# Assignment-3

**Step-1:**
**Case Study Analysis:**

- **Students should summarize the attack, detailing how social engineering was used to breach security.**
- **They should identify vulnerabilities such as lack of employee awareness training, inadequate authentication measures, or poor email security protocols.**
- **Discussing the consequences of the attack on the organization's reputation, financial losses, and customer trust is important.**
- **Recommendations may include implementing regular security training for employees, adopting multi-factor authentication, and improving email filtering systems.**

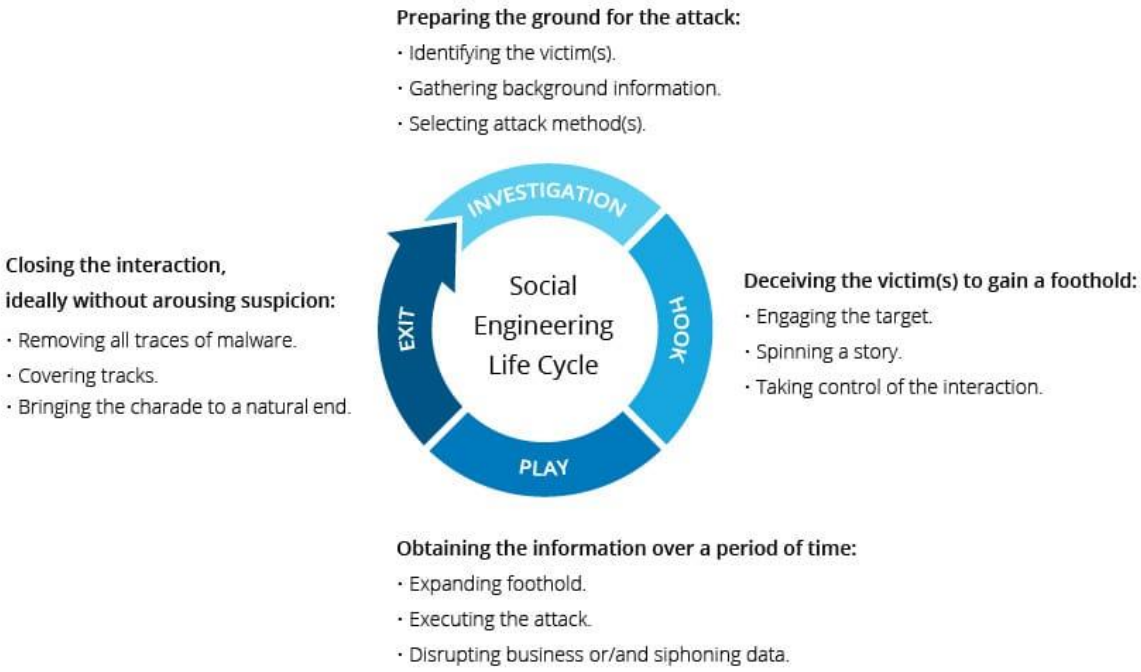
Social engineering attacks manipulate individuals into divulging confidential information or performing actions that compromise security. A notable case involved pretexting via the OmeTV video chat application, where attackers used psychological manipulation to execute a phishing attack1.

Identified Vulnerabilities:

Lack of employee awareness training can leave staff unable to recognize and respond to social engineering tactics.
Inadequate authentication measures, such as single-factor authentication, make unauthorized access easier.
Poor email security protocols can lead to successful phishing campaigns, where malicious emails bypass filters and reach the intended targets.
Consequences of the Attack: The repercussions of social engineering attacks are severe, including:

Reputational Damage: Loss of customer confidence and trust can be devastating and long-lasting.
Financial Losses: Companies have suffered millions in losses; for example, Ubiquity Networks lost $39 million due to a social engineering attack2.
Customer Trust: Breaches can lead to a loss of customer trust, impacting future business and partnerships.
Recommendations: To prevent such attacks, organizations should consider:

Implementing regular security awareness training to educate employees on recognizing and responding to social engineering tactics.
Adopting multi-factor authentication to add an extra layer of security beyond just passwords.
Improving email filtering systems to better detect and block phishing attempts.




