THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Predicted Cyber Threat Activity

Geopolitical Issues

Description

Cyber Threat Forecast: Geopolitical Issues

Amid rising Geopolitical issue and tensions between India and Pakistan, there is a **significant likelihood of reciprocal cyber-attacks** involving hacktivist groups, patriotic collectives, and state-aligned actors from both sides. These actors have historically exploited times of heightened national conflict to launch digital campaigns, including:

- Defacements of national portals
- DDoS attacks on public infrastructure
- Targeted credential theft & data leakage
- Information warfare via social media disinformation

High-Risk Sectors (Both Sides)

Sector	Impact Likelihood	Key Risks
Government / Defense	Critical	C2 implants, credential leaks, military coordination sabotage
Financial Institutions	High	Phishing on net-banking, ATM skimming, SWIFT manipulation
Telecom & ISPs	High	DNS poisoning, BGP hijacking, signal interception
Media & Public Trust	Medium	Disinformation campaigns, hacked Twitter handles

CATEGORY

Nation-State Conflict

SEVERITY

Critical

Platforms

- **Windows, Linux, Web Applications**
- **Public Web Infrastructure & Email Systems**
- **Multi-Platform (Windows, Linux, CMS, DNS)**
- **Cross-Platform (Windows, Linux, Network Appliances)**

IMPACT

- Data Theft and Espionage

Forecasting India-Pak Cyber Hacktivist Groups

Indian-Origin Cyber Threat Actors	Pakistan-Origin Cyber Threat Actors
Hacktivist & Underground Groups	*Hacktivist & Underground Groups*
Indian Cyber Force (ICF)	Pakistan Cyber Army (PCA)
Indian Hackers Online Squad	Pak Cyber Experts / Team Pak Cyber Experts
Indian BlackHats	Pak Cyber Pyrates
IndiShell	Pak Cyber Eaglez
Mallu Cyber Soldiers	Pakistan Cyber Attackers
Kerala Cyber Warriors	Pakistan Haxors Crew
HMG India Cyber Pirates	Code Man
Telangana Cyber Warriors	Mr Z
LulzSec India	Zindabad (part of PCA)
India Black Dragon	Gujjar Injector / Faisal Afzal Gujjar (Pak Cyber Pyrates)
Hunter Khan H4x0r	Muhammad Balil (Pak Cyber Experts)
Nomcat	MaDLeets (Pak faction)
H4$n4!n H4xor	Hell Shield Hackers
HuSsY Indian BlackHat	Dr@cul@
Z Company Hacking Crew	Godzilla (Pak-based)
m1nd Intruder	H4x0r10ux
Godziila Volcanium / G.O.D	Ne0-H4ck3r
Shadow008	Romantic rOOx (Pak-side ops as well)

Forecasting India-Origin Cyber Campaigns & Actors

Threat Actor / Group	Known Campaign / Tool	Predicted Activity
Patchwork APT (Dropping Elephant)	Cyber-espionage via malicious docs	Spear-phishing military and diplomatic sectors
Operation Hangover	Trojanized documents & implants	Malware targeting telecom and defense institutions
APT-C-09 / Monsoon	Credential theft tools	Account harvesting from ISPs and cloud services
Pegasus C&C (Spyware)	Surveillance malware	Potential redeployment for VIP monitoring
Indian Cyber Force, Mallu Cyber Soldiers	Hacktivist operations	DDoS attacks and defacements on .gov.pk, banking, and education portals

Forecasting Pakistan-Origin Cyber Campaigns & Actors

Threat Actor / Group	Known Campaign / Tool	Predicted Activity
Bitter APT (T-APT-17)	Modular backdoors, phishing lures	Targeting Indian ministries, telecom and regional state data centers
Sidewinder APT (APT-C-17)	Android malware and exploit kits	Likely targeting Indian defense apps and election systems
Group 5 (Pakistan Cyber Army)	Nationalist hacktivism, defacements	Increased propaganda defacements and social media impersonation
Bezigate Operators	Credential phishing & DNS spoofing	Spoofed portals mimicking Indian media, finance, and eGov portals
LuminosityLink RAT Campaigns	RATs via phishing & cracked tools	Remote surveillance and access of low-trust Indian infrastructure endpoints

