DeepSeas Threat Intel Report

*The DeepSeas monthly threat intelligence report is a collection of the top reports, threat actor activity, and malware from the month of **May 2025**. Find out how you can get even more curated intelligence reporting by emailing CyberDefense@deepseas.com.*

Malware

DragonForce Uses MSP's Remote Management Tool to Attack

Sophos recently responded to a targeted attack involving a managed service provider (MSP). In this incident, a threat actor gained access to the MSP's SimpleHelp remote monitoring and management (RMM) tool and used it to deploy DragonForce ransomware across multiple endpoints. The attackers also exfiltrated sensitive data, leveraging a double extortion tactic to pressure victims into paying the ransom. The attackers very likely utilized a series of SimpleHelp vulnerabilities reported in January 2025: CVE-2024-57727, CVE-2024-57728, and CVE-2024-57726.

Analysis from DeepSeas: The compromise of an MDR provider is considered a windfall opportunity for ransomware actors, though in previous incidents of this nature even well-resourced ransomware actors found themselves unable to properly capitalize on their

successes. The attack investigated by Sophos was prevented due to controls established to prevent the installation of RMM tools. DeepSeas recommends that similar measures be implemented, and all remote management tools be accounted for and existing instances deprecated if necessary.

iClicker Site Hack Targeted Students with Malware Via Fake CAPTCHA

The website of iClicker, a popular student engagement platform, was compromised in a ClickFix attack that used a fake CAPTCHA prompt to trick students and instructors into installing malware on their devices. iClicker, a subsidiary of Macmillan, is a digital classroom tool that allows instructors to take attendance, ask live questions or take surveys, and track student engagement. It is widely used by 5,000 instructors and 7 million students at colleges and universities across the United States, including the University of Michigan, the University of Florida, and universities in California. According to a security alert from the University of Michigan's safe computing team, the iClicker site was hacked between April 12 and April 16, 2025, to display a fake CAPTCHA that instructed users to press "I'm not a robot" to verify themselves.

Analysis from DeepSeas: The students who went to the iClicker site were instructed to run a PowerShell script on their command prompt to prove they were human. The heavily obfuscated script could detect when running in a sandbox and would not drop the intended malware, so it is not known what malware was delivered by this specific campaign. Because ClickFix is so pervasive, DeepSeas TIDE does not believe that higher education was targeted specifically. Rather, according to iClicker's security bulletin, a vulnerability in their website was leveraged to display the captcha.

Fileless Execution: PowerShell Based Shellcode Loader Executes Remcos RAT

Cyber criminals are progressively turning to PowerShell to launch stealthy attacks that evade traditional antivirus and endpoint defenses. By running code directly in memory, these threats leave minimal evidence on disks, making them particularly challenging to detect. A recent example is Remcos RAT, a well-known remote access trojan recognized for its persistence and stealth. It provides attackers with full control over compromised systems, making it a preferred tool for cyber espionage and data theft. In a recent campaign, threat actors delivered malicious LNK files embedded within ZIP archives, often disguised as MS Office documents. The attack chain leverages mshta.exe for proxy execution during the initial stage.

Unconfirmed reports suggest this new sample is named “K-Loader,” although no conclusive findings have been made.

Analysis from DeepSeas: This activity was derived from a report based off a spearphishing email with an attachment named "new-tax311.zip." It's possible that this campaign is targeting individual users, or it could be targeting finance departments. Because the phishing lure looks similar to those that target individual users, this is likely activity related to infostealers or for initial access brokers, and the access or credentials will be sold on the dark web. DeepSeas TIDE can monitor the dark web for exposed credentials and initial access sellers attempting to exploit credentials or access to organizations with our dark web alerting service.

Vulnerability

SonicWall Confirms Active Exploitation of Flaws Affecting Multiple Appliance Models

SonicWall has revealed that two now-patched security flaws impacting its SMA100 Secure Mobile Access (SMA) appliances have been exploited in the wild.

The vulnerabilities in question are:

- CVE-2023-44221 (CVSS score: 7.2): Improper neutralization of special elements in the SMA100 SSL-VPN management interface allows a remote authenticated attacker with administrative privilege to inject arbitrary commands as a 'nobody' user, potentially leading to OS Command Injection Vulnerability.
- CVE-2024-38475 (CVSS score: 9.8): Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to file system locations that are permitted to be served by the server.

