DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT REPORT

JUNE 2026

Table of Content

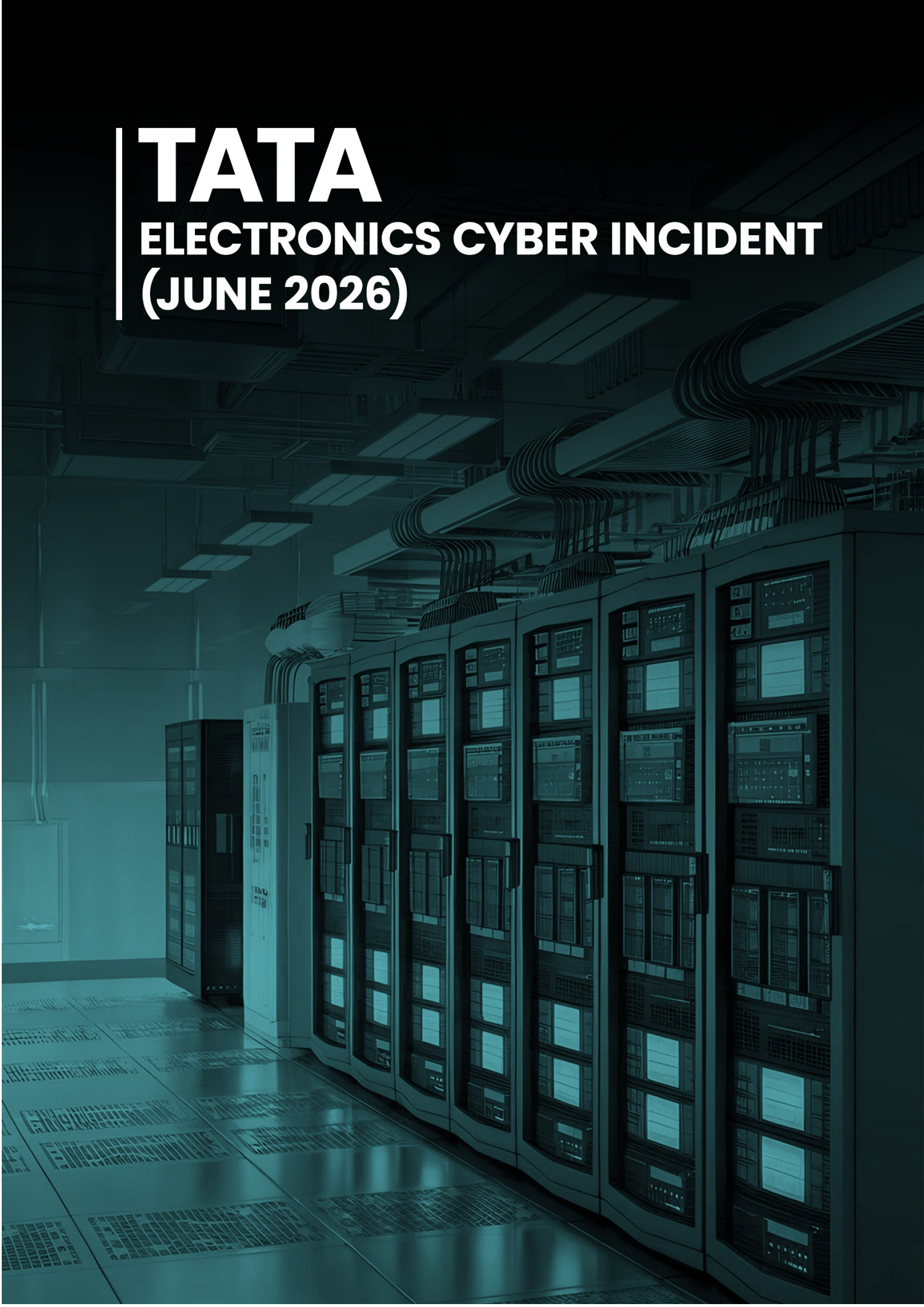
Introduction

The cyber threat landscape continues to evolve at a rapid pace, driven by sophisticated threat actors, accelerated exploitation of newly disclosed vulnerabilities, and the growing convergence of financially motivated cybercrime with state-sponsored operations. Organizations today face persistent risks ranging from large-scale data extortion and supply chain compromises to the rapid weaponization of critical vulnerabilities and emerging AI-enabled attack techniques.

Under the above backdrop, this report provides a comprehensive overview of significant cyber security developments observed during the month of June through three complementary perspectives. The first section analyzes the Tata Electronics cyber incident attributed to the World Leaks extortion group, examining the threat actor's operational model, observed tactics, techniques and procedures (TTPs), attack chain, and associated indicators of compromise. The second section presents an in-depth technical analysis of the ShinyHunters campaign targeting Oracle PeopleSoft environments, detailing the exploitation methodology, MITRE ATT&CK mapping, defensive countermeasures, and actionable recommendations for affected organizations. Finally, the report concludes with a forward-looking threat forecast for July 2026 and the second half of 2026, highlighting anticipated attack trends, emerging risks, and strategic developments that security teams should monitor to strengthen their defensive posture.

By combining incident analysis, adversary tradecraft, and predictive threat assessment, this report aims to provide security practitioners and decision-makers with actionable intelligence to improve situational awareness, support risk-informed decision-making, and enhance organizational resilience against evolving cyber threats.

