Key Insights on SHADOW-AETHER-015 and Earth Preta from the 2025 MITRE ATT&CK Evaluation with TrendAI Vision One™

By By: Trend Micro Jan 13, 2026 Read time: 9 min (2303 words)

Published: 2026-01-13 · Archived: 2026-04-17 02:06:33 UTC

Key takeaways:

- The MITRE ATT&CK Evaluation Round 7 (ER7 2025) validates the progress made by TrendAI Vision One™ toward a unified security operations platform. This blog discusses further the results of TrendAI™ in ER7.
- Scenario 1 (Demeter), an emulation inspired by SHADOW-AETHER-015 shows the complexity of modern cloud attacks, where adversaries can pivot from compromised endpoints to cloud infrastructure, leveraging stolen credentials and tokens to establish persistence, move laterally across hybrid environments, and exfiltrate sensitive data at scale.
- Meanwhile, scenario 2 (Hermes), the emulation inspired by Earth Preta, highlights the sophistication of phishing-based attacks, emphasizing the use of advanced loaders, anti-analysis techniques, lateral movement, credential harvesting, and data exfiltration, followed by meticulous cleanup to reduce forensic traces and hinder detection.
- TrendAI's results in the MITRE ATT&CK ER7 align strongly with the current need for platforms to automatically correlate telemetry into meaningful alerts across hybrid environments. TrendAI Vision One detects and blocks the IoCs related to the threat actors mentioned in this blog. TrendAI customers can also access tailored hunting queries, threat insights, and intelligence reports to better understand and proactively defend against these threat actor groups.

This blog examines notable modern techniques, tactics, and procedures (TTPs) that TrendAI™ Research has observed in the two emulations during the MITRE ATT&CK Evaluation Round 7 (ER7 2025) that featured Earth Preta (also known as Mustang Panda), and SHADOW-AETHER-015 (TrendAI Research's intrusion name for a particular group of activities with modern TTPs characterized by AI-generated attacks, sophisticated phishing attacks, and/or social engineering). These observed, analyzed, and reported TTPs support the performance of TrendAI Vision One™ in ER7, reinforcing the position of TrendAI™ as a trusted leader in detection and response innovation.

The ER7 marked a significant evolution in MITRE's approach where, it now includes both on-premises and cloud-based attacks, as well as the Reconnaissance tactic. This not only simulates hybrid environments that real SOC teams defend against today but also highlights the necessity for SOC teams to rely on effective enterprise tools. TrendAI Vision One's results in ER7 reinforces TrendAI's position as a trusted leader in detection and response innovation. Enterprises can rely on the platform for up to date, and up to standard analytic coverage across all major attack steps, protection across all evaluated attack opportunities, and cloud layer coverage, including both detection and protection.

MITRE scenario 1 (Demeter)

In this emulation, cloud (AWS) scenarios highlighted how attackers can pivot from an endpoint into the cloud where the intrusion begins by phishing an unmanaged workstation using an adversary-in-the-middle SSO kit to steal high-privilege credentials and MFA tokens. This enables RDP access, internal discovery, Active Directory enumeration, and reconnaissance of shared network resources.

The attacker then pivots to AWS, enumerating IAM, S3, VPCs, and costs while evading defenses, establishing persistence through a new admin IAM user, and a privileged EC2 instance. This allows them to harvest secrets and tokens, moving laterally across Linux and Windows systems using tunnelling and RMM tools. The attack concludes with large-scale data collection and exfiltration, syncing application and file-share data from internal systems to attacker-controlled S3 buckets.

This section provides a high-level summary of how Scenario 1 (Demeter) unfolds, highlighting the core execution flow, infrastructure interactions, and progression of the attack chain from initial access through cleanup.

For a detailed, step-by-step breakdown of the scenario that includes emulation context, tooling, and attack objectives, refer to MITRE's official CTI emulation documentation.

More information that enterprises should know about SHADOW-AETHER-015

Scenario 1 is inspired by observed TTPs from SHADOW-AETHER-015, a highly adaptable and aggressive cybercriminal group known for fluent English-language social engineering, particularly vishing and help-desk impersonation, which allows operators to blend effectively into corporate support environments.

