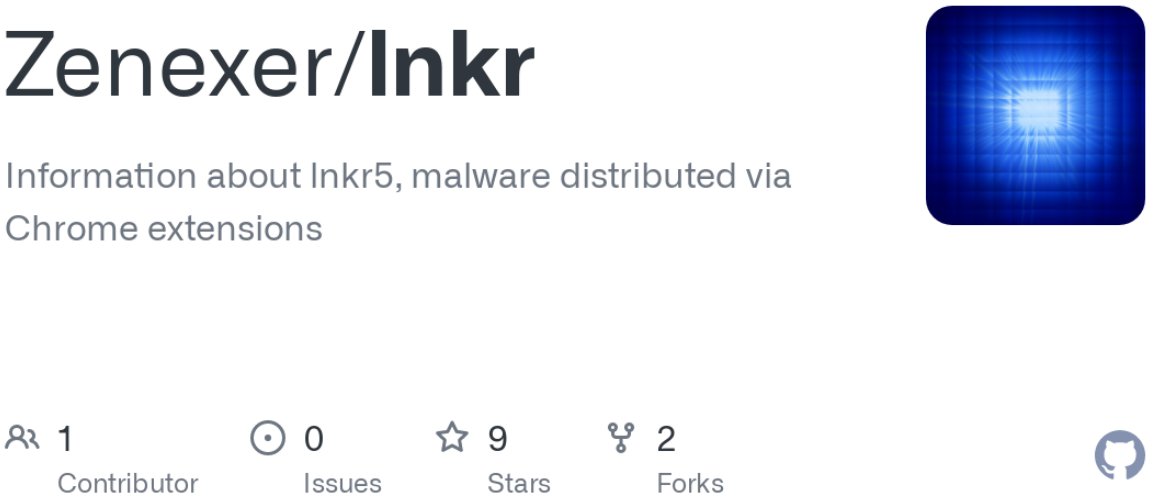
Zenexer/Inkr: Information about Inkr5, malware distributed via Chrome extensions

github.com/Zenexer/Inkr

Zenexer



Inkr

Inkr is a malware campaign that injects scripts into web pages via malicious browser extensions.

The campaign has been identified as belonging to Brocode, a shell company registered in Hong Kong via startupr.com.hk. The attackers are believed to be Eastern European, likely Ukrainian or Russian, but there's no indication that the effort is state-sponsored.

The attackers clone legitimate and semi-legitimate Chrome extensions. Scripts are added to the clones that inject ads into every web page visited by the victim, in addition to potentially sending sensitive data to C2 servers. The C2 communications are disguised as analytics opt-out requests. The malicious code will falsely explain to the victim that the ads suppor the development of the extension, but almost all of the affected extensions aren't developed by the attackers.

The extension that I analyzed, Flash Player + 1.2.0, ID fanagokoaogopceablgmpndejhedkjjb, was a modified, likely unauthorized clone of an extension of the same name, ID fnipglnbhfacfmefbgiiodalehbcgcbm. The malicious clone has been removed from the Chrome Web Store; the original remains.

The attackers make the attack difficult to block. Generic S3 bucket names are used, C2 domain names are frequently rotated, and C2 IP addresses are numerous and spread across many hosting providers. C2 communications are disguised as opt-out requests.

Affected extensions appear widespread and affect a significant percentage of English-speaking Chrome users. The extensions are often removed from the Chrome store before they can be analyzed, which makes it difficult to assess the number of affected extensions. Concentrations appear to be in the United States and India.

At least one extension keeps a log of search keywords. It's not yet certain that this data is stored and transmitted by lnkr, but preliminary evidence points to that conclusion.

The name `lnkr` appears to be the name used by the attackers. The boostrap scripts are prefixed with `lnkr`, and some of the server-side C2 source code is in a folder named `lnkrApi`. `lnkr.us` and `lnkr.fr` both appear to be controlled by the attackers.

Attack analysis

See an analysis of one of the extensions

IOCs

This should not be treated as an exhaustive list.

Domain names

See domains.txt

IP addresses

See ips.txt

URL prefixes

Scheme can be either `http:` or `https:`.

```
//s3.amazonaws.com/jscache/
//s3.amazonaws.com/jscript-cdn/
//s3.amazonaws.com/cashe-js/
//s3.amazonaws.com/jsbooster/
//adrs.me/get?key=6ae9f4bd1dc812dc713d61cba871d8e8&
```

URL contents

```
/api/js-get?sourceId=
/optout/get?jsonp=__twb_cb_
/lnkr5.min.js
/optout/set/lat?jsonp=
/optout/set/lt?jsonp=
/script/d.php?uid=
/www/delivery/avw.php?
/www/delivery/afr.php?
/www/delivery/ck.php?
```

Arbitrary strings

```
lnkr5.min.js
lnkr30_nt.min.js
1100b35355a4776ae9
143e7cdebf193d2764
16a168f0af2da0c3c2
17c9c17dd4d2a394de
1bbe2f4535e7dfb295
1f7cbb02d08cf61dbb
c822bb0d82ad01a5ae
__ckp_srchydx_fired
__ckp_srchmlr_fired
```

Example script URLs

This list is far from exhaustive.

URLs may be requested over plain HTTP or HTTPS.

```
https://netcheckcdn.xyz/addons/lnkr5.min.js
https://netcheckcdn.xyz/addons/lnkr30_nt.min.js
https://s3.amazonaws.com/jscript-cdn/1f404c54c2b0e13e0f.js
https://s3.amazonaws.com/cashe-js/143e7cdebf193d2764.js
https://s3.amazonaws.com/jscache/17c9c17dd4d2a394de.js
https://s3.amazonaws.com/jscache/16a168f0af2da0c3c2.js
```

Analytics IDs

These IDs are seen interspersed with malicious code. They may or may not belong to the attackers or uniquely identify the attacks.

- Mixpanel
  58410f8ab299e0eb2b736f6e233eda37
- Google Analytics
  UA-108823706-1

Abuse report correspondence

I sent an abuse report to Amazon Web Services regarding the S3 buckets. Amazon didn't remove the malicious code. When I questioned why, they forwarded me this response from the attackers. (Some of the text is quoted from my original report; they appear to be addressing the individual points I mentioned.)

> Hello,
> thanks for reaching us out regarding this issue.
>
> 1. Here is a Virustotal report for the object 'jscript-cdn/1f404c54c2b0e13e0f.js' : https://www.virustotal.com/#/url/5f4279d8097fd1fd1c234e992a0c028146e5d102b2a3636fe1a9db3b87240503/detection, as you can see only ESET alerts on this, but from our latest case we figured out that it's a false positive alert on the URL, not for a script content, but haven't got a reply from ESET so far. The same situation is for 'jscript-cdn/1f65199417190d400c.js'.
>
> Anyway this scripts are not in use at this time.
>
> 1. 'jscript-cdn/ is used to host scripts that are part of a malware campaign. The attacker creates malicious duplicates of legitimate extensions in the Chrome web store and injects these scripts into them. The 'jscript-cdn' is used to host scripts for:
>
>   1. Monetization chrome extensions, firefox addons, websites and other web applications.
>   2. Analytics scripts for browser extensions. If the script is used for monetization, it's completely MS and Google Compliance. Nor Monetization of extensions nor Injecting ads in a proper way is not prohibited. There are Extension's Quality Quidlines and Single Purpose Policy. And of course there is no malicious code inside, we check all scripts regularly and are eager to keep them clean. If you find something suspicious in our scripts please let us know and we'll take the action immediately.
> 2. The link is to an old article about the extension that had been using monetization script with search enhanced results, but the integration has been made incorrect that's why some important features, such as Opt Out from ads hadn't been work. But the extension has been dropped from the store not for monetization particularly but for violating single purpose policy.
>
> User installs the extension from official chrome store, if he doesn't like that the extension is monetized with scripts he can easily remove the extension from his browser and install alternative from the store. Usually our clients aware users in the description of the extension that it contains the monetization scripts.
>
> Best wishes, Brocode Team

Ultimate response from AWS:

> Hello,
> Thank you for providing the additional information. We are unable to remove the content at this time as we have no evidence of the reported files are malicious. These files appear to be adware, not malware.
>
> If you have conclusive evidence that the reported files cause harm, please forward the information.
>
> Regards,
>
> AWS Abuse Escalations

WHOIS

lnkr.us

```
Domain Name: lnkr.us
Registry Domain ID: D43534441-US
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: publicdomainregistry.com
Updated Date: 2018-12-22T16:06:01Z
Creation Date: 2013-12-19T21:11:43Z
Registry Expiry Date: 2019-12-18T23:59:59Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C45976584-US
Registrant Name: Sergei Filov
Registrant Organization: N/A
Registrant Street: Svobody street 58
Registrant Street:
Registrant Street:
Registrant City: kiev
Registrant State/Province: Kiev
Registrant Postal Code: 01001
Registrant Country: UA
Registrant Phone: +003.80985512834
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: adverto@mail.com
Registrant Application Purpose: P1
Registrant Nexus Category: C31/UA
Registry Admin ID: C45976584-US
Admin Name: Sergei Filov
Admin Organization: N/A
Admin Street: Svobody street 58
Admin Street:
Admin Street:
Admin City: kiev
Admin State/Province: Kiev
Admin Postal Code: 01001
Admin Country: UA
Admin Phone: +003.80985512834
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: adverto@mail.com
Admin Application Purpose: P1
Admin Nexus Category: C31/UA
Registry Tech ID: C45976584-US
Tech Name: Sergei Filov
Tech Organization: N/A
Tech Street: Svobody street 58
Tech Street:
Tech Street:
Tech City: kiev
Tech State/Province: Kiev
```

```
Tech Postal Code: 01001
Tech Country: UA
Tech Phone: +003.80985512834
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: adverto@mail.com
Tech Application Purpose: P1
Tech Nexus Category: C31/UA
Name Server: vipvdscom.earth.orderbox-dns.com
Name Server: vipvdscom.mars.orderbox-dns.com
Name Server: vipvdscom.mercury.orderbox-dns.com
Name Server: vipvdscom.venus.orderbox-dns.com
```

thisadsfor.us

Domain Name: thisadsfor.us
Registry Domain ID: D46227974-US
Registrar WHOIS Server:
Registrar URL: www.tldregistrarsolutions.com
Updated Date: 2018-05-16T11:14:01Z
Creation Date: 2014-08-08T15:29:34Z
Registry Expiry Date: 2019-08-07T23:59:59Z
Registrar: TLD Registrar Solutions Ltd.
Registrar IANA ID: 1564
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: C46227970-US
Registrant Name: frank medison
Registrant Organization:
Registrant Street: Govanny ave 123
Registrant Street:
Registrant Street:
Registrant City: Brazil
Registrant State/Province:
Registrant Postal Code: 41111
Registrant Country: BR
Registrant Phone: +55.4552132
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: frankomedison1020@gmail.com
Registrant Application Purpose: P3
Registrant Nexus Category: C11
Registry Admin ID: C46227972-US
Admin Name: frank medison
Admin Organization:
Admin Street: Govanny ave 123
Admin Street:
Admin Street:
Admin City: Brazil
Admin State/Province:
Admin Postal Code: 41111
Admin Country: BR
Admin Phone: +55.4552132
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: frankomedison1020@gmail.com
Registry Tech ID: C46227971-US
Tech Name: frank medison
Tech Organization:
Tech Street: Govanny ave 123
Tech Street:
Tech Street:
Tech City: Brazil
Tech State/Province:
Tech Postal Code: 41111
Tech Country: BR
Tech Phone: +55.4552132

```
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: frankomedison1020@gmail.com
Name Server: ns-usa.topdns.com
Name Server: ns-uk.topdns.com
Name Server: ns-canada.topdns.com
```

Related reports