The 'Penquin' Turla

Recently, an interesting malicious sample was uploaded to a multi-scanner service. This immediately triggered our interest because it appears to represent a previously unknown piece of a larger puzzle. That puzzle is "Turla", one of the most complex APTs in the world.

We have written previously about the Turla APT with posts about their Epic Turla operations and Agent.btz inspiration . So far, every single Turla sample we've encountered was designed for the Microsoft Windows family, 32 and 64 bit operating systems. The newly discovered Turla sample is unusual in the fact that it's the **first Turla sample targeting the Linux operating system** that we have discovered.

This newly found Turla component supports Linux for broader system support at victim sites. The attack tool takes us further into the set alongside the Snake rootkit and components first associated with this actor a couple years ago. We suspect that this component was running for years at a victim site, but do not have concrete data to support that statement just yet.

The Linux Turla module is a C/C++ executable statically linked against multiple libraries, greatly increasing its file size. It was stripped of symbol information, more likely intended to increase analysis effort than to decrease file size. Its functionality includes hidden network communications, arbitrary remote command execution, and remote management. Much of its code is based on public sources.

Md5	Size	Verdict Name
0994d9deb50352e76b0322f48ee576c6	627.2 kb	N/A (broken file)
14ecd5e6fc8e501037b54ca263896a11	637.6 kb	HEUR:Backdoor.Linux.Turla.gen

General executable characteristics:

ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.2.5, stripped

Statically linked libraries:

- glibc2.3.2 - the GNU C library

- openssl v0.9.6 - an older OpenSSL library
- libpcap - tcpdump's network capture library

Hardcoded C&C, known Turla activity: **news-bbc.podzone[.]org**
The domain has the following pDNS IP: **80.248.65.183**

```
80.248.65.183
aut-num:       AS30982
```

```
80.248.65.183

aut-num:       AS30982

announcement:   80.248.65.0/24

as-name:       CAFENET

descr:         CAFE Informatique et telecommunications

admin-c:       YN2-AFRINIC

tech-c:        AN39-AFRINIC

org:           ORG-CIet1-AFRINIC

mnt-by:        AFRINIC-HM-MNT

mnt-lower:     CAFENET-NOC

source:        AFRINIC # Filtered
```

Note: the C&C domain is currently sinkholed by Kaspersky Lab.

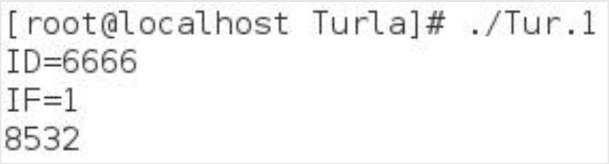
Functional description

The sample is a stealth backdoor based on the cd00r sources.

This Turla cd00r-based malware maintains stealth without requiring elevated privileges while running arbitrary remote commands. It can't be discovered via netstat, a commonly used administrative tool. It uses techniques that don't require root access, which allows it to be more freely run on more victim hosts. Even if a regular user with limited privileges launches it, it can continue to intercept incoming packets and run incoming commands on the system.

Startup and Execution

To start execution, the process requires two parameters: ID (a numeric value used as a part of the "magic packet for authentication") and an existing network interface name. The parameters can be inputted two different ways: from STDIN, or from dropper a launching the sample. This is NOT a command-line parameter, it's a real prompt asking the attacker user to provide the input parameters. After the ID and interface name are entered and the process launched, the backdoor's process PID is returned. Here is a screenshot of this simple interface:



```
[root@localhost Turla]# ./Tur.1
ID=6666
IF=1
8532
```

While there is no initial network callback, a section of code maintains a hardcoded c2 string "news-bbc.podzone[.]org". This fully qualified domain name was first set up in 2010, suggesting that this binary is fairly recent in the string of Turla campaigns. Also, while we haven't seen additional file download activity from this server by this tool, it likely participated as a file server of sorts.

Magic Packets for Remote Command Execution

The module statically links PCAP libraries, and uses this code to get a raw socket, applies a filter on it, and captures packets, checking for a specific condition (the *original cd00r first used this method, based on ports and SYN-packets). This condition is expressed here (it is based on the ID value input at startup by the attacker):

ID = 123 Filter = (tcp[8:4] & 0xe007ffff = 0xe003bebe) or (udp[12:4] & 0xe007ffff = 0xe003bebe) ID = 321 Filter = (tcp[8:4] & 0xe007ffff = 0x1bebe) or (udp[12:4] & 0xe007ffff = 0x1bebe)

In simple terms, it checks for an ACK number in the TCP header, or the second byte from the UDP packet body.

If such a packet is received and the condition check is successful, execution jumps to the packet payload contents, and it creates a regular socket. The backdoor handles this socket as a file with read/write operations. It's not the typical recv/send used in this code. It uses this new socket to connect to the source address of the "magic packets". Then it reports its own PID and IP to the remote address, and starts an endless loop for receiving remote commands. When a command arrives, it is executed with a "/bin/sh -c " script.

Further analysis of the sample's functionality will be updated here.

