Sophisticated Email Phishing Detection and Prevention

Leveraging Opensource Deception, SIEM, SOAR, Threat Intel

All trademarks, logos, and brand names are the property of their respective owners.
PHISHING
A Game of Deception
Phishing – A Game of Deception

The first half of 2021 shows a 22% increase in the volume of Phishing Attacks over the same time period last year.

97% of the Users are unable to recognize a sophisticated Phishing Email.

75% of organizations around the world experienced some kind of Phishing Attack in 2020.

"Infopercept Proprietary Material. Please do not copy or distribute."
Spam and phishing in Q1 2021

Geography of phishing attacks

Organizations under attack

Source: https://securelist.com/spam-and-phishing-in-q1-2021/102018/
1. Attacker sends email

2. Victim clicks on link in the email and goes to malicious website

3. Attacker collects victims credentials

4. Attackers uses victims credentials to access website
Email with attachment

1. Adversaries sends phishing emails with attachment.

2. Victim opens the email and downloads the attachment.

3. Attachment contains Malware. The Malware downloads malicious files.

4. The malicious code encrypts the files.
Secure Email Gateway is NOT that Secure

Attacker

- Zero Day Attack
- Business Compromise Email Attack
- Signature-less threat
- Internal email threat

Email Security Gateway

Email Service

"Infopercept Proprietary Material - Please do not copy or distribute"
We start with Email security to prevent usual phishing attacks. Where phishing gets sophisticated and smart with deception, we also make our anti-phishing approach smart with deception.
Next Gen Managed SOC

1. Personalized Threat Intelligence
2. Detection
3. Prevention
How we work?

We create social media decoy using real company details and email id as a deception for attackers.

E.g.: abc@example.com

Adversaries get phished with our deception to launch their phishing attack using the decoy email id.

Office 365

Notification

DejaVu

Deception Monitoring

WAZUH

SOC Monitoring

Firewall

Action

Email Security Gateway

Action

MISP

Threat Intelligence- Exchange of IOCs

SOAR – Orchestration and Automation

“Infopercept Proprietary Material - Please do not copy or distribute.”
Steps

1. We Create One Email Address in Our Email Address like: stevend@example.com or stevend@myexample.com

2. We Create that user Social Media Account
### Decoy Management

#### Manage Decoys

<table>
<thead>
<tr>
<th>Decoy Name</th>
<th>Network Location</th>
<th>Interface</th>
<th>Services</th>
<th>IP Address</th>
<th>Apache files</th>
<th>SMB files</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Image of a dashboard interface with a table for managing decoys.*
Now we are adding to Email Client Decoy

Go to Decoy Management and Click on Add Client Decoy and Select the Email Client

"Infopercept Proprietary Material - Please do not copy or distribute"
Now we are adding to Email Client Decoy

Once Fill This All-Required Details Click on Save Button and See next Slid for Decoy IP Address Settings

After Click Email Client the Email Decoy Settings Box Pop-up Automatically
Now we are adding to Email Client Decoy

Once All Settings are Done Click on Submit Button to save this Decoy in Dejavu Engine – after Click On Submit it will take 20 Sec Time to Update Decoy Settings
Now you can see we added Email Client Decoy go to Decoy Management

The Click to Manage Decoy you can See the Added Decoy List in Left Side Decoy Management Page.
Now you can see the below image that is Dejavu Console

Page to See the Active Attacks – as of now we don’t have any Active Attack Logs on Console
Now I am Sending an Email to 
Stevend@myexmaple.com user for Phishing Purpose.
user mailbox is Empty no any Emails Are There
You see that phishing email address is showing to Dejavu Attacks logs. For details logs and see the email content you need to click View Logs.
### Email Phishing Client Detail Logs

If you want to see that phishing Email Content the click on Envelop icon and Download the email

