The marvin.funkfeuer.at GRIZZLY STEPPE hack

Authored by the forensics team.

2017-1-18

Contents

Deutsche FAQ - German FAQ **2**
- Was ist mit dem Marvin passiert? . . . 2
- In welchem Zeitraum wurde Marvin für die Angriffe verwendet? . . . 2
- Sind die IP Adressen der Angreifer und der Bots bekannt? . . . 2
- Warum hatte Funkfeuer noch Logfiles aus 2015? . . . 2
- Wie kamen die Angreifer auf den Marvin? . . . 2
- Warum wurde der Marvin Opfer? . . . 3
- Wir waren der einzige Server in der Liste des DHS aus Österreich, ist das Zufall? . . . 3
- Gab es Root access? Gab es Zugriffe auf andere Services am Marvin? 3
- Waren sich die Angreifer bewusst, dass noch weitere Funkfeuer-Services auf dem Server laufen? . . . 3
- Was macht ein C2 Server bzw wie funktionierte das C2 Netzwerk in dem Marvin teilgenommen hat? . . . 3
- Woher wissen wir soviel über die Funktionsweise des C2 Netzwerks? . 4
- Waren es die Russen? . . . 4

English Report **4**
- TLP . . . 4

Overview **4**

Who (initial forensics)? **7**

Open questions **8**

Interesting findings **8**
- Keying material and communication pattern . . . 8

Version: 1.0

Deutsche FAQ - German FAQ

(For the full public english report, skip this section.)

Was ist mit dem Marvin passiert?

Am 31.12.2016 wurde Funkfeuer über eine Liste mit knapp 900 IP-Adressen des Department of Homeland Security darauf aufmerksam, dass einer seiner Server für den eMail-Diebstahl bei der US Demokratischen Partei verwendet wurde.

In welchem Zeitraum wurde Marvin für die Angriffe verwendet?

- 4.3.2015 10:47 - Über eine Lücke in Cacti Weathermap installieren unbekannte Angreifer eine Command-Control (C2) Software am Webserver.
- 4.3.2015 11:27 bis 21.7.2015 16:19 - Marvin wird (neben seiner normalen Tätigkeit) als C2 Server verwendet: Verschlüsselte Jobs werden an Bots übergeben, und die Ergebnisse wieder eingesammelt. Danach gab es keine Zugriffe mehr die eindeutig auf die C2 Tätigkeit zurückzuführen sind.
  Der C2 Server beinhaltete eine Selbstzerstörungs-Funktion mit der er sich selbst entfernen hätte können, diese wurde aber nie ausgelöst oder war nicht erfolgreich.

Sind die IP Adressen der Angreifer und der Bots bekannt?

Ja, aber wir haben starke Hinweise darauf, dass diese nur Proxies waren, und nicht direkt die Angreifer oder die gesteuerten Bots.

Warum hatte Funkfeuer noch Logfiles aus 2015?

Die Logfiles am Server werden via Logrotate (je nach Typ des Log) nach wenigen Wochen bis einigen Monaten automatisch ersetzt.

Im September 2015 wurde der Marvin von seiner Hardware auf einen Virtuelle Maschine transferiert. Die alte Festplatte wurde abgelegt und nicht wieder verwendet. Auf dieser befanden sich die Logfiles bis Ende August 2015.

Wie kamen die Angreifer auf den Marvin?

Ein Plugin (weathermap) für Cacti hatte eine Lücke die es erlaubte neue Dateien zu erzeugen. Dadurch konnten die Angreifer neue Skrtipts und Code am Server ablegen und ausführen.

Warum wurde der Marvin Opfer?

Angreifer suchen oft nach einer verwundbaren Software (automatisch) per Suchmaschinen und infizieren diese dann. Cacti wird oft als internes Tool verwendet und ist in den meisten Fällen nicht öffentlich erreichbar. Manche Angreifer prüfen zusätzliche Parameter: Hat ein Server eine gute Internet-Verbindung? Hat der Rechner eine lange uptime und einen alten Kernel? Dann wird er offensichtlich nicht übermäßig gewartet und gemonitored.

Wir waren der einzige Server in der Liste des DHS aus Österreich, ist das Zufall?

Kann sein dass es mehrere infizierte Server in Österreich gab, aber

1. nicht durch das DHS erkannt wurden
2. nicht den Anforderungen der Angreifer entsprachen (siehe oben)
3. auf Vorrat für spätere Kampangien gehalten werden.

Gab es Root access? Gab es Zugriffe auf andere Services am Marvin?

Wir haben keine Hinweise gefunden.

