INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 13:42 UTC

Dutch FIOD Dismantles Sanctions-Evasion Bulletproof Hosting Network Supporting Russian Cyber and Disinformation Operations

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0355
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Stark Industries hosting infrastructure, WorkTitans B.V. / THE.Hosting, Mirhosting, European-hosted servers used by pro-Russian threat actors
Published	2026-05-22T13:24:52
Discovery Source	Rss

Executive Summary

Dutch law enforcement arrested two individuals and seized roughly 800 servers from WorkTitans B.V. / THE.Hosting, a bulletproof hosting shell linked to Stark Industries Solutions that provided operational infrastructure for pro-Russian hacktivist group NoName057(16) and associated disinformation campaigns. The network systematically reconstituted under new corporate identities each time EU sanctions were applied, enabling sustained DDoS attacks against European government, financial, and democratic institutions. Organizations in these sectors face continued risk from affiliated groups, as the infrastructure seizure degrades but does not eliminate operational capability.

Technical Analysis

The FIOD action targeted the infrastructure layer of a sanctions-evasion network operated by WorkTitans B.V. (brand: THE.Hosting), linked to Stark Industries Solutions and Mirhosting. Approximately 800 servers were seized across European hosting facilities. The network supported NoName057(16) TTPs documented under MITRE ATT&CK: volumetric and direct-path DDoS (T1498, T1498.001, T1499), resource hijacking (T1496), acquisition of bulletproof hosting and virtual private servers (T1583.003, T1583.004), compromise of third-party infrastructure (T1584.004), use of compromised accounts (T1586), target reconnaissance including victim organization and personnel enumeration (T1591, T1589), and infrastructure obfuscation / hide artifacts (T1665). Stark Industries has a documented pattern of preemptively spinning up new corporate shells before EU sanctions take effect, preserving BGP routing and server capacity under new legal entities. No CVE or CWE

applies, this is a threat infrastructure disruption, not a software vulnerability. Affected infrastructure is confirmed as Stark Industries / WorkTitans B.V. / Mirhosting ASNs and associated IP ranges; Recorded Future and GreyNoise have published ASN and IP attribution data for these entities.

