INTRUSIVENT

Threat Actor Profile

Agrius

Hybrid Advanced Operations Group | Pink Sandstorm | Agonizing Serpens

ALIAS ACTIVITY	TLP:CLEAR
Last Update: March 27, 2026	Analysis Level: Level 1 - Initial

Intrusiveny Technologies

ADD YOUR LOGO HERE or ✉

12+

2 actors (Agrius and Lunder) active from Deployment Since 2021

Operations Against Critical Infrastructure, Technology & Financial Sectors

Attribution & Identity

OPERATIONAL CONFIDENCE: LOW

Agrius is associated with high confidence to an offensive cyber operations group exploiting zero-day vulnerabilities and deploying destructive wiper malware against critical infrastructure, technology, and financial sectors. The group's operational tempo, tool development, and target selection are consistent with state-sponsored activity. Attribution to a specific nation-state remains unverified. Confidence in the group's existence and capabilities is high; confidence in its attribution is low.

Background

Agrius is a threat actor assessed to have been active since at least late 2020, conducting hybrid cyber operations that combine ransomware deployment with data destruction and wiper malware. The group's operational tempo, tool development, and target selection are consistent with state-sponsored activity. Attribution to a specific nation-state remains unverified. Confidence in the group's existence and capabilities is high; confidence in its attribution is low.

Lunder is a threat actor assessed to have been active since at least late 2021, conducting hybrid cyber operations combining ransomware deployment with data destruction and wiper malware. The group's operational tempo, tool development, and target selection are consistent with state-sponsored activity. Attribution to a specific nation-state remains unverified. Confidence in the group's existence and capabilities is high; confidence in its attribution is low.

Both actors have been observed deploying custom ransomware, including Apostle, Detonate, Retadup, Chaos, and Sphinx, and frequently use custom wipers or ransomware before exfiltration. The actors' tradecraft includes persistent, hands-on-keyboard activity, lateral movement, and the exploitation of internet-facing vulnerabilities.

Both actors have been observed using custom tools for credential theft, persistence, and data staging. Public reporting has described the use of custom implants such as Kapeka, Chaos, and variants of Sphinx. Many operations include data exfiltration prior to ransomware or wiper deployment, consistent with double extortion and pre-encryption data theft.

Public reporting has described overlapping tools, infrastructure, and tradecraft between Agrius and Lunder, including shared use of custom implants and ransomware families. This overlap is consistent with a shared operational environment, but does not by itself establish a single operator or a single nation-state actor.

Aliases

- Hybrid Advanced Operations Group
- Pink Sandstorm
- Agonizing Serpens
- Lunder
- Pink Sandstorm
- Agonizing Serpens

Operational Focus

- Ransomware
- Wiper
- Data Destruction
- Credential Theft
- Persistence
- Lateral Movement

Sectors Observed

- Energy: Oil & Gas, Utilities
- Technology: Software, Cloud Infrastructure
- Financial Services: Banking, Payment Processing
- Manufacturing: Industrial Equipment
- Telecommunications: Carrier Networks
- Government: Critical Infrastructure, Defense

Geographic Footprint

- Middle East: Israel, UAE, Saudi Arabia
- Eastern Europe: Ukraine, Poland
- Western Europe: Germany, Netherlands, Switzerland
- North America: United States, Canada
- Asia-Pacific: Japan, South Korea, Taiwan, Australia

Infrastructure Footprint

- Hosting: Bulletproof hosting providers, VPS providers, Cloud provider abuse
- Domains: Typosquatting, DDNS providers, Dynamic DNS
- Tunneling/Proxy: VPN, Tor, SOCKS proxies, Residential proxy networks
- Exfiltration: Cloud storage, File sharing services, Messaging platforms
- Persistence: Scheduled tasks, Registry run keys, Service installation
- Lateral Movement: SMB, RDP, WMI, PsExec, Remote PowerShell
- Initial Access: Exploitation of internet-facing vulnerabilities, Credential abuse, Phishing
- Malware Delivery: Custom implants, Ransomware, Wiper malware
- Data Staging: Archive tools, Encrypted containers, Cloud storage
- Data Exfiltration: Cloud storage, File sharing services, Messaging platforms