**Step-2 Role-play Exercise:**

- **After the role-play, students should identify the social engineering tactics used by the attacker, such as authority exploitation, urgency, or familiarity.**
- **Discussing the victim's susceptibility to these tactics and the importance of skepticism and verification in communication is crucial.**
- **Strategies to mitigate such attacks may include implementing strict verification protocols for sensitive information requests and fostering a culture of security awareness within the organization.**

After the role-play, it's essential to identify the tactics used by the attacker. Common tactics include:

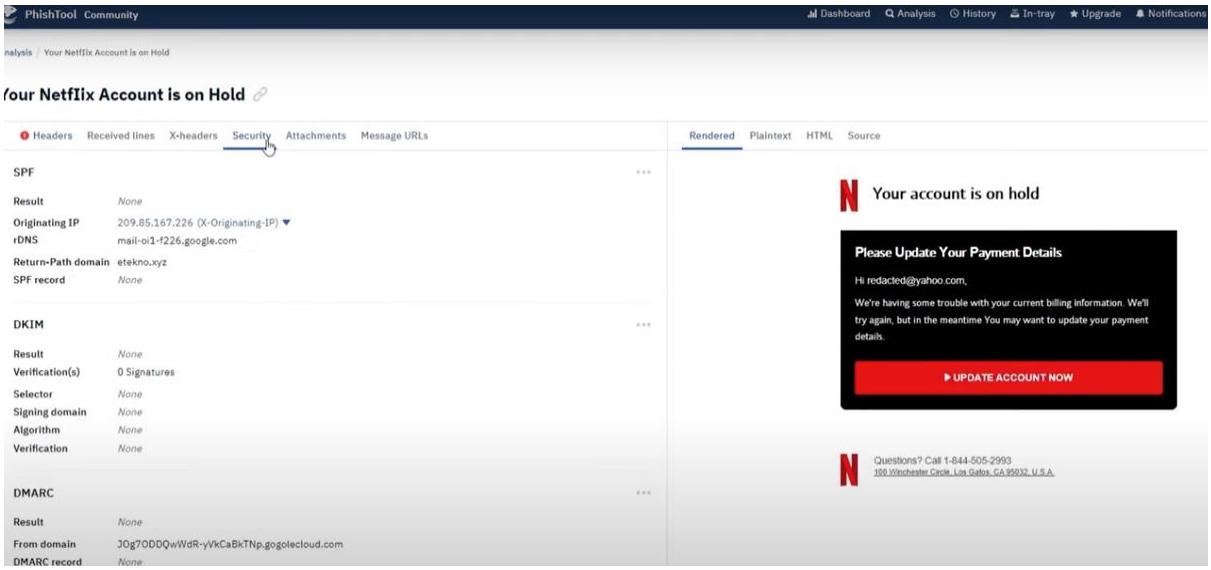
Authority Exploitation: The attacker pretends to be someone in power to coerce the victim into compliance.
Urgency: Creating a false sense of urgency to rush the victim into making a decision without proper verification.
Familiarity: Using personal information to appear as a trusted contact, thus lowering the victim's guard.
Victim's Susceptibility: Discuss why the victim was susceptible to these tactics. Factors could include:

Lack of training on recognizing social engineering attempts.

Natural human tendencies to trust authority figures or urgent requests.
The psychological principle of liking and reciprocation, which can be exploited by attackers feigning familiarity.
Importance of Skepticism and Verification: Highlight the importance of maintaining a healthy level of skepticism in communications. Encourage practices like:

Verifying the identity of the person making the request, especially if sensitive information is involved.
Taking time to think critically about the request, even if it seems urgent.
Consulting with colleagues or superiors before taking action on unusual requests.
Mitigation Strategies: To mitigate such attacks, organizations can:

Implement strict verification protocols for sensitive information requests.
Foster a culture of security awareness within the organization.
Conduct regular training sessions to educate employees about social engineering tactics and prevention strategies.




