OFFICE OF THE ADDITIONAL DIR. GENERAL OF POLICE,
MAHARASHTRA CYBER, MUMBAI

SR.NO	DESCRIPTION	REMARKS
	Subject - Approval for Cyber Threat Intelligence Advisory on APT36 Campaign Targeting Indian Government Infrastructure	
1.	Respected Sir, The Additional Director General of Police, Maharashtra Cyber, through the dedicated MH-CERT division, has proactively gathered intelligence using CERT tools and continuous monitoring through the Threat Intelligence Platform. Recent analysis indicates a sharp rise in cyber threats targeting Indian citizens and government entities following the April 2025 Pahalgam terror attack. These include disinformation campaigns, targeted phishing, and sophisticated malware deployments by state-aligned actors.	
2.	**Findings by MH-CERT:** • **Disinformation Campaigns:** Circulation of false information and fake press releases designed to incite panic and erode trust in government institutions. • **Phishing and Credential Theft**: Spear-phishing emails targeting Indian government officials and defence personnel, using spoofed domains and malicious PDFs. • **Malware Deployment:** Use of macro-enabled documents and clipboard-based execution techniques to deliver Crimson RAT and other remote access malware.	
3.	Your kind approval is sought to release/publish this advisory on the MahaCERT Portal. **(Sandip Patil)** Police Inspector Maharashtra Cyber, Mumbai	
4.	Superintendent of Police (Admin), Maharashtra Cyber	
5.	Deputy Inspector General of Police, Maharashtra Cyber	
6.	Additional Director General of Police, Maharashtra Cyber	

Targeted APT36 Campaign Exploiting Pahalgam Terror Incident for Cyber Espionage

MH CERT

Advisory ID: CERTMH_CTI_2025_20

Date: 09th May 2025

This Page is intentionally left blank

Contents

SUMMARY

Transparent Tribe, also known as **APT36**, is a Pakistan-based advanced persistent threat (APT) group that primarily targets Indian diplomatic, military, Defence, and aerospace sectors. This group also operates under several other aliases, including ***APT-C-56***, ***Copper Fieldstone***, ***Earth Karkaddan***, ***Green Havildar***, ***Mythic Leopard***, ***ProjectM***, ***STEPPY-KAVACH***, *and* ***TEMP.Lapis***. It is well-known for its cyber espionage campaigns aimed at Indian government organizations, military personnel, and Defence contractors.

Transparent Tribe has been observed using modern techniques such as **clickjacking** to trick users into unintentionally interacting with malicious content. Their operations commonly involve spear-phishing emails, remote access Trojans (RATs), and data exfiltration mechanisms. Recent notable campaigns attributed to the group include ***Operation Transparent Tribe*** **and** ***Operation C-Major***, which involved sending malicious emails to Indian embassies and Defence personnel.

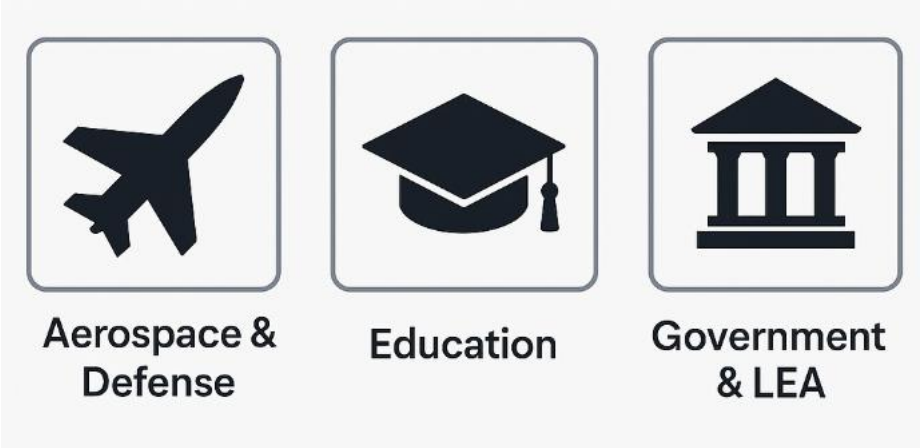
ORIGIN

Target Countries

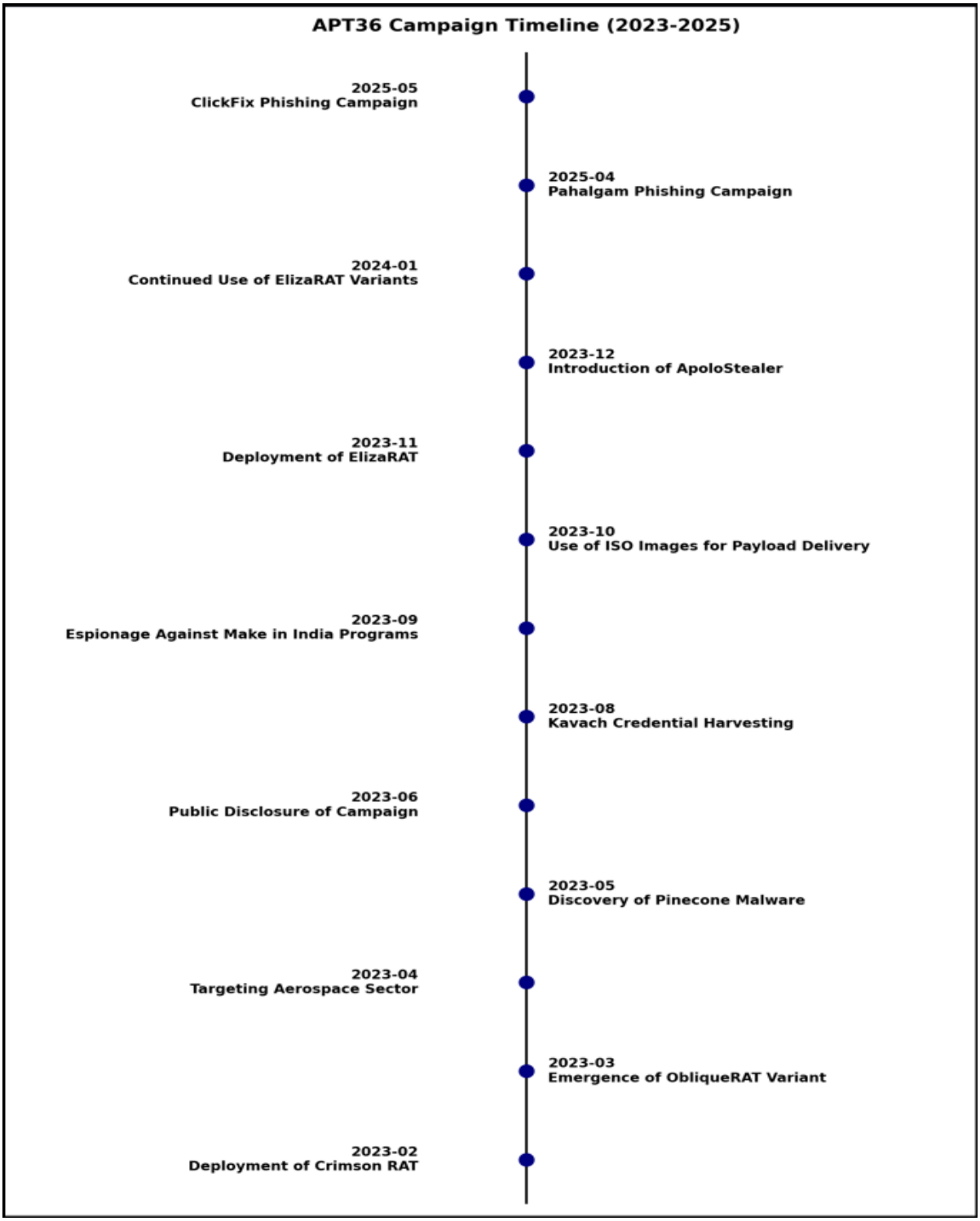
Country Flag	Country Name	Country Flag	Country Name
	United Arab Emirates (AE)		Canada (CA)
	Afghanistan (AF)		China (CN)
	Austria (AT)		Czech Republic (CZ)
	Australia (AU)		Germany (DE)
	Azerbaijan (AZ)		Spain (ES)
	Belgium (BE)		United Kingdom (GB)
	India (IN)		Oman (OM)