Operational Tempo

- Active Campaigns: Multiple concurrent campaigns across different sectors
- Tool Development: Rapid iteration, custom tool development observed
- Target Selection: Opportunistic + targeted, vulnerability-driven
- Attribution Confidence: Low — Consistent with state-sponsored activity, nation-state attribution unverified

Targeting Profile

Sector Focus

- **Industrial (ICS/OT):** (2020–2026) Oil & gas, utilities, manufacturing. Wiper deployment, data destruction.
- **Technology:** (2021–2026) Software, cloud infrastructure. Ransomware, supply chain compromise.
- **Financial Services:** (2021–2026) Banks, payment processors. Ransomware, credential theft.
- **Government:** (Recent, 2025) Defense, critical infrastructure. Espionage, data exfiltration.

Geographic Focus

- **Israel** (Primary, 2020–present)
- **Gulf States** (Secondary, 2021–present): UAE, Saudi Arabia
- **Eastern Europe** (Secondary, 2022–present): Ukraine, Poland
- **Global** (Opportunistic, 2021–present): Victims in 30+ countries

Target Selection Criteria

- **Initial Access Exploitation:** (2020–present) Internet-facing vulnerabilities, VPN, RDP, web applications
- **Lateral Movement:** (2020–present) SMB, RDP, WMI, PsExec, Remote PowerShell
- **Data Staging:** (2020–present) Archive tools, encrypted containers, cloud storage
- **Exfiltration:** (2020–present) Cloud storage, file sharing services, messaging platforms
- **Persistence:** (2020–present) Scheduled tasks, registry run keys, service installation

Exploitation Vectors

- **Internet-facing vulnerabilities:** (2020–present) VPN, RDP, web applications
- **Credential abuse:** (2020–present) Valid accounts, password spraying
- **Phishing:** (2020–present) Spear phishing, credential harvesting

Victim Profile

- **Industrial (ICS/OT):** (2020–present) Oil & gas, utilities, manufacturing. Wiper deployment, data destruction.
- **Technology:** (2021–present) Software, cloud infrastructure. Ransomware, supply chain compromise.
- **Financial Services:** (2021–present) Banks, payment processors. Ransomware, credential theft.
- **Government:** (Recent, 2025) Defense, critical infrastructure. Espionage, data exfiltration.

Operational Impact

- **Primary:** Data destruction, ransomware deployment, credential theft, persistent access
- **Secondary:** Espionage, data exfiltration, supply chain compromise

Tactics, Techniniques & Procedures

INITIAL ACCESS

- **T1190** – Exploit Public-Facing Application: Exploitation of internet-facing vulnerabilities (VPN, RDP, web applications)
- **T1133** – External Remote Services: Abuse of VPN, RDP, and other remote access services

PERSISTENCE

- **T1053** – Scheduled Task/Job: Scheduled tasks for persistence
- **T1547** – Boot or Logon Autostart Execution: Registry run keys, service installation

COMMAND & CONTROL

- **T1090** – Proxy: Use of proxies and tunneling for C2 obfuscation
- **T1071** – Application Layer Protocol: HTTP/HTTPS, DNS, SMB for C2 communication

DISCOVERY

- **T1082** – System Information Discovery: Enumeration of OS, hardware, and network configuration
- **T1083** – File and Directory Discovery: Enumeration of files and directories

LATERAL MOVEMENT

- **T1021** – Remote Services: Lateral movement via SMB, RDP, WMI, PsExec, Remote PowerShell

DEFENSE EVASION

- **T1027** – Obfuscated Files or Information: Custom encoding and obfuscation

EXFILTRATION

- **T1041** – Exfiltration Over C2 Channel: Data exfiltration over command and control channel
- **T1048** – Exfiltration Over Alternative Protocol: Exfiltration via HTTP/HTTPS, DNS, SMB

