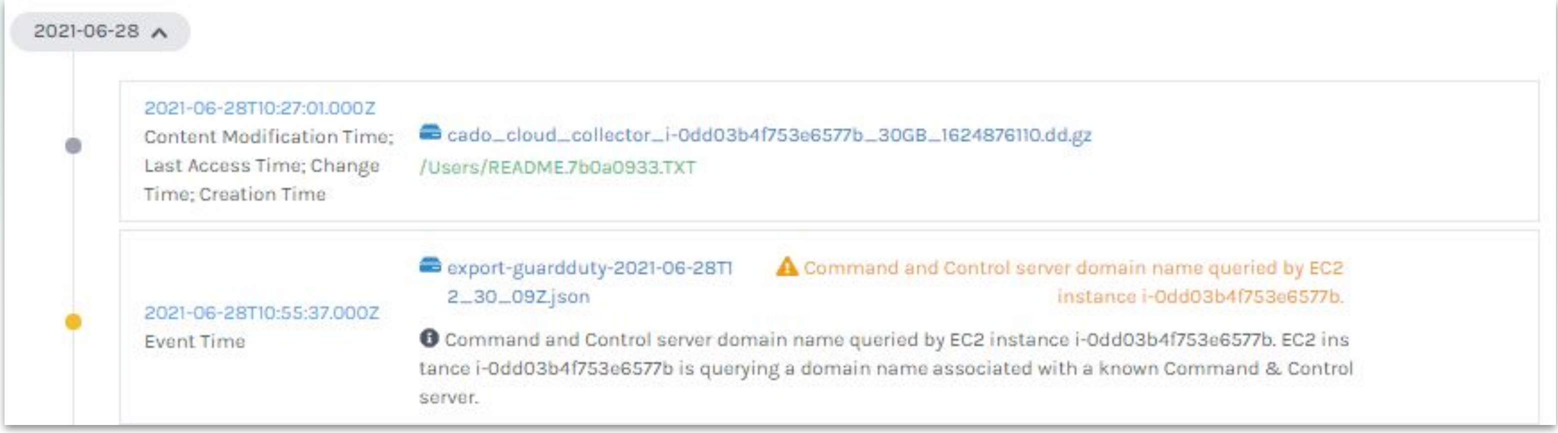


```
[
  {
    "schemaVersion": "2.0",
    "accountId": "493863667xxx",
    "region": "us-west-2",
    "partition": "aws",
    "id": "5ebd292153eb47462d348479c170c26d",
    "arn": "arn:aws:guardduty:us-west-2:493863667531:detector/eebd2668c9064ee1f460d48c77d51ff4/finding/
    5ebd292153eb47462d348479c170c26d",
    "type": "Backdoor:EC2/C&CActivity.B!DNS",
    "resource": {
      "resourceType": "Instance",
      "instanceDetails": {
        "instanceId": "i-0dd03b4f753e65xxx",
        "instanceType": "t3a.2xlarge",
        "launchTime": "2021-06-28T10:17:36Z",
        "platform": "windows",
        "productCodes": [],
        "iamInstanceProfile": null,
        "networkInterfaces": [
          {
            "networkInterfaceId": "eni-0f423e8db6d0101a6",
            "privateIpAddresses": [
              {
                "privateDnsName": "ip-172-31-51-245.us-west-2.compute.internal",
                "privateIpAddress": "172.31.51.245"
              }
            ],
```

☑ △ Backdoor:EC2/C&CActivity.B!DNS

Amazon GuardDuty detections for DarkSide ransomware

As GuardDuty primarily operates at the network level, its detections are somewhat limited; however, these detections can often provide hints of where to look on the disk for more detailed information.



2021-06-28

2021-06-28T10:27:01.000Z
Content Modification Time; Last Access Time; Change Time; Creation Time

cado_cloud_collector_i-0dd03b4f753e6577b_30GB_1624876110.dd.gz
/Users/README.7b0a0933.TXT

2021-06-28T10:55:37.000Z
Event Time

export-guardduty-2021-06-28T12_30_09Z.json

⚠ Command and Control server domain name queried by EC2 instance i-0dd03b4f753e6577b.

Command and Control server domain name queried by EC2 instance i-0dd03b4f753e6577b. EC2 instance i-0dd03b4f753e6577b is querying a domain name associated with a known Command & Control server.

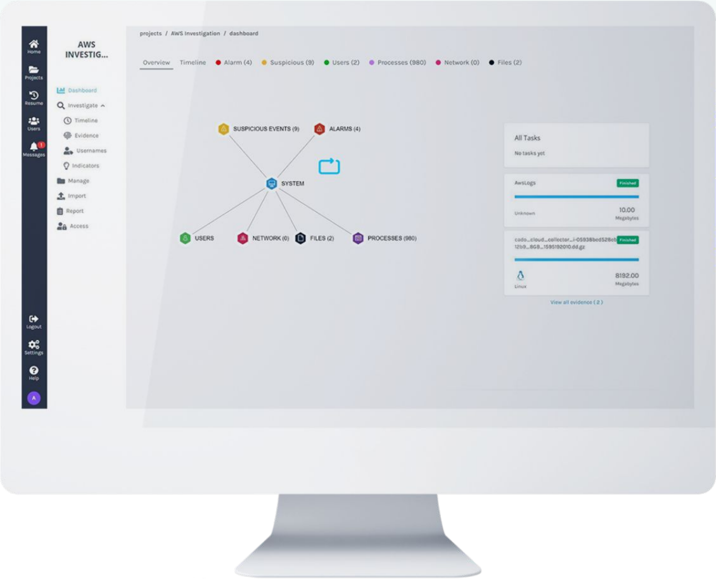
Outside of this, Amazon provides some additional guidance on how to prevent ransomware within AWS. And Microsoft, for mitigating ransomware within Azure.

Response and Remediation

If you're dealing with manually-deployed ransomware, such as DarkSide, you will need to consider a number of steps in your response. Some useful references can be found here, and here. If it's an opportunistic attack, identify the initial method of intrusion and close all gaps. For example, if the initial infection was through an exploit kit, make sure your network is patched against the successful exploit. To ensure timely recovery, it's important that you have off-site data backups and have tested that you can successfully restore the data into a new environment. If this isn't the case, consider how effective your backup strategies are and if they can be improved. In addition, any passwords or credentials used on the infected system should be considered compromised, and reset. Normally the infected system should be wiped and reinstalled after any data for an investigation has been captured. US-CERT provides additional guidance around responding to ransomware.

Cado Response

Cado Response is the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing, security teams can quickly and precisely understand the impact of compromises and respond to data breaches faster. Cado Response enables incident response investigations across cloud environments including short-term data environments such as containers and auto-scaling infrastructures.



Automated Capture

Parallel Processing

Powerful Analytics

Start Free Trial

Cado Security provides the first and only cloud-native digital forensics platform for enterprises. By automating data capture and processing across cloud and container environments, Cado Response enables security teams to efficiently investigate and respond to cyber incidents at cloud speed. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security is based in London. For more information, please visit www.cadosecurity.com or follow us on Twitter @cadosecurity.

CADO//