TATA
ELECTRONICS CYBER INCIDENT (JUNE 2026)



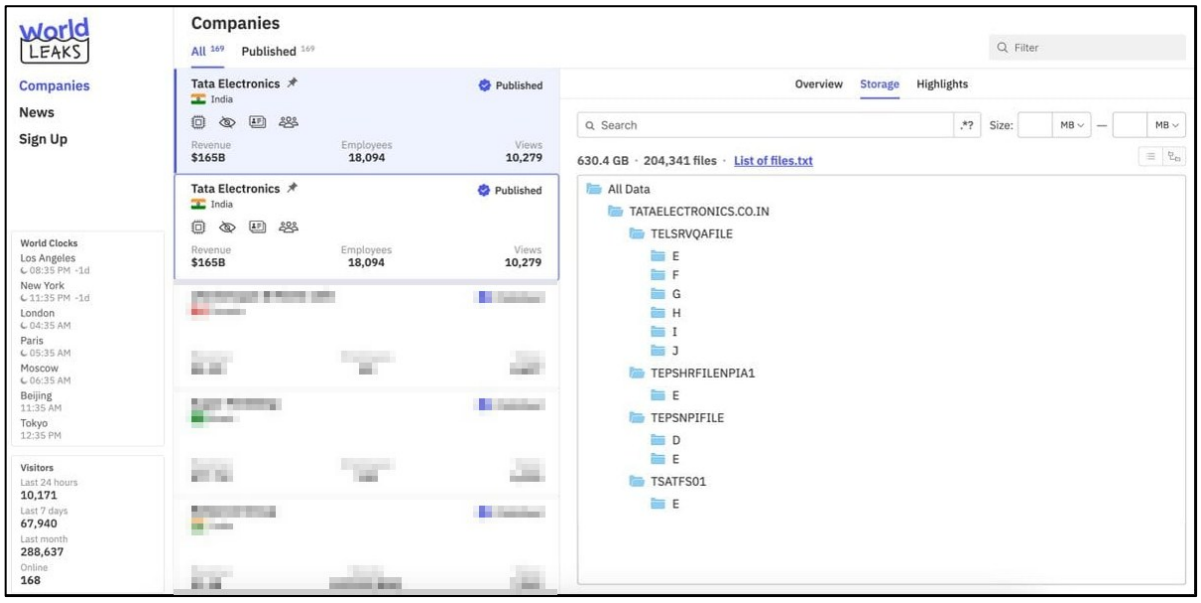
Tata Electronics Cyber Incident (June 2026)

Overview

In June 2026, Tata Electronics confirmed a cybersecurity incident after the ransomware/extortion group World Leaks claimed responsibility for exposing the organization's internal environment. The group published more than 200,000 files totaling over 630 GB on their dark web leak portal. Tata confirmed the cybersecurity incident a few weeks prior, around early June with response protocols activated, internal access hardened and forensic investigators engaged. This ransomware campaign appears to follow the data theft and extortion model where attackers prioritize data exfiltration and public disclosure over operational disruption.

Affected Entities

Affected Entity	Data Exposed
Tata Electronics	Internal emails, employee data including passport scans, manufacturing records, event logs, SAPI/Outlook data, etc. [3]
Apple	*"com.apple.factorydata,"* component/supplier lists and specs for iPhone, material specifications, prototype photos and other confidential documents.
Tesla	Engineering drawing schematics, trade secrets and manufacturing related files.
Others	Documents related to Qualcomm, TSMC.



Threat Actor - World Leaks

World Leaks is a new cyber extortion group and Ransomware-as-a-Service (RaaS) operation that emerged in January 2025. It is believed to be a rebrand or evolution of Hunters Imternational ransomware syndicate which ceased traditional ransomware operations around July 2025 due to law enforcement pressure, increased risk, and declining profits. [1][5]

It focuses purely on

- Large-scale data theft
- Extortion through public exposure
- Dark web leak site publication
- Reputation damage
- Intellectual property theft

This evolution reflects an industry-wide shift where many attackers avoid deploying ransomware binaries that attract immediate law enforcement attention and instead rely solely on stolen confidential data.

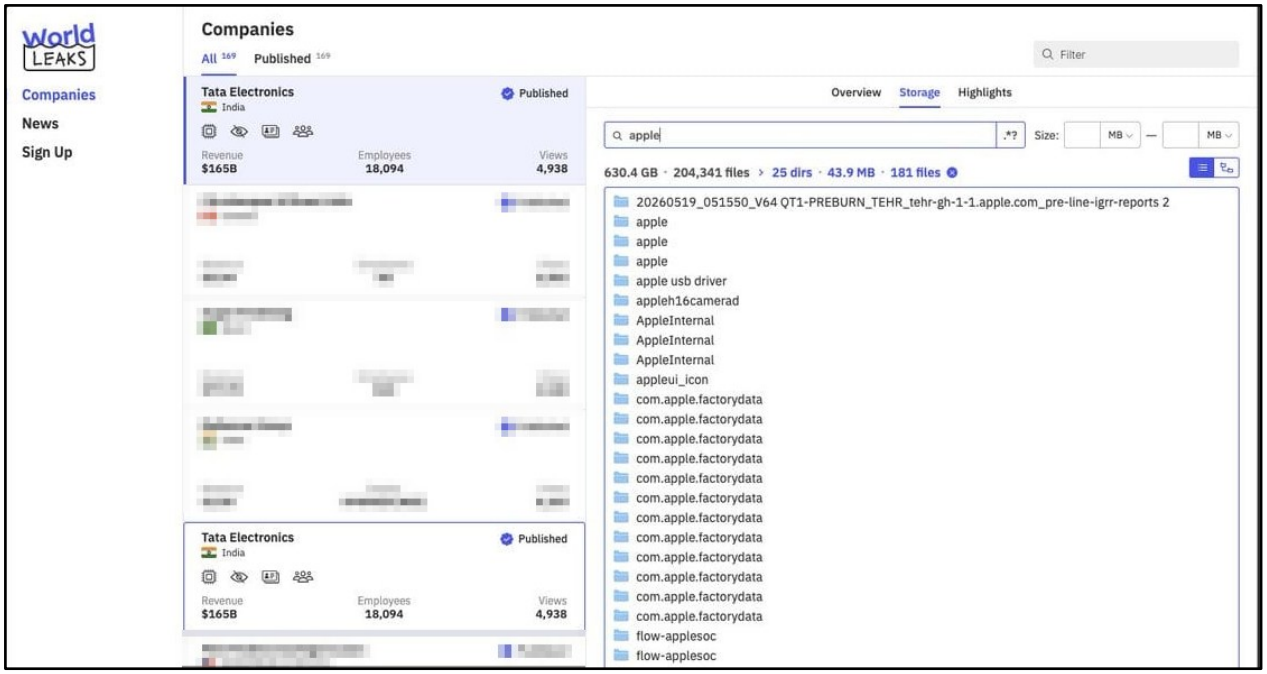
Platform Used by World Leaks

Operators provide a custom built, allegedly Fully Undetectable (FUD) Storage Software exfiltration tool. The infrastructure is believed to be a four-platform infrastructure:

- A tor leak website
- Victim negotiation portal (live chat)
- Affiliate panel
- Insider journalist portal (24-hour early access of stolen data before public release)

The storage software uses SOCKSv5 proxy, Tor-based communications, and metadata indexing, eliminating full data uploads to central servers. The World Leaks group also confirmed their collaboration with Secp0 ransomware group as Secp0's stolen data was frequently published on the World Leaks platform, which is known to give media outlets early access to breach data to maximize pressure on victims.