Für die Angreifer war es wahrscheinlich wichtiger unerkannt zu bleiben und den Rechner möglichst lang zu verwenden - dh. möglichst under-cover zu bleiben und nichts versuchen dass Alarm auslösen könnte.

Waren sich die Angreifer bewusst, dass noch weitere Funkfeuer-Services auf dem Server laufen?

Wahrscheinlich nicht. Wir haben keine Hinweise darauf gefunden, dass Zugriffe ausserhalb von Cacti und Smokeping stattfanden.

Was macht ein C2 Server bzw wie funktionierte das C2 Netzwerk in dem Marvin teilgenommen hat?

Ein C2 Server steuert andere infizierte Rechner in dem er Tasks oder neue Malware an diese Rechner vergibt und evt Ergebnisse wieder einsammelt und an die Auftraggeber weiterleitet.

Woher wissen wir soviel über die Funktionsweise des C2 Netzwerks?

Der C2 Server war ein zweifach ineinander verschlüsseltes PHP Skript. Wir konnten es entschslüsseln und analysieren. Von einem Software-Engineering Standpunkt gesehen war es eine sehr sauber geschrieben objektorientierte Software welche direkt die Objekte (Clients/Tasks) auf die Festplatte serialisiert und wieder lädt. Wir wissen dass die Tasks mit einem individuellen Schlüssel für jeden Bot verschlüsselt waren, so daß kein C2 Server oder Proxy mitlesen konnte, was gerade passiert.

Waren es die Russen?

Wir wissen es nicht.

Die proffesionallität der C2 Software läßt vermuten, dass es keine "Skript-Kiddies" waren.

English Report

TLP

Figure 1: This report is **Traffic Light Protocol:WHITE**

This report is public.

Also there is a news report on this case: http://derstandard.at/2000050143907/Russische-Hacker-nutzten-laut-FBI-auch-Rechner-in-Wien (german)

Overview

This text is written in english. The reason is that we might want to share the findings with a larger circle of people. Hence - english.

Funkfeuer.at is a non-commercial association ("Verein"), which built a small datacenter in Vienna and runs a wireless community mesh network (Rooftop network). See www.funkfeuer.at for a description of the project. It is well known, was widely reported about in the press and is generally seen as a

nice and friendly place to meet other people interested in building computer networks. It attracts a lot of capable engineers in IT. Funkfeuer runs a small data center ("server housing") in the 1st district of Vienna. Pictures and infos here: https://housing.funkfeuer.at/.

Funkfeuer is generally sort of well run, members can join the project but have to register via name, email and telephone number. The server housing project is self-sustaining (members pay a certain amount of EURs per server to sustain the operations). Work is mostly volunteer-driven.

On 30th of Dec 2016 Funkfeuer learned that one of it's central servers ("marvin.funkfeuer.at", ip: 193.238.157.16) was supposedly a "command & control server" (C2, C&C server) for the operations against the Democratic National Congress in the US.

The marvin.funkfeuer.at server ("marvin") is a virtualised server (moved from a physical server onto a Xen domU virtualised system in fall of 2015). It contains the central billing database, the members database, a whois service, an ftp server for uploading web cam pictures of the data center, old mailing list archives, an ssh server, the central dokumentation for system administrators for the whole Funkfeuer network and housing (dokuwiki) (including passwords of switches), a smokeping installation (for pingin network devices), a Cacti installation, etc. It is probably *the most central server* in the Funkfeuer housing project.

We found out that the attackers came in via a very old Cacti installation which was **not maintained anymore at Funkfeuer**.

Since the Funkfeuer board learned via CERT.at and the DHS report that marvin.funkfeuer.at had been hacked, the board and CERT.at initiated a forensics investigation. In addition to the forensic investigation (which created two reports, an internal one and the public one), the board of Funkfeuer created a task force to identify weaknesses and is (hopefully) working on improving things.

Since beginning of January, the server is shut down and not operational anymore.

Reconstructed time-line of the incident

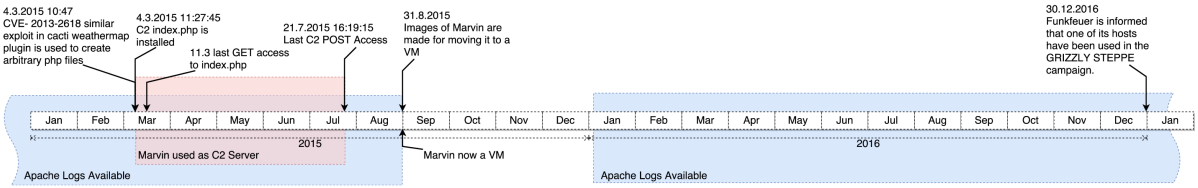

Figure 2: timeline.pdf

An overview of the timeline is:

- Server started operations in ~ 2004 or 2005
- Server was behaving strangely in 2015.

