

# 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

MAIN CHANNEL		INVESTIGATION CHANNEL		CLOSED ALERTS		
SEVERITY	DATE	RULE NAME		EVENTID	TYPE	ACTION
^ High	Jun. 13, 2021, 02:13 PM	★ SOC146 - Phishing Mail Detected - Excel 4.0 Macros		93	Exchange	» ✓
★ This alert was generated from a real phishing attack.						
EventID :		93				
Event Time :		Jun. 13, 2021, 02:13 PM				
Rule :		SOC146 - Phishing Mail Detected - Excel 4.0 Macros				
Level :		Security Analyst				
SMTP Address :		24.213.228.54				
Source Address :		trenton@tritowncomputers.com				
Destination Address :		lars@letsdefend.io				
E-mail Subject :		RE: Meeting Notes				
Device Action :		Allowed				
Show Hint Ⓞ						

## 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](mailto:trenton@tritowncomputers.com)
- **Destination Address:** [lars@letsdefend.io](mailto:lars@letsdefend.io)
- **Email Subject:** RE: Meeting Notes
- **Device Action:** Allowed

← From: trenton@tritowncomputers.com  
To: lars@letsdefend.io  
Subject: RE: Meeting Notes  
Date: Jun, 13, 2021, 02:11 PM  
Action: [Action](#)



Hello! Please inspect your docs as one document that you can find through the attachment.

#### Attachments

 11f44531fb088d31307d87b01e8eabff

Password: infected

## 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](#)

11  
/ 64

Community Score -3

11/64 security vendors flagged this file as malicious

Reanalyze Similar More

6cec2bf8e5bde0a9d885ca6276d5a3d77affe4225824836a762984e7ecdc8a40

Size 106.82 KB

Last Analysis Date 4 days ago

ZIP

11f44531fb088d31307d87b01e8eabff.zip

zip encrypted long-sleeps sets-process-name contains-pe checks-user-input detect-debug-environment

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 16+

This file is password-protected, security vendors may not have been able to look into it

Popular threat label trojan.casdet

Threat categories trojan

Family labels casdet

Security vendors' analysis ⓘ

Do you want to automate checks?

AliCloud	<span>!</span> Trojan:Unknow/Casdet.Gen	Arcabit	<span>!</span> Trojan.Generic.D3CE4978
BitDefender	<span>!</span> Trojan.GenericKD.63850872	CTX	<span>!</span> Zip.trojan.casdet
Elastic	<span>!</span> Malicious (moderate Confidence)	Emsisoft	<span>!</span> Trojan.GenericKD.63850872 (B)
eScan	<span>!</span> Trojan.GenericKD.63850872	GData	<span>!</span> Trojan.GenericKD.63850872
Ikarus	<span>!</span> Trojan.Win32.Casdet	Skyhigh (SWG)	<span>!</span> Artemis!Trojan
VIPRE	<span>!</span> Trojan.GenericKD.63850872	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Alibaba	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Avast	✓ Undetected	Avast-Mobile	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected

Unzipped Contents:

research-1646684671.xls iroto.dll iroto1.dll

Bundled Files (3) ⓘ			
Scanned	Detections	File type	Name
^ 2025-10-03	38 / 62	MS Excel Spreadsheet	research-1646684671.xls
SHA-256	1df68d55968bb9d2db4d0d18155188a03a442850ff543c8595166ac6987df820		
^ 2025-10-03	13 / 72	Win32 DLL	iroto.dll
SHA-256	055b9e9af987aec9ba7adb0eef947f39b516a213d663cc52a71c7f0af146a946		
^ 2025-10-03	12 / 71	Win32 DLL	iroto1.dll
SHA-256	e05c717b43f7e204f315eb8c298f9715791385516335acd8f20ec9e26c3e9b0b		

• **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 ../irototo.dll regsvr32.exe -s ../irototo1.dll`
```

13.06.2021 14:20

regsvr32.exe -s ../irototo.dll

13.06.2021 14:21

regsvr32.exe -s ../irototo1.dll

- **Host and Network Indicators**

**Affected Host:**

- **Hostname:** LarsPRD
- **IP Address:** 172[.]16[.]17[.]57

**Endpoint Information**

Host Information

**Hostname:** LarsPRD  
**Domain:** letsdefend.local  
**IP Address:** 172.16.17.57  
**Bit Level:** 64  
**OS:** Windows 10  
**Primary User:** Lars  
**Client/Server:** Server  
**Last Login:** Jun, 13, 2021, 02:47 PM

Action

**Containment:** ☒ Host Contained

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](https://royalpalm[.]sparkblue[.]lk/vCNhYrq3Yg8/dot.html) – Contacted URL
  - [https://nws\[.\]visionconsulting\[.\]ro/N1G1KCXA/dot.html](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	<b>T1566.001</b>
Execution	User Execution: Malicious File	<b>T1204.002</b>
Defense Evasion	Signed Binary Proxy Execution (regsvr32)	<b>T1218.010</b>

## 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.
-