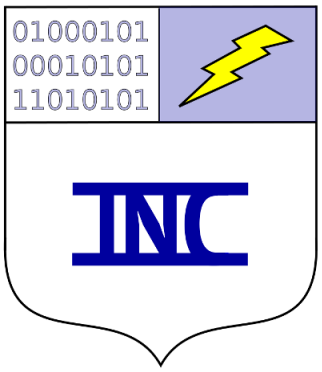
Panther Shadow: A Linux Worm

Brent Kirkpatrick *

June 29, 2018

Intrepid Net Computing



www.intrepidnetcomputing.com

*bbkirk@intrepidnetcomputing.com

Document Revision History

June 25, 2018 Draft

June 29, 2018 Final Revisions

Abstract

In February 2018, Intrepid Net Computing encountered a worm that spreads by exploiting Meltdown and Spectre. This worm infects Linux operating systems, including: Chrome Panther OS and CentOS. The payload of the worm is transmitted to an end-user computer when the computer connects to the Internet. Recent patches for Meltdown and Spectre are sufficient to block the spread of this worm.

This worm infects the memory of a host computer and downloads a root-kit payload. The eighteen files in the root kit are listed along with their checksums for two operating systems.

There is no Trojan associated with this worm.

When citing this work, please refer to this document by name and date or to Intrepid Net Computing Case #1757926.

1 Introduction

Worms are some of the most pernicious exploits. Modern worms can infect all major operating systems, and hackers have come to increasingly target Linux and BSD.

On February 4, 2018, we discovered a network infected with the Panther Shadow worm. The infected portions of the network include routers and two endpoint Linux machines (Chrome Panther OS and CentOS).

We quickly discovered that the infection is a Linux worm. This worm exploits Meltdown and Spectre in its probe. Computers that are vulnerable to infection have not been patched for Meltdown and Spectre. This worm infects multiple variants of Linux.

Much of the Internet routing infrastructure is based on Linux. We recommend that these machines be immediately patched for Meltdown and Spectre.

2 Indicators

This worm is difficult to detect. Its presence is detectable by its payload or by network traffic.

The most reliable way to detect this worm is to scan for its root kit. The payload of this worm is present only after the host computer has connected to the Internet and the worm has had the opportunity to install the root kit. This root kit infects several variants of the Linux operating system. We list the sha1sum checksums for the files in the root kit for both Panther OS, Table 1, and CentOS, Table 2.

A less reliable way to detect this worm is from the network traffic that it generates. From an analysis of network traffic, we were able to discover strange traffic between the host computer and several IP addresses. Recall that these IP addresses are only red-flags and may lead us to other infected servers.

These IP addresses, shown in Table 3, were collected from an infected computer that had the worm payload installed We have reason to suspect that the IP address 68.114.38.101 may be used by the payload of the worm to phone home.

There is no Trojan detected in association with this worm. A thorough search was made for Trojans. They were absent.

3 Speed of Infection

This worm spreads rapidly between sub-networks that are connected to each other. This worm spreads to computers that are not patched for Meltdown or Spectre.

4 Conclusions

Response to this worm is necessary. Since this worm likely exploits multiple vulnerabilities, we recommend addressing the worm at multiple levels. Patching for Meltdown and Spectre is necessary. Any computers that have the root kit installed must be repaired.