IMPACT

- **T1486** – Data Encrypted for Impact: Ransomware deployment
- **T1561** – Disk Wipe: Wiper deployment, data destruction

Kill Chain Analysis: Exploitation, Persistence, Data Staging

Tooling & Infrastructure

Known Malware

Malware	Type	Notes
Apostle (Agrius)	Ransomware	Custom ransomware deployed against critical infrastructure. Observed in operations Since 2021. File extension: .encrypted. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable.
Detonate (Agrius)	Ransomware	Custom ransomware deployed against critical infrastructure. Observed in operations Since 2021. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable.
Retadup (Agrius)	Botnet / Backdoor	Custom botnet with ransomware capabilities. Observed in operations Since 2021. Used for initial access and persistence. Ransomware: Sphinx.
Chaos (Agrius)	Ransomware	Ransomware deployed against critical infrastructure. Observed in operations Since 2021. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable.
Sphinx (Agrius)	Ransomware	Ransomware deployed against critical infrastructure. Observed in operations Since 2021. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable.
Kapeka (Lunder)	Backdoor	Custom implant observed in ransomware operations. Used for persistence and command execution. Observed in operations Since 2021.
Wiper (Agrius)	Wiper	Custom wiper deployed in destructive operations. Observed in operations Since 2021. Used prior to ransomware deployment in some operations.

Infrastructure

Category	Details
Hosting	Bulletproof hosting providers, VPS providers, Cloud provider abuse. Observed in operations Since 2021. Used for C2 servers and data staging.
Domains	Typosquatting, DDNS providers, Dynamic DNS. Observed in operations Since 2021. Used for C2 domains and phishing infrastructure.
Tunneling/Proxy	VPN, Tor, SOCKS proxies, Residential proxy networks. Observed in operations Since 2021. Used for C2 obfuscation and lateral movement.
Exfiltration	Cloud storage, File sharing services, Messaging platforms. Observed in operations Since 2021. Used for data exfiltration.

Software Tools (Other/Third Party)

Tool	Purpose
Cobalt Strike	Post-exploitation framework used for lateral movement, persistence, and command and control. Observed in operations Since 2021.
Mimikatz	Credential dumping tool used for credential access. Observed in operations Since 2021.
Impacket	Network protocol implementation used for lateral movement. Observed in operations Since 2021.
PsExec	Remote execution tool used for lateral movement. Observed in operations Since 2021.
Rclone	Cloud syncing tool used for data exfiltration. Observed in operations Since 2021.
WMI	Windows Management Instrumentation used for persistence and lateral movement. Observed in operations Since 2021.
Custom Scripts	Custom scripts for data staging and automation. Observed in operations Since 2021.

Intrusion Campaigns

SHAR Insurance Attack (Blackthorn) Active Threat

Since: Late 2025 | Sectors: Insurance

Threat actor exploiting a zero-day vulnerability in the "Blackthorn" platform, the pre-authentication RCE vulnerability, to gain initial access to insurance organizations. Post-exploitation activity includes credential harvesting, lateral movement, and data exfiltration, consistent with ransomware operations. The campaign established the pattern of using Blackthorn exploitation for initial access across multiple victims.

Bar Ilan University (Apostle v2) Active Threat

Since: Late 2025 | Sectors: Education

Deployment of Apostle ransomware v2 (.encrypted extension) against Bar-Ilan University, a major Israeli university. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable. Part of a broader campaign against Israeli educational institutions using Apostle ransomware. Data exfiltration prior to encryption is assessed but not confirmed.

Cyberserv / Intel Data Lost (Blackthorn) Active Threat

Since: Late 2025 | Sectors: Technology, Data Services

Exploitation of Blackthorn platform vulnerabilities, an email data security company, gaining access to data from multiple customers. The incident affected at least 20 organizations, including a major Israeli telecommunications provider. Data was exfiltrated and subsequently extorted from the victims. The operation demonstrated the ability to pivot from a single vulnerable platform to many downstream victims.