Their activity is characterized by identity abuse, and cloud compromise. The group is also known to use multi-pressure extortion: high-value data theft, leak threats, ransomware, cloud/VMware disruption, and employee intimidation. SHADOW-AETHER-015 primarily targets identity and access management systems such as Okta and Azure AD/Entra ID, abusing social engineering, MFA fatigue, token theft, and adversary-in-the-middle phishing to bypass authentication controls. After gaining identity access, the threat actors leverage legitimate credentials with IAM misuse and configuration abuse to move laterally across SaaS and cloud environments, including AWS, Azure, and Google Workspace.

Activities linked to the group initially focused on SIM-swapping and telecommunications fraud, but has since evolved to target cloud, SaaS, and enterprise environments for data theft and, in some cases, ransomware deployment. The group diversifies monetization through cryptocurrency theft, account-takeover resale, long-term cloud persistence, partnerships with multiple RaaS groups, and selling large customer datasets.

SHADOW-AETHER-015 is a group focused on high-value, high-leverage intrusions, and have been observed to consistently pursue enterprises with massive data, complex IT operations, and low tolerance for downtime. Their list of victims suggest that the group prioritizes sectors rich in credit-card data, travel records, healthcare and loyalty information.

The group's operations have affected telecommunications and business process outsourcing (BPO) providers. The group has also compromised tech SaaS and identity platforms to obtain privileged access into enterprise environments, alongside notable intrusions in hospitality and gaming organizations. Additional targets include

finance and insurance firms, aviation and travel operators, and managed service provider (MSP) and IT companies.

SHADOW-AETHER-015 has been observed to be most active in English-speaking countries such as the US, UK, Canada, and Australia, with additional victim presence in India, Singapore, Thailand, and Brazil.

The earliest structured campaigns linked to the group occurred in from March to July 2022 under the “0ktapus” phishing campaign, but it should be noted that some SIM-swapping activity that could be potentially linked to early SHADOW-AETHER-015 operators predates this.

The group’s progression shows rapid improvement in both technical sophistication and operational ambition as shown in figure 1.

MITRE Scenario 2 (Hermes)

In scenario 2, the attack begins with a phishing email that delivers a malicious document, leading the victim to download a password-protected archive and execute a malicious LNK file that side-loads the ORPHEUS loader.

The loader performs anti-analysis checks, injects into a trusted process, loads shellcode in memory, and establishes encrypted command-and-control (C&C). From there, the attacker conducts host and network discovery, pivots laterally using remote execution techniques, and establishes a remote command interface on higher-value systems.

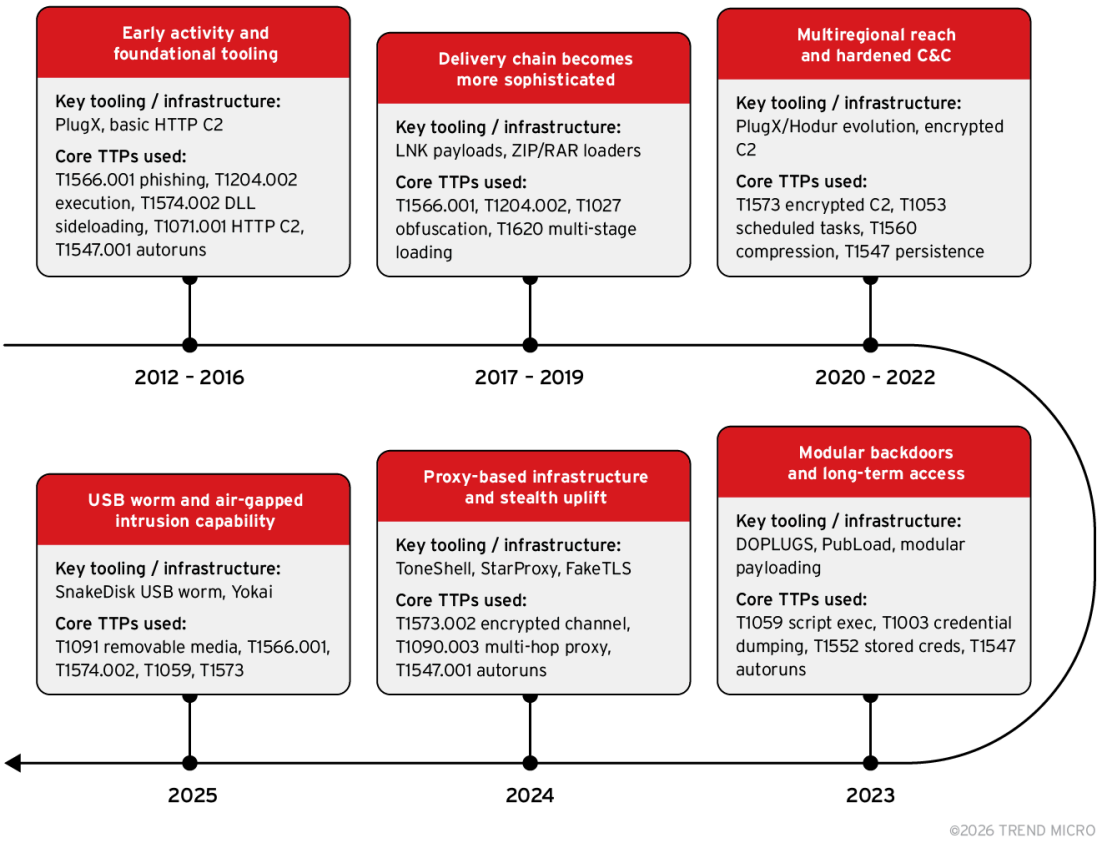
Credential access is achieved by extracting directory service databases and registry hives, which are staged and exfiltrated for offline cracking. Persistence is then established through registry run keys and scheduled tasks to maintain access. The attacker proceeds to collect and compress targeted documents using archiving utilities, exfiltrating the data via command-line transfer tools over existing C&C channels.