	Iran (IR)		Pakistan (PK)
	Japan (JP)		Romania (RO)
	Kenya (KE)		Saudi Arabia (SA)
	Kazakhstan (KZ)		Sweden (SE)
	Malaysia (MY)		Thailand (TH)
	Netherlands (NL)		Turkey (TR)
	Nepal (NP)		Russia (RU)

Target INDUSTRY/SECTOR



APT36 Timeline



Key Recent Incidents

April 2025: Pahalgam Attack-Themed Phishing

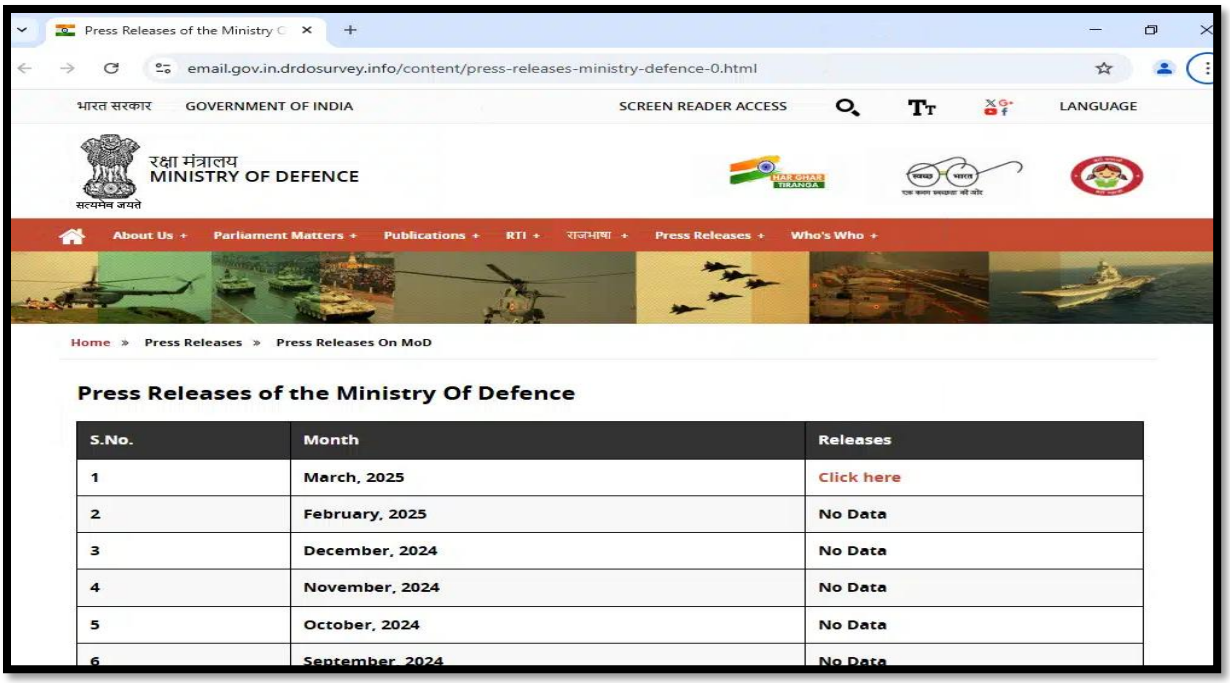
- APT36 used documents themed around the April 22, 2025, Pahalgam terror attack to target Indian government and Defence personnel.
- The campaign involved credential phishing and malware deployment, with fake domains impersonating the Jammu & Kashmir Police and Indian Air Force.
- Malicious PDFs and macro-laced documents were used to deliver Crimson RAT, a remote access trojan.

March 2025: Fake India Post Website

- APT36 created a fraudulent website mimicking India Post ("postindia[.]site") to infect both Windows and Android users ("indiapost[.]apk").
- Windows users were tricked into running a PowerShell command via a malicious PDF, while Android users were prompted to install a fake app that steals data and monitors activity.
- The campaign leveraged metadata and infrastructure linked to Pakistan’s Prime Minister Youth Laptop Scheme.

TECHNICAL ANALYSIS

Threat actors used branding spoofing to deliver cross-platform malware targeting Indian government infrastructure. They mimicked official press releases and employed ClickFix techniques to execute malicious commands silently.