Factory Supply Chain Attack Active Threat

Since: Late 2025 | Sectors: Manufacturing, Supply Chain

Agrius is assessed to have compromised software vendor Factory for Network Monitoring to deploy the Sphinx ransomware. The vendor's software was used by multiple manufacturing customers, enabling the attack to propagate across customer networks. Sphinx ransomware was deployed on systems managed by Factory, affecting downstream customers. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable. Data exfiltration prior to encryption is assessed but not confirmed. Factory has been notified and is investigating the compromise.

Algiers Educational Scan Harvester Campaign Active Threat

Since: Late 2025 | Sectors: Education, Research

Mass scanning and exploitation of internet-facing educational infrastructure in Algiers, Algeria. Observed activity includes port scanning, vulnerability probing, and credential harvesting against educational institutions. Scanning infrastructure overlaps with Lunder operations. Target selection is opportunistic, consistent with automated vulnerability scanning rather than targeted intrusion. Data exfiltration and ransomware deployment have not been observed in this campaign. Assessed with low confidence as part of Lunder operational tempo.

Ransomware/Extortion Active Threat

Since: Late 2020 | Sectors: Multi-sector

Ransomware deployment and double extortion across multiple sectors. Victims include organizations in Israel, UAE, Saudi Arabia, Ukraine, Poland, Germany, Netherlands, Switzerland, United States, Canada, Japan, South Korea, Taiwan, and Australia. Ransom demands typically range from 0.5 BTC. Data exfiltration prior to encryption is assessed but not confirmed. Decryptors are unavailable for all known ransomware families.

Ukrainian Currency Scanning Active Threat

Since: Late 2025 | Sectors: Financial Services

Scanning the Factory Web Server (CVE-2025-2825), Agrius's Shared Infrastructure, for exploitable Ukrainian currency exchange services. Activity includes port scanning and vulnerability probing against Ukrainian financial services. Target selection is opportunistic, consistent with automated vulnerability scanning. Data exfiltration and ransomware deployment have not been observed in this campaign. Assessed with low confidence as part of Lunder operational tempo.

BlackMagic (Sanctioned Israeli Employer) Active Threat

Since: Late 2025 | Sectors: Technology, Defense, Manufacturing

Agrius is assessed to have compromised a sanctioned Israeli employer, BlackMagic, to gain access to customer networks. Post-compromise activity includes credential harvesting and lateral movement. All three victim deployments used a Cobalt Strike beacon.

Aquarelle Gas Corp Pressure Active Threat

Since: Late 2025 | Sectors: Energy, Oil & Gas

Attempted ransomware against Aquarelle Gas Corp, a major Israeli gas utility, on December 2025. Ransom demand: 0.5 BTC. Contact: tutanota.com/protonmail.com. Decryptor unavailable. Data exfiltration prior to encryption is assessed but not confirmed. Part of a broader campaign against Israeli critical infrastructure using Apostle ransomware.

Detection & Response Recommendations

Detection Opportunities

Wiper Activity Detection

- Monitor for mass file modification activity (modification events, deletions)
- Alert on bulk modification or MBR writing attempts
- Correlate wiper activity with prior ransomware deployment (multi-stage attack)
- Monitor for SMB/RDP connections with mass compromise indicators
- Alert on PsExec or scheduled task mass compromise

Ransomware-as-Cover Indicators

- Ransomware deployment after wiper activity
- Unusual ransomware ransom amounts (0.5 BTC pattern)
- Ransomware deployment on systems previously wiped
- Multi-stage attack: wiper → ransomware

Data Exfiltration

- Monitor for unusual outbound traffic patterns
- Detect large data transfers (archive creation, encryption)
- Alert on unusual cloud storage access
- Monitor DNS for tunneling indicators

Lateral Movement & Persistence

- Monitor for SMB, RDP, WMI, PsExec, Remote PowerShell activity
- Alert on new scheduled tasks, registry run keys, service installation
- Track credential access events (LSASS access, credential dumping)
- Monitor for Kerberos ticket anomalies (Kerberoasting, Golden Ticket)

