2SECURE safeguarding your data | Fu SIEM THE KUNG FU SIEM

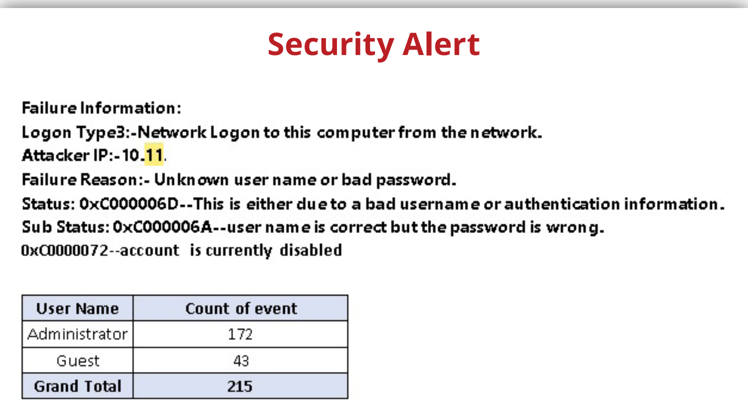
CASE STUDY: IoT DEVICE BRUTE-FORCE ATTACK DETECTION & RESPONSE

Preface

The adoption of IoT devices is a known security risk which ALL companies should address before introducing such devices into its corporate network, since these devices are much less secure.

The Case

Our monitoring tools detected intrusion attempts from an IoT device. These attempts are called brute-force attacks, and are characterized by having an attacker attempt to guess account credentials by using hundreds of possible passwords. In our case, an attacker was trying to obtain the correct passwords for the Administrator and Guest accounts. An alert was triggered by our monitoring tool, and our SoC team immediately contacted the IT Manager to confirm the activity. We were able to mitigate the attack before the brute-force attacker was able to successfully log in.



Security Alert

```
Failure Information:
Logon Type3:-Network Logon to this computer from the network.
Attacker IP:-10.11.
Failure Reason:- Unknown user name or bad password.
Status: 0xC000006D--This is either due to a bad username or authentication information.
Sub Status: 0xC000006A--user name is correct but the password is wrong.
0xC0000072--account  is currently disabled
```

User Name	Count of event
Administrator	172
Guest	43
Grand Total	215

In Conclusion

The client has achieved better security, and has discovered that our security systems are highly effective in preventing hackers from breaking into corporate computers and other systems.

2SECURE safeguarding your data

About 2 Secure

2Secure is a Cyber Security firm which takes a PROACTIVE approach to solving network security problems. We provide the right strategy, people, and tools to fix problems the first time around – in fact, we guarantee it!