Panther OS sha1sum	**File**
c197eae325928ac2e5fa978fbb72870df63788cf	/sbin/fdisk
93884abd33c431392728cf7f8cc5b6d8d744cbee	/sbin/runuser
c5ff4235764ada0b3d45cb68d23ae7f14a4ad76d	/usr/sbin/rsyslogd
5fc8f38a9efb4ab4fcc928086cb7013aa76ecab2	/bin/ping
b629ceb5d63ddc4cd2fce8f228bd590fe716e09d	/bin/bash
1225338a415d35e7ee7ff5a32dcefe654dfb2666	/sbin/sulogin
46e78eb70430558bef714dcf3ee5756076bead09	/bin/su
e7ec2e377c806906c5b0bd1876734f0b0648d462	/bin/passwd
2b6f7596496e8d5d64b32b746a08c82cd203f498	/bin/kill
c3996a99de7ee8f6617f6a328adef471db1afad0	/bin/ssh-add
1434de77eb9a9da878ef31faa515d02c199a530e	/usr/sbin/chpasswd
4c276d8d32ec92032dddfe7f5a00dbccc9948967	/usr/bin/sudo
269ff0fd848e0ebef383d5284a68f96f66a34015	/usr/bin/netstat
aaa61a46088c768ea36b699015a12a498ff7aac0	/usr/bin/ssh
9de268e9f1a8ef044f4daa9eab05f777aecb9cbc	/usr/bin/sudoreplay
889df17e13060536010d83cf0c4a04b73ad58722	/usr/bin/find
4f3283c05cdeec804ce096a79000bf5ed6685ca3	/usr/bin/chrt
187f738e716c3d0471325abff4943b9fee8808a8	/usr/sbin/pppd

Table 1: On Chrome Panther OS, for each file in the root kit, there is a sha1sum checksum. The operating system is Linux version 3.8.11 (chrome-bot@cros-beefy239-c2) (gcc version 4.9.x 20150123 (prerelease) (4.9.2_cos_gg_4.9.2-r172-0c5a656a1322e137fa4a251f2ccc6c4022918c0a_4.9.2-r172)).

CentOS sha1sum	**File**
00d808ffbe1e428cd8ce2637e8846d308544b6f3	/usr/sbin/fdisk
06ea76a3d99e29d304fe742e4737a152ad38a4cf	/usr/sbin/runuser
187b499684b4cc6f65e9120ca6aecc67ceee3a18	/usr/sbin/rsyslogd
1bc2892139c74bf6309ffb65b8b3633d95aaab2c	/usr/bin/ping
2923d129fd912fc501c0cd1b37172c9091d29b0a	/usr/bin/bash
2ba1454b3274177b5de986b9c793a8eb30541c4d	/usr/sbin/sulogin
2d3090b8963771f6943851492e020d80dc9e03f1	/usr/bin/su
393d9501a912121cc09928ae69bfe34b9bfbb690	/usr/bin/passwd
46e13697878872ce21cd815cb18b6ee666a6d628	/usr/bin/kill
66fcf3185b1609265ba4d3956f1dafc8eb95562b	/usr/bin/ssh-add
6ef94b04be8fc06ecdc1d5350a2424509af90a62	/usr/sbin/chpasswd
85ed2f5c9a9839e2d0beca022bfa71a521e6279f	/usr/bin/sudo
8c1609ac972bcacb6dcbd2d7e60105e6d8ef3547	/usr/bin/netstat
9dddd21ca133a104a9925c720da58c039cf66991	/usr/bin/ssh
a5d9d4327dd88de38348ee9a40bddaa748c031ab	/usr/bin/sudoreplay
bc284cd392dbb1fbacf004ca8aedf57be57b290d	/usr/bin/find
c2b7ba26b4aab4b0bc1ae18d6d839179a2c5e787	/usr/bin/chrt
c379335320a003847b2f8ed51afa003cc919d6f5	/usr/sbin/pppd

Table 2: On CentOS Linux, for each file in the root kit, there is a sha1sum checksum. The operating system is Linux version 3.10.0-327.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc version 4.8.3 20140911 (Red Hat 4.8.3-9) (GCC))

IP Address	Protocol
107.175.144.206	ntp
192.96.202.120	ntp
199.180.249.103	ntp
216.58.217.42	https
216.6.2.70	ntp
68.114.38.101	bootps

Table 3: These are the red-flag IP addresses detected from an infected Panther OS.

Biography

Dr. Kirkpatrick has a bachelor's in computer science from Montana State University-Bozeman, a master's and a Ph.D. in computer science from the University of California, Berkeley. He is former faculty at the University of Miami, Department of Computer Science. Dr. Kirkpatrick is an expert in deterministic and statistical computer algorithms, and his main application area is the field of computational biology, in particular genetics. However, Dr. Kirkpatrick's algorithms expertise is general to the entire field of computer science, and he has recently had cause to specialize in algorithms for computer systems.