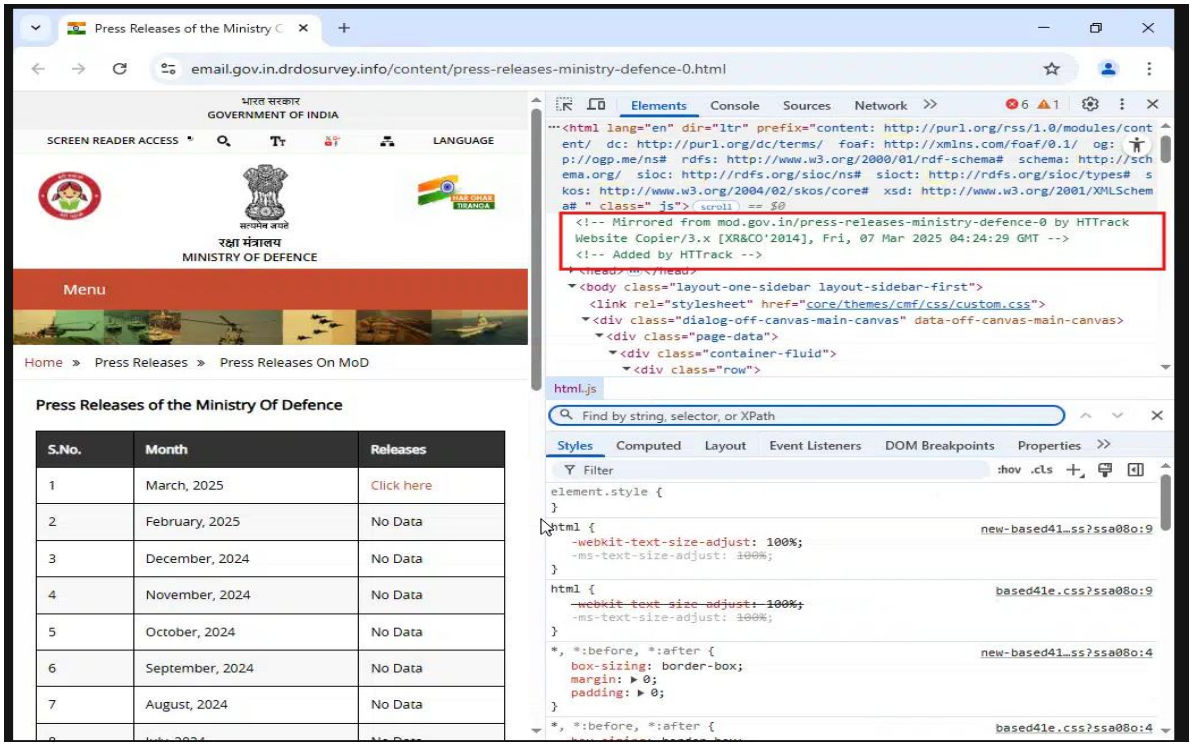


Picture 1: Mimic Page screenshot showing only March 2025 link

- MH-CERT has found a sophisticated cyber intrusion campaign targeting Indian government infrastructure. The attack employs multiple vectors, beginning with social engineering and reaching in data exfiltration through encrypted channels.
- While surveying domains imitating official government websites security researcher identified email.gov.in.drdosurvey[.]info serving content spoofing India's Ministry of Defence. Visiting the site in a browser revealed a page mimicking the Ministry's official press release archive, with **a** structure and layout closely modeled on the legitimate portal.
- The domain "email.gov.in[.]drdosurvey[.]info" is registered with NameCheap, Inc. and its WHOIS server is "whois.namecheap.com". The domain was created on March 19, 2025, and has an expiration date of March 19, 2026. It was last updated on April 15, 2025.

On above spoofed portal, only a single active link for March 2025 is functional, guiding users into a tailored ClickFix social engineering trap. Depending on the victim's operating system, the attack redirects to specific PHP pages- /captcha/windows.php for Windows and /captcha/linux.php for Linux. Windows users encounter a faux "For Official Use Only (FOUO)" warning overlay with a blurred background of a legitimate government site, followed by a clipboard command executing a remote payload via mshta.exe from trade4wealth[.]in, delivering a .NET-based loader connecting to a malicious IP (185.117.90[.]212).

We identified that the domain email.gov.in.drdosurvey[.]info is a cloned website created by the attacker using HTTrack Website Copier, as evidenced in the screenshots provided below.

