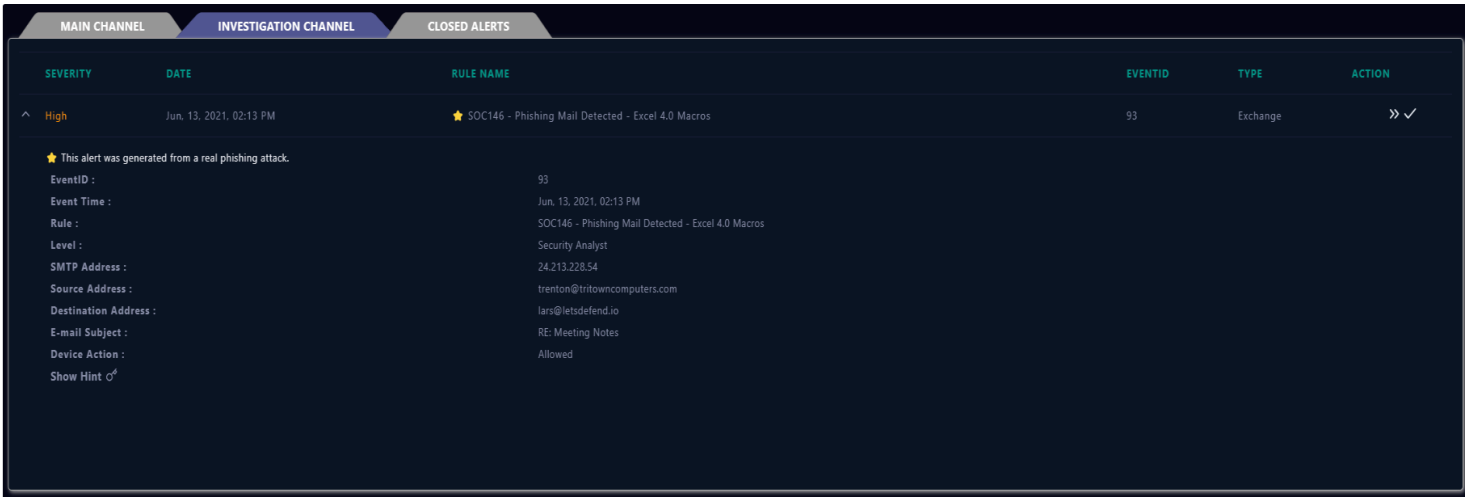
EventID@93 - SOC146 - Phishing Mail Detected - Excel 4.0 Macros

1. Alert Overview

- **Alert Name:** SOC146 - Phishing Mail Detected - Excel 4.0 Macros
- **Alert Source:** Exchange / Email Security System
- **Alert Severity:** High
- **Event ID:** 93
- **Event Time:** June 13, 2021, 02:13 PM
- **Detection Rule:** SOC146 - Phishing Mail Detected - Excel 4.0 Macros
- **Analyst Level:** Security Analyst