SHA-256

8c233e13a0bc27bce7555b9a89f63c0eadaa5c618fe7301eebd7a32e2bd79bcf

bf93ca5f497fc7f38533d37fd4c083523ececc34aa2d3660d81014c0d9091ae3

17c3d0fe08e1184c9737144fa065f4530def30d6591e5414a36463609f9aa53a

8e0574ebf3dc640ac82987ab6ee2a02fc3dd5eaf4f6b5275272ba887acd15ac0

0c63ef29d5a9674a00bb71a150d2ae6f3dc856a43291e79260992f08fdcd53d3

0c63ef29d5a9674a00bb71a150d2ae6f3dc856a43291e79260992f08fdcd53d3

722e8909235ae572c7baa522a675ce45ac7e10170be7428de74d04f051f473c9

f61aa8c6590926533b67467603d2f42cdb1d5e1f20a5439d7e58fdaf81710711

c9642f44d33e4c990066ce6fa0b0956ff5ace6534b64160004df31b9b690c9cd

b25e4b7f2a66d41afdb5fbe7535b2f9ac8ebe920a1af18387d58113d27719971

770f78c2633530293f6966d0c50b58dddc50e7d0a7522b06c1f4e4784cd40e97

4f1949262a876df0a64d8934518b3626d3e69d182f2b44e04ca1dfd9c4dd7b0a

56bad93d98a01a820555357beb03a691f523ebb289b9c821ad85ee65137d29f9

b25e4b7f2a66d41afdb5fbe7535b2f9ac8ebe920a1af18387d58113d27719971

c299063e3eae8ddc15839767e83b9808fd43418dc5a1af7e4f44b97ba53fbd3d

7841fe621eb9bf443e19bb88c5df1d9ea14feed829d18e84258380dc462816fd

63a3c1b2e1ca65bf71322b84305f612bc625ac40eff667f56655022d05cf0be0

bf4bedf2722525ae269db0d661d38010671144dec9dc38471f77915dcfb6772d

fc869c9853eef46976ecc03bf109f409bf391413862637dec98951df1c8c8b7d

1dd50966db005e30f7a69b6d16dfe8b9810dba3cdbe43bebb136f8786d027ed1

b0b687977eee41ee7c3ed0d9d179e8c00181f0c0db64eebc0005a5c6325e8a82

f7ed5eec6d1869498f2fca8f989152326b2d8cee8dcacf3bcb9315ae7566963db

49e95828b00e2622e5644776de4c083ae0b658a02e6bc44f9ebd0dff0720ed6c

b7765ff16398aacff3b19d1a15dd7850a16493f264f19335ea860ab57e5d6f02

ce922a20a73182c18101dae7e5acfc240deb43c1007799c20ea74c1ddd52db12

e4545764ec054ed1e1321a038fac1921b5b70a591c95b24127f1b9de7212af8e

fa0ed2faa3da831976fee9860ac39d50484b20beee692ce7f0ec35a15670fa92

3fdf291e39e93305ebc9df19b48a0ebd6845053b8be620cbf482d0f09f4d3

69b397400043ec7036e23c225d8d562fdcd3be887f0d076b93f6fcaae8f3dd61

90fd32f8f7b494331ab1429712b1735c3d864c8ca2461a5ab67b058023821787

7b64a73983c66b436c179eac37c446fee5ba5abc6cc96206fc8e457444adcd5f2

26b3c9a507723c1bbb5c5b4fc5513e3e0b54a735c32ae96a0d6dc1e1d7e4cc8f

1a749857e726960a83d6df68a459f973dffd6ed82ac9f38d097154ab7ab462bc

522e4d8a0006b6c4c97c2933d139fdda76179b4956673796336cff1a2eb865ef5

b8aaed906fa01b6724a436b521f756c2970615817a8cbf7d747fb7ca9aaae7a6

dcf5ea6163e7508c44756b6727061743db1dee778692f1532bb53ea8cd1d15666

d9e373aeea5fe0c744f0de94fdd366b5b6da816209ac394cbbda1c64c03b50b1

865f5b3b1ee94d89ad9a9840f49a17d477cddfc3742c5ef78d77a6027ad1caa5

fa95fadc73e5617305a6b71f77e9d255d14402650075107f2272f131d3cf7b00

SHA-1

```
1ef9ade3cf8bbfda23e57df470e449961552645e
406c74e8eb89fa7b712a535dd38c79c1afd0c6fe
9cdbb41f83854ea4827c83ad9809ed0210566fbc
9034c8bfac8385a29f979b1601896c6edb0113b2
11064dcef86ac1d94c170b24215854efb8aad542
5de78801847fe63ce66cf23f3ff3d25a28e2c6fe
478a41f254bb7b85e8ae5ac53757fc220e3ab91c
1e39ff194c72c74c893b7fd9f9d0e7205c5da115