Threat actors use this access and leak site to steal sensitive corporate data, bypassing traditional encryption and demanding payment under threat of leaking the data publicly.



Key Incidents

Entity	Time Period	Incident
Nike	January 2026	Claimed to have stolen ~1.4 TB of data compromising 188,347 files related to research, design, manufacturing, technical packs, bills etc. [6]
Dell Technologies	July 2025	Claimed to have stolen around 1.3 TB of data from Dell's Customer Solution Center (demo/test environments). Dell confirmed the compromise but stated that it mostly contained demo or synthetic; no major customer impact reported. [7]
SonicWall SMA 100	July 2025	UNC6148 data breach campaign compromised VPN credentials and used OVERSTEP rootkit to exploit end-of-life SonicWall SMA 100. [4]
Chain IQ / UBS	June 2025	Massive data breach at global procurement services firm Chain IQ leaked over 130,000 employee and contractor records belonging to Swiss bank UBS. [7]

Attack Chain

Tata Electronics has not yet publicly disclosed the detailed forensic findings of the intrusion, hence the attack chain presented below is synthesized from the known tactics, techniques, and procedures (TTPs) of the **World Leaks** ransomware group. It is primarily based on World Leaks intrusion observed between **October 2025 and January 2026**, supplemented by publicly documented tradecraft associated with the group. While the exact initial access vector and subsequent activities in the Tata Electronics incident remain unconfirmed, the attack chain represents a plausible sequence of operations consistent with World Leaks' observed methodology and should be considered a reference model rather than the confirmed timeline of the breach.

Initial Access

The first observed malicious activity occurred in mid-October 2025 on a network appliance using compromised “administrator” credentials. Although the initial compromise vector could not be determined, the appliance functioned as the patient-zero device from which the attackers established their foothold before expanding further into the environment. [2]

Reconnaissance

Following initial access, the attackers conducted internal reconnaissance by performing TCP and UDP port scanning to enumerate accessible hosts, identify exposed services, and understand the network topology prior to lateral movement.

Lateral Movement

The attackers conducted extensive lateral movement from the patient-zero device using multiple remote administration mechanisms. SMB administrative shares were used to transfer tools and payloads, including installers like **chromeremotedesktophost.msi**, scripts like **OpenSSHUtils.psm1**, and executables like **ssh-sk-helper.exe**. PsExec facilitated remote process execution, while Windows Remote Management (WinRM), RDP, and Chrome Remote Desktop provided additional means of accessing internal systems. Activity was also observed against Domain Controllers, and anomalous authentication attempts from previously unseen devices were also observed, indicating credential abuse and privilege expansion.

Command and Control (C2) & Persistence

Approximately one month after the initial compromise, the attackers established persistent remote access using Cloudflare Tunnel (formerly Argo Tunnel), with outbound connections observed to hostnames such as **region2.v2.argotunnel[.]com**. By leveraging Cloudflare Tunnel, the threat actors were able to create encrypted outbound connections that bypassed traditional inbound firewall restrictions, enabling covert remote access without exposing externally accessible services. In addition, SSH connections to external IP addresses were observed, providing alternate command-and-control channels. Darktrace also detected suspicious outbound communications to known C2-related IP addresses, including traffic over **OpenVPN (port 1194)**, further indicating active attacker control. These mechanisms enabled

the attackers to maintain persistent access and operate within the environment for several months before the final ransomware deployment.

Data Exfiltration

In November 2025, the attackers conducted multiple large-scale data exfiltration activities, with individual transfers approaching approximately 80 GB. The stolen data was uploaded to cloud storage services, primarily **MEGA** and **Backblaze B2**, using **Rclone** (identified through user agents such as **rclone/v1.69.0**). By leveraging encrypted **HTTPS** connections to legitimate cloud storage providers, the attackers were also able to blend malicious traffic with normal network activity, making detection more challenging. This use of trusted cloud services for data theft aligned with World Leaks' known tradecraft, which emphasizes data exfiltration as a precursor to extortion and, in this case, preceded the eventual deployment of ransomware.

Ransomware Deployment and Encryption

Despite publicly portraying itself as a data-extortion-only group, World Leaks ultimately deployed an encryption payload. The ransomware executable (*world.exe*) and accompanying batch script (*task.bat*) were distributed over SMB using compromised *"localadmin"* credentials. Encrypted files were renamed with a randomized nine-character prefix and a new extension, while ransom notes named **[random-string].README.txt** explicitly attributed the attack to World Leaks. The encryption phase occurred only after prolonged persistence and significant data exfiltration, demonstrating that the group continued to maintain encryption capabilities despite claims to the contrary.

MITRE ATT&CK Matrix

Phase	Tactic & Technique	Observed Activities
Initial Access	T1190: Exploit Public-Facing Application	Foothold gained via network appliance, exploitation of internet facing VPN
	T1078: Valid Accounts	Use of compromised 'administrator' credentials (likely brute-force or reuse), to access the device and begin deep network activity
Reconnaissance	T1595.001: Active Scanning: Scanning IP Blocks	Port and network scanning to identify open UDP and TCP ports within the environment