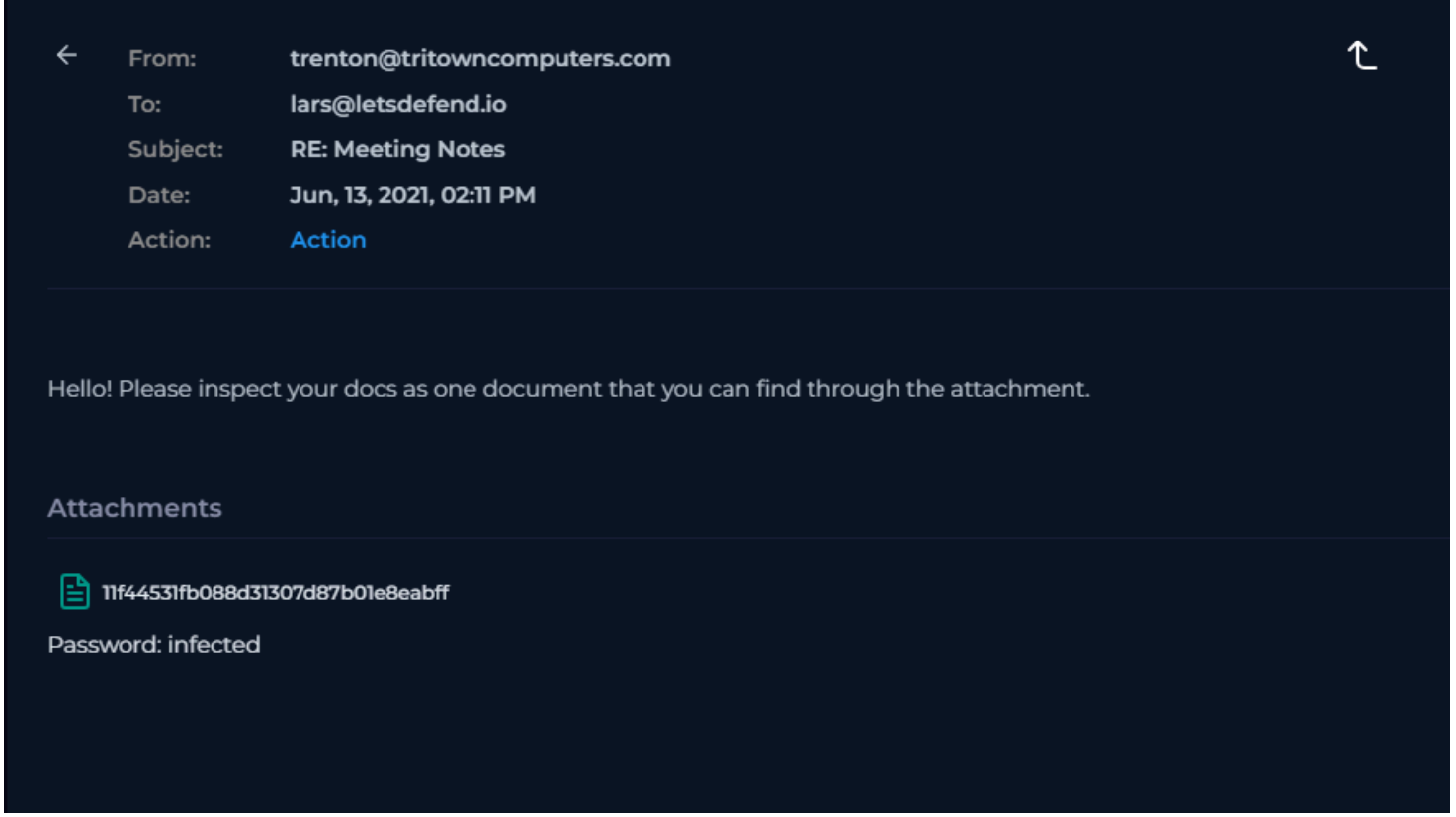


---

2. Initial Alert Details

This alert was generated when a phishing email containing a attachment was detected, a known technique used by attackers to deliver payloads to initiate further compromise.

- **SMTP Address:** 24.213.228.54
- **Source Address:** trenton@tritowncomputers.com
- **Destination Address:** lars@letsdefend.io
- **Email Subject:** RE: Meeting Notes
- **Device Action:** Allowed



---

3. Investigation Steps

- **Email Inspection**
  The phishing email was received on **June 13, 2021, at 02:11 PM**.

Email Details:

- **SMTP Address:** 24.213.228.54
- **Sender:** `trenton@tritowncomputers[.]com`
- **Recipient:** `lars@letsdefend[.]io`
- **Subject:** `RE: Meeting Notes`
- **Attachment:** `11f44531fb088d31307d87b01e8eabff.zip`
- **Action:** Allowed (email delivered to user)

The email content appeared suspicious due to its poor grammar and the presence of a **single attachment** with no meaningful body text — a typical indicator of phishing.