**Step-3 Phishing Email Analysis:**

**● Red flags could include misspelled domain names, urgent language, requests for sensitive information, and generic greetings.**

**● Students should explore psychological factors such as curiosity, fear, or urgency that might lead individuals to overlook these red flags.**

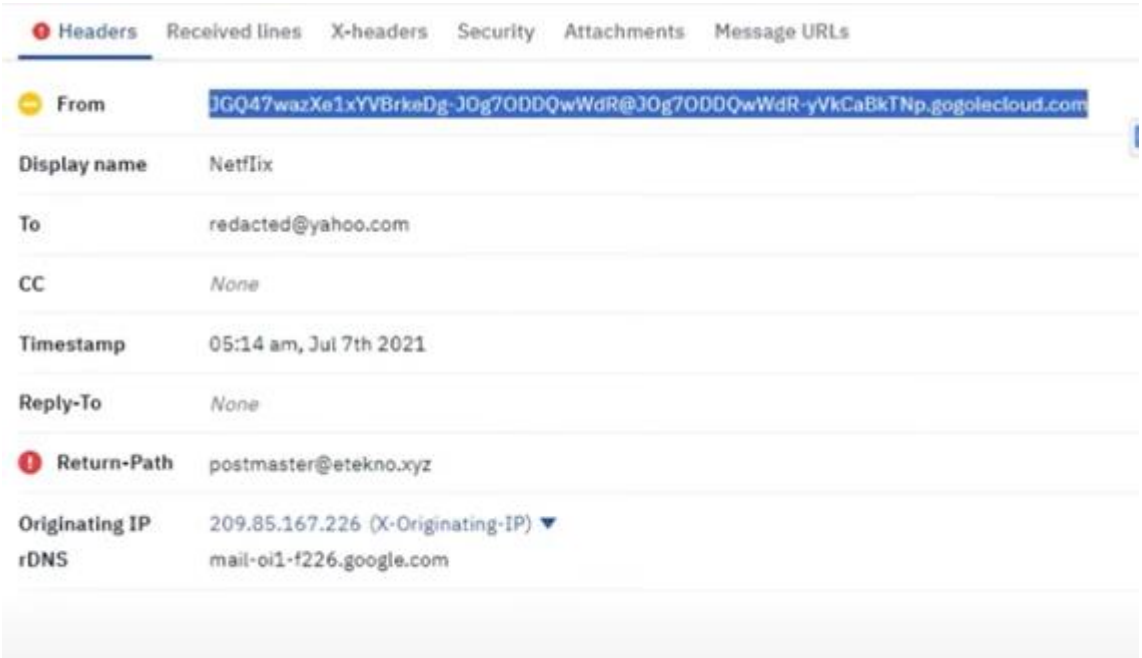
**● Strategies for email authentication, such as checking email headers and verifying sender identities, should be discussed as preventive measures against phishing attacks.**

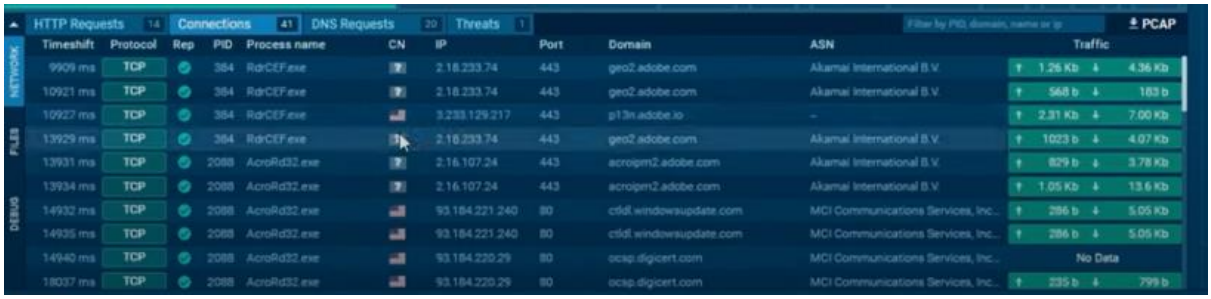
Phishing emails often contain several red flags that can alert a recipient to their malicious intent:

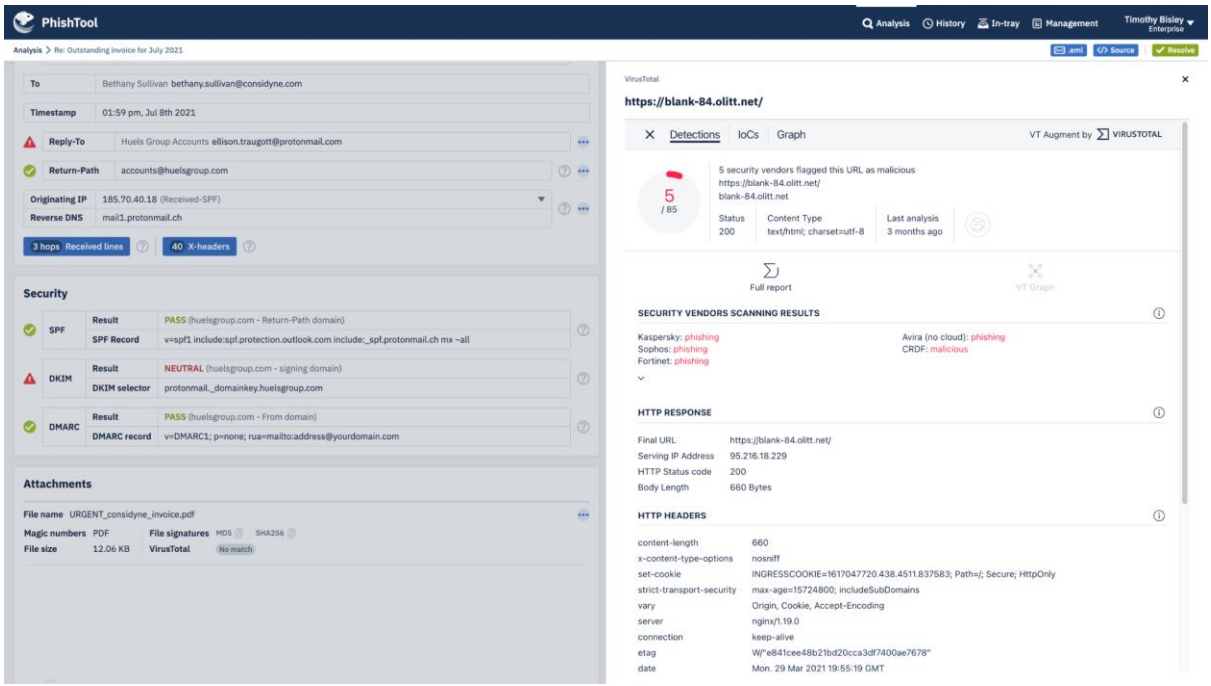
Misspelled Domain Names: Look for subtle misspellings or incorrect domains in the sender's email address.
Urgent Language: Phrases like "Immediate action required" or "Urgent response needed" are common tactics to create a sense of urgency.
Requests for Sensitive Information: Legitimate organizations typically do not ask for sensitive information via email.
Generic Greetings: Phishing emails often use non-personalized greetings like "Dear Customer" or "Dear User."
Psychological Factors: Certain psychological factors can make individuals more susceptible to phishing emails:

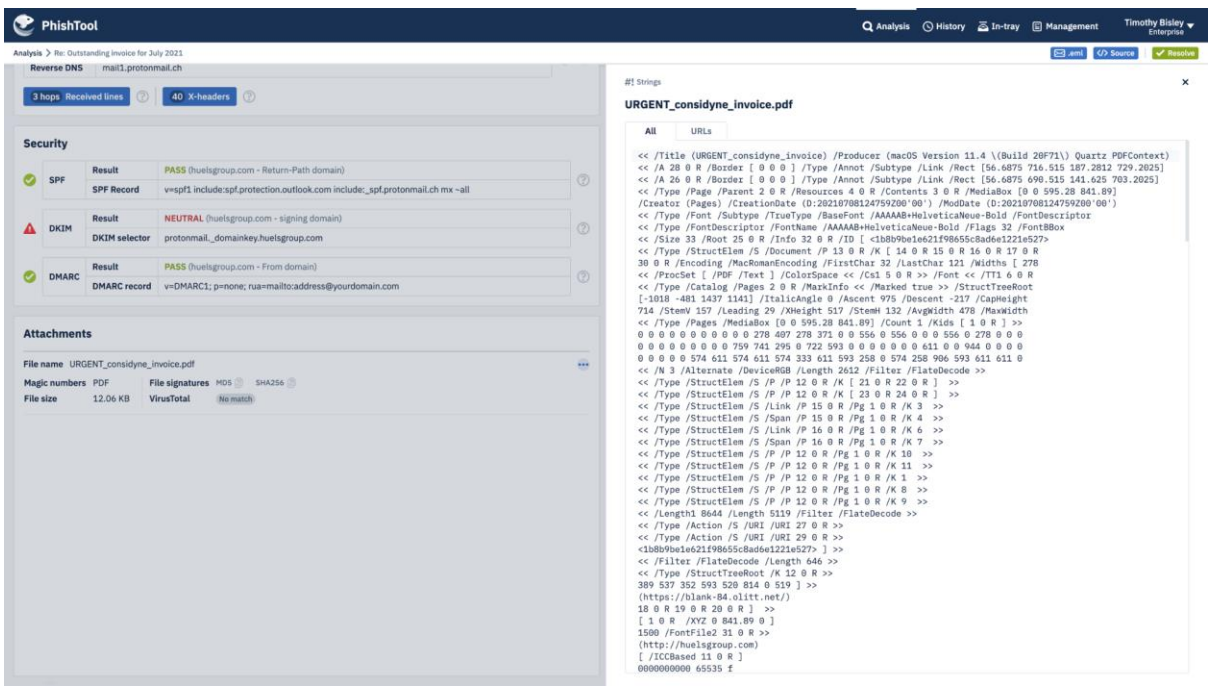
Curiosity: Intriguing or enticing offers can lead to clicking on links without proper scrutiny.
Fear: Threats of account closure or legal action can provoke a fear response, overriding rational judgment.
Urgency: A false sense of urgency can cause individuals to act quickly, bypassing normal security checks.
Email Authentication Strategies: To combat phishing, several email authentication strategies can be employed:

Checking Email Headers: Analyze the technical details within the email header to verify the sender's route.
Verifying Sender Identities: Cross-reference email addresses with known contacts or official communication channels.
Educating Users: Regular training on recognizing phishing attempts and safe email practices is crucial.




HTTP Requests 14
Connections 41
DNS Requests 20
Threats 1
PCAP
NETWORK
FILES
DEBUG
Timeshift Protocol Rep PID Process name CN IP Port Domain ASN Traffic
9909 ms TCP 384 RdrCEF.exe 2.18.233.74 443 geo2.adobe.com Akamai International B.V. 1.26 Kb 4.36 Kb
10921 ms TCP 384 RdrCEF.exe 2.18.233.74 443 geo2.adobe.com Akamai International B.V. 568 b 183 b
10927 ms TCP 384 RdrCEF.exe 3.233.129.217 443 p13n.adobe.io - 2.31 Kb 7.00 Kb
13929 ms TCP 384 RdrCEF.exe 2.18.233.74 443 geo2.adobe.com Akamai International B.V. 1023 b 4.07 Kb
13931 ms TCP 2088 AcroRd32.exe 2.16.107.24 443 acroipm2.adobe.com Akamai International B.V. 829 b 3.78 Kb
13934 ms TCP 2088 AcroRd32.exe 2.16.107.24 443 acroipm2.adobe.com Akamai International B.V. 1.05 Kb 13.6 Kb
14932 ms TCP 2088 AcroRd32.exe 93.184.221.240 80 ctldl.windowsupdate.com MCI Communications Services, Inc... 286 b 5.05 Kb
14935 ms TCP 2088 AcroRd32.exe 93.184.221.240 80 ctldl.windowsupdate.com MCI Communications Services, Inc... 286 b 5.05 Kb
14940 ms TCP 2088 AcroRd32.exe 93.184.220.29 80 ocsp.digicert.com MCI Communications Services, Inc... No Data
18037 ms TCP 2088 AcroRd32.exe 93.184.220.29 80 ocsp.digicert.com MCI Communications Services, Inc... 235 b 799 b


