DRONA CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

GODDAMN RANSOMWARE: Hyadina's Sophisticated Evasion Campaign

An expert technical threat intelligence advisory detailing the rebranding of the Beast and Monster ransomware families into the highly destructive GodDamn strain. This campaign leverages Microsoft-signed malicious kernel drivers to systematically blind endpoint security solutions prior to final execution.

PREPARED BY

Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE

July 13, 2026

CLASSIFICATION MATRIX

HIGH: RED MED LOW

THREAT AWARENESS ADVISORY

Hyadina Deploys GodDamn Ransomware With Malicious Evasion Driver

Issued By: Drona Cyber Solutions Pvt Ltd | **Intelligence Source:** Drona Threat Intel

HIGH RISK

EXECUTIVE SUMMARY

Drona Threat Intel has identified a highly sophisticated campaign involving the deployment of GodDamn ransomware, the latest operational iteration developed by the prominent threat actor group known as Hyadina [cite: 32]. This ransomware represents a strategic rebrand of the legacy Beast and Monster ransomware families, which were first observed in active environments in 2022 [cite: 33].

The comprehensive attack chain begins with initial compromise via currently undetermined vectors, followed by the explicit manual setup of AnyDesk within non-standard directories to establish remote control infrastructure [cite: 34]. Once remote access is stabilized, the operators exploit an aggressive credential-harvesting toolkit alongside advanced defense-evasion techniques [cite: 35]. Specifically, the operators utilize a Microsoft-signed malicious kernel driver named PoisonX to unhook critical security APIs and terminate security endpoint tracking systems, leaving the environment completely vulnerable right before executing the final ransomware encryption payload [cite: 36, 37].

> **[CRITICAL WARNING COMPONENT: KERNEL-LEVEL BLINDING]**
>
> The core danger of this threat vector relies heavily on the PoisonX malicious kernel driver. Because the driver holds a valid signature from Microsoft, standard operating system endpoint defenses fail to block its installation [cite: 37, 50]. Once active, it operates with absolute kernel-level privileges to dismantle endpoint detection and response (EDR) software, unhook kernel-level APIs, and completely blind security monitors before the final ransomware payload initializes encryption protocols [cite: 37, 75].

ATTACK CHAIN & DISTRIBUTION PHASES

- **Initial Ingress and Setup:** Attackers obtain initial access to the target network via unknown means and immediately deploy a legitimate remote management binary (AnyDesk) inside a hidden or non-standard user directory (specifically `csidl_profile\music\anydesk.exe`) to establish an interactive remote presence [cite: 34, 44].
- **Persistent Command and Control:** The rogue AnyDesk process immediately establishes multiple outbound network tunnels targeting authorized relay nodes (including IPs `15.235.230[.]188` and

185.229.191[.]39) [cite: 45] while altering underlying access control parameters to completely bypass visual interactive user consent prompts [cite: 59].

- **Internal Network Discovery:** The actors utilize automated network evaluation scanners (such as `Netscan.exe`) alongside custom staged command utilities to fully blueprint local adjacent internal networking layouts [cite: 52].
- **Credential Harvesting and Movement:** A comprehensive suite consisting of 14 separate credential extraction tools, including Mimikatz and various NirSoft software packages, is systematically dropped to extract high-privilege credentials [cite: 51]. These credentials facilitate lateral movement through target environments utilizing administrative shares and PsExec [cite: 54, 57].
- **Defense Dismantling Action:** The actors drop an evasion tool named `symantec.exe` [cite: 48], which extracts and loads the Microsoft-signed `PoisonX` driver (`gll.sys`) [cite: 49, 50]. This is combined with automated PowerShell scripts to explicitly disable built-in host tracking systems, including Windows Defender real-time monitoring [cite: 56].
- **Payload Execution and Impact:** Once defensive systems are neutralized across multiple targeted endpoints, the formal ransomware payload (`encrypter-windows-gui-x86.exe`) is executed, encrypting data and appending a customized string based on the victim organization's formal name [cite: 64, 65].