	T1595.002: Active Scanning: Vulnerability Scanning	Mapping the internal network for services and weaknesses after initial access
Lateral Movement	T1021: Remote Services	Use of RDP (.001), WinRM (.006) and SMB (.002) for movement across systems; SMB file writes for tool transfer
	T1570: Lateral Tool Transfer	Transfer of files (msi installers, OpenSSH components) over SMB from patient-zero device
	T1080: Taint Shared Content	Writing legitimate-looking scripts/executables *(OpenSSHUtils.psm1, ssh-sk-helper.exe)* to shared locations
Persistence	T1078: Valid Accounts	Masquerading as privileged users *('administrator', 'localadmin')* across devices
Command and Control (C2)	T1572: Protocol Tunnelling	Extensive use of Cloudflare Tunnel (Argo Tunnel) with connections to specific hostnames (*region2.v2.argotunnel[.]com*)
	T1090: Proxy	SSH connections to external IPs; additional C2 via suspicious IPs over OpenVPN (Port 1194)
Data Exfiltration	T1567.002: Exfiltration to Cloud Storage	Large-scale uploads (80+ GB) to MEGA and Backblaze clous services
	T1041: Exfiltration Over C2 Channel	Use of Rclone (rclone/v1.69.0) for managed transfers to cloud endpoints
Impact	T1486: Data Encrypted for Impact	Deployment of ransomware payload *(world.exe, task.bat via SMB)*; encryption of files with random prefix with extension; ransom note creation

**The MITRE ATT&CK mapping presented above is based on publicly available technical analysis of the World Leaks intrusion published by Darktrace and has been adapted to align with the observed tactics, techniques, and procedures (TTPs) relevant to this report.*

Indicators of Compromise (IoCs)

Indicators	Description
world.exe	Executable file
task.bat	Script file
'^[A-Z][a-z]{3}[A-Z][a-z][A-Z]{3}[.]README[.]txt'	Ransom note
[.]^[A-Z][a-z]{3}[A-Z][a-z][A-Z]{3}	Ransomware file extension
51.15.106[.]222	Possible C2 Infrastructure
193.161.193[.]99	Possible C2 Infrastructure

**The Indicators of Compromise (IoCs) listed above have been compiled from publicly available threat intelligence published by Darktrace and are included for reference purposes.*

Conclusion

World Leaks, operating as an Extortion-as-a-Service platform and rebrand of Hunters International, shows the evolving ransomware landscape by prioritizing data theft and public leaks over traditional encryption; though hybrid attacks still occur. The Tata Electronics breach, where the group allegedly exfiltrated over 630 GB of sensitive files including Apple and Tesla supply chain data, highlights the risks to global manufacturing and IP-heavy organizations through third-party compromises. By leveraging a sophisticated platform featuring a dark web leak site, victim negotiation portal, affiliate tools, and early journalist access, World Leaks amplifies pressure on victims while lowering operational barriers for affiliates. This incident highlights the need for robust supply chain security, as even major players remain vulnerable to prolonged, stealthy intrusions focused on high-value data exfiltration.

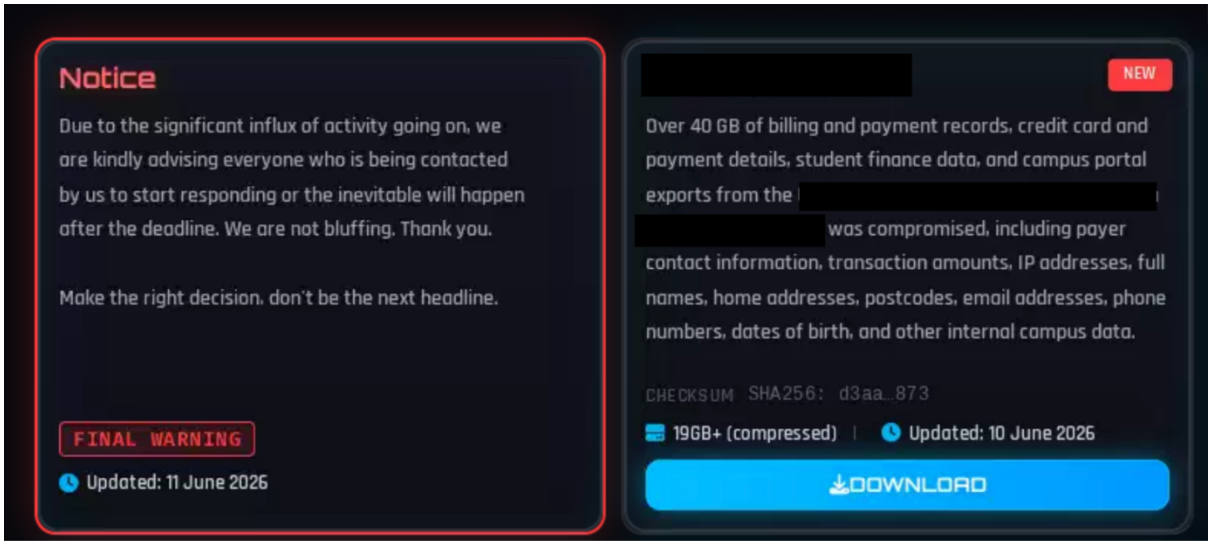
SHINYHUNTERS

ORACLE PEOPLESOFT CAMPAIGN

Introduction

In late May 2026 a criminal group known as ShinyHunters broke into more than a hundred organizations by abusing a serious flaw in Oracle PeopleSoft.[1] The flaw is tracked as CVE - 2026 - 35273. It let an attacker take full control of a PeopleSoft server over the internet without any username or password,[2] because PeopleSoft holds sensitive records like student data, staff details, payroll and financial information, a single break-in could expose a huge amount of personal data all at once.

The attackers used the flaw for about two weeks before Oracle knew about it.[1] Oracle put out an emergency warning on 10 June 2026, and the United States cyber agency CISA added the flaw to its list of actively attacked bugs two days later.[2][3] By then data had already been stolen and posted online. Universities were hit the hardest. The University of Nottingham confirmed a cyber incident affecting its student records but has not formally attributed the attack. ShinyHunters claimed to have stolen around 40 GB of data, and Have I Been Pwned later counted roughly 455,000 unique email addresses in the leaked dataset.[9] However, the university did not confirm the figures.