Action Checklist

1. Step 1: Containment, Block inbound and outbound traffic to IP ranges and ASNs attributed to Stark Industries Solutions, WorkTitans B.V. / THE.Hosting, and Mirhosting at your perimeter firewall and upstream DDoS mitigation provider. Reference GreyNoise and Recorded Future published attribution data for current IP ranges. Prioritize internet-facing government portals, banking applications, and election-adjacent systems matching NoName057(16) target profiles.
2. Step 2: Detection, Query firewall, NetFlow, and DDoS protection logs for volumetric spikes (T1498), SYN/UDP/HTTP flood patterns (T1498.001), and application-layer exhaustion (T1499) originating from Stark Industries / Mirhosting ASNs. Search SIEM for reconnaissance indicators: automated enumeration of public-facing endpoints, login-page probing bursts, and credential stuffing patterns against externally exposed applications (NIST SI-4, CIS 8.2 audit logging controls). Alert on any new BGP announcements from ASNs historically associated with these entities.
3. Step 3: Eradication, Remove any access rules or allow-list entries permitting traffic from attributed Stark Industries IP space. If your organization uses any THE.Hosting or Mirhosting services (even indirectly through upstream providers), identify and terminate those dependencies. Rotate credentials for any accounts that may have been exposed to reconnaissance activity (NIST IA-4 Credential Management and IA-5 Authentication Mechanisms). Verify that DDoS scrubbing services and rate-limiting rules are enforced across all internet-facing properties (CIS 4.4, CIS 4.5).
4. Step 4: Recovery, Confirm DDoS mitigation controls are active and capacity-tested against volumetric thresholds relevant to your sector. Validate NIST AU-6 (Audit Record Review) processes are generating alerts on anomalous traffic volumes. Test contingency plans for service degradation under sustained DDoS per NIST CP-4 (Contingency Plan Testing). Confirm alternate processing and telecommunications paths are available per NIST CP-7 and CP-8 if primary infrastructure is targeted.
5. Step 5: Post-Incident, Assess whether your organization's internet-facing asset inventory (CIS 1.1) and exposure surface matches NoName057(16) historical target profiles (government, financial, democratic institutions). Review IP blocklist update frequency, static block lists will not track Stark Industries reconstitution events. Establish a recurring review process for new corporate shells and ASN registrations linked to known bulletproof hosting networks, using threat intelligence feeds that cover infrastructure-layer indicators. Document gaps in DDoS response playbooks per NIST IR-8 (Incident Response Plan).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and upstream DDoS mitigation provider if sustained volumetric traffic from Stark Industries / Mirhosting ASNs causes measurable service degradation to internet-facing portals (>5% error rate or latency increase >200ms), if any THE.Hosting or Mirhosting infrastructure dependency is discovered in your supply chain (triggering potential EU sanctions compliance exposure), or if reconnaissance patterns indicate active credential harvesting against externally exposed applications serving citizens or account holders (triggering breach notification assessment obligations under GDPR Article 33 or applicable national law).
Recovery Notes	Following containment, maintain enhanced traffic monitoring on internet-facing portals for a minimum of 30 days — NoName057(16) has demonstrated a pattern of pausing DDoS campaigns and resuming after defenders stand down, particularly targeting European government and financial services during high-visibility political events such as elections or NATO-related announcements. Validate daily that your IP blocklist reflects current Stark Industries-attributed CIDR ranges by diffing against GreyNoise community data and Spamhaus DROP updates, as the Stark Industries reconstitution model means new hosting ASNs may become active within days of the FIOD seizure as the network rebuilds under new corporate identities. Confirm all DDoS scrubbing, rate-limiting, and alternate processing path controls remain enforced and have not been silently disabled or misconfigured during the recovery push, and schedule a CP-4 contingency plan retest within 30 days.
Forensic Artifacts	NetFlow records (nfcapd binary files or exported CSV/JSON) from the 72-hour window bracketing first observed Stark Industries ASN traffic, preserving source IP, destination IP, protocol, packet count, byte count, and flow start/end timestamps — these establish flood onset, peak, and withdrawal timing specific to NoName057(16) DDoS campaign pacing | Web server access logs (nginx /var/log/nginx/access.log or Apache /var/log/apache2/access.log) with complete fields including source IP, HTTP method, URI, status code, response size, User-Agent, and X-Forwarded-For headers — filter for high-frequency POST requests to authentication endpoints from Mirhosting and WorkTitans B.V. CIDR ranges as evidence of pre-DDoS credential-stuffing reconnaissance | Upstream DDoS mitigation provider attack reports and scrubbing statistics (Cloudflare Analytics exports, Akamai Prolexic attack logs, or equivalent) capturing peak PPS and Gbps volumetrics, attack vector breakdown (SYN flood vs. HTTP flood vs. UDP amplification), and geo/ASN attribution — these are the primary artifacts establishing T1498 and T1498.001 technique application specific to this campaign | RIPE NCC WHOIS database snapshots and BGP routing table exports (RouteViews MRT archives) capturing the ASN prefixes and routing announcements from AS48715 and associated Stark Industries downstream ASNs active during the incident — these document the specific infrastructure layer indicators and serve as fingerprints for detecting future reconstitution events under new corporate shell registrations | Firewall state table dumps and ACL change logs from the containment window, capturing both the pre-block allow-list state (to identify any inadvertent permitted traffic from attributed IP space) and the timestamps of all block rule insertions — these establish the incident timeline and support any regulatory reporting obligations under NIS2 Directive Article 23 for operators of essential services in EU member states

Per-Action IR Details

Step 1: Containment — Block inbound and outbound traffic to IP ranges and ASNs attributed to Stark Industries Solutions, WorkTitans B.V. / THE.Hosting, and Mirhosting at your perimeter firewall and upstream DDoS mitigation provider. Reference GreyNoise and Recorded Future published attribution data for current IP ranges. Prioritize internet-facing government portals, banking applications, and election-adjacent systems matching NoName057(16) target profiles.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 — not in IG1 reference above; apply NIST SC-5 (Denial of Service Protection) as primary DDoS control citation, MITRE ATT&CK T1498 (Network Denial of Service) and T1583.003 (Acquire Infrastructure: Virtual Private Server)

Compensating: For teams without commercial threat intel subscriptions: pull current Stark Industries / Mirhosting ASN ranges from public BGP data using tools such as 'whois -h whois.radb.net AS48715' and 'bgp.he.net' lookups for ASN AS48715 (Stark Industries) and associated downstream ASNs. Feed resulting CIDR blocks into iptables or Windows Firewall via a scripted blocklist: 'iptables -I INPUT -s -j DROP && iptables -I OUTPUT -d -j DROP'. Cross-reference with abuse.ch Feodo Tracker and Spamhaus DROP list for overlapping entries. A 2-person team can automate daily refresh with a cron job pulling from public blocklist feeds and re-applying iptables rules.

