



THREAT HUNTING

LAB

RedFlick: Star Blizzard's New Single-Click Delivery Chain for the CosmicPulse Backdoor

Global Weekly Threat Overview

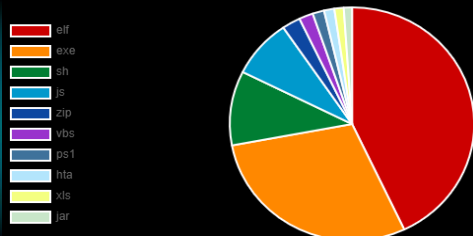
Global Weekly Notable One

Threat Hunting Activity

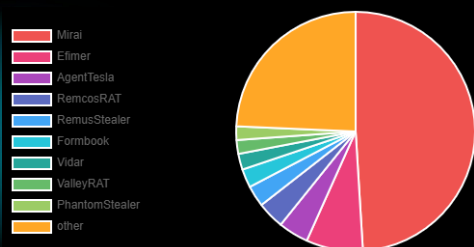
Global Weekly Threat Overview

A critical memory overflow vulnerability in Citrix NetScaler ADC and Gateway, tracked as CVE-2026-88772 (CVSS 9.5), has been detailed following active exploitation in the wild. The flaw sits in the DTLS handling of the NetScaler Packet Processing Engine (NSPPE) and allows a pre-authenticated attacker to corrupt heap memory and divert control flow to execute arbitrary shellcode with root privileges on the underlying FreeBSD platform. Alongside the related CVE-2026-88771, it was added to CISA's Known Exploited Vulnerabilities catalog on September 27, 2026, with opportunistic exploitation reported from multiple threat actors, including suspected state-sponsored groups, since early September.

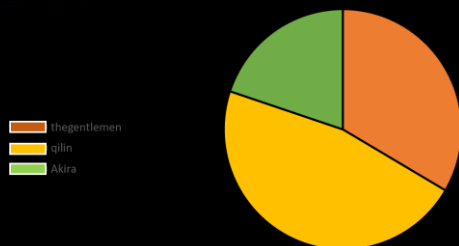
Top 10 file types



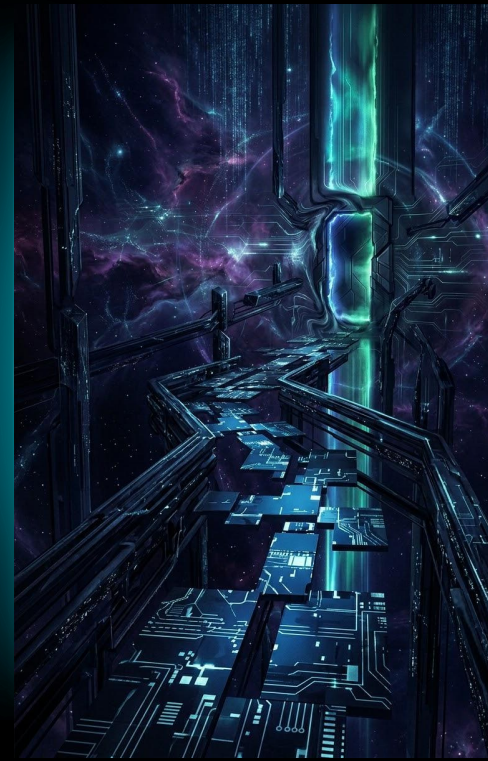
Top 10 malware family



Top 3 Ransomware Group



A new botnet named Carbonato targets Docker hosts with unauthenticated daemons exposed on port 2375. After gaining access via a privileged container, it opens a reverse SSH tunnel for persistence and deploys an open-source AI agent framework (Hermes Agent), overwriting its persona file with a prompt that turns it into an unrestricted "operator" receiving tasks over Telegram to harvest credentials, API keys, and execute commands. The botnet rescans nearby networks every five minutes to propagate further, worm-style.



Persistence: Scheduled Task

A state-sponsored threat actor has refined its malware delivery chain to reduce the number of user interactions required for a successful compromise, moving from a multi-step infection flow to one that completes after a single click on a disguised shortcut file. The updated chain is designed specifically to evade detection controls that had become effective against the actor's previous delivery method, while supporting a parallel shift toward larger-scale, less targeted phishing operations.