Finally, cleanup scripts are executed to remove persistence mechanisms and on-disk artifacts, reducing forensic evidence and hindering detection.

This section provides a high-level summary of how scenario 2 (Hermes) unfolds, highlighting the core execution flow, infrastructure interactions, and progression of the attack chain from initial access through cleanup.

For a detailed, step-by-step breakdown of the scenario that includes emulation context, tooling, and attack objectives refer to MITRE’s official CTI emulation documentation

Figure 2 shows a timeline of notable pivots in Earth Preta’s tooling, infrastructure, and core TTPs used, as monitored by TrendAI Research.



More information that enterprises should know about Earth Preta

Scenario 2 is inspired by Earth Preta, a China-based advanced persistent threat (APT) group that has been active since at least 2012. Earth Preta's operations are primarily driven by state-aligned intelligence objectives. The group focuses on political and military intelligence collection, long-term strategic awareness, and surveillance of communities, prioritizing sustained access and information gathering over direct financial gain.

The group's activity shows a strong concentration in Asia and Southeast Asia, reflecting strategic regional interests. However, Earth Preta has also demonstrated the capability and intent to operate beyond this region, extending campaigns into Europe and other global locations when aligned with broader geopolitical objectives.

While government-related entities remain the primary targets, Earth Preta campaigns frequently expand into strategic industries such as energy, maritime, infrastructure, manufacturing, telecommunications, and transportation. Targeting these sectors suggests an interest in economic, industrial, and critical infrastructure intelligence, that are integral to a country's position in international relations.

Earth Preta carefully selects infrastructure that enables persistent access and intelligence collection, often prioritizing government networks, enterprise environments, and systems supporting domain services, file storage, and internal communications. Their targeting reflects an emphasis on environments that provide broad visibility into organizational operations and strategic decision-making processes. Earth Preta's operations are also marked by frequent updates to tooling, flexible infection and persistence mechanisms, and a willingness to shift tactics, all of which suggest significant resources, sophistication, and the intention to stay continue operating long-term. These are further discussed in table 1.

Over time the group has adopted many aliases, including Bronze President, TA416, RedDelta, HIVE0154, and Stately Taurus, which can be both for operational rebranding and attribution uncertainty.