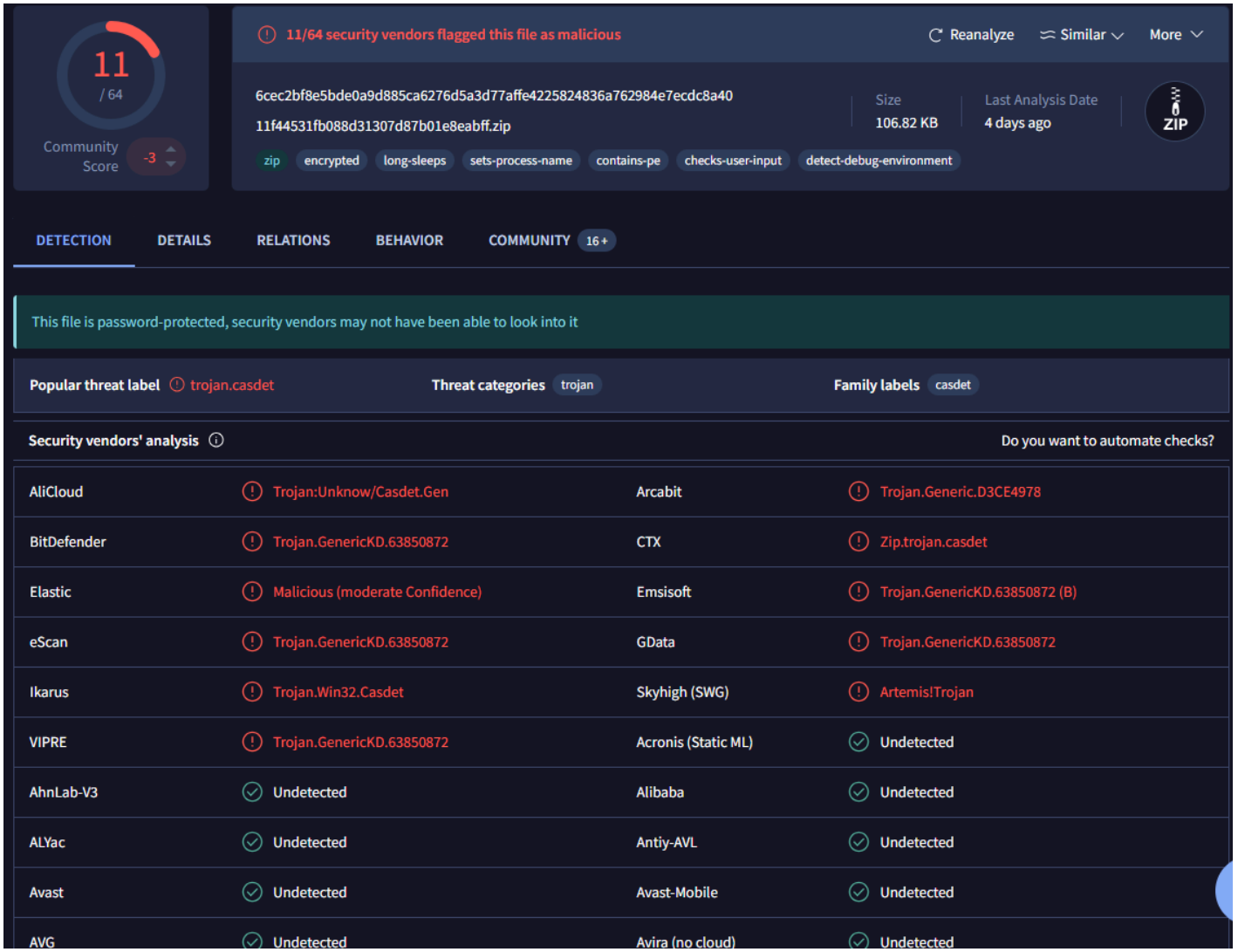
- **Attachment Analysis**
  We downloaded the attachment `11f44531fb088d31307d87b01e8eabff.zip` for further examination in a **secure isolated environment** using **Remnux Linux**, a distribution built for malware analysis and reverse engineering.

Attachment Hash:
`SHA256: 6CEC2BF8E5BDE0A9D885CA6276D5A3D77AFFE4225824836A762984E7ECDC8A40`

VirusTotal Results:

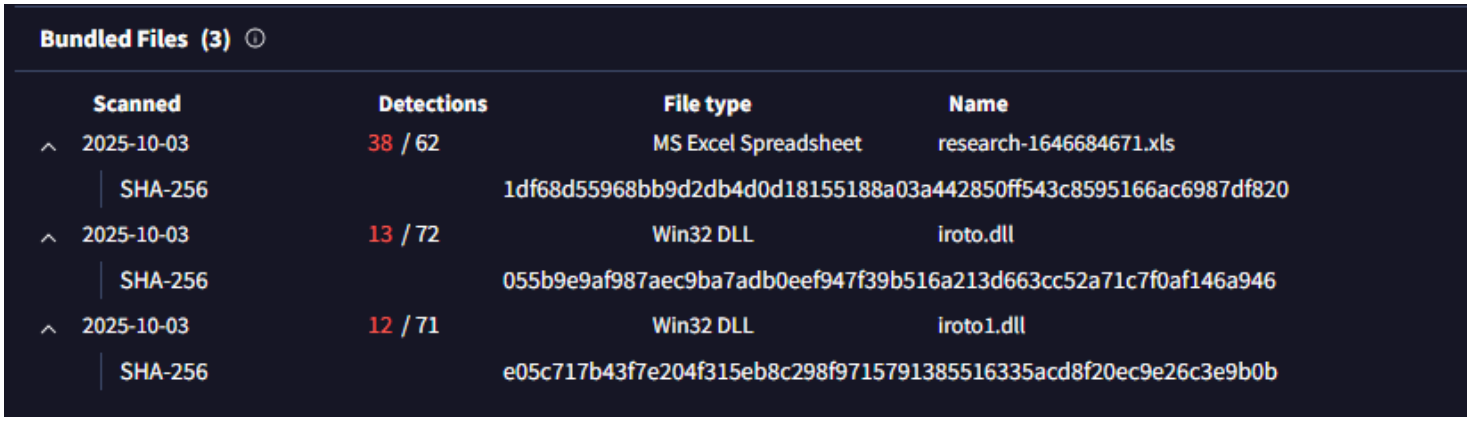
- 11 out of 63 antivirus engines flagged the file as **malicious**.

- VirusTotal Analysis Link



Unzipped Contents:

`research-1646684671.xls iroto.dll iroto1.dll`

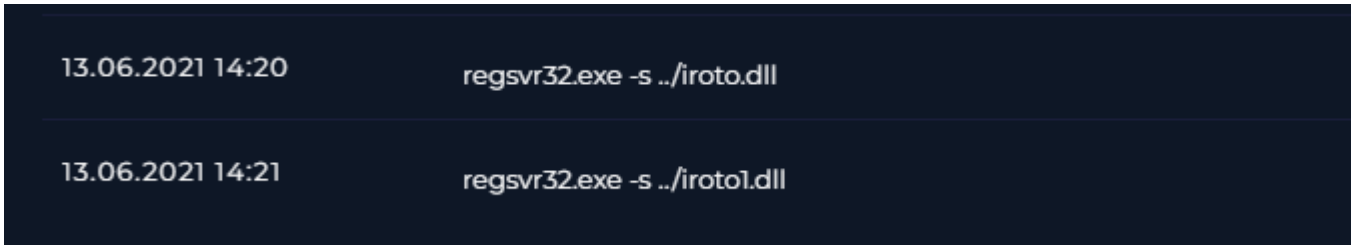


- **Sandbox Analysis**
  We used multiple dynamic analysis platforms to confirm the malicious nature of the extracted files:
- AnyRun Report
- VirusTotal Report
- Hybrid Analysis Report

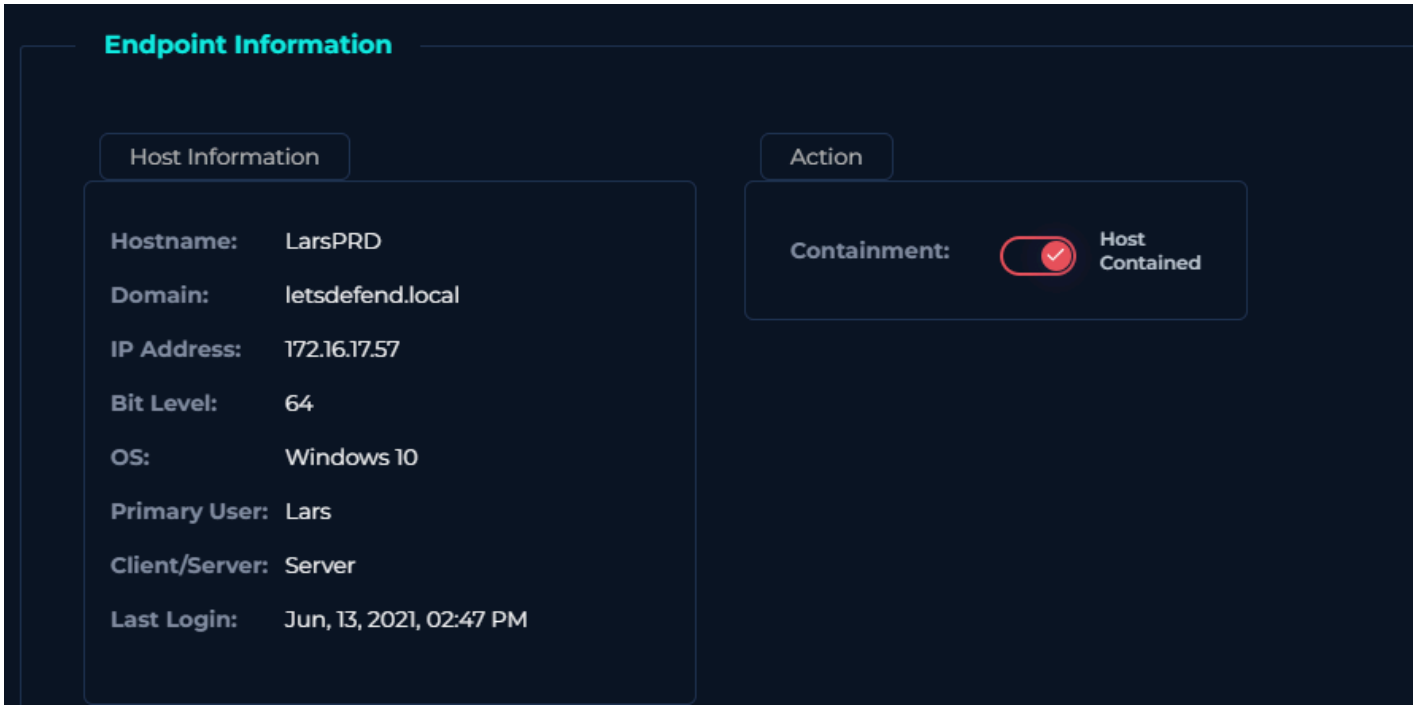
  Findings:
- The Excel file is equipped with **malicious macros** that automatically download and execute external payloads.
- It attempts to **register DLLs** using `regsvr32.exe`, a known LOLBin often abused by attackers.