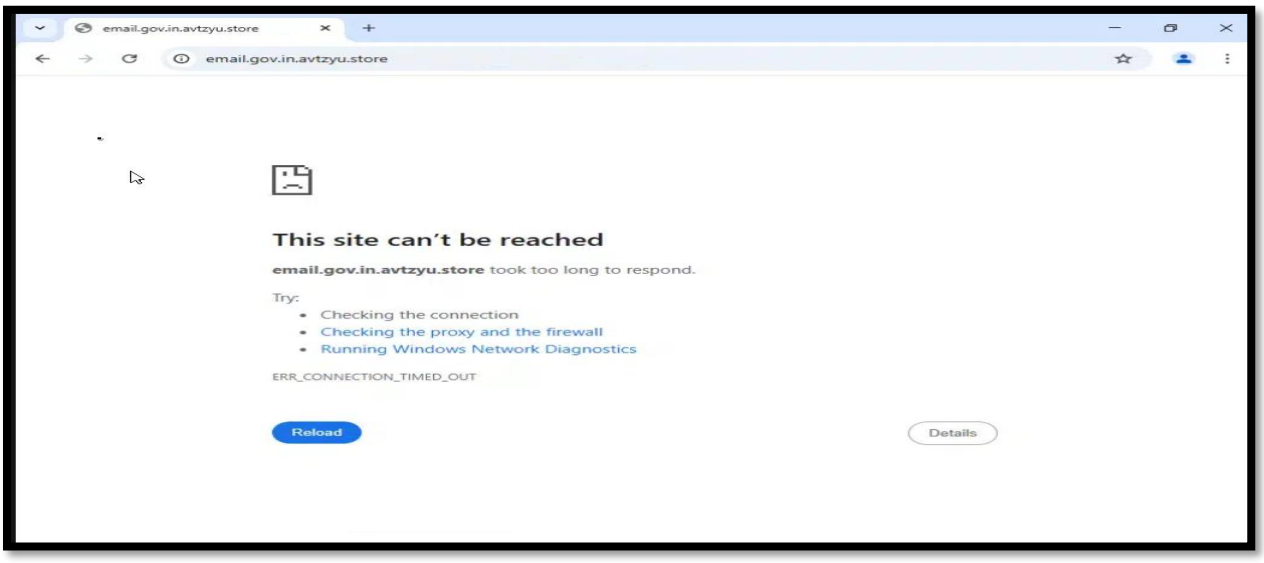


Picture 2: Used HTTrack Website Copier tool to clone the website

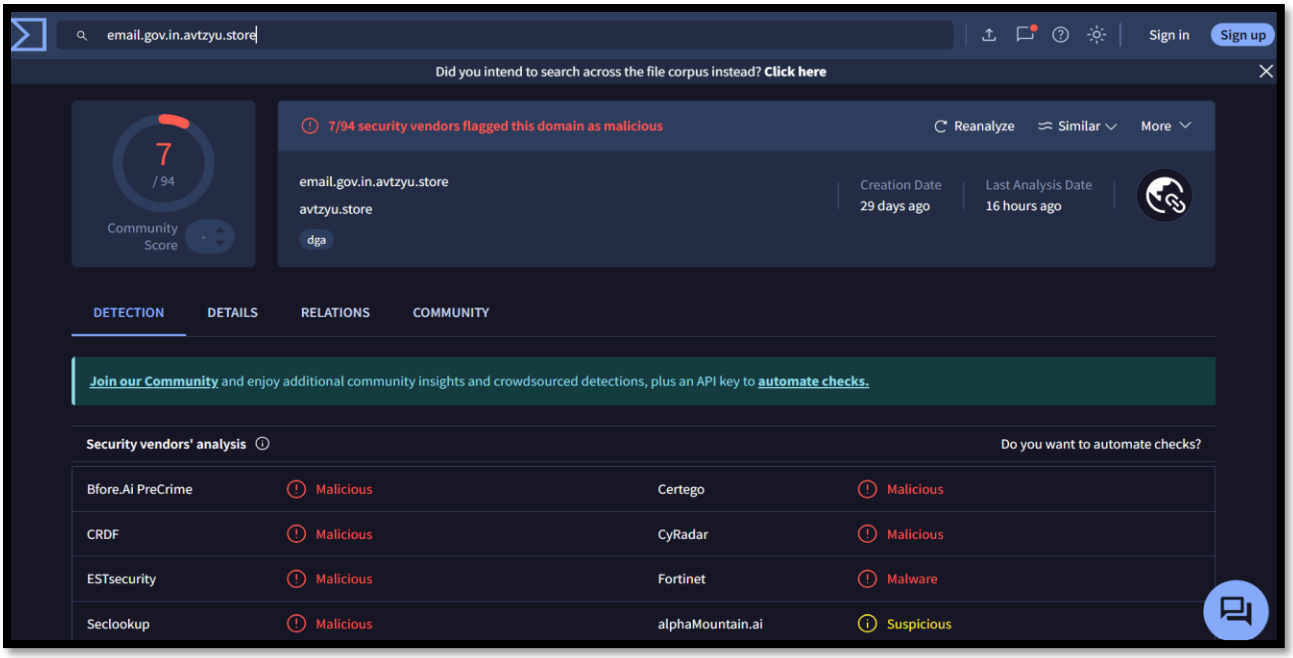
On Windows systems, clicking the March 2025 link redirects the user to /captcha/windows.php, which displays a full-screen overlay mimicking a government-style disclosure warning labeled "**For Official Use Only (FOUO)"**

Picture 3: windows.php page with FOUO warning

After victims interact with the spoofed portal by clicking the "Continue" button, they are redirected to another malicious domain: email[.]gov[.]in[.]avtzyu[.]store. MH-CERT security team has conducted sandbox analysis of this secondary domain, revealing its role in the attack chain.



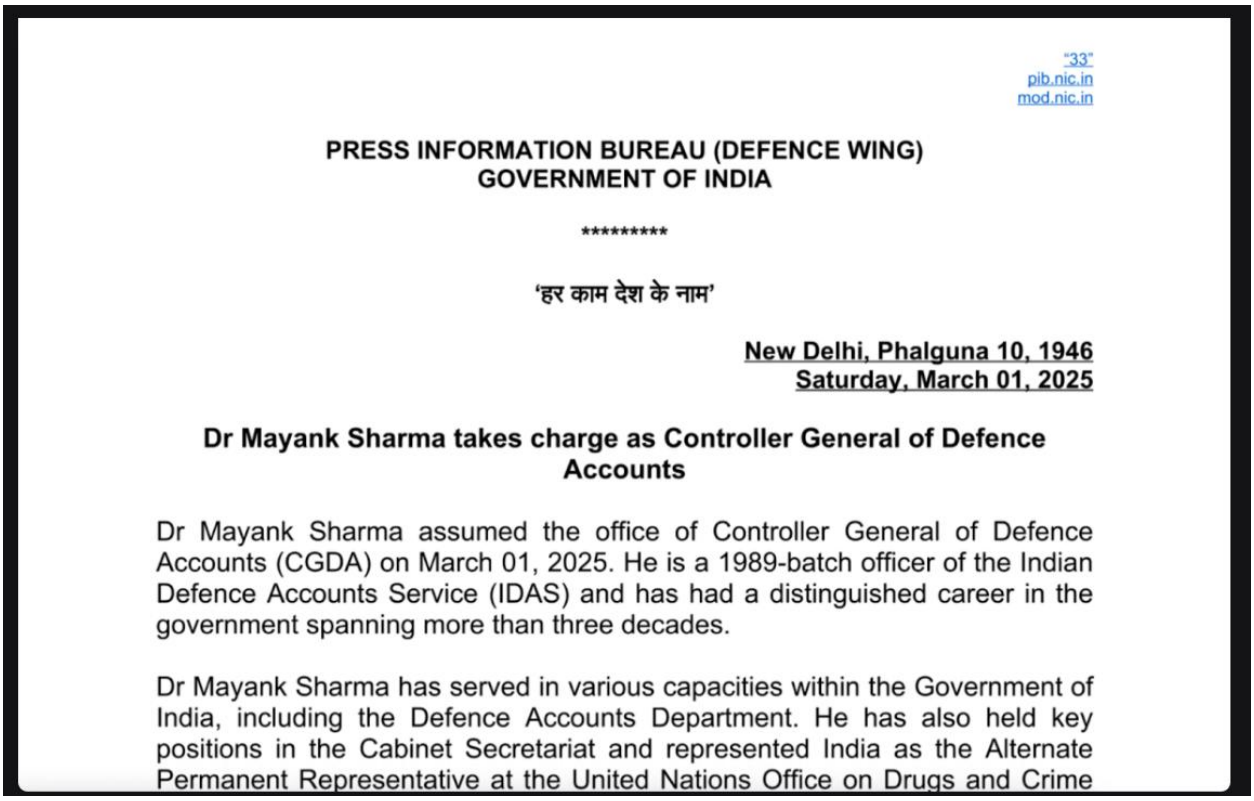
Picture 4: Redirect to another malicious domain



Picture 5: Result of another malicious domain

The sandbox analysis indicates that this domain serves as the next stage in the attack sequence, likely delivering malware or executing additional credential-harvesting operations.