Incident Overview

Between 27 May and 9 June 2026, the group quietly attacked PeopleSoft servers around the world. No fix existed yet, so every exposed system was at risk. On 9 June the group began posting stolen data on its public leak site. On 10 June Oracle released an out of band security alert, meaning a warning outside its normal monthly update schedule, and named the flaw CVE-2026-35273.[2] On 11 June the security firm Mandiant published its findings and tied the attacks to ShinyHunters.[1] On 12 June CISA added the flaw to its Known Exploited Vulnerabilities list, signalling that everyone needs to patch right away.[3]

The key point is timing. The attacks came first and the warning came second. Any organization that had an exposed PeopleSoft server during that window may already have been breached, even if it patched the moment the fix arrived. A list of what this campaign targeted

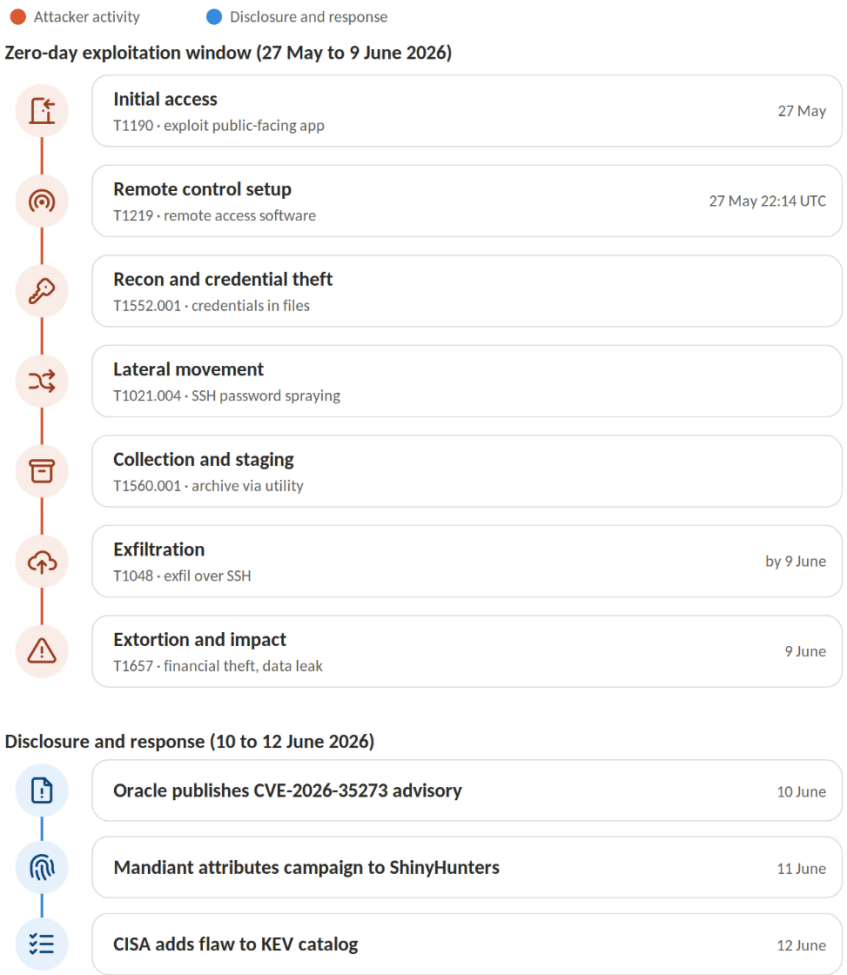
- PeopleSoft PeopleTools 8.61 and 8.62
- Environment Management Hub (PSEMHUB) service
- /PSEMHUB/hub and /PSIGW/HttpListeningConnector endpoints
- psappsrv.cfg application server credentials
- WebLogic configuration files (config.xml)
- Internal hosts listed in /etc/hosts
- Administrative and application SSH credentials
- Student records and enrolment data
- Financial aid and billing data
- Staff payroll and salary data
- Personal identifiers (names, addresses, passport numbers)
- Sensitive attributes (ethnicity, disability status)

Field	Details
Campaign Name	ShinyHunters Oracle PeopleSoft campaign
Threat Actor	ShinyHunters (tracked by Mandiant as UNC6240)
Vulnerability	CVE-2026-35273 (CVSS 9.8, unauthenticated RCE)
Target	Oracle PeopleSoft Enterprise PeopleTools (8.61 and 8.62)
Affected Component	Environment Management Hub (PSEMHUB)
Affected Scope	100-plus organizations notified by Mandiant, 68 percent higher education; ShinyHunters separately claimed about 300 instances (unverified)
Primary Objective	Data theft and extortion
Initial Access	SSRF via PSIGW to the internal /PSEMHUB/hub servlet, then XMLDecoder deserialization to RCE
Tooling (abused)	MeshCentral, a legitimate open source remote management tool, abused by the attackers (agents masqueraded as Azure services)
Execution Method	Server-side code execution as the PeopleSoft service account
Lateral Movement	SSH credential spraying via fanout.sh script
Exfiltration	zstd compression, sent over SSH to leak site

Field	Details
Exploitation Window	27 May to 9 June 2026 (zero-day, predating patch)
Disclosure	Oracle advisory 10 June, CISA KEV listing 12 June 2026
Potential Impact	Mass data breach, extortion, exposure of student, staff, HR, payroll and financial records

Attack Chain Analysis

The ShinyHunters campaign followed a clear set of stages, from the first break into stealing the data. Therefore, Mandiant, the GoogleCloud subsidiary, was able to recover their command history and rebuild the full chain because the group accidentally left one of its own staging servers open to the internet.[1] This is why each phase below can be described with confidence rather than guesswork. The phases are laid out in the order they happened.



Phase 1: Initial Access (Tactic: Initial Access)

The attack began with a single web request. The group sent a specially built, unauthenticated request to the exposed Environment Management Hub at the /PSEMHUB/hub address. No username or password was needed. The flaw was a two stage chain. A server side request forgery in the PSIGW Integration Gateway was used to reach the internal only PSEMHUB servlet, which was not meant to be reachable from outside.[1][4] The attacker controlled data that reached it and then processed it by Java XMLDecoder, which deserializes the data unsafely and runs code inside the WebLogic Java virtual machine. In effect, one web request gained full control of the PeopleSoft machine, running as the PeopleSoft service account.

Phase 2: Setting Up Remote Control (Tactics: Persistence, Command and Control)

With a foothold on the server, the group needed a reliable way to keep control and issue commands. They installed MeshCentral, a genuine remote management tool that admins normally use, and disguised their copy as a Microsoft cloud service so it would not stand out. The agent was set to phone home to azurenetfiles.net, a web address chosen to look like a real Microsoft Azure service. Records show they built this control server on 27 May and used an automated certificate tool so their fake domain would have a valid-looking security certificate. [1][6]This gave them a hidden, always available route for getting back into the environment.