  Observed Commands Executed:

`regsvr32.exe -s ../iroto.dll` regsvr32.exe -s ../iroto1.dll`



- **Host and Network Indicators**
  Affected Host:
- **Hostname:** `LarsPRD`
- **IP Address:** `172[.]16[.]17[.]57`



After executing the malicious file, the host established outbound connections to the following URLs:

`https[:]//royalpalm[.]sparkblue[.]lk/vCNhYrq3Yg8/dot[.]html`
`https[:]//nws[.]visionconsulting[.]ro/N1G1KCXA/dot[.]html`

From above all this we can say that the phishing email was successfully delivered to the recipient's mailbox (`lars@letsdefend.io`) and Connection logs confirm the infected host (`172.16.17.57`) reached out to the malicious infrastructure shortly after the email was received, verifying that **the user opened the Excel file**, triggering the macro execution.

---

4. Investigation Artifacts

- trenton@tritowncomputers[.]com – Source Email Address
- lars@letsdefend[.]io – Destination Email Address
- 24[.]213[.]228[.]54 – SMTP Address
- 172[.]16[.]17[.]57 – LarsPRD Machine
- b775cd8be83696ca37b2fe00bcb40574 – MD5 Hash of the Excel File
- 188[.]209[.]214[.]83 – Contacted Host
- 188[.]213[.]19[.]81 – Identified C2 IP Address

- https://royalpalm[.]sparkblue[.]lk/vCNhYrq3Yg8/dot.html – Contacted URL
- https://nws[.]visionconsulting[.]ro/N1G1KCXA/dot.html – Contacted URL
- 192[.]232[.]219[.]67 – DNS Request

---

5. Response & Remediations

Immediate Action:

- Quarantined and deleted the email from user inboxes.
- Blocked sender domain and associated IP addresses.
- Implemented URL filtering for the identified malicious URLs.
- Disabled Excel 4.0 macros organization-wide.
  Recommended Next Steps:
- Conduct endpoint scan on `LarsPRD` to identify residual artifacts.
- Update detection rules to monitor for `regsvr32.exe` macro-related activity.
- Enhance user training on identifying phishing attempts.

6. MITTRE ATT&CK Mapping

Tactic	Technique	ID
Initial Access	Phishing: Spearphishing Attachment	**T1566.001**
Execution	User Execution: Malicious File	**T1204.002**
Defense Evasion	Signed Binary Proxy Execution (regsvr32)	**T1218.010**

7. Lessons Learned

- Even older attack vectors like **Excel 4.0 macros** remain active in phishing campaigns.
- End-user awareness and secure attachment handling are crucial.
- Regular sandbox analysis and hash reputation checks are effective validation measures.