PhishTool
Analysis History In-tray Management
Timothy Bisley
Enterprise
Analysis > Re: Outstanding invoice for July 2021
.eml Source Resolve
To Bethany Sullivan bethany.sullivan@considyne.com
Timestamp 01:59 pm, Jul 8th 2021
Reply-To Huels Group Accounts ellison.traugott@protonmail.com
Return-Path accounts@huelsgroup.com
Originating IP 185.70.40.18 (Received-SPF)
Reverse DNS mail1.protonmail.ch
3 hops Received lines
40 X-headers
Security
SPF Result PASS (huelsgroup.com - Return-Path domain)
SPF Record v=spf1 include:spf.protection.outlook.com include:_spf.protonmail.ch mx ~all
DKIM Result NEUTRAL (huelsgroup.com - signing domain)
DKIM selector protonmail._domainkey.huelsgroup.com
DMARC Result PASS (huelsgroup.com - From domain)
DMARC record v=DMARC1; p=none; rua=mailto:address@yourdomain.com
Attachments
File name URGENT_considyne_invoice.pdf
Magic numbers PDF
File size 12.06 KB
File signatures MD5 SHA256
VirusTotal No match
VirusTotal
https://blank-84.olitt.net/
Detections IoCs Graph
VT Augment by VIRUSTOTAL
5 / 85
5 security vendors flagged this URL as malicious
https://blank-84.olitt.net/
blank-84.olitt.net
Status 200
Content Type text/html; charset=utf-8
Last analysis 3 months ago
Full report
VT Graph
SECURITY VENDORS SCANNING RESULTS
Kaspersky: phishing
Sophos: phishing
Fortinet: phishing
Avira (no cloud): phishing
CRDF: malicious
HTTP RESPONSE
Final URL https://blank-84.olitt.net/
Serving IP Address 95.216.18.229
HTTP Status code 200
Body Length 660 Bytes
HTTP HEADERS
content-length 660
x-content-type-options nosniff
set-cookie INGRESSCOOKIE=1617047720.438.4511.837583; Path=/; Secure; HttpOnly
strict-transport-security max-age=15724800; includeSubDomains
vary Origin, Cookie, Accept-Encoding
server nginx/1.19.0
connection keep-alive
etag W/"e841cee48b21bd20cca3df7400ae7678"
date Mon, 29 Mar 2021 19:55:19 GMT