Period	Key event
2012 – 2016	**Early activity and foundational tooling** Earth Preta first appeared using PlugX/Korplug RAT, delivered through basic spear-phishing attachments and decoy documents. The group's C&C setup was simple: it relied on direct servers with minimal obfuscation and standard DLL sideloading for execution and persistence. It initially targeted mostly NGOs, policy institutes, and government-linked bodies in Asia.
2017 – 2019	**Delivery chain becomes more sophisticated** During this time, the group improved their phishing tactics with policy- and diplomacy-themed lures, often packaged in ZIP/RAR archives or malicious LNK shortcuts for initial access. Infrastructure saw more rotating C&C servers, modular loaders, and slightly more stealth.
2020 – 2022	**Multiregional reach and hardened C&C** Earth Preta expanded operations into Europe and refined multi-stage loader chains, adding encrypted C&C traffic, obfuscation layers, and PlugX variants like Hodur. This period marks the transition toward targeted, persistent espionage campaigns. During this period, TrendAI reporting documented PlugX evolution and campaign activity.
2023	**Modular backdoors and long-term access** Campaigns such as Stately Taurus highlight intrusions into Southeast Asian government environments, supported by DOPLUGS and PubLoad loaders for modular payload execution. The groups target scope for intelligence gathering also widened to include systems tied to policy and strategic value such as energy, manufacturing, academic networks, and maritime assets.
2024	**Proxy-based infrastructure and stealth uplift** Earth Preta began employing StarProxy to mask beaconing and route C&C traffic, alongside ToneShell, which leverages FakeTLS encrypted communication, making detection challenging. Its C&C stack matured into a proxy with layered backdoor structure. TrendAI Research highlights DOPLUGS/ToneShell campaigns and stealth behavior.
2025	**USB worm and air-gapped intrusion capability**

	Earth Preta's recent activity features SnakeDisk, a USB-propagating worm used to deliver Yokai and updated ToneShell backdoors, enabling compromise of air-gapped or restricted networks. Initial access is still commonly via spear-phishing attachments, followed by DLL sideloading, execution using command/scripting interpreters, and encrypted C&C channels for stealth.

Table 1. A timeline of notable events observed from the APT group Earth Preta

MITRE ATT&CK Techniques Observed

MITRE ATT&CK Evaluation Results

TrendAI demonstrated strong detection and coverage in ER7 for both scenarios. A detailed breakdown of TrendAI's performance and detection capabilities is available in our official analysis that can be found here.

MITRE ATT&CK Evaluations provide an industry-standard, threat-informed framework for understanding attacker behaviors, techniques, and tactics. These evaluations allow organizations to:

- Benchmark security solutions against real-world attack scenarios.
- Identify gaps in detection and response capabilities.
- Stay updated on the latest adversary techniques and trends.

Solutions and platforms like TrendAI Vision One operationalize and automate the identification of gaps in detection and response capabilities by producing a balanced set of high-confidence alerts across all major attack steps, enough to ensure full visibility without overwhelming analysts or masking key attacker activity. TrendAI Vision One

- Monitors and tracks attack routines as they attempt to move and execute within the organization's networks, systems, and infrastructure.
- Detects and blocks threats as early as possible in the attack lifecycle.
- Provides actionable insights that are mapped to the MITRE ATT&CK framework, enabling SOC teams to better understand and respond to threats.

TrendAI's results in ER7 align strongly with the current need for platforms to automatically correlate telemetry into meaningful alerts across hybrid environments, specifically when multiple data sources must come together to explain details about a significant event. MITRE's insights also align with the enhancements already underway across the TrendAI Vision One platform.

Enterprises must regularly review MITRE ATT&CK Evaluations and leverage platforms like TrendAI Vision One to map their organization's detection and response coverage, identify gaps, and continuously improve your security poture.

TrendAI Vision One Threat Intelligence

To stay ahead of evolving threats, TrendAI Vision Oneone-platform customers can access a range of Intelligence Reports and Threat Insights within Vision One. Threat Insights helps customers stay ahead of cyber threats before they happen and allows them to prepare against emerging threats by offering comprehensive information on threat actors, their malicious activities, and their techniques. By leveraging this intelligence, customers can take proactive steps to protect their environments, mitigate risks, and effectively respond to threats.

TrendAI Vision One Intelligence Reports App related entries [IOC Sweeping]

- Earth Preta Campaign Uses DOPLUGS to Target Asia
- - Vision One Emerging Threat
-
- Earth Preta Evolves its Attacks with New Malware and Strategies
- - Vision One Emerging Threat
-
- Earth Preta Mixes Legitimate and Malicious Components to Sidestep Detection
- - Vision One Emerging Threat

TrendAI Vision One Threat Actor Profiles

- - Earth Preta
    - - Earth Preta IoC sweeping
- - SHADOW-AETHER-015
    - - SHADOW-AETHER-015 IoC sweeping
-

Hunting Queries

TrendAI Vision One Search App

TrendAI Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Hunting queries in the TrendAI Vision One Search App are available for Vision One customers with Threat Insights Entitlement enabledone-platform.