<table>
<thead>
<tr>
<th>Decoy Name</th>
<th>Network Location</th>
<th>Service Deployed</th>
<th>Event Type</th>
<th>Decoy IP</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailClient045</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: Kalpesh Panchal <a href="mailto:kalpesh.panchal@infopercept.com">kalpesh.panchal@infopercept.com</a> TO: <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: Credit Card Payment</td>
<td>10.10.3.50</td>
<td>2021-10-03 12:28:03</td>
</tr>
<tr>
<td>EmailClient045</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:security@facebook.com">security@facebook.com</a> TO: Steven Dall <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: Facebook primary email address changed</td>
<td>10.10.3.50</td>
<td>2021-10-03 11:14:05</td>
</tr>
<tr>
<td>EmailClient045</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:registration@facebook.com">registration@facebook.com</a> TO: Steven Dall <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: Welcome to Facebook</td>
<td>10.10.3.50</td>
<td>2021-10-03 11:14:05</td>
</tr>
<tr>
<td>EmailClient045</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:registration@facebook.com">registration@facebook.com</a> TO: Steven Dall <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: FB-67461 is your Facebook confirmation code</td>
<td>10.10.3.50</td>
<td>2021-10-03 11:14:05</td>
</tr>
</tbody>
</table>
Now I am Sending an Email to Stevend@myexample.com user for Phishing Purpose

Note: this Logs We Triger on WAZUH SIEM TOOL
Phishing Email Alert on Dejavu Console

Dejavu Console

Filter Logs

Show 10 entities

<table>
<thead>
<tr>
<th>Decoy Name</th>
<th>Network Location</th>
<th>Service Deployed</th>
<th>Event Type</th>
<th>Decoy IP</th>
<th>Attacker IP</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: Kalpesh Panchal <a href="mailto:kalpeshinfoot@gmail.com">kalpeshinfoot@gmail.com</a> TO: <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: WAZIH LOGS - CISCO</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-07</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: Kalpesh Panchal <a href="mailto:kalpeshinfoot@gmail.com">kalpeshinfoot@gmail.com</a> TO: <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: TEST - YASH</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-06</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: Kalpesh Panchal <a href="mailto:kalpeshinfoot@gmail.com">kalpeshinfoot@gmail.com</a> TO: <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: TEST AWS CONSOLE</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-06</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:securityfacebook@me.com">securityfacebook@me.com</a> TO: Steven <a href="mailto:Dell@infopercept.com">Dell@infopercept.com</a> SUBJECT: Heres an easy way to log in to Facebook</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-04</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: Kalpesh Panchal <a href="mailto:kalpeshinfoot@gmail.com">kalpeshinfoot@gmail.com</a> TO: <a href="mailto:steven@infopercept.com">steven@infopercept.com</a> SUBJECT: Credit Card Payment</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-03</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:securityfacebook@me.com">securityfacebook@me.com</a> TO: Steven <a href="mailto:Dell@infopercept.com">Dell@infopercept.com</a> SUBJECT: Facebook primary email address changed</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-03</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:securityfacebook@me.com">securityfacebook@me.com</a> TO: Steven <a href="mailto:Dell@infopercept.com">Dell@infopercept.com</a> SUBJECT: Welcome to Facebook</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-03</td>
</tr>
<tr>
<td>EmailClient645</td>
<td>StaffNetwork</td>
<td>EMAILCLIENT</td>
<td>Email Received: FROM: &quot;Facebook&quot; <a href="mailto:securityfacebook@me.com">securityfacebook@me.com</a> TO: Steven <a href="mailto:Dell@infopercept.com">Dell@infopercept.com</a> SUBJECT: FB-6749s is your Facebook confirmation code</td>
<td>10.10.3.50</td>
<td></td>
<td>2021-10-03</td>
</tr>
</tbody>
</table>

Showing 1 to 8 of 8 entries

"Infopercept Proprietary Material - Please do not copy or distribute"
WAZUH – Dashboard Alert

Elastic

Dashboard Editing Dejavu (unsaved)

Options Share Add Cancel Save Reporting

Search

KQL Last 24 hours

Show dates Refresh

Decoy-Failed-Login

<table>
<thead>
<tr>
<th>data.servicetype: Descending</th>
<th>decoder.name: Descending</th>
<th>data.eventtype: Descending</th>
<th>Failed Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>dejaVu,decoder</td>
<td>Failed Authentication for username &quot;kalpesh&quot; using password &quot;kalpesh&quot;</td>
<td>2</td>
</tr>
<tr>
<td>SSH</td>
<td>dejaVu,decoder</td>
<td>Failed Authentication for username &quot;cisco&quot; using password &quot;amtam&quot;</td>
<td>1</td>
</tr>
<tr>
<td>SSH</td>
<td>dejaVu,decoder</td>
<td>Failed Authentication for username &quot;kalpesh&quot; using password &quot;**&quot;</td>
<td>1</td>
</tr>
<tr>
<td>SSH</td>
<td>dejaVu,decoder</td>
<td>Failed Authentication for username &quot;kalpesh&quot; using password &quot;cisco&quot;</td>
<td>1</td>
</tr>
<tr>
<td>SSH</td>
<td>dejaVu,decoder</td>
<td>Failed Authentication for username &quot;kalpesh&quot; using password &quot;lcp&quot;</td>
<td>1</td>
</tr>
</tbody>
</table>
| RDP                         | dejaVu,decoder          | RDP Request: Input = asicdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasdasda...
## WAZUH – Phishing Email Event Log