Evidence: Before blocking, capture a full NetFlow or pcap sample of any active sessions from Stark Industries / Mirhosting IP ranges using 'tcpdump -i eth0 -w stark_pre_block_$(date +%Y%m%d%H%M%S).pcap net ' to document pre-containment traffic patterns. Export firewall connection state tables showing established sessions from Mirhosting and WorkTitans B.V. ASN space. Preserve upstream DDoS mitigation provider dashboards (screenshots or API exports) showing volumetric baselines and spike timestamps before ACLs are applied, as these establish the attack timeline for NIST IR-5 (Incident Monitoring) documentation.

Step 2: Detection — Query firewall, NetFlow, and DDoS protection logs for volumetric spikes (T1498), SYN/UDP/HTTP flood patterns (T1498.001), and application-layer exhaustion (T1499) originating from Stark Industries / Mirhosting ASNs. Search SIEM for reconnaissance indicators: automated enumeration of public-facing endpoints, login-page probing bursts, and credential stuffing patterns against externally exposed applications (NIST SI-4, CIS 8.2 — Collect Audit Logs). Alert on any new BGP announcements from ASNs historically associated with these entities.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1498 (Network Denial of Service), MITRE ATT&CK T1498.001 (Direct Network Flood), MITRE ATT&CK T1499 (Endpoint Denial of Service), MITRE ATT&CK T1595 (Active Scanning) for reconnaissance phase

Compensating: Without a SIEM, use ntopng (free community edition) or 'nfdump' against collected NetFlow data to identify volumetric anomalies: 'nfdump -r /var/cache/nfdump/nfcapd.current -s ip/bytes -n 20 -o extended' to surface top talkers from Stark Industries ASN ranges. For HTTP-layer exhaustion detection against web portals, parse nginx or Apache access logs with: 'awk '{print $1}' /var/log/nginx/access.log | sort | uniq -c | sort -rn | head -30' to identify IP addresses generating login-page request bursts consistent with NoName057(16) credential-stuffing TTPs. For BGP monitoring without enterprise tooling, subscribe to free RIPE NCC BGP update streams via Routeviews and configure bgpmon alerts on ASN prefixes associated with Stark Industries. Use the free Sigma rule 'proc_creation_win_net_use_enumeration.yml' adapted for web log sources to flag automated endpoint enumeration patterns.

Evidence: Collect nginx/Apache access logs covering the 72-hour window preceding detection, specifically filtering for high-frequency GET/POST requests to '/login', '/auth', '/admin', and '/api' endpoints from Mirhosting CIDR ranges — these URI patterns align with NoName057(16) pre-DDoS reconnaissance methodology. Export NetFlow records (nfcapd files) showing SYN packet rates exceeding 10,000 PPS from Stark Industries ASN space as evidence of T1498.001 flood initiation. Capture DNS query logs from your recursive resolver showing mass lookups against your public-facing subdomains — NoName057(16) commonly performs DNS enumeration prior to targeting. Preserve WAF logs (if present) showing HTTP 429 rate-limit triggers and blocked flood requests with source IP, User-Agent, and URI fields intact per NIST AU-3 (Content of Audit Records) requirements.

Step 3: Eradication — Remove any access rules or allow-list entries permitting traffic from attributed Stark Industries IP space. If your organization uses any THE.Hosting or Mirhosting services (even indirectly through

upstream providers), identify and terminate those dependencies. Rotate credentials for any accounts that may have been exposed to reconnaissance activity (D3-CRO — Credential Rotation). Verify that DDoS scrubbing services and rate-limiting rules are enforced across all internet-facing properties (CIS 4.4, CIS 4.5).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST IA-5 (Authenticator Management), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Audit firewall allow-list rules for Stark Industries / THE.Hosting / Mirhosting IP space using: 'iptables -L -n -v | grep -E "|"' substituting actual CIDR blocks from your blocklist. For upstream provider dependency discovery without a CMDB, run 'curl -s https://ipinfo.io/' against any third-party service IPs in your DNS config and cross-reference ASN field against Stark Industries-associated ASNs. For credential rotation targeting accounts probed during NoName057(16) reconnaissance (login-page burst targets), extract exposed usernames from access logs with: 'grep -E "POST /login|POST /auth" /var/log/nginx/access.log | awk '{print $7, $1}' | sort -u' and force password resets for all matched accounts via your IdP admin panel. Rate-limiting enforcement can be validated with 'ab -n 10000 -c 100 https://yourportal.example.com/login' using Apache Bench to confirm 429 responses trigger at configured thresholds.

Evidence: Before removing allow-list entries, export the complete firewall ruleset ('iptables-save > pre_eradication_ruleset_$(date +%Y%m%d).txt') to document which rules permitted Stark Industries IP space — this establishes whether access was inadvertent or the result of a misconfiguration introduced during a prior reconstitution event. Capture the output of 'traceroute' or 'mtr' to any THE.Hosting-hosted service endpoints your organization touches, preserving upstream provider routing paths that may pass through sanctioned infrastructure. Document all accounts whose credentials appeared in login-page enumeration bursts from Mirhosting IPs, retaining the original access log lines as evidence for NIST IR-5 (Incident Monitoring) tracking and potential regulatory notification if PII-associated accounts were targeted.

Step 4: Recovery — Confirm DDoS mitigation controls are active and capacity-tested against volumetric thresholds relevant to your sector. Validate NIST AU-6 (Audit Record Review) processes are generating alerts on anomalous traffic volumes. Test contingency plans for service degradation under sustained DDoS per NIST CP-4 (Contingency Plan Testing). Confirm alternate processing and telecommunications paths are available per NIST CP-7 and CP-8 if primary infrastructure is targeted.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-4 (Contingency Plan Testing), NIST CP-7 (Alternate Processing Site), NIST CP-8 (Telecommunications Services), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: For teams without enterprise DDoS mitigation platforms, validate capacity-tested thresholds using Cloudflare's free tier (which provides volumetric DDoS protection for registered domains) and confirm anycast absorption is active by checking 'dig +short myip.opendns.com @resolver1.opendns.com' before and after enabling proxy mode — the returned IP should shift to Cloudflare's anycast range. To simulate NoName057(16)-style HTTP flood load against a staging instance of your portal, use 'hping3 -S --flood -V -p 443 ' for SYN flood testing and 'ab -n 50000 -c 500 https://staging.yourportal.example.com/' for HTTP layer, confirming rate-limiting engages below service-impact thresholds. For AU-6 alerting without SIEM, configure logwatch or 'fail2ban' with a custom filter matching volumetric thresholds: create '/etc/fail2ban/filter.d/ddos-detect.conf' targeting nginx access logs for >500 requests per minute per source IP, consistent with NoName057(16) HTTP flood volumetrics documented in public threat reports.

Evidence: Before declaring recovery, capture post-mitigation NetFlow baselines to compare against pre-incident normal traffic profiles — retain both sets per NIST AU-11 (Audit Record Retention) for the duration of your records retention policy. Document CP-4 test results including the specific volumetric thresholds tested (PPS, Gbps) and whether alternate paths per CP-7/CP-8 successfully absorbed load, as NoName057(16) has demonstrated sustained multi-day DDoS campaigns against European government targets that outlast initial mitigation responses. Verify that all

DDoS scrubbing provider logs capturing the incident timeline are exported and preserved before provider log-retention windows expire — Cloudflare, Akamai, and similar providers typically retain detailed attack logs for 30-90 days.

Step 5: Post-Incident — Assess whether your organization's internet-facing asset inventory (CIS 1.1) and exposure surface matches NoName057(16) historical target profiles (government, financial, democratic institutions). Review IP blocklist update frequency — static block lists will not track Stark Industries reconstitution events. Establish a recurring review process for new corporate shells and ASN registrations linked to known bulletproof hosting networks, using threat intelligence feeds that cover infrastructure-layer indicators. Document gaps in DDoS response playbooks per NIST IR-8 (Incident Response Plan).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-8 (Incident Response Plan), NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), NIST RA-3 (Risk Assessment), NIST AU-11 (Audit Record Retention), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For infrastructure-layer threat intelligence without a commercial feed subscription, configure a weekly cron job using 'whois' and RIPE NCC's REST API to monitor for new ASN registrations that share RIPE registrant organization fields, abuse contact emails, or netname patterns with previously sanctioned Stark Industries shells (e.g., 'curl https://rest.db.ripe.net/search?query-string=Stark+Industries&type-filter=aut-num' and parse the response for new entries). Subscribe to the free Spamhaus BGPf feed and CINS Army blocklist, which have historically tracked Stark Industries reconstitution events, and script weekly diff comparisons against your current blocklist to detect newly added CIDRs. For CIS 1.1 asset inventory gap assessment, run 'nmap -sn ' weekly to enumerate all internet-facing assets and compare against your documented inventory — any unlisted hosts represent exposure surface that NoName057(16) reconnaissance could discover before your team does.

