INCIDENT RESPONSE

GROUP MEMBERS:-

BASIL PAUL

PAUL JOSE

MANIKYA CHAUDHARY

RDP BRUTE FORCE – INCIDENT RESPONSE SIMULATION

ROLES & RESPONSIBILITIES

- Incident Response Manager: **Manikya Chaudhary**
- Security Analyst: **Paul Jose**
- IT Specialist: **Basil Paul**
- Legal/Compliance Officer
- Communication Officer

ALERT!!

- **High April 11, 2024, 01:51 PM SOC210 - Possible Brute Force Detected on VPN 162 Brute Force**

EventID : 162
Event Time : April 11, 2024, 01:51 PM
Rule : SOC210 - Possible Brute Force Detected on VPN
Level : Security Analyst
Source Address : 37.19.221.229
Destination Address : 33.33.33.33
Destination Hostname : ABC123
Username : sfarooq@conestogac.on.ca
Alert Trigger Reason :
A successful VPN login was detected shortly after failed login attempts from the same source IP address

PREPARATION

- Identification & documentation of all assets to be protected.
- Identification & documentation of all known relevant threats, vulnerabilities, and indicators of compromise.
- Development of incident response procedures.
- Training IR team members and assessing incident response capabilities.
- Assessment of incident response procedures.
- Preparation of Cyber Security Incident Response Team including technical, legal counsel, and communication experts to respond to an incident.
- Policy and procedures should be routinely assessed by the compliance team to ensure compliance.

