1 Overview

"Ocean Lotus", also known as APT32 and OceanLotus, is a hacker group from Southeast Asia. The organization has been active since at least 2012, and has long targeted China's energy industry, maritime agencies, border defense agencies, health departments, maritime construction departments, scientific research institutes, and shipping companies. In addition to China, the targets of "Ocean Lotus" also include governments, military agencies and large enterprises around the world, as well as domestic media, human rights and civil society related organizations and individuals.

In historical attack methods, APT32 has been trying different methods to execute malicious code on target systems and bypass security detection. In the long-term research and confrontation of APT32 by the Weibu Intelligence Bureau, an undisclosed Linux backdoor "Buni" of APT32 was captured in the second half of last year, and under the continuous monitoring of the threat hunting system, it was found that it has become active again recently.

2 Details In the process of investigating APT32's assets in 2021, the Weibu Intelligence Bureau found another undisclosed Linux backdoor of APT32. The backdoor design idea is similar to APT32's "Double-headed Dragon" and MacOS backdoor. This backdoor also has structured traffic. The technical characteristics of a single process instance, information collection, and C2 encoding are almost the same as those of the "Double-headed Dragon", but the instruction types are different, and the traffic encryption method is relatively simple. The information collection uses the commands "/dev/disk/by-uuid/" and "cat /etc/*release | uniq" to extract the prefixes of the words By and uniq, and name it Buni. At first analysts thought Buni was the predecessor of the "Double-headed Dragon", a weapon no longer used by APT32, but recently it was discovered that this Linux backdoor is active again. The hard-coded C2 in the Buni backdoor utilizes some compromised IoT devices and controls a large number of hosts. The hard-coded C2 in the Buni historical sample file has been used for 2.5 years. As of 2022, some Buni samples have maintained 0 antivirus detection results on the VT platform for two full years; as of the latest time, only two antivirus detections have been detected.

3 Sample characteristics 1. Release method a) Buni consists of two parts: the installer and the Core. The installer is responsible for releasing the Core and maintaining the permissions. After execution, it will be deleted. In the observed installers, the “crontab” method of maintaining permissions is used.

b) Sandbox process relationship, as shown in the following figure:

2. Single process instance Buni implements a single process instance through file locking, and there are two different paths for root and non-root permissions, namely "/tmp/.etxh" and "/tmp/.edv". The code layer looks like this:

3. Process camouflage Buni generates a random length string of 6-12 through a random function, calls the prctl function to set a random process name, and pretends to be a system process.

4.C2 encoding method The C2 string is hardcoded and stored in the .data section, which is XORed and decrypted with the 0xB1 byte after the backdoor is loaded.

5. Information collection Buni collects the basic information of the system through various system commands, including: CPU architecture, process PID, user name, host name, network card information, etc. In addition, various constants are also carried in the generated data packets, and finally the various information Concatenated to form a data packet in array format, which can be parsed by JSON. The specific functions/commands to be called are shown in the following table:

command\function

Uname

cat /etc/*release | uniq

cat /etc/issue

Gethostname

sysinfo

readlink /proc/self/exe

/proc/cpuinfo

a) uname

b) cat /etc/*release | uniq & cat /etc/issue

c) gethostname

d) sysinfo

e)获取各类信息构成的数据，会在上线请求时一并被发送，格式化后的数据如下：

6.结构化流量 a)Buni 拥有其自定义的通信协议，通信数据包具有一定的结构，数据在构造后经过 XOR 加密，部分命令会存在附加数据，附加数据部分通过 GZIP 方式压缩，其流量结构如下： b)类C结构表示如下：

c)在代码中则是通过逐字节 recv 接收的方式解析成流量结构：

7.指令分发&响应 a)指令解析和响应包的构造在同一个函数中所实现，在接收到服务端发送的数据包后逐字节解析后被传入该函数，对解析得到的指令类型执行对应的操作。

b)在指令分发执行完成后，会构造相同类型数据包进行应答，在响应包中会携带执行结果与错误号。

c)具体支持的指令类型，如下表所示：

说明	类型
上线信息	0x5C37
命令执行\运行插件	0x5C7C
交付文件	0xB616、0x1CE3
心跳（指定睡眠时间）	0xDAFE
	0x7221
	0x48B8

3 总结

APT32 拥有 Windows、Linux、MacOS 等不同操作系统的作战武器，覆盖移动端、桌面端、IoT多平台，纵观 Linux 和 MacOS 平台中的作战工具同源程度，这必然是属于同一公司所开发的工具，在同一源码上不停的分化迭代，形成了各种针对多架构、多平台、多操作系统的不同类型作战武器。

4 IOC

C2

zabbixasaservice.com 139.162.58.101 - END -

关于微步在线研究响应中心

微步情报局，即微步在线研究响应中心，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

The Weibu Intelligence Bureau is composed of senior experts who are proficient in Trojan analysis and forensics technology, Web attack technology, traceability technology, big data, AI and other security technologies. Through automated intelligence production system, cloud sandbox, hacker portrait system, threat hunting system, Tracking traceability system, threat perception system, big data correlation knowledge graph and other self-developed systems, conduct real-time automatic analysis and homology of millions of sample files, tens of millions of URLs, PDNS, and Whois data newly added by Weibu Online every day. Analysis and big data correlation analysis. Since its establishment, the Weibu Intelligence Bureau has been the first to discover targeted attacks by dozens of foreign advanced APT organizations against my country's key infrastructure and industries such as finance, energy, government, and high-tech, assisting hundreds of leading customers in various industries. He has dealt with the WannaCry extortion incident that ravaged the world, the BlackTech targeted attack on my country's securities and high-tech incidents, the long-term targeted attack on my country's maritime/high-tech/finance by OceanLotus, and the OldFox targeted attack on hundreds of companies in the mobile phone industry across the country.