PhishTool
Analysis History In-tray Management
Timothy Bisley
Enterprise
Analysis > Re: Outstanding invoice for July 2021
.eml Source Resolve
Reverse DNS mail1.protonmail.ch
3 hops Received lines
40 X-headers
Security
SPF Result PASS (huelsgroup.com - Return-Path domain)
SPF Record v=spf1 include:spf.protection.outlook.com include:_spf.protonmail.ch mx ~all
DKIM Result NEUTRAL (huelsgroup.com - signing domain)
DKIM selector protonmail._domainkey.huelsgroup.com
DMARC Result PASS (huelsgroup.com - From domain)
DMARC record v=DMARC1; p=none; rua=mailto:address@yourdomain.com
Attachments
File name URGENT_considyne_invoice.pdf
Magic numbers PDF
File size 12.06 KB
File signatures MD5 SHA256
VirusTotal No match
#! Strings
URGENT_considyne_invoice.pdf
All URLs
<< /Title (URGENT_considyne_invoice) /Producer (macOS Version 11.4 \(Build 20F71\) Quartz PDFContext)
<< /A 28 0 R /Border [ 0 0 0 ] /Type /Annot /Subtype /Link /Rect [56.6875 716.515 187.2812 729.2025]
<< /A 26 0 R /Border [ 0 0 0 ] /Type /Annot /Subtype /Link /Rect [56.6875 690.515 141.625 703.2025]
<< /Type /Page /Parent 2 0 R /Resources 4 0 R /Contents 3 0 R /MediaBox [0 0 595.28 841.89]
/Creator (Pages) /CreationDate (D:20210708124759Z00'00') /ModDate (D:20210708124759Z00'00')
<< /Type /Font /Subtype /TrueType /BaseFont /AAAAAB+HelveticaNeue-Bold /FontDescriptor
<< /Type /FontDescriptor /FontName /AAAAAB+HelveticaNeue-Bold /Flags 32 /FontBBox
<< /Size 33 /Root 25 0 R /Info 32 0 R /ID [ <1b8b9be1e621f98655c8ad6e1221e527>
<< /Type /StructElem /S /Document /P 13 0 R /K [ 14 0 R 15 0 R 16 0 R 17 0 R
30 0 R /Encoding /MacRomanEncoding /FirstChar 32 /LastChar 121 /Widths [ 278
<< /ProcSet [ /PDF /Text ] /ColorSpace << /Cs1 5 0 R >> /Font << /TT1 6 0 R
<< /Type /Catalog /Pages 2 0 R /MarkInfo << /Marked true >> /StructTreeRoot
[-1018 -481 1437 1141] /ItalicAngle 0 /Ascent 975 /Descent -217 /CapHeight
714 /StemV 157 /Leading 29 /XHeight 517 /StemH 132 /AvgWidth 478 /MaxWidth
<< /Type /Pages /MediaBox [0 0 595.28 841.89] /Count 1 /Kids [ 1 0 R ] >>
0 0 0 0 0 0 0 0 0 0 0 278 407 278 371 0 0 556 0 556 0 0 0 556 0 278 0 0 0
0 0 0 0 0 0 0 0 0 759 741 295 0 722 593 0 0 0 0 0 0 0 611 0 0 944 0 0 0 0
0 0 0 0 0 574 611 574 611 574 333 611 593 258 0 574 258 906 593 611 611 0
<< /N 3 /Alternate /DeviceRGB /Length 2612 /Filter /FlateDecode >>
<< /Type /StructElem /S /P /P 12 0 R /K [ 21 0 R 22 0 R ] >>
<< /Type /StructElem /S /P /P 12 0 R /K [ 23 0 R 24 0 R ] >>
<< /Type /StructElem /S /Link /P 15 0 R /Pg 1 0 R /K 3 >>
<< /Type /StructElem /S /Span /P 15 0 R /Pg 1 0 R /K 4 >>
<< /Type /StructElem /S /Link /P 16 0 R /Pg 1 0 R /K 6 >>
<< /Type /StructElem /S /Span /P 16 0 R /Pg 1 0 R /K 7 >>
<< /Type /StructElem /S /P /P 12 0 R /Pg 1 0 R /K 10 >>
<< /Type /StructElem /S /P /P 12 0 R /Pg 1 0 R /K 11 >>
<< /Type /StructElem /S /P /P 12 0 R /Pg 1 0 R /K 1 >>
<< /Type /StructElem /S /P /P 12 0 R /Pg 1 0 R /K 8 >>
<< /Type /StructElem /S /P /P 12 0 R /Pg 1 0 R /K 9 >>
<< /Length1 8644 /Length 5119 /Filter /FlateDecode >>
<< /Type /Action /S /URI /URI 27 0 R >>
<< /Type /Action /S /URI /URI 29 0 R >>
<1b8b9be1e621f98655c8ad6e1221e527> ] >>
<< /Filter /FlateDecode /Length 646 >>
<< /Type /StructTreeRoot /K 12 0 R >>
389 537 352 593 520 814 0 519 ] >>
(https://blank-84.olitt.net/)
18 0 R 19 0 R 20 0 R ] >>
[ 1 0 R /XYZ 0 841.89 0 ]
1500 /FontFile2 31 0 R >>
(http://huelsgroup.com)
[ /ICCBased 11 0 R ]
0000000000 65535 f