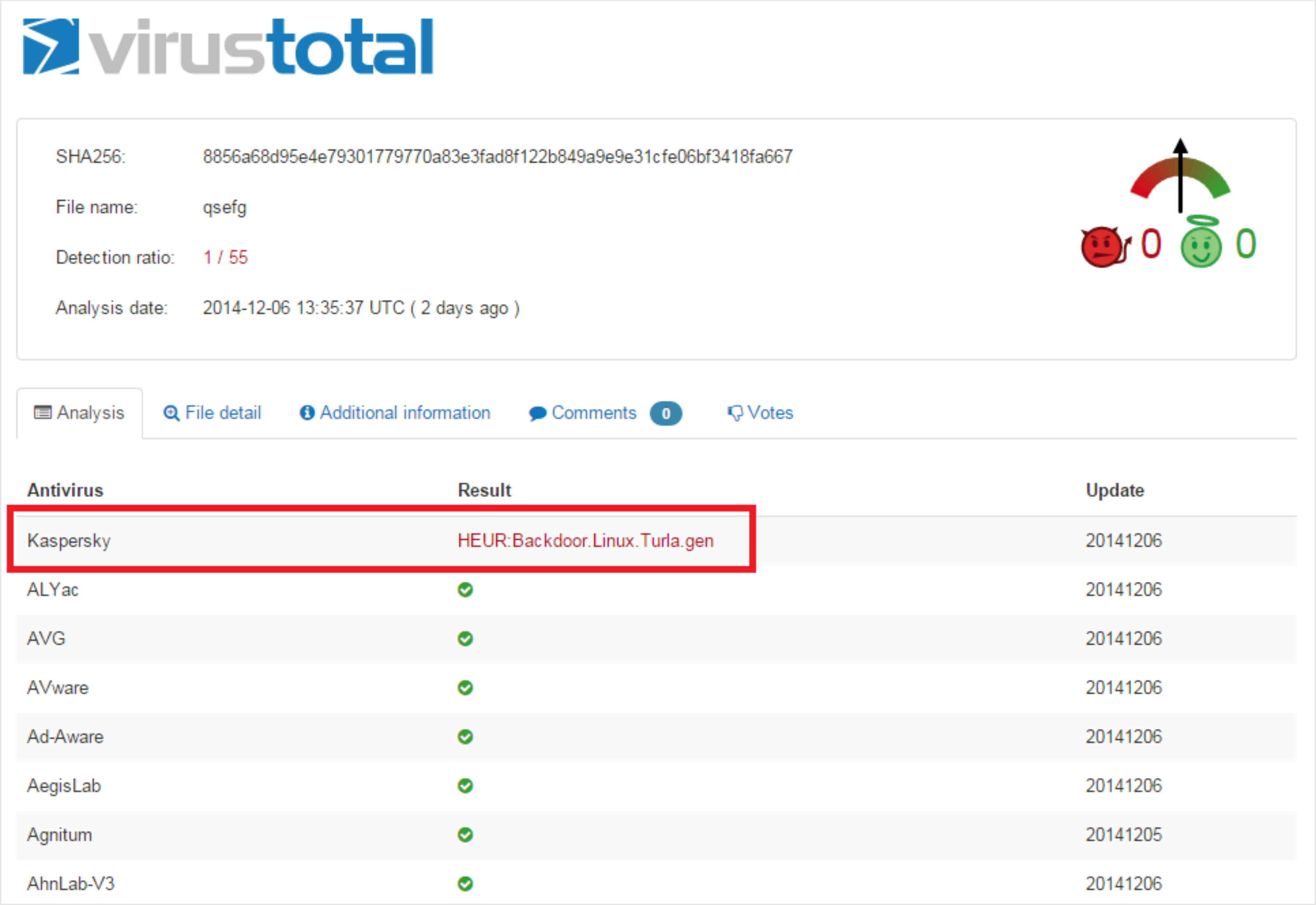
Conclusions

Although Linux variants from the Turla framework were known to exist, we haven't seen any in the wild yet.

This specific module appears to have been put together from public sources with some added functionality from the attackers. Some of the malicious code appears to be inactive, perhaps leftovers from older versions of the implant. Perhaps the most interesting part here is the unusual command and control mechanism based on TCP/UDP packets, as well as the C&C hostname which fits previously known Turla activity.

The discovery of this Turla module rises one big question: how many other unknown Turla variants exist?

Update: Since the publishing of this blogpost, we have discovered another Linux Turla module, which apparently represents a different malware generation than the previously known samples:



SHA256: 8856a68d95e4e79301779770a83e3fad8f122b849a9e9e31cfe06bf3418fa667

File name: qsefg

Detection ratio: 1 / 55

Analysis date: 2014-12-06 13:35:37 UTC (2 days ago)

Antivirus	Result	Update
Kaspersky	HEUR:Backdoor.Linux.Turla.gen	20141206
ALYac	✓	20141206
AVG	✓	20141206
AVware	✓	20141206
Ad-Aware	✓	20141206
AegisLab	✓	20141206
Agnitum	✓	20141205
AhnLab-V3	✓	20141206

The new sample was heuristically detected by our product due to similarities with the previously discovered samples.

Md5	Size	Verdict Name
19fbd8cbfb12482e8020a887d6427315	801,561 bytes	HEUR:Backdoor.Linux.Turla.gen

Related research:

- BAE Systems - The Snake Campaign

- Kaspersky Lab - The Epic Turla Operation
- "TR-25 Analysis - Turla / Pfinet / Snake/ Uroburos" by CIRCL.LU
- "Uroburos: the snake rootkit", technical analysis by deresz and tecamac
- Agent.BTZ - A Source of Inspiration?