Analysis from DeepSeas: Both the flaws impact SMA 100 Series devices, including SMA 200, 210, 400, 410, 500v, and were addressed in the following versions:

- CVE-2023-44221 - 10.2.1.10-62sv and higher versions (Fixed on December 4, 2023)
- CVE-2024-38475 - 10.2.1.14-75sv and higher versions (Fixed on December 4, 2024)

Even though these are older vulnerabilities, their exploitation suggests that threat actors are aware that many organizations do not patch their network equipment quickly or properly and

that targeting older, known vulnerabilities is still a reliable method of gaining access to target networks.

Billions of Apple Devices at Risk from “AirBorne” AirPlay Vulnerabilities

Cybersecurity firm Oligo has revealed major vulnerabilities, dubbed AirBorne, in Apple’s AirPlay, a wireless system used by iPhones, iPads, Macs, and third-party devices for audio and video streaming. These flaws in Apple’s AirPlay software tools for other companies could let hackers take control of devices on the same Wi-Fi network.

Analysis from DeepSeas: Two key vulnerabilities (CVE-2025-24252 and CVE-2025-24132) could allow wormable attacks, spreading harmful software automatically across networks. This could lead to serious issues like spying and ransomware. Millions of Apple devices and third-party AirPlay devices, including those in cars (CarPlay), are potentially affected. The main recommendations for remediation of this vulnerability are to disable Apple AirPlay when not in use and limit AirPlay's access to networks.

Critical Langflow RCE Flaw Exploited to Hack AI App Servers

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has tagged a Langflow remote code execution vulnerability as actively exploited, urging organizations to apply security updates and mitigations as soon as possible. The vulnerability is tracked as CVE-2025-3248 and is a critical unauthenticated RCE flaw that allows any attacker on the internet to take full control of vulnerable Langflow servers by exploiting an API endpoint flaw. Langflow is an open-source visual programming tool for building LLM-powered workflows using LangChain components. It provides a drag-and-drop interface to create, test, and deploy AI agents or pipelines without writing full backend code.

Analysis from DeepSeas: AI level exploits are useful to threat actors because APIs generally have escalated privileges, and most organizations don't have the ability to do code level security analysis of every API they are using within their environment. This vulnerability was addressed in an update released on April 1 but is now being exploited in the wild on unpatched systems.

BianLian and RansomExx Exploit SAP NetWeaver Flaw to Deploy PipeMagic Trojan

At least two different cyber crime groups BianLian and RansomExx are said to have exploited a recently disclosed security flaw in SAP NetWeaver tracked as CVE-2025-31324, indicating that multiple threat actors are taking advantage of the bug.

Cybersecurity firm ReliaQuest, in a new update published today, said it uncovered evidence suggesting involvement from the BianLian data extortion crew and the RansomExx ransomware family, which is traced by Microsoft under the moniker Storm-2460. BianLian is assessed to be involved in at least one incident based on infrastructure links to IP addresses previously identified as attributed to the e-crime group.

Analysis from DeepSeas: Threat actors routinely target publicly disclosed vulnerabilities within 24 - 48 hours of their disclosure. Initial reporting on these vulnerabilities showed Chinese nation-state threat actors were exploiting them. RansomExx and BianLian likely targeted the vulnerabilities after their disclosure. DeepSeas TIDE does not concur with ReliaQuest's analysis that BianLian is involved since they have shown no activity on their Data Leak Site (DLS) since February, which suggests the group is defunct, and there was no response from the group when physical letters were sent to offices claiming to be from BianLian.