  - Root Cause: mainboard breakdown. 1:1 replacement did not boot from SATA disk (known BIOS bug, BIOS upgrade not done/found)
  - Hardware migration to Board with Intel G45 Chipset (DG45FC), frequent lockups, IIRC known bug for G45 with this old kernel version
- Server was virtualised in fall of 2015 -> running stable.
- The initial forensic analysis discovered an encrypted PHP C2 code which was not installed by Funkfeuer and which could serve as a C2 server. The timestamp of the PHP code file is 4th of March 2015. The decrypted PHP code script is not attached to this report - but can be requested for academic purposes.
- The initial forensic analysis discovered that some log files were missing and/or modified - later turned out to be a logrotate configuration problem.
- Netflow only exists as aggregated data (sum of bytes/packets per IP per day). This was done as a policy decision some years ago. So netflows were not used in this analysis
- Subsequent analysis of older disk images revealed a well preserved apache log file which shows the IP addresses which communicated with the PHP C2 server.

Initial compromise

- The intruder seems to have used a vulnerability in cacti's weathermap plugin similar to CVE-2013-2618
- The most important log entries of the exploit are:

```
178.33.X.X - - [04/Mar/2015:10:47:24 +0100] "GET
 /cacti/plugins/weathermap/editor.php?mapname=blank.php&action=newmap&plug=
 HTTP/1.1" 200 31336 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0)
 Gecko/20100101 Firefox/32.0"
178.33.X.X - - [04/Mar/2015:10:47:30 +0100] "POST
 /cacti/plugins/weathermap/editor.php HTTP/1.1" 200 31359 "-" "Mozilla/5.0
 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0"
178.33.X.X - - [04/Mar/2015:10:49:55 +0100] "GET
 /cacti/plugins/weathermap/configs/blank.php HTTP/1.1" 200 686 "-" "Mozilla/5.0
 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
178.33.X.X - - [04/Mar/2015:10:49:58 +0100] "GET
 /cacti/plugins/weathermap/configs/blank.php HTTP/1.1" 200 686 "-" "Mozilla/5.0
 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
178.33.X.X - - [04/Mar/2015:10:50:00 +0100] "POST
 /cacti/plugins/weathermap/configs/blank.php HTTP/1.1" 200 691 "-" "Mozilla/5.0
 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
178.33.X.X - - [04/Mar/2015:10:50:03 +0100] "POST
 /cacti/plugins/weathermap/configs/blank.php HTTP/1.1" 200 686 "-" "Mozilla/5.0
 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
178.33.X.X - - [04/Mar/2015:10:50:06 +0100] "GET
 /cacti/plugins/weathermap/configs/compress.php HTTP/1.1" 200 120 "-" "Mozilla/5.0 #
 (Windows NT 6.3; rv:36.0) Gecko/20100101 Firefox/36.0"
```

- compress.php was a webshell that was called 18 times, before the final C2 script /smokeping/index.php appeared on disk and was subsequently used.

Overview of disk images / disks of marvin.funkfeuer (and their age):

- physical discs from before the virtualisation exist: this was a RAID-1.
- There are two other copies (`dd`) of the disk images from the time the server was virtualised. Hence, the forensics team had enough data to work with.

From the disk images, the forensics team got the evidence of a PHP C2 script which was indeed installed on /var/www/smpkeping/index.php. The forensics team found out from the GRIZZLY STEPPE report from DHS, that the GRIZZLY STEPPE attack happened in mid 2015. From one set of the dd images the forensis team got a lot of well preserved apache log file which showed exactly which IP Addresses were communicating with the PHP C2 script. The IP addresses (and the frequency of their access to the PHP C2 code) are:

```
% zgrep '"POST /smokeping/index.php' *| sed -E 's/.*([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-

 60597 141.255.X.X "Python-urllib/2.7"
 25601 62.68.X.X "Python-urllib/2.7"
 19438 141.255.X.X "Python-urllib/2.7"
 16903 198.15.X.X "Python-urllib/2.7"
 15990 178.209.X.X "Python-urllib/2.7"
  1719 178.33.X.X "Python-urllib/2.7"     <----- same as .... the last on this list
  1701 82.221.X.X "Python-urllib/2.7"
    60 50.202.X.X "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
    40 41.194.X.X "Python-urllib/2.7"
     1 178.33.X.X "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0'
```

(note: pseudonomyzed for this report. The full IPs are known to the forensics team)

Note the access by Mozilla/5.0 on Windows NT 6.1 This is a hint of which IP address the attacker was actually using - for example for the initial infection.