Initial Access

- Monitor for exploitation of internet-facing vulnerabilities (VPN, RDP, web applications)
- Alert on unusual remote access patterns (geo-anomalies, off-hours access)
- Track failed authentication attempts (password spraying, brute force)

Sample Detection Queries

Splunk (Wiper Activity)

```
index=windows (EventCode=4663 OR EventCode=4660)
| stats count by host, EventCode
| where count > 100
| eval severity="Mass File Modification"
| table _time, host, EventCode, count, severity
| sort - count
```

Custom Sigma Rule

```
title: Agrius Wiper Activity - Mass File Modification
logsource:
  product: windows
  service: security
detection:
  selection:
    EventCode: 4663
    ObjectName|contains: '*'
  timeframe: 5m
  condition: selection | count > 100
fields:
  - ComputerName
  - SubjectUserName
  - ObjectName
  - EventCode
  - count
```

Splunk (Lateral Movement)

```
index=windows (EventCode=4624 OR EventCode=4625)
| stats count by Source_Network_Address, Logon_Type
| where count > 50
| eval severity="Lateral Movement"
| table _time, Source_Network_Address, Logon_Type, count, severity
| sort - count
```

Splunk (Data Exfiltration)

```
index=network (sourcetype=firewall OR sourcetype=proxy)
| stats sum(bytes_out) by src_ip, dest_ip
| where sum(bytes_out) > 1073741824
| eval severity="Data Exfiltration"
| table _time, src_ip, dest_ip, sum(bytes_out), severity
| sort - sum(bytes_out)
```

Sigma Rule (Credential Access)

```
title: Agrius Credential Access - Mass Credential Access Events
logsource:
  product: windows
  service: security
detection:
  selection:
    EventCode: 4663
    ObjectName|contains: '*'
  timeframe: 5m
  condition: selection | count > 100
fields:
  - ComputerName
  - SubjectUserName
  - ObjectName
  - EventCode
  - count
```

Sigma Rule (Data Exfiltration)

```
title: Agrius Data Exfiltration - Large Outbound Transfer
logsource:
  product: network
  service: firewall
detection:
  selection:
    bytes_out: > 1073741824
  timeframe: 1h
  condition: selection
fields:
  - src_ip
  - dest_ip
  - bytes_out
```

Sigma Rule (Lateral Movement)

```
title: Agrius Lateral Movement - Mass Remote Logon Attempts
logsource:
  product: windows
  service: security
detection:
  selection:
    EventCode: 4624
    Source_Network_Address|contains: '*'
  timeframe: 5m
  condition: selection | count > 50
fields:
  - ComputerName
  - SubjectUserName
  - Source_Network_Address
  - Logon_Type
  - EventCode
  - count
```

Wiper Activity Detection

```
Monitor for:
- Mass file modification events (EventCode 4663)
- Bulk deletion patterns
- MBR writing attempts
- Correlate with ransomware deployment (multi-stage attack)
```

Ransomware-as-Cover Indicators

```
Monitor for:
- Ransomware deployment after wiper activity
- Unusual ransom amounts (0.5 BTC pattern)
- Ransomware deployment on systems previously wiped
- Multi-stage attack: wiper → ransomware
```

Data Exfiltration

```
Monitor for:
- Unusual outbound traffic patterns
- Large data transfers (archive creation, encryption)
- Unusual cloud storage access
- DNS tunneling indicators
```

Lateral Movement & Persistence

```
Monitor for:
- SMB, RDP, WMI, PsExec, Remote PowerShell activity
- New scheduled tasks
- Registry run keys
- Service installation
- Credential access events (LSASS access, credential dumping)
- Kerberos ticket anomalies (Kerberoasting, Golden Ticket)
```

Initial Access

```
Monitor for:
- Exploitation of internet-facing vulnerabilities (VPN, RDP, web applications)
- Unusual remote access patterns (geo-anomalies, off-hours access)
- Failed authentication attempts (password spraying, brute force)
```