Phase 3: Reconnaissance and Credential Theft (Tactics: Discovery, Credential Access)

Once settled in, the attackers studied the environment. They read PeopleSoft configuration files, including one named **psappsrv.cfg** that stores login details, and pulled credentials out of it.[1][8] They also mapped the layout of the system, identifying the web layer that users see, the application layer that does the processing, and the background job layer. This gave them both the keys and the map they needed to move deeper.

Phase 4: Lateral Movement (Tactic: Lateral Movement)

The group did not stay on the first server. They ran a script that took a list of usernames and passwords and tried them one after another over SSH against other internal servers listed on the machine. This technique is called credential spraying.[1][7] As the script spread, it dropped a file named **README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT** into PeopleSoft folders on each system it touched. That file acted as both a taunt and an early warning of the extortion to come. Reusing common or shared passwords is what let this spread work.

Phase 5: Collection and Staging (Tactic: Collection)

Before removing anything, the attackers gathered the data they wanted and prepared it for a quiet exit. They compressed the stolen files using a tool called zstd. Compression shrinks the data so it moves faster and is less likely to trip alarms as it leaves the network.[1]

Phase 6: Exfiltration (Tactic: Exfiltration)

The group sent the compressed data out of the network over an SSH connection to their own servers. SSH is encrypted, so using it to carry the data out also helped hide what was being taken. From there the data reached the servers hosting the ShinyHunters leak site.

Phase 7: Extortion and Impact (Tactics: Impact)

The final stage is where the group encashes the opportunity. Unlike ransomware crews, ShinyHunters does not lock up systems. Instead, it holds the stolen data over the victim. Each confirmed organization received a demand for payment, with the threat that the data would be published if they refused. [1]The group began posting stolen data on its public leak site on 9 June. The University of Nottingham breach is the most public example: ShinyHunters claimed around 40 GB of data, and Have I Been Pwned counted roughly 455,000 unique email addresses in the leaked set.[9] The university confirmed the incident but did not verify the actor's figures.

MITRE ATT&CK Mapping[10]

Tactic	Technique (ID)	Technique (Name)	Procedure
Initial Access	T1190	Exploit Public-Facing Application	Sent an unauthenticated crafted request to the exposed /PSEMHUB/hub endpoint, triggering XMLDecoder deserialization to run code on the server
Execution	T1059	Command and Scripting Interpreter	Ran administrative commands on compromised hosts through the MeshCentral command line utility meshctrl.js
Command and Control	T1219	Remote Access Tools	Deployed customized MeshCentral RMM agents (meshagent64-azure-ops.exe) to keep remote control of compromised systems

Tactic	Technique (ID)	Technique (Name)	Procedure
	T1071.001	Application Layer Protocol: Web Protocols	Agents beaconed to the C2 server over a web channel at wss://azurenetfiles[.]net:443/agent.ashx
	T1573	Encrypted Channel	Used an encrypted WebSocket over TLS channel for C2 traffic to resist inspection
Defense Evasion	T1036.005	Masquerading: Match Legitimate Resource Name or Location	Named agents and the C2 domain to imitate Microsoft Azure, with azurenetfiles.net posing as Azure NetApp Files
Credential Access	T1552.001	Unsecured Credentials: Credentials In Files	Read the psappsrv.cfg application server config file to pull stored PeopleSoft credentials
	T1110.003	Brute Force: Password Spraying	The fanout.sh script sprayed a hardcoded list of usernames and passwords against internal hosts
Discovery	T1082	System Information Discovery	Inspected mount points, the process scheduler config and WebLogic config.xml to map the PeopleSoft setup
	T1018	Remote System Discovery	Parsed /etc/hosts to identify other internal PeopleSoft hosts to reach
Lateral Movement	T1021.004	Remote Services: SSH	Moved to other internal PeopleSoft servers over SSH
Collection	T1560.001	Archive Collected Data: Archive via Utility	Compressed the stolen data with the zstd utility before removal
Exfiltration	T1048	Exfiltration Over Alternative Protocol	Sent the compressed data out over SSH to attacker servers hosting the leak site
Impact	T1491.001	Defacement: Internal Defacement	Dropped a marker file README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT into PeopleSoft directories

Tactic	Technique (ID)	Technique (Name)	Procedure
	T1657	Financial Theft	Issued extortion demands and published stolen data on the ShinyHunters leak site to pressure victims

MITRE D3FEND Countermeasure Mapping[11]

Tactic	Technique (ID)	Technique (Name)	Procedure
Harden	D3-ACH	Application Configuration Hardening	Disable the Environment Management Hub service or remove the PSEMHUB application, then apply the Oracle patch
Isolate	D3-ITF	Inbound Traffic Filtering	Block external access to /PSEMHUB/* and /PSIGW/HttpListeningConnector at the perimeter
	D3-OTF	Outbound Traffic Filtering	Restrict outbound connections from PeopleSoft servers to cut C2 and exfiltration paths
	D3-NI	Network Isolation	Segment PeopleSoft tiers so a single foothold cannot spray credentials across internal hosts
Detect	D3-NTA	Network Traffic Analysis	Watch for anomalous outbound SMB on TCP 445 and unusual data transfers from PeopleSoft hosts
	D3-DNSTA	DNS Traffic Analysis	Alert on DNS lookups or connections to azurenetfiles.net from internal hosts
	D3-SFA	System File Analysis	Hunt for the dropped marker file and for new or changed .xml files under the envmetadata directory
Harden	D3-MFA	Multi-factor Authentication	Require MFA on administrative and SSH access to limit credential spraying success
	D3-CRO	Credential Rotation	Rotate all credentials exposed in psappsrv.cfg and remove shared administrative passwords

Indicators of Compromise (IOCs)

SHA-256 Hashes:
Attacker .bash_history file (identical across all five staging hosts):
2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35

meshagent64-azure-ops.exe:
f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e37225d24fc
meshagent64-v2.exe:
d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13a86ce2f
meshagent32-azure-ops.exe:
c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187351711f
meshagent (unconfigured Linux agent):
68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e93bc309

