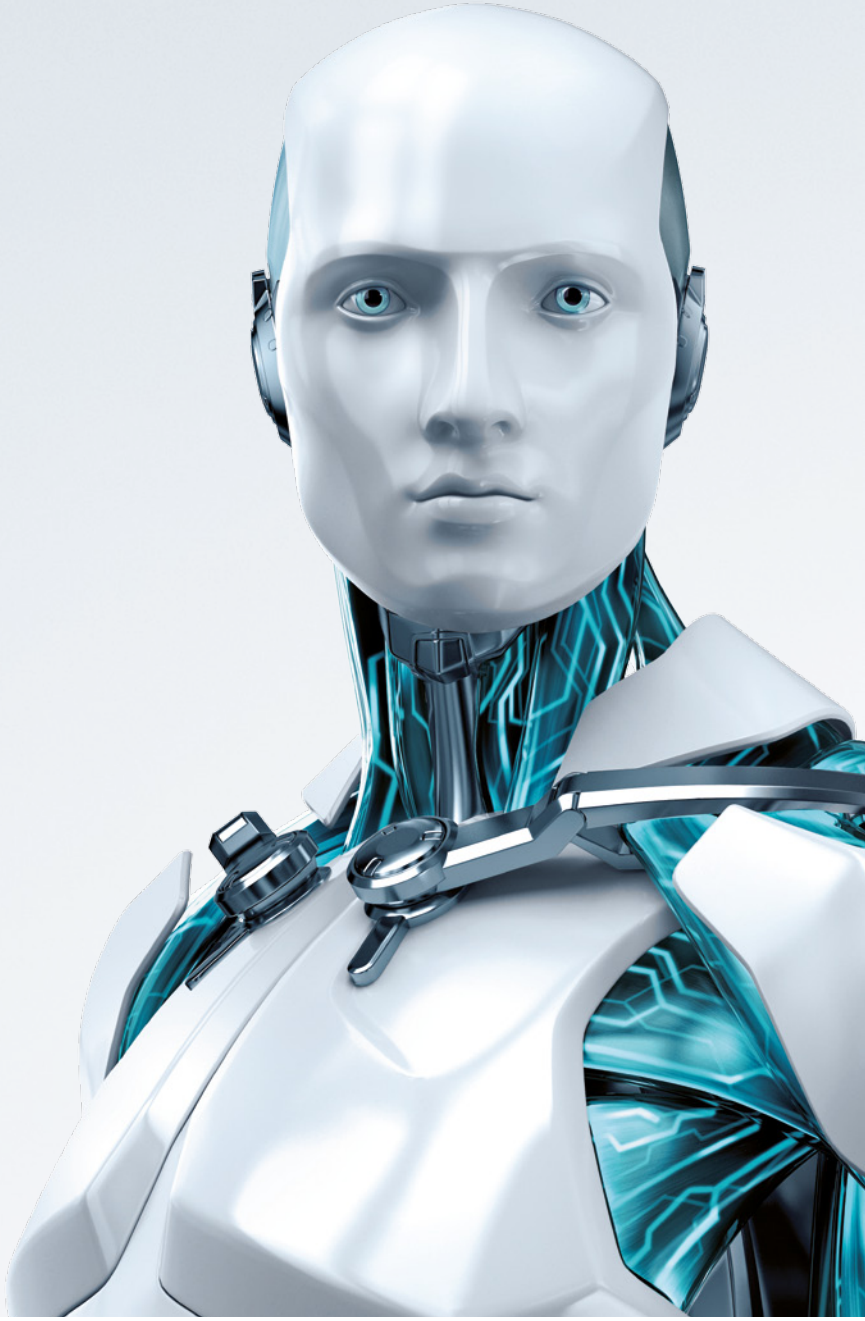
‘PokerAgent’

Stealing over 16000 Facebook Credentials



The 'PokerAgent' botnet, which we have tracked in 2012, was designed to harvest Facebook log-on credentials, also collecting information on credit card details linked to the Facebook account and Zynga Poker player stats, presumably with the intention to mug the victims. The threat was mostly active in Israel.

Introduction

ESET Security Research Lab has discovered an attention-grabbing Trojan horse about a year ago. The signs which indicated that it would be something interesting were references to Facebook, its Zynga Poker App (seen from the text strings in the binary), the executable name "PokerAgent" and botnet features – the Trojan would request tasks from a C&C server.

ESET has been detecting the different variants of the Trojan generically as **MSIL/Agent.NKY**. After the initial discovery, we were able to find other versions of the Trojan, both older and newer, and acquire detection statistics which have revealed that the Trojan was most active in the country of Israel.

