Hildegard, Software S0601 | MITRE ATT&CK®

Archived: 2026-04-05 17:30:31 UTC

Enterprise T1071 Application Layer Protocol

Hildegard has used an IRC channel for C2 communications.[1]

Enterprise T1059 .004 Command and Scripting Interpreter: Unix Shell

Hildegard has used shell scripts for execution.[1]

Enterprise T1609 Container Administration Command

Hildegard was executed through the kubelet API run command and by executing commands on running containers.[1]

Enterprise T1613 Container and Resource Discovery

Hildegard has used masscan to search for kubelets and the kubelet API for additional running containers.[1]

Enterprise T1136 .001 Create Account: Local Account

Hildegard has created a user named "monerodaemon".[1]

Enterprise T1543 .002 Create or Modify System Process: Systemd Service

Hildegard has started a monero service.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Hildegard has decrypted ELF files with AES.[1]

Enterprise T1611 Escape to Host

Hildegard has used the BOtB tool that can break out of containers. [1]

Enterprise T1068 Exploitation for Privilege Escalation

Hildegard has used the BOtB tool which exploits CVE-2019-5736.[1]

Enterprise T1133 External Remote Services

Hildegard was executed through an unsecure kubelet that allowed anonymous access to the victim environment.[1]

Enterprise T1574 .006 Hijack Execution Flow: Dynamic Linker Hijacking

Hildegard has modified /etc/ld.so.preload to intercept shared library import functions.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Hildegard has modified DNS resolvers to evade DNS monitoring tools.[1]

Enterprise T1070 .003 Indicator Removal: Clear Command History

Hildegard has used history -c to clear script shell logs.[1]

.004 Indicator Removal: File Deletion

Hildegard has deleted scripts after execution.[1]

Enterprise T1105 Ingress Tool Transfer

Hildegard has downloaded additional scripts that build and run Monero cryptocurrency miners.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Hildegard has disguised itself as a known Linux process.[1]

Enterprise T1046 Network Service Discovery

Hildegard has used masscan to look for kubelets in the internal Kubernetes network.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Hildegard has packed ELF files into other binaries.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Hildegard has encrypted an ELF file.[1]

Enterprise T1219 Remote Access Tools

Hildegard has established tmate sessions for C2 communications.[1]

Enterprise T1496 .001 Resource Hijacking: Compute Hijacking

Hildegard has used xmrig to mine cryptocurrency.[1]

Enterprise T1014 Rootkit

Hildegard has modified /etc/ld.so.preload to overwrite readdir() and readdir64().[1]

Enterprise T1082 System Information Discovery

Hildegard has collected the host's OS, CPU, and memory information.[1]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Hildegard has searched for SSH keys, Docker credentials, and Kubernetes service tokens.[1]

.004 Unsecured Credentials: Private Keys

Hildegard has searched for private keys in .ssh.[1]

.005 Unsecured Credentials: Cloud Instance Metadata API

Hildegard has queried the Cloud Instance Metadata API for cloud credentials.[1]

Enterprise T1102 Web Service

Hildegard has downloaded scripts from GitHub.[1]