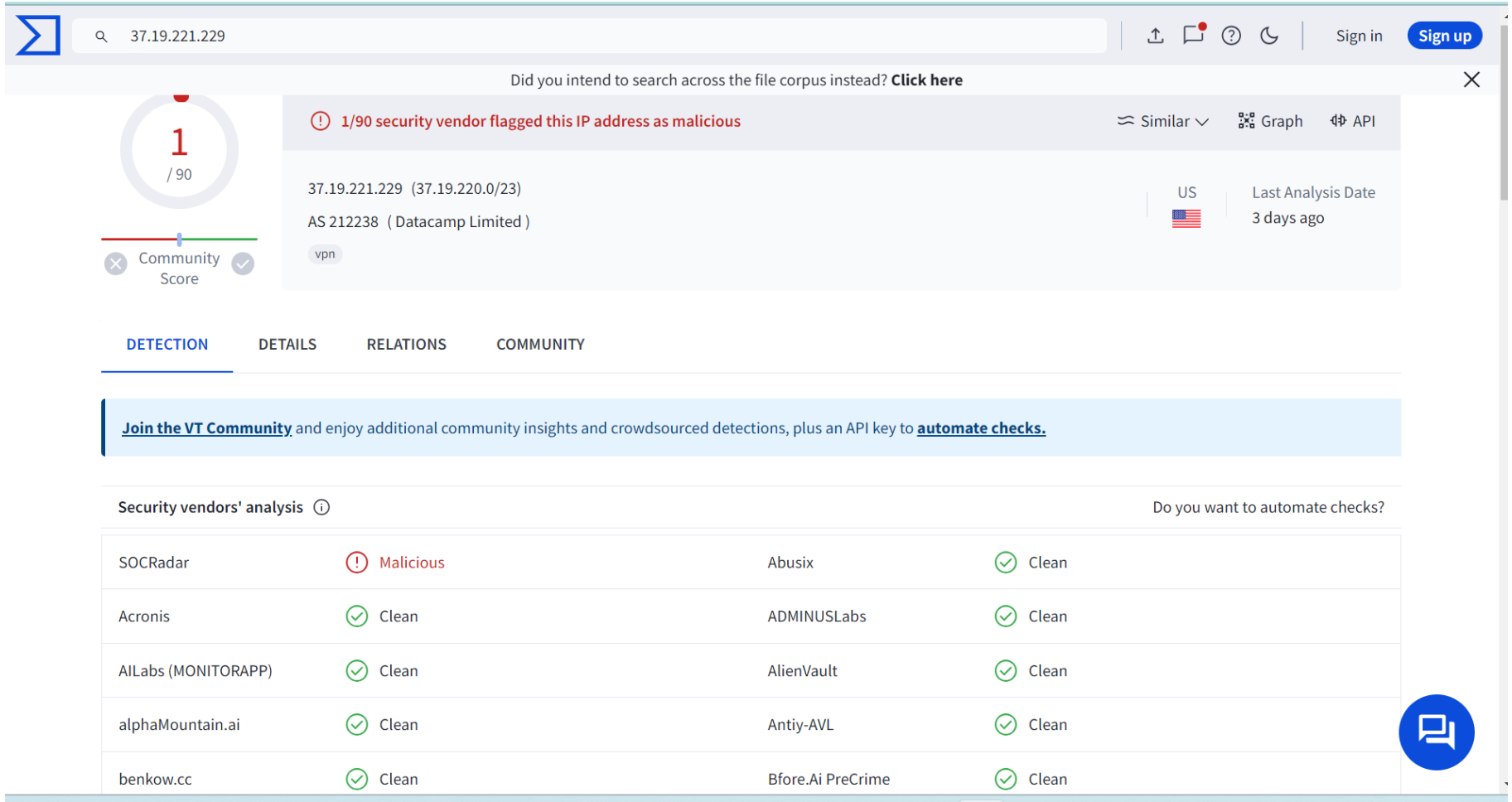
PHASE 1: DETECTION AND ANALYSIS

- **Security Analyst:**

1. **Alerts:**
    - **Continuously monitor the SIEM (Security Information and Event Management) system for alerts.**
    - **Identify any suspicious patterns related to RDP login attempts (e.g., multiple failed logins from the same IP address).**
    - **Mitre Att&ck Technique – Credential Access**

- **IR Manager:**

1. **Incident Coordination:**
    - **Assemble the incident response team.**
    - **Ensure clear communication channels among team members.**
    - **Approve escalation of the incident.**
    - **Impact Assessment**


37.19.221.229
Sign in
Sign up
Did you intend to search across the file corpus instead? Click here
1
/ 90
Community Score
1/90 security vendor flagged this IP address as malicious
Similar
Graph
API
37.19.221.229 (37.19.220.0/23)
AS 212238 (Datacamp Limited)
vpn
US
Last Analysis Date
3 days ago
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
SOCRadar Malicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
alphaMountain.ai Clean
Antiy-AVL Clean
benkow.cc Clean
Bfore.Ai PreCrime Clean

PHASE EXIT CRITERIA

- The Event is confirmed to be an Incident.
- Category, Scope & Impact Assessment is complete.
- Required parties are informed (e.g. authorities).
- All Incident-related is information is collected & documented.

PHASE 2: CONTAINMENT

- **Security Analyst:**

1. **Isolation:**
    - **Block RDP Traffic:**
        - **Configure network devices (firewalls, routers) to block RDP traffic to the affected server.**
    - **Account Disabling:**
        - **Disable compromised user accounts associated with suspicious login attempts.**

- **IT Specialist:**

1. **Temporary RDP Service Disabling:**
    - **Temporarily disable RDP services on the affected server to prevent further unauthorized access.**

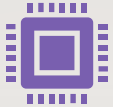
- **Legal Compliance Officer:**

1. **Data Protection Compliance**:
    - Ensure compliance with data protection laws during containment.
    - Review privacy policies and legal obligations related to data breach notification.
    - Ensures preservation of forensics-related information.

PHASE EXIT CRITERIA

- Affected assets are identified.
- Threat is isolated and contained (is unable to spread and cause further damage).
- Forensics-relevant information has been preserved, documented, and collected.
- Incident documentation is updated with information from the containment phase.

PHASE 3: ERADICATION



IT Specialist:

Password Changes and Patching:

- Change passwords for all accounts on the affected server.
- Apply necessary security patches to address vulnerabilities exploited during the attack.

Security Analyst:

System Scan:

- Conduct a thorough system scan using security tools (antivirus, anti-malware) to identify any remaining threats.
- Remove any malicious files or backdoors.

IR Manager:

System Reconfiguration Approval:

- Review the eradication efforts.
- Approve the reconfiguration of the affected system.

PHASE EXIT CRITERIA

- Root cause has been identified and vulnerabilities have been remediated.
- Threat has been removed from infrastructure.
- Infrastructure has been updated/amended to be immune to the same attack.
- Incident documentation is updated with information from the eradication phase.

PHASE 4: RECOVERY

- **IT Specialist:**

1. **Service Restoration**:
    - Restore RDP services on the affected server after implementing security measures.
    - Monitor logs for any anomalies or signs of reinfection.

- **Communication Officer:**

1. **Communication Preparation**:
    - Prepare internal and external communication regarding the incident and recovery progress.
    - Draft notifications for stakeholders (employees, customers, regulatory bodies).

PHASE EXIT CRITERIA

- Business operations have been restored to optimal levels.

PHASE 5: POST-INCIDENT ACTIVITIES & LESSONS LEARNED

IR Manager:

1. **Post-Incident Review**:
    - Conduct a meeting with the incident response team.
    - Document lessons learned, including what worked well and areas for improvement.
    - Update incident response procedures based on insights from the incident.

Legal Compliance Officer:

1. **Legal Procedure Review**:
    - Review incident handling procedures for legal compliance.
    - Ensure alignment with relevant laws and regulations.

Security Analyst:

1. **Rule Updates**:
    - Update detection rules based on insights gained during the incident.
    - Enhance monitoring capabilities to prevent similar incidents in the future.

PHASE EXIT CRITERIA

- How did the cyber-attack happen?
- How well did staff and management perform in dealing with the incident?
- What would the staff and management do differently the next time a similar incident occurs?
- Any novel precursors or indicators should be watched for in the future to detect similar incidents?

REFERENCES

GETTING STARTED TO LETSDEFEND. (N.D.). HTTPS://APP.LETSDEFEND.IO/MONITORING

THANK YOU!