While the malware executes in the background, the user is shown a decoy document- an apparently legitimate press release themed around the Indian Ministry of Defence. The PDF appears to have been cloned directly from the actual press release portal, likely intended to reinforce the illusion of legitimacy.



"33"
pib.nic.in
mod.nic.in

PRESS INFORMATION BUREAU (DEFENCE WING)
GOVERNMENT OF INDIA

****

'हर काम देश के नाम'

New Delhi, Phalguna 10, 1946
Saturday, March 01, 2025

Dr Mayank Sharma takes charge as Controller General of Defence Accounts

Dr Mayank Sharma assumed the office of Controller General of Defence Accounts (CGDA) on March 01, 2025. He is a 1989-batch officer of the Indian Defence Accounts Service (IDAS) and has had a distinguished career in the government spanning more than three decades.

Dr Mayank Sharma has served in various capacities within the Government of India, including the Defence Accounts Department. He has also held key positions in the Cabinet Secretariat and represented India as the Alternate Permanent Representative at the United Nations Office on Drugs and Crime

Picture 6: Decoy PDF shown to the victim during malware execution

The campaign's tradecraft, including government-themed lures, HTA payloads, and typosquatting, aligns with patterns historically linked to APT36 (Transparent Tribe), a Pakistan-aligned threat actor known for targeting Indian government entities, suggesting medium-confidence attribution to this group. This attack underscores the evolving reuse of familiar ClickFix techniques with subtle innovations, emphasizing the need for vigilance against clipboard-based execution, spoofed subdomains, and shallow website clones.

Potential Impact: Geopolitical and Cybersecurity

- **DISRUPTION OF GOVERNMENT OR MILITARY OPERATIONS:** Interaction with the malicious document by officials or Defence personnel could compromise their systems, potentially resulting in unauthorized access and data leakage.

- **INFORMATION MANIPULATION:** The campaign could facilitate the spread of disinformation, cause reputational damage, and promote false narratives intended to undermine trust in institutions.

- **ESPIONAGE AND DATA EXFILTRATION:** Successful phishing attempts could lead to unauthorized access to sensitive data, deployment of malware, and long-term surveillance of targeted individuals or organizations.

Conclusion

The tradecraft observed in this campaign use of government-themed lure content, HTA-based delivery, decoy documents, and operational targeting of Indian government infrastructure.

APT36 is a Pakistan-aligned threat actor known for:

- Longstanding focus on Indian government, military, and diplomatic targets.
- Repeated use of .NET-based malware, HTA delivery, and cloned login or press release content.
- Infrastructure that frequently includes typosquatting, misuse of legitimate services, and publicly visible scripting errors.
- Domains mimicking Indian government subdomains, particularly variations of email.gov[.]in, appended to attacker-controlled parent domains (e.g., drdosurvey[.]info, avtzyu[.]store)
- HTA payloads staged deep in URL paths masquerading as benign directories
- Spelling anomalies, such as "I'm not a rebot" and "officia use only", may reflect a deliberate attempt to bypass pattern-based detection or user familiarity.
- Cross-platform delivery using clipboard-based execution on both Windows (mshta.exe) and Linux (curl + chmod + bash) further supports staging.

Recommendation by MH-CERT

Note: *MH-CERT recommends implementing the below strategic security controls to mitigate risks from that are arising out of the these highly active APT groups that are targeting India's Critical Infrastructure Sectors. it is strongly advised that organizations perform thorough business impact analysis,* ***carefully evaluate each control in the context of their operational environment and business continuity requirements before applying below recommendations.***

Enterprise IT & Network Security Recommendations

- **IOC-Based Defence (Multi-Layered Application)**
  - **Firewall / IPS / Perimeter Devices:** Block malicious IP addresses, C2 domains, and URL patterns through perimeter firewalls, UTM, or NGFW with threat feeds.
  - **Endpoint Detection and Response (EDR/XDR):** Block and monitor execution of malicious hashes (MD5/SHA256), file paths, and process behaviours.
  - **Web Proxy / Secure Web Gateway (SWG):** Apply domain-based IOC filtering to block malicious or typosquatted domains and suspicious URLs used in phishing lures or redirections.
  - **Email Security Gateway:** Filter attachments, URLs, and sender domains associated with malicious campaigns. Use IOC-based allow/block lists to filter at MTA level.

- **Endpoint Protection & EDR Hardening:**
  - Implement EDR rules to block execution based on file extensions commonly used in malicious campaigns (e.g., .bat, .sh, .vbs, .js, .ps1).
  - Disable PowerShell access for non-administrative users to limit post-exploitation lateral movement.
  - Block USB storage devices and memory card slots at the OS level unless explicitly required. Use device control features of EDR.
  - Ensure SMBv3 or later is used with signing enforced to secure file-sharing protocols.
  - Disable NTLM authentication or enforce NTLMv2 at minimum; prefer Kerberos wherever possible.

- **Email and Supply Chain Threat Protection**
  - Harden email gateway policies to block high-risk file types (.bat, .js, .vbs, .sh, .exe, .lnk) from untrusted sources.
  - Implement advanced anti-phishing and anti-spoofing controls (SPF, DKIM, DMARC) and enhanced sandboxing for external attachments.
  - Enable aggressive spam and scam heuristics for all inbound messages from non-whitelisted domains.
  - Review third-party and supply chain communication flows—enable domain-based trust validation and enforce communication only through vetted channels.
  - Segment and audit supplier access and establish fallback plans for critical dependencies during heightened threat periods.

- **Network Security and Proxy Layer**
  - Review secure web gateway and proxy configurations to enforce domain filtering, SSL inspection, and malware scanning.
  - Deploy next-gen firewalls with threat intel integration to detect known APT infrastructure.
  - Implement Anti-APT appliances or sandboxes at critical egress/ingress points for zero-day and behavioral detection.
  - Deploy SSL inspection and TLS 1.3 proxying where legally and technically feasible.

- **DDoS and Critical Infrastructure Readiness**
  - Engage with ISPs to implement Clean Pipe / DDoS scrubbing services, especially for public-facing applications.
  - Run DDoS readiness tests and simulate failovers to alternate geo-redundant routes.
  - Update incident response playbooks to include high-scale volumetric and application-layer DDoS events.

- **Backup & Recovery Controls**
  - Ensure immutable backups stored across different geo-locations, with at least one copy in a non-seismic and non-network-accessible environment.
  - Test disaster recovery and data restoration procedures regularly for ransomware scenarios.
  - Isolate backup systems from production domains using logical or physical segregation.

- **Authentication and Access Control**
  - Enforce Multi-Factor Authentication (MFA) for all privileged and remote access.
  - Apply the Principle of Least Privilege (PoLP) to all users and service accounts.
  - Continuously review and revoke unused privileges in critical systems.
  - Implement Windows security policies to restrict access to vssadmin, wmic, and PowerShell for regular users.

- **Active Directory and Privileged Access Management**
  - Conduct Active Directory security reviews including group memberships, admin roles, and GPO policies.
  - Deploy tiered admin access model (Tier 0, 1, 2) to segregate domain controllers and sensitive systems.
  - Perform regular tests of your Disaster Recovery Plan (DRP) and Domain Controllers (DCs) for failover reliability.
  - Log, Monitor and alert on suspicious AD changes and privilege escalations**.**
  - Use EDR solutions that detect and alert on bulk shadow copy deletions

- **Mobile Device Security**
  - Implement Mobile Device Management (MDM) on smartphones.
  - Limit app installations to authorized stores only and disable the "Install from Unknown Sources" option.
  - Continuously monitor Android devices for signs of CapraRAT and other mobile Remote Access Trojans (RATs).

- **Awareness & Governance**
  - Conduct frequent cybersecurity awareness sessions focusing on phishing, USB hygiene, and reporting procedures.
  - Conduct Table Top – Incident Response Testing for CSIRT teams and Table Top Cyber Crisis Management Testing for Executive Leadership.

MITRE ATTACK (TTP)

Tactic	Technique ID	Details
Reconnaissance	T1598.003	Phishing for Information: Spearphishing Link
Resource Development	T1583.001	Acquire Infrastructure: Domains
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.001	User Execution: Malicious Link
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.005	Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Defence Evasion	T1140	Deobfuscate/Decode Files or Information
	T1027.010	Obfuscated Files or Information: Command Obfuscation
Discovery	T1033	System Owner/User Discovery
	T1057	Process Discovery
	T1082	System Information Discovery
	T1083	File and Directory Discovery
Collection	T1005	Data from Local System
	T1113	Screen Capture
Exfiltration	T1041	Exfiltration Over C2 Channel

Indicator of Compromise

IoC	Type	Target_Industries	Related_Malware_Families
192[.]64[.]118[.]76	IPv4	Government & LEA	Crimson RAT
185[.]117[.]90[[.]]212	IPv4	Government & LEA	Crimson RAT
188[.]254[.]50[.]180	IPv4	BFSI, Government & LEA	CapraRAT,CobaltStrike,DarkComet,Dropbox,P2Pinfect,Pikabot,RDP,RemcosRAT,SideWinder,StrelaStealer,XMRig
104[.]16[.]155[.]36	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
104[.]20[.]16[.]242	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT, Crimson RAT,Dridex,Lazarus,LokiBot,Soul
104[.]20[.]17[.]242	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
109[.]123[.]244[.]46	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash,Uroburos
130[.]185[.]119[.]198	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash,Uroburos
140[.]82[.]57[.]249	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,RemcosRAT,Soul
144[.]126[.]154[.]84	IPv4		Crimson RAT,TinyTurla,Uroburos
154[.]53[.]42[.]194	IPv4		ActionRAT,Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash,Uroburos
162[.]213[.]195[.]129	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash,Uroburos
173[.]249[.]18[.]251	IPv4		Crimson RAT,TinyTurla,Uroburos,Wainscot
176[.]119[.]1[.]100	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
176[.]119[.]1[.]102	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
176[.]119[.]1[.]104	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul

176[.]119[.]1[.]99	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
183[.]82[.]101[.]78	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Emotet,Lazarus,LokiBot,Soul
184[.]254[.]253[.]254	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
185[.]213[.]27[.]94	IPv4		Crimson RAT,TinyTurla,Uroburos
185[.]217[.]125[.]195	IPv4		Uroburos
185[.]244[.]29[.]15	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
185[.]77[.]129[.]142	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
192[.]169[.]69[.]25	IPv4		Android RAT,AsyncRAT,Emotet,Mirai,NanoCore,NanoCore RAT,njRAT,QuasarRAT,RemcosRAT,SpyNote RAT,TrickBot
194[.]5[.]98[.]65	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NetWire RC,Soul
197[.]254[.]253[.]254	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
199[.]187[.]208[.]75	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
209[.]145[.]52[.]172	IPv4		ActionRAT,Crimson RAT,TinyTurla,TwoDash,Uroburos
37[.]60[.]236[.]186	IPv4		Crimson RAT,TinyTurla
38[.]242[.]207[.]36	IPv4		Crimson RAT,TinyTurla
38[.]242[.]211[.]87	IPv4		Crimson RAT,TinyTurla,Uroburos
45[.]14[.]194[.]253	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash,Uroburos
45[.]248[.]84[.]7	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
46[.]165[.]254[.]214	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
5[.]189[.]183[.]63	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash

66[.]42[.]78[.]193	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Soul
79[.]134[.]225[.]52	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NetWire RC,RemcosRAT,Soul
91[.]234[.]33[.]48	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash
94[.]177[.]198[.]94	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash
95[.]111[.]229[.]253	IPv4		Amadey,Crimson RAT,MiniPocket,TinyTurla,TwoDash
94[.]156[.]35[.]94	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Sliver,Soul
87[.]236[.]176[.]82	IPv4	BFSI	Agent Tesla,Amadey,Arkei Stealer,CapraRAT,Cobalt Strike,DarkComet,ftp,Hajime,Infostealer,IRATA,Mirai,Mozi,njRAT,RDP,RedLine,Smoke Loader,Stealc,Stealer,VNC,XMRig,ZXShell
143[.]110[.]179[.]176	IPv4	Aerospace & Defence, Government & LEA	ElizaRAT,httpclient
38[.]54[.]84[.]83	IPv4	Aerospace & Defence, Government & LEA	ElizaRAT,httpclient
64[.]227[.]134[.]248	IPv4	Aerospace & Defence, Government & LEA	ElizaRAT
83[.]171[.]248[.]67	IPv4	Aerospace & Defence, Government & LEA	ElizaRAT
84[.]247[.]135[.]235	IPv4	Aerospace & Defence, Government & LEA	ElizaRAT
103[.]1[.]184[.]108	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
103[.]200[.]5[.]128	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
104[.]206[.]98[.]246	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
104[.]244[.]75[.]220	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,RemcosRAT,Soul

109[.]230[.]215[.]181	IPv4	Aerospace & Defence, Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,QuasarRAT,Soul
142[.]44[.]161[.]51	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
151[.]106[.]56[.]110	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
160[.]202[.]163[.]240	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
160[.]202[.]163[.]244	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
173[.]254[.]223[.]125	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
178[.]124[.]140[.]145	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,Ave Maria,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
178[.]239[.]21[.]116	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
178[.]239[.]21[.]3	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
178[.]239[.]21[.]5	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
181[.]52[.]103[.]29	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
181[.]52[.]252[.]80	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
184[.]57[.]168[.]28	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
184[.]75[.]209[.]169	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul

184[.]75[.]209[.]190	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]101[.]94[.]172	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,Soul
185[.]105[.]236[.]134	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]105[.]236[.]176	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]140[.]53[.]140	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]140[.]53[.]149	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]140[.]53[.]175	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]140[.]53[.]253	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]140[.]53[.]64	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]140[.]53[.]76	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
185[.]140[.]53[.]91	IPv4		Ave Maria,NanoCore,RemcosRAT
185[.]140[.]53[.]95	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]163[.]45[.]199	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]114	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]121	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul

185[.]165[.]153[.]16	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]199	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]165[.]153[.]209	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]218	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]22	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]165[.]153[.]228	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]165[.]153[.]249	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]33	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]35	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]56	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]165[.]153[.]84	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]165[.]153[.]85	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]19[.]85[.]136	IPv4	Aerospace & Government & LEA	Agent Tesla,Akira,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]19[.]85[.]139	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul

185[.]19[.]85[.]141	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]19[.]85[.]177	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]19[.]85[.]183	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,Ave Maria,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]217[.]1[.]135	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]217[.]1[.]156	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]217[.]1[.]168	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]217[.]1[.]173	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
185[.]244[.]129[.]107	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]244[.]30[.]102	IPv4		NanoCore
185[.]244[.]30[.]121	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]244[.]31[.]18	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]244[.]31[.]24	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]247[.]228[.]17	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]4[.]29[.]173	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
185[.]84[.]181[.]67	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul

194[.]5[.]97[.]23	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]103	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]11	IPv4	Aerospace & Government & LEA	Agent Tesla,Akira,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]122	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]127	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]139	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,PowerShell RAT,RMS,Soul
194[.]5[.]98[.]14	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]16	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]17	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]186	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]21	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]23	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,RemcosRAT,Soul
194[.]5[.]98[.]251	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]26	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul,Warzone RAT

194[.]5[.]98[.]28	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]98[.]4	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]98[.]46	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,BitRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
194[.]5[.]99[.]121	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]99[.]14	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]99[.]22	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,Soul
194[.]5[.]99[.]222	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]5[.]99[.]9	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
194[.]67[.]209[.]128	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,RemcosRAT,Soul
198[.]23[.]210[.]211	IPv4		NanoCore
199[.]195[.]250[.]222	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
205[.]185[.]125[.]42	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
212[.]7[.]208[.]102	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,Soul
212[.]7[.]208[.]105	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
213[.]183[.]40[.]60	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,Soul

213[.]208[.]129[.]215	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
213[.]208[.]152[.]196	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
213[.]208[.]152[.]217	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
216[.]38[.]2[.]215	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
23[.]105[.]131[.]129	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
23[.]105[.]131[.]170	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
23[.]105[.]131[.]171	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
23[.]105[.]131[.]229	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
31[.]220[.]7[.]204	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
36[.]255[.]97[.]73	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
5[.]188[.]9[.]57	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
5[.]196[.]203[.]64	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
51[.]89[.]142[.]95	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
54[.]37[.]235[.]82	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul

67[.]253[.]236[.]155	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]100	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]102	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]103	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]104	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]105	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]106	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]108	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]11	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,Ave Maria,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]110	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]111	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]114	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]115	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,Mirai,NanoCore,Pay2Key,QuasarRAT,RemcosRAT,Soul
79[.]134[.]225[.]116	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul

79[.]134[.]225[.]119	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]12	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]120	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]121	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]122	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,RemcosRAT,Soul
79[.]134[.]225[.]123	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]125	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]126	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,RemcosRAT,Soul
79[.]134[.]225[.]13	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RedLine,RemcosRAT,Soul
79[.]134[.]225[.]19	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]23	IPv4	Aerospace & Government & LEA	Agent Tesla,Akira,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]26	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]27	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]32	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul

79[.]134[.]225[.]35	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]39	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]42	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]46	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,Astaroth,CapraRAT,Coinminer,Crimson RAT,DONOT,Dridex,Formbook,Lazarus,LokiBot,Meterpreter,NanoCore,Parallax RAT,PlugX,PowerShell RAT,RecordBreaker,RemcosRAT,Socelars,Soul,Stealc
79[.]134[.]225[.]48	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]55	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]58	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]6	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,RemcosRAT,Soul
79[.]134[.]225[.]69	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,Soul
79[.]134[.]225[.]7	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]72	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]73	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,BitRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,RMS,Soul
79[.]134[.]225[.]75	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul

79[.]134[.]225[.]79	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,QuasarRAT,RemcosRAT,Soul
79[.]134[.]225[.]83	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]84	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]85	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
79[.]134[.]225[.]87	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,PowerShell RAT,RemcosRAT,Soul
79[.]134[.]225[.]9	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]90	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,RemcosRAT,Soul,ViperSoftX
79[.]134[.]225[.]91	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
79[.]134[.]225[.]92	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]94	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,Astaroth,CapraRAT,Coinminer,Crimson RAT,DONOT,Dridex,Formbook,Lazarus,LokiBot,Meterpreter,NanoCore,Parallax RAT,PlugX,RecordBreaker,RemcosRAT,Socelars,Soul,Stealc
79[.]134[.]225[.]95	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,Astaroth,AsyncRAT,CapraRAT,Coinminer,Crimson RAT,DONOT,Dridex,Formbook,Lazarus,LokiBot,Meterpreter,NanoCore,Parallax RAT,PlugX,RecordBreaker,RemcosRAT,Socelars,Soul,Stealc
79[.]134[.]225[.]96	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,RemcosRAT,Soul

79[.]134[.]225[.]97	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul ,XpertRAT
79[.]134[.]225[.]98	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
79[.]134[.]225[.]99	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
80[.]85[.]153[.]187	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
88[.]150[.]227[.]112	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]109[.]178[.]4	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,QuasarRA T,Soul
91[.]109[.]178[.]8	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,QuasarRA T,Soul
91[.]109[.]182[.]3	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
91[.]109[.]184[.]2	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]109[.]184[.]9	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
91[.]109[.]186[.]4	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,Soul
91[.]189[.]180[.]211	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]189[.]180[.]216	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]189[.]180[.]218	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul

91[.]192[.]100[.]11	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]192[.]100[.]14	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]192[.]100[.]16	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]192[.]100[.]25	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
91[.]192[.]100[.]39	IPv4	Aerospace & Defence,BFSI,Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Cobalt Strike,Crimson RAT,DarkComet,DragonEgg,Dridex,Emotet,GuLoader,Lazarus,LokiBot,Mirai,NanoCore,NanoCore RAT,P2Pinfect,Pay2Key,RDP,Soul,WyrmSpy,XWorm
91[.]192[.]100[.]4	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
91[.]192[.]100[.]7	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
91[.]193[.]75[.]138	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]193[.]75[.]139	IPv4	Aerospace & Government & LEA	Agent Tesla,Android RAT,AndroRAT,AsyncRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul,ZXShell
91[.]193[.]75[.]218	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]193[.]75[.]239	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,RemcosRAT,Soul
91[.]193[.]75[.]25	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
91[.]193[.]75[.]252	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,njRAT,RemcosRAT,Soul
91[.]193[.]75[.]53	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul

91[.]218[.]65[.]24	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,Soul
91[.]233[.]116[.]105	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,NanoCore RAT,QuasarRAT,Soul
92[.]53[.]66[.]44	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,QuasarRAT,Soul
94[.]130[.]239[.]15	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,Soul
95[.]213[.]251[.]165	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Lazarus,LokiBot,NanoCore,PowerShell RAT,Soul
144[.]139[.]247[.]220	IPv4	Aerospace & Government & LEA	DoubleZero,Emotet,TrickBot,ZXShell
181[.]143[.]194[.]138	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Emotet,Lazarus,LokiBot,Soul
182[.]76[.]6[.]2	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Emotet,Lazarus,LokiBot,Soul
186[.]75[.]241[.]230	IPv4	Aerospace & Government & LEA	Emotet,ZXShell
67[.]225[.]229[.]55	IPv4	Aerospace & Government & LEA	Agent Tesla,AndroRAT,CapraRAT,Crimson RAT,Dridex,Emotet,Lazarus,LokiBot,Soul
80[.]11[.]163[.]139	IPv4	Aerospace & Government & LEA	DoubleZero,Emotet,ZXShell
87[.]236[.]176[.]87	IPv4	BFSI	AgentTesla,Amadey,AsyncRAT,CapraRAT,ClearFake,Cobalt Strike,DarkComet,Epsilon Stealer,Fabookie,ftp,Gh0st RAT,Glupteba,Hajime,Infostealer,IRATA,LaplasClipper,Mirai,Mozi,njRAT
78[.]187[.]21[.]105	IPv4	BFSI, Government & LEA	Agent Tesla,Amadey,AsyncRAT,Ave Maria,BokBot,CapraRAT,Cobalt
71[.]6[.]232[.]27	IPv4	BFSI	CapraRAT,Cobalt Strike,DarkComet,Dropbox,MintStealer,Mirai,Moudoor,RDP,VNC
87[.]236[.]176[.]120	IPv4	Aerospace & Defence,BFSI,Government & LEA	AnyDesk,BlackCat,CapraRAT,Cobalt Strike,Deadglyph,ftp,LockBit,Metasploit,Meterpreter,Mirai,QakBot,RDP,RemcosRAT,Spyder,VNC,WinSCP

IoC	Type	Target_Industries	Related_Malware_Families
20b4eb5787faa00474f7d27c0fea1e4b	FileHash-MD5	Government & LEA	DISGOMOJI
9f3359ae571c247a8be28c0684678304	FileHash-MD5	Government & LEA	DISGOMOJI
e0102071722a87f119b12434ae651b48	FileHash-MD5	Government & LEA	DISGOMOJI
13ee4bd10f05ee0499e18de68b3ea4d5	FileHash-MD5	Government & LEA	DISGOMOJI
f2501e8b57486c427579eeda20b729fd	FileHash-MD5	Government & LEA	DISGOMOJI
f14e778f4d22df275c817ac3014873dc	FileHash-MD5	Government & LEA	DISGOMOJI
635864ff270cf8e366a7747fb5996766	FileHash-MD5	Government & LEA	DISGOMOJI
60fc5dc410b7482566a74d03549d8246	FileHash-MD5	Government & LEA	DISGOMOJI
c9969ece7bb47efac4b3b04cdc1538e5	FileHash-MD5	Government & LEA	DISGOMOJI
ee8d767069faf558886f1163a92e4009	FileHash-MD5	Government & LEA	DISGOMOJI
7c736e2d2333463fbfe179b1929e3317	FileHash-MD5	Government & LEA	HTA file associated with the Windows ClickFix technique
026e8e7acb2f2a156f8afff64fd54066	FileHash-MD5		Crimson RAT
70b8040730c62e4a52a904251fa74029	FileHash-MD5		Crimson RAT
d946e3e94fec670f9e47aca186ecaabe	FileHash-MD5		Crimson RAT
fb64c22d37c502bde55b19688d40c803	FileHash-MD5		Crimson RAT
e948aa916d1f9f9b5bba72ad7de7e27f	FileHash-MD5		Crimson RAT
2fde001f4c17c8613480091fa48b55a0	FileHash-MD5		Crimson RAT
b03211f6feccd3a62273368b52f6079d	FileHash-MD5		Crimson RAT
c1f4c9f969f955dec2465317b526b600	FileHash-MD5		Crimson RAT
e18c4172329c32d8394ba0658d5212c2	FileHash-MD5		Crimson RAT
3efec6ffcbfe79f71f5410eb46f1c19e	FileHash-MD5		Crimson RAT
905134a46153e071d453e086dc37c47a	FileHash-MD5		
609308aa7da464c40cb2927ebf01793a	FileHash-MD5		
e2babc163a149bc6ff79a3d43aeb54e7	FileHash-MD5		

IoC	Type	Target_Industries
expressholidays[.]co[.]in	Domain	Government & LEA
avtzyu[.]store	Domain	Government & LEA
drdosurvey[.]info	Domain	Government & LEA
nationaldefensecollege[.]com	Domain	
nationaldefencebackup[.]xyz	Domain	