The image shows a screenshot of the WAZUH platform with a focus on a specific event log related to phishing emails. The log details an email that was sent on October 7, 2021, with the sender's email address being "kalavala.panci@gmail.com". The log entry indicates that the email was identified as a phishing attempt.

### Expanded Document

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>agent.id</code></td>
<td>WEB</td>
</tr>
<tr>
<td><code>agent.name</code></td>
<td>stewart.com</td>
</tr>
<tr>
<td><code>data.tid</code></td>
<td>1638023901.S01</td>
</tr>
<tr>
<td><code>data.decodetype</code></td>
<td>EMAILDECOD</td>
</tr>
<tr>
<td><code>data.eventtype</code></td>
<td>Email Phishing: FROM: Kalavala Panci</td>
</tr>
<tr>
<td><code>data.decrypted</code></td>
<td></td>
</tr>
<tr>
<td><code>data.service</code></td>
<td>EMAIL/CLIENT</td>
</tr>
<tr>
<td><code>decoder.name</code></td>
<td></td>
</tr>
<tr>
<td><code>data.decryptedsize</code></td>
<td>45926 bytes</td>
</tr>
<tr>
<td><code>data.encryptedsize</code></td>
<td>45926 bytes</td>
</tr>
<tr>
<td><code>data.TID</code></td>
<td>1638023901.S01</td>
</tr>
<tr>
<td><code>data.service</code></td>
<td>EMAIL/CLIENT</td>
</tr>
</tbody>
</table>

The screenshot also includes a view of the WAZUH interface, highlighting the module and showing the event log details.
WAZUH SIEM – SHUFFLE SOAR Integration through Webhook

```
<integration>
<name>custom-shuffle</name>
<hook_url>https://10.0.3.241:3443/api/v1/hooks/webhook_5c9c65db-1028-4a05-afb5-2fd039c11e2e</hook_url>
<rule_id>100012</rule_id>
>alert_format>json</alert_format>
</integration>
```

Wazuh SIEM Integration with Shuffle SOAR for automated playbook to be executed for blocking the IP Address
How Playbook would work?

1. DeJavu triggers an alert and send it to Wazuh SIEM through syslog configuration.
2. Integration of Wazuh SIEM done with Shuffle.
3. When an alert triggers in Wazuh from Deception Email Client it will trigger the Shuffle Workflow.
4. Start analysis of the email header and ip Address.
5. Push the IP address to MISP Threat Exchange Database for future reference and mark as blacklisting.
6. Create a case in Case Management Tool.
7. Block IP Address in Email Security Gateway and Firewall.
For cybersecurity to have upper hand, attacker sense is the most important approach. Like anti-phishing, in every counter, attackers' tactics can be used to design and execute a proactive cybersecurity. Open source cybersecurity innovations help to leverage attacker intelligence to prepare counter cybersecurity intelligence.
Automatic Incidence Response for Anti-Phishing Leveraging Deception

1. OBSERVE
   - Social Media Decoy
     - Email Decoy
   - Wazuh SIEM
   - DejaVu
     - On Sending Email on Decoy
   - WAZUH
   - Shuffle
     - Webhook
   - API

2. ORIENT
   - Personalized Threat Intelligence Gathering
     - Check Reputations
     - Check Existing DB
   - MISP
     - Threat Sharing

3. DECIDE
   - Case Management for SOC Team
     - Notification ➔ SMS, Email
     - Notification ➔ Email
     - Open Ticket ➔ Ticket

4. ACT
   - Block IOC in Email
   - Block IP in Network
   - Firewall
   - Security Gateway

"Infopercept Proprietary Material - Please do not copy or distribute"
Thank You