At the center of the new chain is an installer that establishes persistence by creating multiple scheduled tasks disguised as legitimate system or network maintenance components. Each task plays a distinct role in the infection process, and together they are responsible for retrieving and launching a custom backdoor used for long-term access, credential theft, and ongoing espionage activity against the actor's targets.

Threat Hunting Activity

TACTIC

Persistence

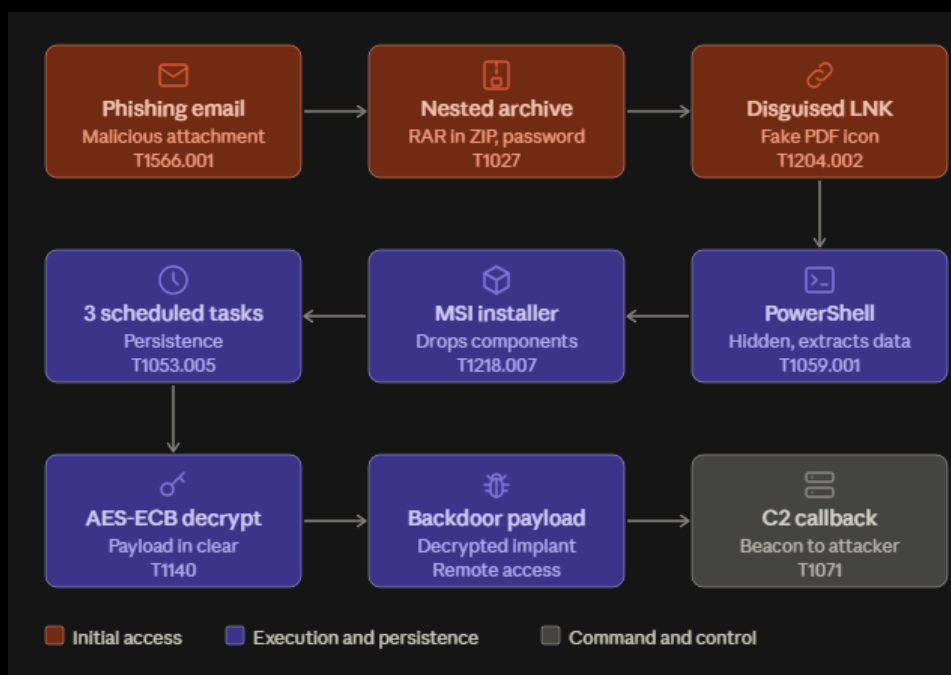
TECHNIQUES

T1053 – Scheduled Task

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The `schtasks` utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel.

Threat Hunting Activity

The lure arrives as a password-protected RAR archive nested inside a ZIP file, delivered via a large-scale phishing email impersonating event invitations or official notices. Inside the RAR is a shortcut (LNK) file disguised with a PDF icon and filename. Once opened, the LNK silently downloads a second file presented as a PDF, which actually contains encoded data; a hidden-window command line extracts and runs this data via PowerShell to retrieve an MSI installer from attacker infrastructure (including compromised WordPress/cPanel sites).



The MSI installer creates three scheduled tasks disguised as legitimate Windows or network maintenance components (e.g., connectivity test, network configuration, system health monitor names). Each task carries out a distinct step of the chain; in observed incidents either the first or the third task was responsible for deploying the final payload. The payload is a custom downloader/backdoor, which also masquerades as a Control Panel applet, and is decrypted from a second ZIP archive using an AES-ECB key embedded in the installer before execution. Once running, the backdoor communicates with remote infrastructure (including WebDAV) for command-and-control.

Threat Hunting Activity

Detection can be on Event ID 4698 looking for three scheduled tasks created within a short time window from a non-administrative parent process, each disguised with network/maintenance-sounding task names.

```
A scheduled task was created.

Subject:
  Security ID:      AzureAD\██████████
  Account Name:     ██████████
  Account Domain:   AzureAD
  Logon ID:         0x5C76041

Task Information:
  Task Name:        \Network Maintenance
  Task Content:      <?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2026-10-14T10:32:31</Date>
    <Author>AzureAD\██████████</Author>
    <URI>\Network Maintenance</URI>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger>
      <StartBoundary>2026-10-14T16:00:00</StartBoundary>
      <Enabled>true</Enabled>
```



THREAT HUNTING



SORINT_{SEC}