Evidence: Conduct a structured lessons-learned review per NIST 800-61r3 §4 within 72 hours of incident closure, preserving the complete incident timeline including: first observed indicator timestamp from NetFlow/firewall logs, time-to-detection, time-to-containment, and any service degradation durations — these metrics directly inform IR-8 playbook gap identification. Archive all RIPE NCC WHOIS records, BGP route announcements, and corporate registration data for WorkTitans B.V. / THE.Hosting and Mirhosting captured during the incident as reference fingerprints for identifying the next reconstitution event; Stark Industries' documented pattern of re-emerging under new EU-registered shells means these artifacts have direct predictive intelligence value. Document whether static blocklists failed to capture any Stark Industries IPs that were active during the incident, and record the lag time between public attribution (GreyNoise/Recorded Future publication dates) and your blocklist update — this delta is the primary metric for measuring intel-to-block cycle time improvement.

Detection Guidance

Primary detection focus is volumetric and application-layer DDoS originating from Stark Industries / Mirhosting IP space, plus pre-attack reconnaissance activity. Query NetFlow and firewall logs for traffic spikes exceeding baseline thresholds from ASNs attributed to these entities; GreyNoise and Recorded Future have published associated ASN and IP range data to serve as your starting IOC set. In your SIEM, build rules for: (1) HTTP request rates exceeding 10x baseline per source IP or IP range against login pages, APIs, or public portals; (2) SYN flood patterns with high packet-per-second rates and low bytes-per-packet ratios; (3) UDP amplification signatures on DNS/NTP ports from Stark Industries netblocks. For reconnaissance detection, alert on automated enumeration of user accounts or endpoint paths (T1591, T1589) from previously unseen source IPs on Stark Industries ASNs. Monitor OSINT channels for NoName057(16) target announcements on Telegram, the group publicly declares targets before launching campaigns, providing a short warning window. Cross-reference any new corporate shell registrations or ASN announcements against known Stark Industries naming patterns (historical: Stark Industries Solutions, WorkTitans, Mirhosting). NIST AU-6 and CIS 8.2 controls

should be verified as active across all internet-facing systems.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`THE.Hosting`	Brand name of WorkTitans B.V., the seized bulletproof hosting shell linked to Stark Industries Solutions	HIGH
DOMAIN	`mirhosting.com`	Mirhosting — alternate corporate shell linked to Stark Industries sanctions-evasion pattern	HIGH
DOMAIN	`stark-industries.solutions`	Stark Industries Solutions — parent bulletproof hosting entity; historical ASN and IP ranges published by GreyNoise and Recorded Future	HIGH

Framework Mappings

MITRE-ATTACK

- **T1591** — Gather Victim Org Information
- **T1583.003** — Virtual Private Server
- **T1499** — Endpoint Denial of Service
- **T1498** — Network Denial of Service
- **T1584.004** — Server
- **T1665** — Hide Infrastructure
- **T1583.001** — Domains
- **T1496** — Resource Hijacking
- **T1586** — Compromise Accounts
- **T1498.001** — Direct Network Flood
- **T1583.004** — Server
- **T1589** — Gather Victim Identity Information

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1591	Gather Victim Org Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1583.003	Virtual Private Server	Resource-Development
T1499	Endpoint Denial of Service	Impact
T1498	Network Denial of Service	Impact
T1584.004	Server	Resource-Development
T1665	Hide Infrastructure	Command-And-Control
T1583.001	Domains	Resource-Development
T1496	Resource Hijacking	Impact
T1586	Compromise Accounts	Resource-Development
T1498.001	Direct Network Flood	Impact
T1583.004	Server	Resource-Development
T1589	Gather Victim Identity Information	Reconnaissance

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/netherlands-seizes-8...	T3
Bulletproof Host Stark Industries Evades EU Sanctions	https://cybersecurity.fullcoll.edu/2025/09/11/bulletproof-host-star...	T1
One Step Ahead: Stark Industries Solutions Preempts EU Sanctions	https://www.recordedfuture.com/research/one-step-ahead-stark-indust...	T3
The Stark Industries Shell Game - When Bulletproof Hosting Proves ...	https://www.greynoise.io/blog/stark-industries-shell-game	T3
WorkTitans B.V. - Krebs on Security	https://krebsonsecurity.com/tag/worktitans-b-v/	T3

Generated 2026-05-23 13:42 UTC by TJS Security Command Center