TECHNICAL ANALYSIS OF CORE CAPABILITIES

An analysis of the operational timeline reveals that the operators maintain persistent dwell time within the target infrastructure prior to initiating ransomware deployment. In typical engagements, the GodDamn ransomware payload is systematically staged and executed approximately four days after the primary network intrusion and AnyDesk setup phases conclude [cite: 64]. Drona Threat Intel discovered that persistence is rigidly enforced by registering multiple auto-start operating system services, namely `AnyDeskService` and `AnyDesk_D`, pointing directly to persistent execution blocks on the secondary `D:` drive [cite: 60].

The technical manipulation of the host's kernel layer underscores a growing standard of engineering within the Hyadina group's toolsets [cite: 72]. The evasion binary drops `gll.sys`, a driver that holds genuine cryptographic validation through official channels [cite: 50]. By operating within ring 0 space, the driver overrides user-mode restrictions and active hooks placed by EDR agents, rendering the host defenseless [cite: 50, 75]. Drona Threat Intel notes that while historical campaigns focused squarely on targeting standard Windows systems, recent behavioral telemetry strongly implies that the Hyadina threat actors are expanding payload delivery packages to aggressively target cross-platform hypervisors, including Linux and ESXi architectures [cite: 76, 77].

STRATEGIC RECOMMENDATIONS & MITIGATIONS

MITIGATION VECTOR	ACTIONABLE SECURITY REQUIREMENT
Access Controls	RESTRICT the use of legitimate remote administration tools, such as AnyDesk, and monitor for their installation in non-standard locations or with unusual configurations [cite: 82].
Application Whitelisting	ENFORCE application control policies to prevent the execution of unauthorized executables from user-profile directories, such as Music or Downloads folders [cite: 83].
Endpoint Auditing	IMPLEMENT robust endpoint detection and response (EDR) solutions capable of detecting and blocking credential dumping tools like Mimikatz and the execution of various NirSoft utilities [cite: 84].
Driver Monitoring	AUDIT and monitor for suspicious driver installations and the use of tools known to disable security controls, such as the PoisonX driver or Defender Control [cite: 85].
Network Hardening	ENFORCE network segmentation to limit lateral movement, making it more difficult for attackers to propagate across the environment using tools like PsExec [cite: 87].
Business Continuity	MAINTAIN a comprehensive offline backup strategy and regularly test data recovery procedures to ensure business continuity in the event of a ransomware attack [cite: 88].

DRONA CYBER SOLUTIONS

INDICATORS OF COMPROMISE (IOCS)

INDICATOR TYPE	VALUE / STRING	CONTEXT / DESCRIPTION
SHA256 Hash	`b29f91a440527fb621d106a2048f6379fff3263c60aeda9c82ff8c1d5ae880a8`	symantec.exe Defense Evasion Tool [cite: 49]
SHA256 Hash	`2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d`	PoisonX Malicious Kernel Driver (gll.sys) [cite: 50]

INDICATOR TYPE	VALUE / STRING	CONTEXT / DESCRIPTION
SHA256 Hash	`17fb52476016677db5a93505c4a1c356984bc1f6a4456870f920ac90a7846180`	Malicious File Hash [cite: 94]
SHA256 Hash	`19bab15a34d5ad838ccf4d187eb40379c335fa56446d0f9621865b2767d4ac7d`	Malicious File Hash [cite: 94]
IPv4 Address	`15.235.230[.]188`	AnyDesk Relay Infrastructure Connection [cite: 45]
IPv4 Address	`185.229.191[.]39`	AnyDesk Relay Infrastructure Connection [cite: 45]
IPv4 Address	`141.95.145[.]210`	AnyDesk Relay Infrastructure Connection [cite: 45]
IPv4 Address	`162.19.171[.]150`	AnyDesk Relay Infrastructure Connection [cite: 45]