Nation-State

New Russia-affiliated Actor Void Blizzard Targets Critical Sectors for Espionage

Microsoft Threat Intelligence Center has discovered a cluster of worldwide cloud abuse activity conducted by a threat actor that Microsoft tracks as Void Blizzard (LAUNDRY BEAR), who Microsoft assesses with high confidence is Russia-affiliated and has been active since at least April 2024. While Void Blizzard has a global reach, their cyber espionage activity disproportionately targets NATO member states and Ukraine, indicating that the actor is likely collecting intelligence to help support Russian strategic objectives. In particular, the threat actor’s prolific activity against networks in critical sectors poses a heightened risk to NATO member states and allies to Ukraine in general. Void Blizzard’s cyber espionage operations tend to be highly targeted at specific organizations of interest to the Russian government, including government, defense, transportation, media, non-governmental organizations (NGOs), and healthcare sectors primarily in Europe and North America. The threat actor uses

stolen credentials — which are likely procured from commodity infostealer ecosystems — and collects a high volume of email and files from compromised organizations.

Analysis from DeepSeas: The VOID BLIZZARD activity observed by Microsoft may be standard espionage activity conducted by the Russian government, but the activity also highlights the long-standing connections between Russian cyber criminal groups and nation-state espionage. Maintaining vigilance against commodity infostealer malware will serve to disrupt this activity in the short term, though it is also likely to lead to the VOID BLIZZARD actors changing their tactics, requiring constant monitoring of the group's activities by western governments.

Storm-0558 and the Dangers of Cross-Tenant Token Forgery

Modern cloud ecosystems often place a single identity provider in charge of handling logins and tokens for a wide range of customers. This approach streamlines single sign-on (SSO) for end users, but it also places enormous trust in a single set of signing keys. If those private keys are compromised, attackers can create tokens that appear valid to any service that relies on them. Storm-0558 is a prime example of how this can backfire - a key that was intended for one context ended up creating tokens accepted in a different environment, bypassing every normal safeguard.

Analysis from DeepSeas: This threat activity targeted Microsoft but it does show a fail point in how many cloud providers secure their systems. Because the Russian threat actors were able to obtain a signing key intended for Microsoft consumer accounts, they were able to issue tokens for enterprise Azure AD services and Microsoft did not differentiate between consumer keys and enterprise keys allowing the threat actors to access resources within the Microsoft environment. DeepSeas TIDE recommends that customers implement key management and rotation, as well as logging and monitoring of cloud resources for suspicious behavior such as tracking what key or issuer is used for which tokens to detect suspicious behavior and the use of forged tokens.

Cyber Crime

Darkforums User 303 Claims to Have Stolen Source Code for DeLoitte

On May 30, 2025, Darkforums user **303** claimed to have accessed and exfiltrated data from British consulting firm DeLoitte. **303** claims that this data includes Github credentials and

source code. If accurate, this data could lead to cyber criminal syndicates finding penetration methods into Deloitte servers proper, possibly leading to a ransomware attack or the exfiltration and sale of sensitive PII or proprietary data.

UK Retail Giant Co-op Shuts Down IT Systems After Attempted Cyber Attack

The Co-operative Group has confirmed it shut down parts of its IT network after detecting an attempted cyber attack in what is the latest incident to affect a major UK retailer. The move was described as precautionary and aimed at containing the threat before any systems could be compromised. Although the shutdown affected internal functions such as virtual desktops, stock systems, and contact center operations, Co-op reassured the public that all food stores, home delivery services, and funeral operations are running as normal.

Analysis from DeepSeas: This threat activity and other related retail-based ransomware attacks have been linked to Scattered Spider and DragonForce. This link is likely due to a known Scattered Spider TTP where they will contact the IT help desk posing as an employee and requesting their credentials be reset. This tactic has been successful because many organizations have lax or unenforced identity verification for help desk activities and commonly use third-parties for IT support.

Luna Moth Extortion Hackers Pose as IT Help Desks to Breach US Firms

The data-theft extortion group known as Luna Moth, aka Silent Ransom Group, has ramped up callback phishing campaigns in attacks on legal and financial institutions in the United States. According to EclecticIQ researcher Arda Büyükkaya, the ultimate goal of these attacks is data theft and extortion. Luna Moth, known internally as Silent Ransom Group, are threat actors who previously conducted BazarCall campaigns as a way to gain initial access to corporate networks for Ryuk, and later, Conti ransomware attacks.

Analysis from DeepSeas: The social engineering tactic of posing as help desk employees is not new and has been successful in the past. Silent is a new cyber criminal group as of April 2025, but as stated in the report they likely operated as an affiliate of other ransomware groups.