Threat Hunting Queries

Splunk (Wiper Activity)

```
index=windows (EventCode=4663 OR EventCode=4660)
| stats count by host, EventCode
| where count > 100
| eval severity="Mass File Modification"
| table _time, host, EventCode, count, severity
| sort - count
```

Splunk (Lateral Movement)

```
index=windows (EventCode=4624 OR EventCode=4625)
| stats count by Source_Network_Address, Logon_Type
| where count > 50
| eval severity="Lateral Movement"
| table _time, Source_Network_Address, Logon_Type, count, severity
| sort - count
```

Splunk (Data Exfiltration)

```
index=network (sourcetype=firewall OR sourcetype=proxy)
| stats sum(bytes_out) by src_ip, dest_ip
| where sum(bytes_out) > 1073741824
| eval severity="Data Exfiltration"
| table _time, src_ip, dest_ip, sum(bytes_out), severity
| sort - sum(bytes_out)
```

Splunk (Credential Access)

```
index=windows (EventCode=4663 OR EventCode=4660)
| stats count by host, EventCode
| where count > 100
| eval severity="Credential Access"
| table _time, host, EventCode, count, severity
| sort - count
```

Appendix A: Indicators of Compromise

Attacking Infrastructure & File Hash Classifications

- **C2 Infrastructure** (Command & Control): Active command and control servers.
- **Exploitation Infrastructure**: Servers used for vulnerability exploitation (such as Typeframe), gas, cloud, or other attack-enabling infrastructure.
- **Malware Hosting**: Servers hosting malicious payloads.
- **Exploitation Activity**: Observed exploitation attempts.
- **Malware Activity**: Observed malware execution.
- **Scanning Activity**: Reconnaissance or vulnerability scanning.
- **Victim Activity**: Confirmed victim connections.
- **Stage 1 Payload**: Initial malware payload.
- **Stage 2 Payload**: Secondary payload.
- **Stage 3 Payload**: Tertiary payload.
- **Malware Variant**: Specific malware variant.
- **Ransomware Activity**: Ransomware deployment.
- **Data Exfiltration Activity**: Data exfiltration activity.
- **Credential Theft Activity**: Credential theft activity.
- **Lateral Movement Activity**: Lateral movement activity.
- **Persistence Activity**: Persistence mechanism activity.
- **Defense Evasion Activity**: Defense evasion activity.
- **Discovery Activity**: Discovery activity.
- **Command Execution Activity**: Command execution activity.
- **Initial Access Activity**: Initial access activity.
- **Impact Activity**: Impact activity.

IP Addresses

IP Address	Type	Notes
185.193.126.237	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.235	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.236	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.238	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.239	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.240	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.241	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.242	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.243	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.244	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.245	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.246	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.247	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.248	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.249	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.250	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.251	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.252	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.253	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.254	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.255	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.256	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.257	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.258	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.259	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.260	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.261	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.262	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.263	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.264	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.265	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.266	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.267	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.268	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.269	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.270	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.271	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.272	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.273	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.274	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.275	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.276	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.277	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.278	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.279	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.280	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.281	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.282	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.283	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.284	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.285	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.286	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.287	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.288	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.289	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.290	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.291	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.292	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.293	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.294	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.295	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.296	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.297	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.298	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.299	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.300	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.301	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.302	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.303	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.304	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.305	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.306	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.307	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.308	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.309	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.310	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.311	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.312	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.313	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.314	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.315	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.316	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.317	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.318	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.319	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.320	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.321	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.322	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.323	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.324	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.325	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.326	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.327	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.328	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.329	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.330	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.331	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.332	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.333	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.334	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.335	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.336	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.337	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.338	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.339	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.340	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.341	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.342	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.343	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.344	C2 Infrastructure	Apostle ransomware v2 C2 server. Bar Ilan University attack. Observed Since 2025.
185.193.126.345	C2