f7d9e0c7714578eb29716c1d2f49ef0defbf112a
d4e59940c5a16c0284b6303840386dd4478a8f73
f5f78dd593a57f480508bd45ca4f85911a8e6af4
4d577d58717055b43fd33aa2f947d5bba86a14bd
83a5074c677a96f1c9f67b758e5e399e401dde41
d4e59940c5a16c0284b6303840386dd4478a8f73
a6dcdfc8e97616c07549290950e78b145883e532
30baa6bd3d8519181e03b7563e4c851d1223b7fe
58b25b7adffdcb07c4e362c45565a801b39aefc5
87d6e9de115ada1fd246db2bac8def8de057d07a
38303c37768af60f53d8feabcb94fe8effa8cc0e
2f4c75347aada1894e6b90d1162374ef3ce7bedf
0cbf8c7ff9faf01a9b5c3874e9a9d49cbbf5037b
25092b60d972e574ed593a468564de2394fa088b
4fbde39a0735d1ad757038072cf541dfdc65faa3
5a972665b590cc77dcdfb4500c04acda5dc1cc4e
530f597666afc147886f5ad651b5071d0cc894ba
04a75df9b60290efb1a2d934570ad203a23f4e9c
aeb02ac0c0f0793651f32a3c0f594ce79ba99e82
b12e459dd3857f5379ac99e48def4ad2b8a3aa16
bcd7a2191af9ddb1bd627e36a55fc55680e36f51
b17f0381fc7e4c4c6bb15dfcc0c37d29452666ce
7a94a3dcd68792877a4ca8747e23ec084b12da16
3ba50221785aa8d1f2dea2894f9ca9449e826724
33f7efb563052da4d25405dd7f0366bb3bff5b26
81f6de303ce9279744bb1a00e70ea62428bf28e
82633aeb799995f7e154d2494cc12437223aad2
d2970513f991d9567cb3b8c1ed7cb2d3b2f758d
5a12b7f4214ac1f79f2b613fb482e58701dfaaa6
84b4b2705018e38253796cd3f84ee68694d9b9c0
96cafccda39d2dd06e22b33ca37504405439c23d
```

Indicator of Compromise

MD5

```
3e8aff5697a513a749869744ad0ce135
eddb8990632b7967d6e98e4dc1bb8c2f
233a71ea802af564dd1ab38e62236633
7a662144f9d6bada8aea09b579e15562
aa755fc3521954b10fd65c07b423fc56
d8102a24ca00ef3db7d942912765441e
eddb8990632b7967d6e98e4dc1bb8c2f
fb52fbd9b3b465453276f42c46350c25
85144918f213e38993383f0745d7e41e
2d8243b47953bf7f1a19b011de33fded
d2276557a2dff4bebef4a2f55e774ad9
6a80a88a1f2a1d0ab2fe0c7f69e165fa
ec4e3a9a7b64ad404c29063b7a39eaee
16807cb880073b1c21009f7749c8fe7f
5e5201514800509b2e75a3fcffad7405
527dc131149644af439e0e8f96a2c4eb
2c8ed4045b76a1eca8cd8616a4b65ec
2a340b72e16fb1ece13d7f553ec3c266
2454a5b5f7793d372c96fd572c1de2cc
bdbbd70229591fb1102f365f4bb22196b
b9025eca96614a473e204e9e8a873e1d
54f54d9bdb6afceb670978cf98f5c2be
25a16bf0cfa9acd71450e02a341064c8d
72a7130e98191ecd70c4e0f6ce9c0030
bf51139c8b0673a9cfee1c384d1e236a
59b043a913014a1f03258c695b9333af
5e5201514800509b2e75a3fcffad7405
527dc131149644af439e0e8f96a2c4eb
2c8ed4045b76a1eca8cd8616a4b65ec
2a340b72e16fb1ece13d7f553ec3c266
e9726519487ba9e4e5589a8a5ec2f933
d36a67468d01c4cb789cd6794fb8bc70
313f9bbe6dac3edc09fe9ac081950673
bd8043127abe3f5cfa61bd2174f54c60
e0bce049c71bc81afe172cd30be4d2b7
872c2ddf6467b1220ee83dca0e118214
3d9961991e7ae6ad2bae09c475a1bce8
b510120966ae2b95f96e34dffb58f277
7c27b7369ddd2a6e528b1103d6c252e3
```

Indicator of Compromise

Domains

http://www.epg-cn.com
http://chinastrat.com
http://www.chinastrats.com
http://www.newsnstat.com
http://cnmilit.com
http://163-cn.org
alfred.ignorelist.com

ThreatCure

Cyber Threat Advisory

Secure your byte world

Predicted Cyber Threat Activity

Geopolitical Issues

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net