Domains:
azurenetfiles[.]net

C2 Channels:
wss://azurenetfiles[.]net:443/agent.ashx

IP Addresses:
142.11.200[.]186
142.11.200[.]187
142.11.200[.]188
142.11.200[.]189
142.11.200[.]190

176.120.22[.]24 (clearnet mirror of the ShinyHunters leak site, SSH exfiltration destination)

File Names:
README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT
[victim_abbreviation]_fanout.sh
meshagent64-azure-ops.exe

Exploited Endpoints:
/PSEMHUB/hub
/PSIGW/HttpListeningConnector

File Path Indicators:
psappsrv.cfg
config.xml
<docroot>/envmetadata/data/environment/*.xml

Tool Artifacts:
MeshCentral server 1.1.59

meshctrl.js
acme-client (npm package)

Behavioral Indicators:
Possible outbound SMB (TCP 445) from PeopleSoft hosts to external addresses (a Mandiant hunting hypothesis for NetNTLM hash capture, not a confirmed observed indicator).

External POST requests to /PSEMHUB/hub dated 27 May 2026 or later
DNS lookups or connections to azurenetfiles[.]net from internal hosts

The complete list of IOCs is available Here.

Recommendations

Short Term (Immediate Actions)

- Patch on an emergency basis. Apply the Oracle fix for CVE-2026-35273 through My Oracle Support at once, outside the normal update cycle. Patch Availability Document CPU187 covers PeopleTools 8.61 and 8.62.[2]
- Shut down the exposed service. In multi-server setups, disable the Environment Management Hub service. In single server setups, remove the PSEMHUB application. If neither is possible right now, block external access to /PSEMHUB/* and /PSIGW/HttpListeningConnector at the firewall.
- Assume a possible breach and hunt. Because the attacks began before the patch existed, patching alone does not tell you whether you were already hit. Search for the marker file README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT, for MeshCentral agents posing as Azure services, and for connections to azurenetfiles[.]net. Check web server logs for POST requests to the two endpoints dated 27 May 2026 or later.
- Rotate exposed credentials. Rotate anything stored in psappsrv.cfg and remove shared administrative passwords so a single stolen credential cannot open many doors.
- Isolate anything suspicious. If you find signs of compromise, isolate the affected hosts, preserve logs and disk images for investigation, and review account activity before rebuilding.
- Deploy detection now. Load the campaign IOCs into your SOC and EDR tooling and turn on the vendor detection signatures for the flaw, such as the SSRF and PSEMHUB exploit rules published by security vendors.

Long Term (Durable Improvements)

- Reduce external exposure. Keep ERP administrative interfaces like PSEMHUB and the Integration Gateway off the public internet by default. Put them behind a VPN or an internal segment so they are never reachable from untrusted networks.

- Segment the PeopleSoft environment. Separate the web, application and batch tiers so that a single foothold cannot spray credentials and spread freely across internal hosts.
- Enforce strong authentication. Require multi-factor authentication on administrative and SSH access and remove reused or shared credentials across servers so credential spraying cannot succeed.
- Improve logging and monitoring. Enable comprehensive logging across PeopleSoft hosts, and monitor for anomalous outbound traffic, unexpected SMB on TCP 445, unauthorized remote management tools, and unusual data transfers.
- Stay current and patch on a schedule. Keep PeopleTools on a supported version, since unsupported releases receive no fixes, and apply Oracle Critical Patch Updates and out of band alerts promptly through a defined patch process.

Manage exposure continuously. Run regular external attack surface scans to catch internet facing PeopleSoft endpoints before attackers do and treat any newly exposed admin service as a priority to lock down.

Prepare for extortion scenarios. Maintain tested offline backups, keep an incident response and legal plan ready for data theft and extortion cases, and rehearse it so decisions are not made under pressure during a live event.

THREAT FORECAST
JULY 2026 AND THE H2 2026 OUTLOOK

Threat Forecast - July 2026 and the H2 2026 Outlook

> This section is expanded as per the reporting requirement for particular focus on the forward view. It comprises a near-term (July) tactical forecast, a second-half strategic outlook synthesized from major vendor and multilateral projections, an early-warning watch list, and structural predictions. Likelihoods follow the estimative-language standard (ICD 203); confidence codes follow the NATO Admiralty System.

July 2026 Tactical Forecast

Forecast	Likelihood	Rationale
Continued Shai-Hulud-lineage worm waves across npm/PyPI/RubyGems	**Almost Certain**	Source code public since May; four June waves; low barrier to replication
Sustained PeopleSoft (CVE-2026-35273) exploitation and new victim disclosures	**Highly Likely**	100-plus notified organizations; unpatched instances remain; extortion pipeline active
Mass exploitation of Citrix NetScaler CVE-2026-8451 ("CitrixBleed"-lineage)	**Almost Certain**	In-the-wild within 24 hours of the June 30 disclosure; already underway in early July
SharePoint CVE-2026-45659 (Storm-2603 to Warlock) broadens	**Highly Likely**	KEV-listed July 1; ToolShell lineage historically weaponized rapidly
ShinyHunters Salesforce/extortion confirmations continue	**Highly Likely**	Large backlog of claimed victims yet to be leaked or confirmed
Fallout and further disclosure from the DHS HSIN intrusion	**Likely**	Confirmed publicly July 1; congressional scrutiny beginning; scope still emerging
AI-augmented loaders/stealers proliferate (e.g., Armored Likho-class)	**Likely**	First such campaign surfaced July 3; technique maturing across actors
Additional edge-appliance zero-days exploited within days of disclosure	**Highly Likely**	Multi-quarter pattern reinforced across June (Cisco, Ivanti, Fortinet, Citrix)
Iranian-aligned retaliation as the banking-sector conflict continues	**Likely**	Post-blackout tempo recovering; tit-for-tat pattern in the Israel-Iran theater

Near-term calendar markers: **Scattered Spider TfL sentencing (July 16)** and the **extradition of a further Scattered Spider member ("Bouquet," July 1)** will shape the group's operational posture; the **FBI IC3 TeamPCP FLASH (July 2)** signals continued federal focus on the supply-chain actor.

