360 Netlab Blog - Network Security Research Lab at 360

By lvxing

Published: 2024-06-14 · Archived: 2026-04-05 18:51:45 UTC

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

概述 2022年10月21日，360Netlab的蜜罐系统捕获了一个通过F5漏洞传播，VT 0检测的可疑ELF文件ee07a74d12c0bb3594965b51d0e45b6f，流量监控系统提示它和IP45.9.150.144产生了SSL流量，而且双方都使用了伪造的Kaspersky证书，这引起了我们的关注。经过分析，我们确认它由CIA被泄露的Hive项目server源码改编而来。这是我们首次捕获到在野的CIA HIVE攻击套件变种，基于其内嵌Bot端证书的CN=xdr33， 我们内部将其命名为xdr33。关于CIA的Hive项目，互联网中有大量的源码分析的文章，读者可自行参阅，此处不再展开。 概括来说，xdr33是一个脱胎于CIA Hive项目的后门木马，主要目的是收集敏感信息，为后续的入侵提供立足点。从网络通信来看，xdr33使用XTEA或AES算法对原始流量进行加密，并采用开启了Client-Certificate Authentication模式的SSL对流量做进一步的保护；从功能来说，主要有beacon，trigger两大任务，其中beacon是周期性向硬编码的Be

---