Wonderland SOC

Incident Investigation Notes

Finding name: Frothly Insider Investigations

Analyst assigned: Robin

Description of System(s)	
Type (Laptop/Desktop/Server/VM/etc.	
System Operating System	
System Name	
System IP Address	
Other hosts involved: Hostname/IP address	

User information (as applicable)	
User(s) involved in incident	
Other user(s) alias involved	

MITRE ATT&CK info	
Tactic / Technique - ID	

Wonderland SOC

Incident Investigation Notes

Investigation Details
1.1.a Physical Security Audit- During the physical security audit, we noted anomalies that should be investigated further by Frothly for individuals Mateo, Richard, and Nathaniel at Thirsty Berner Brewe 1.1.b Chasing Remote Access- During the investigation of remote access, we noted irregularities in location used for Richard Schlitzer's SalesForce credentials. Frothly will need to investigate further. 1.1.c Alarming File System Activity- Ransomware has been identified on Richard Schlitzer's host. F and Wonderland SOC will need to coordinate containment and recovery.

Additional Artifacts

Final Analysis

Wonderland SOC

Incident Investigation Notes

SPL Searches

1.1a Physical Security Audit

```
index=main sourcetype=st_frothly_events reader_desc="THIRSTY*
```Searches for  badge activity from any of the physical readers at Thirsty Berner Brewing```
| stats count by reader_desc employee_first_name employee_job_title
```The "stats count by"creates counts of each reader + employee first name + employee job title combination```
```

```
index=main sourcetype=st_frothly_events reader_desc="THIRSTY_BERNER BREW SUPPLY" event_desc="Access Granted" employee_first_name="*"
| timechart count by employee_first_name limit=10
```The "timechart count by" command works like stats, but timechart will group the events into buckets of time designated by a time span.```
```

```
index=main sourcetype=st_frothly_events event_desc="Access Denied Unauthorized Entry Level" OR event_desc="Access Denied Unauthorized Time" reader_desc="THIRSTY_BERNER BREW SUPPLY"
``` The “OR” operator allows you to search for two types of events descriptions that appear when access is denied.```
| stats count by reader_desc, employee_first_name employee_job_title
```

1.1.b Chasing Remote Access

```
index=main sourcetype="cp_log" user=richards
```

```
index=main sourcetype="cp_log" user="richards"
| iplocation src
| where City!=""
```Using the iplocation command with the src field where the city is not (!=) empty helps us remove events with an empty city.```
| table src City Region Country lat long _time
```The, we build a table and deduplicate logins from the same IP address.```
| dedup src
| sort _time
```Finally, all that data is sorted by time. ```
```

```
index=main source="sfdc_streaming_api_events://login_events" Username="richard@yellowtalon.co"
``` This source shows us the authentication data for SalesForce logins. ```
| iplocation src
```The iplocation command and the argument of “src” will help us access the information about where these logins originated from, based on the IP address. ```
```
```

```
| where City!=""
| table _time Username SourceIp City
| dedup _time
| sort -_time
```

```
index=main (sourcetype="cp_log" OR source="sfdc_streaming_api_events:///login_events")
(user=Richards OR Username="richard@yellowtalon.com")
``` Here we have combined the data sources and username information to capture both the VPN logins and SaleForce logins together. ```
| iplocation src
| where City!=""
| geostats count by City latfield=lat longfield=lon
```

```
index=main (source="sfdc_streaming_api_events://login_events" OR sourcetype="cp_log")
(Username="richard@yellowtalon.co" OR user=richards)
| eval src=coalesce(src,SourceIp)
```The eval command and “coalesce” are used here to map either src from the VPN logins or SourceIp to SalesForce Logins and store it in a field called “src”. You can see a similar operation below for the “user” and “State”. ```
| eval user=coalesce(Username, user)
| iplocation src
| eval State=coalesce(Region, Subdivision)
| where City!=""
| table _time user src City State Country
| dedup _time
| sort -_time
```

1.1.c Alarming File System Activity

```
index=dtex sourcetype=dtex_st_activities Activity_Group=FileSystemActivity
```