H2 2026 Strategic Outlook

The following themes are synthesized from major vendor and multilateral forecasts (Verizon 2026 DBIR, CrowdStrike 2026 Global Threat Report, Google Cloud Cybersecurity Forecast 2026, WEF Global Cybersecurity Outlook 2026, Unit 42 2026 IR Report, GreyNoise 2026 State of the Edge, Check Point Q1 2026). **Important provenance caveat:** these outlooks were published between November 2025 and February 2026 with study windows largely covering 2025; their specific statistics are cited as directional context, not as June 2026 data, and each should be verified against its primary source before external quotation.

- **Agentic AI moves from experiment to production - on both sides.** The World Economic Forum (WEF) found AI the top driver of cyber risk (approximately 94% of leaders) and the fastest-growing risk (approximately 87%). June provided concrete proof-points in both directions: offensive (Hades LLM-scanner evasion, AI-discovered CVE-2026-49160) and defensive (Anthropic's Mythos surfacing 10,000-plus vulnerabilities). Expect agentic attack tooling and agentic SOC adoption to accelerate through H2 2026. Confidence: B2.
- **Edge and identity remain the dominant intrusion surfaces.** GreyNoise reported billions of malicious edge-directed sessions with a majority of RCE attempts from previously-unseen IPs; Unit 42 found identity implicated in roughly 90% of incidents. June's edge zero-day cadence and FortiBleed are leading indicators; expect edge-appliance and identity-centric intrusion to define H2. Confidence: B2.
- **Vulnerability exploitation and speed-to-exploit keep rising.** Verizon's DBIR put vulnerability exploitation at roughly a third of breaches with widening patch gaps; the June Ivanti Sentry case (about 24 hours PoC-to-exploitation, first three-day federal deadline) and record Patch Tuesday volume suggest the exploitation window will keep compressing. Confidence: B2.
- **Supply-chain worms normalize as a persistent threat class.** With the toolkit public and four June waves, expect continued cross-ecosystem worm activity and a defensive shift toward provenance-plus-behavior verification and runner isolation. Confidence: B2.
- **Ransomware stays cartelized and extortion-led.** Check Point's Q1 data (2,122 victims; top-ten groups roughly 71% of activity) and June's DragonForce/Qilin/Gentlemen activity point to continued consolidation, data-theft-only extortion, and BYOVD/trusted-channel evasion. Confidence: B2.
- **Nation-state operations blur with criminal supply-chain abuse.** June showed China (UNC6508), North Korea (Mastra, crypto theft), and the Iran-Israel theater all active; expect the CRINK (China-Russia-Iran-North Korea) axis to keep exploiting the same open-source and edge surfaces criminals use. Confidence: C3.
- **The quantum horizon lengthens as a planning parameter.** "Harvest-now-decrypt-later" collection continues against long-lived secrets; NSA's CNSA 2.0 timeline (post-quantum cryptography by 2030) makes crypto-agility an H2 planning priority even absent a near-term cryptographically relevant quantum computer. Confidence: C3.

Early-Warning Watch List (Indicators to Monitor)

- New Shai-Hulud-lineage package names, `easy-day-js`-style malicious dependencies, and exfiltration to `adjective-creature`/`stygian-cerberus`/`tartarean-charon`-pattern GitHub repositories.
- CISA KEV additions for Citrix NetScaler, SharePoint, and any new edge-appliance flaw - treat same-week exploitation as the default assumption.
- New ShinyHunters, FulcrumSec, Icarus, and World Leaks leak-site postings; expansion of the Klue-style OAuth-cascade model to other SaaS vendors.
- Escalation in the Iran-Israel banking-sector exchange and any Iranian-aligned offensive resumption.
- AI-augmented malware families following the Armored Likho and Hades patterns (LLM-driven tooling, scanner evasion).

References

1. Halcyon. (2025). World Leaks threat group. https://www.halcyon.ai/threat-group/worldleaks
2. Darktrace. (2026). When reality diverges from the playbook: Darktrace identifies encryption in a World Leaks ransomware attack. https://www.darktrace.com/blog/when-reality-diverges-from-the-playbook-darktrace-identifies-encryption-in-a-world-leaks-ransomware-attack
3. Reuters. (2026, June 22). India's Tata Electronics hit by cyber breach claiming expose Apple, Tesla trade. https://www.reuters.com/business/media-telecom/indias-tata-electronics-hit-by-cyber-breach-claiming-expose-apple-tesla-trade-2026-06-22/
4. The Hacker News. (2025). UNC6148 backdoors fully patched. https://thehackernews.com/2025/07/unc6148-backdoors-fully-patched.html
5. Blackpoint Cyber. (2025). World Leaks ransomware threat profile. https://blackpointcyber.com/threat-profile/world-leaks-ransomware/
6. BleepingComputer. (2026). Nike investigates data breach after extortion gang leaks files. https://www.bleepingcomputer.com/news/security/nike-investigates-data-breach-after-extortion-gang-leaks-files/
7. CyberDesserts. (2025). WorldLeaks ransomware group. https://blog.cyberdesserts.com/worldleaks-ransomware-group/
8. Mandiant / Google Threat Intelligence Group. https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit
9. Oracle Security Alert https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
10. CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
11. Rapid7 https://www.rapid7.com/blog/post/etr-active-exploitation-of-oracle-peoplesoft-zero-day-cve-2026-35273/

12. Intel 471 https://www.intel471.com/blog/shinyhunters-0-day-attacks-after-patching-find-out-if-you-were-breached
13. CSO Online https://www.csoonline.com/article/4184408/oracle-peoplesoft-zero-day-fuels-shinyhunters-extortion-spree.html
14. The Hacker News https://thehackernews.com/2026/06/shinyhunters-exploits-oracle-peoplesoft.html
15. Help Net Security https://www.helpnetsecurity.com/2026/06/11/oracle-peoplesoft-under-attack-cve-2026-35273/
16. MITRE ATT&CK https://attack.mitre.org/
17. MITRE D3FEND https://d3fend.mitre.org/

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

The Data Security Council of India (DSCI), a Nasscom initiative, is a premier think tank on data protection, cyber security and emerging tech in India. DSCI engages with governments, regulators, industry, and academia to build a secure and trusted cyberspace through policy advocacy, thought leadership, and capacity-building initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips