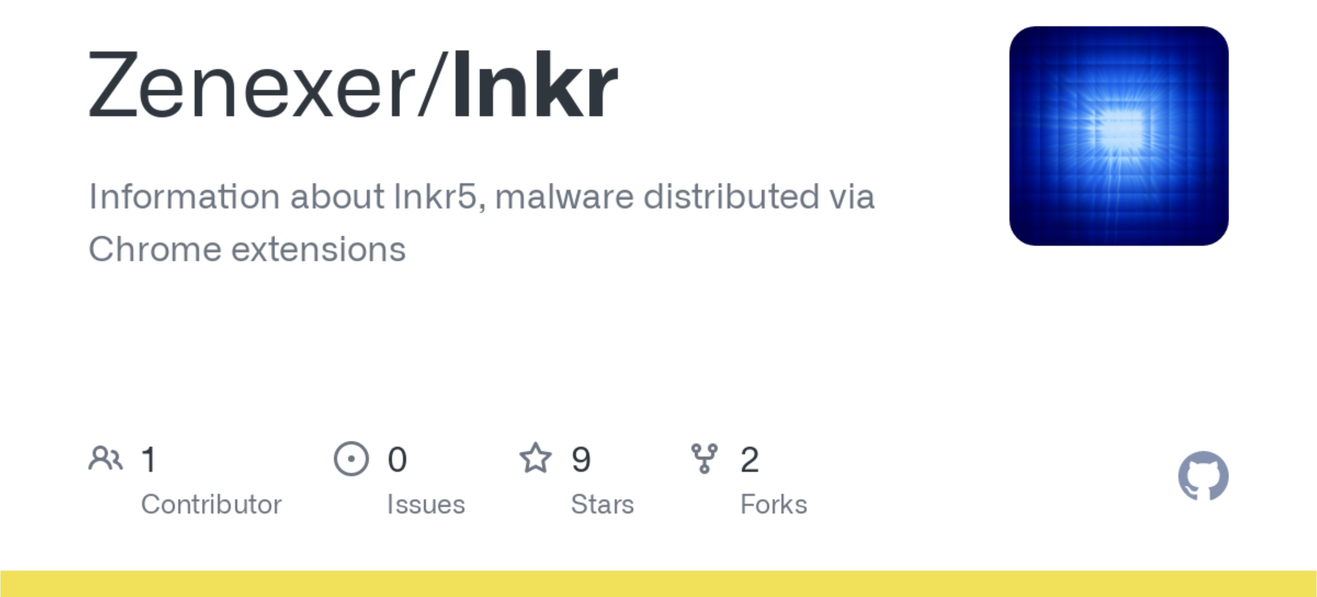
lnkr/README.md at master · Zenexer/lnkr · GitHub

github.com/Zenexer/lnkr/blob/master/recon/extensions/fanagokoaogopceablgmpndejhedkjjb/README.md

Zenexer



Zenexer/**lnkr**

Information about lnkr5, malware distributed via Chrome extensions

Extension analysis

ID
`fanagokoaogopceablgmpndejhedkjjb`

Name
Flash Playlist

Version
1.2.0

This extension is a modified, likely unauthorized clone of `fnipglnbhfacfmefbgiiodalehbcgcbm`. The malicious clone has since been removed from the Chrome Web Store.

Flow

Unix timestamps have been replaced with `[timestamp]`

1. `manifest.json` specifies `background.js` as a background script

2. `manifest.json` specifies `content_page.js` as a content script, which appears to be a standard Mixpanel script
3. `background.js` performs an ajax request for `http://flashplaylist.com/api/?action=params&id=fanagokoaogopceablgmpndejhedkjjb&version=1.2.0`
4. `background.js` stores the result in Chrome local storage via `chrome.storage.local.set`; the result includes a value for `MIXPANEL_CUSTOM_LIB_URL`
5. User visits an arbitrary website
6. `content_page.js` injects a `<script>` tag for the script specified in local storage for `MIXPANEL_CUSTOM_LIB_URL`, which is `//serenityart.biz/1f7cbb02d08cf61dbb.js`
7. `1f7cbb02d08cf61dbb.js` performs a JSONP request for `https://serenityart.biz/optout/get?jsonp=__twb_cb_6375332&key=1f7cbb02d08cf61dbb&t=[timestamp]`
8. `1f7cbb02d08cf61dbb.js` loads several tracking GIFs based on the page load status in the form of `https://serenityart.biz/metric/?mid=&wid=52096&sid=&tid=8060&rid=[rid]&custom1=netops.is&custom2=/&custom3=serenityart.biz&t=[timestamp]`, where `[rid]` is each of:
    1. `LOADED`
    2. `FINISHED`
    3. `BEFORE_OPTOUT`
    4. `LAUNCHED`
9. `1f7cbb02d08cf61dbb.js` performs JSONP requests for:
    1. `https://serenityart.biz/optout/set/lat?jsonp=__twb_cb_699176887&key=1f7cbb02d08cf61dbb&cv=[timestamp]&t=[timestamp]`
    2. `https://serenityart.biz/optout/set/lt?jsonp=__twb_cb_903372803&key=1f7cbb02d08cf61dbb&cv=6&t=[timestamp]`
10. injects a `<script>` tag for `https://srvvtrk.com/91a2556838a7c33eac284eea30bdcc29/validate-site.js?uid=52096x8060x&r=[timestamp]`
11. injects a `<script>` tag for `https://serenityart.biz/addons/lnkr5.min.js`

12. performs loads several additional tracking GIFs in the form of `https://serenityart.biz/metric/?mid=[mid]&wid=52096&sid=&tid=8060&rid=[rid]&t=[timestamp]`, where `[mid]` and `[rid]` are each of:
    1. `mid=18918`, `rid=MNTZ_INJECT`
    2. `mid=`, `rid=OPTOUT_RESPONSE_OK`
    3. `mid=cd1d2`, `rid=MNTZ_INJECT`
    4. `mid=18918`, `rid=MNTZ_LOADED`
    5. `mid=90f06`, `rid=MNTZ_INJECT`
    6. `mid=cd1d2`, `rid=MNTZ_LOADED`
    7. `mid=90f06`, `rid=MNTZ_LOADED`

Responses

`http://flashplaylist.com/api/`

```
{
        "analyticsId": "UA-108823706-1",
        "mixpanelId": "58410f8ab299e0eb2b736f6e233eda37",
        "vars": {
                "MIXPANEL_CUSTOM_LIB_URL":
"\/\/serenityart.biz\/1f7cbb02d08cf61dbb.js"
        },
        "validateFields": null
}
```

`https://serenityart.biz/optout/get`

```
__twb_cb_6375332({
        "success": "1",
        "targeting": "0",
        "country": "US",
        "userId": "64",
        "strTm": "[timestamp]",
        "lt": "0",
        "lat": "[timestamp]",
        "limits": "",
        "lcFlag": "",
        "optout": ""
});
```