Access pattern:

Who (initial forensics)?

The forensics was done by an experienced team of IT security professionals in Vienna.

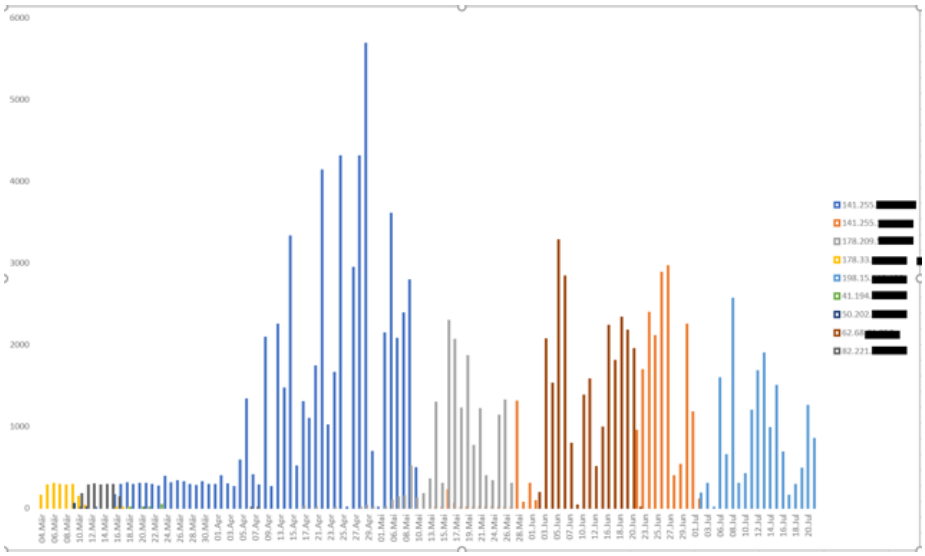

Figure 3: matches-public.png

Open questions

- **Q:** Where there any rootkits/ root access?

  A: most probably not. We did not find anything and thus can assume that the server was only mis-used as a C2 server and that the attackers were not particularly interested in the data of a small association which is on the hard disk.

- **Q:** Are therer any clients admin traces? Structure of the network?

  A: each communication with the C2 server code was encrypted. It was impossible to find out, what data was being sent over the C2 server. See below.

- **Q:** Could we find any access to the member's data?

  A: no.

Interesting findings

Keying material and communication pattern

- The communication with the C2 server PHP code was encrypted. We found some things (PHP serialized data structures) in a file called "Deutsch-

land.png". The filename was specifically chosen to blend into the existing directory structure.

- Inspection of "Deutschland.png" reveals interesting results: it is the PHP serialized state, including keying material.

```
O:14:"ClientsHandler":3:{s:7:"clients";a:1:{i:0;O:6:"Client":5:{s:4:"uuid";s:12:"Z20H-GC7CRP
```

In readable format:

```
O:14:"ClientsHandler":3:{
    s:7:"clients";
    a:1:{
        i:0;
        O:6:"Client":5:{
            s:4:"uuid";
            s:12:"Z20H-GC7CRPG";
            s:10:"created_at";
            i:1425906019;
            s:9:"prev_last";
            i:1426016953;
            s:4:"last";
            i:1426072109;
            s:5:"tasks";
            a:0:{}
            }
        }s:3:"key";
        s:40:"EZ5ci7rH/KsME7n+y2lH5GToIPewZ1e60pOK1w==";
        s:6:"key_at";
        i:1464760742;
    }
```

- The source code of the C2 server is a rather clean type of code. It uses an object-oriented architecture to manage tasks and clients and persists the serialized object structure to disk (see above). The snapshot of the recovered file, does not contain tasks (any more).
- We find out (by other sources) that this C2 server seems to have been a root tree node for the (encrypted) command chain. Different (probably also hacked) servers log in and request commands and receive commands from the C2 server.
- Since we do not find any interesting log files on the running server, we decide to create forensic images.
- LVM snapshot of the disk filesystem from marvin done via these instructions: http://www.tldp.org/HOWTO/LVM-HOWTO/snapshots_backup.html

```
root@vogsphere:/mnt2# lvcreate -L 20G  -s -n marvin.funkfeuer.at-rootfs-snapshot -v  /dev/vo
root@vogsphere:/mnt2# dd if=/dev/vogsphere/marvin.funkfeuer.at-rootfs-snapshot of=/mnt/marvi
```