We have performed a deep analysis of the Trojan's source code (which was quite trivial as it was programmed in C#, which is easily to decompile) and started monitoring the botnet. The findings are presented below.

Malware functionality

The malware author/attacker has an extensive database of **stolen Facebook credentials** – login names and passwords. At first, we didn't know how he had acquired the credentials, but later on in the investigation this became clear. When the bot connects to the C&C server, it requests tasks to carry out. One such "task" equals one Facebook user. The Trojan is programmed to log into this Facebook account, and collect the following information:

1. **Zynga Poker stats** for the given Facebook ID
2. **Number of payment methods** (i.e. credit cards) saved in the Facebook account

The Zynga Poker user statistics are acquired by parsing the response from the URL: http://facebook2.poker.zynga.com/poker/inc/ajax/profile_popup.php?zid=1:%_FACEBOOK_ID%&signed_request=%_SIGNATURE% &platform=1

This returned response looks something like the one below, and contains various information about the user, such as his or her name, gender, profile picture, Zynga poker rank and points, number of 'buddies' and statistics on hands played in the game.

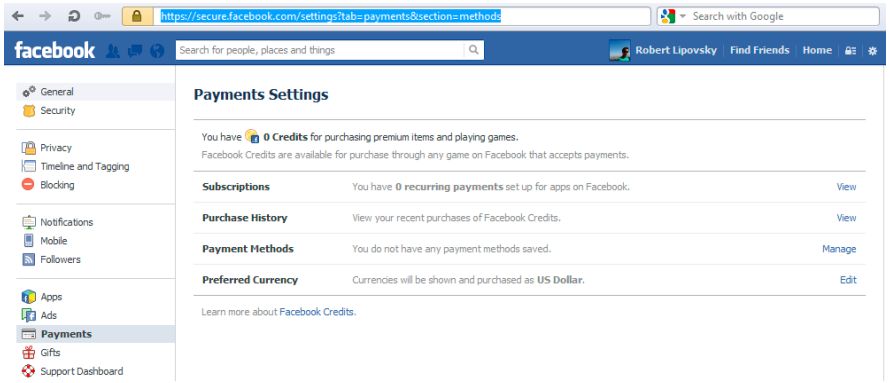
```
{
"name":"Gertruda",
"gender":"fem",
"profile_pic":
"https:\/\/zynga1-a.akamaihd.net\/pokerimages\/poker\/image_proxy.php\/aHR0cDovL3Byb2ZpbGUuYW[redacted]
"rank":"1K+",
"xp":"1 - Fish I",
"install":"December 07, 2011",
"points":"2998",
"buddies":1,
"network":"",
"stats":{
    "biggest_pot":0,
    "best_hand":["",[]],
    "hands_played":"1",
    "hands_won":0,
    "shootouts_won_pct":0,
    "sitngos_won_pct":0,
    "recent_achieves":{
        "34":{
            "id":"34",
            "profile_url":"http:\/\/statics.poker.static.zynga.com\/poker\/img\/shouts\/012_welcome_100.png"
            }
                    },
    "recent_gifts":[]
        },
"zid":"1:10000[redacted]
}
```


The Trojan is only interested in the gender of the user, points and rank. This information is sent back to the C&C server.

Note that in order to pose the query, the perpetrator only needs the victim's numerical Facebook ID and a valid signed request parameter for the Zynga Poker application. Throughout the different versions of the bot, we have observed different parameters being used.

More information on the popular game Zynga Poker can be found here.

In order to ascertain the number of payment methods linked into the Facebook account, the bot first has to log into the account (using a Facebook username and password already in the perpetrator's possession). The Trojan then browses to https://secure.facebook.com/settings?tab=payments&section=methods and simply parses the number between html tags in the following string "You have X payment methods saved." from the HTML page.



We advise careful consideration before storing credit card details into any app, not only Facebook! Again, this information is sent back to the C&C server to update the attacker's victim database.

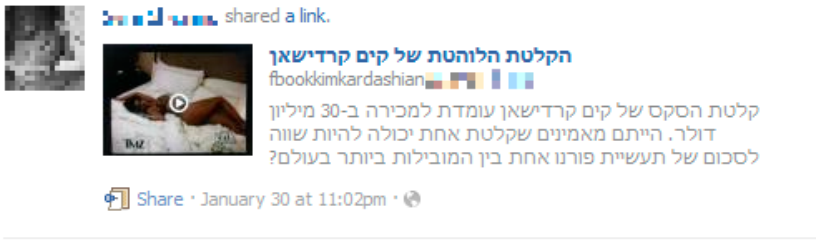
The infected bot can be instructed to perform one other important task on behalf of a Facebook victim:

3. Publish links on the Facebook user's wall

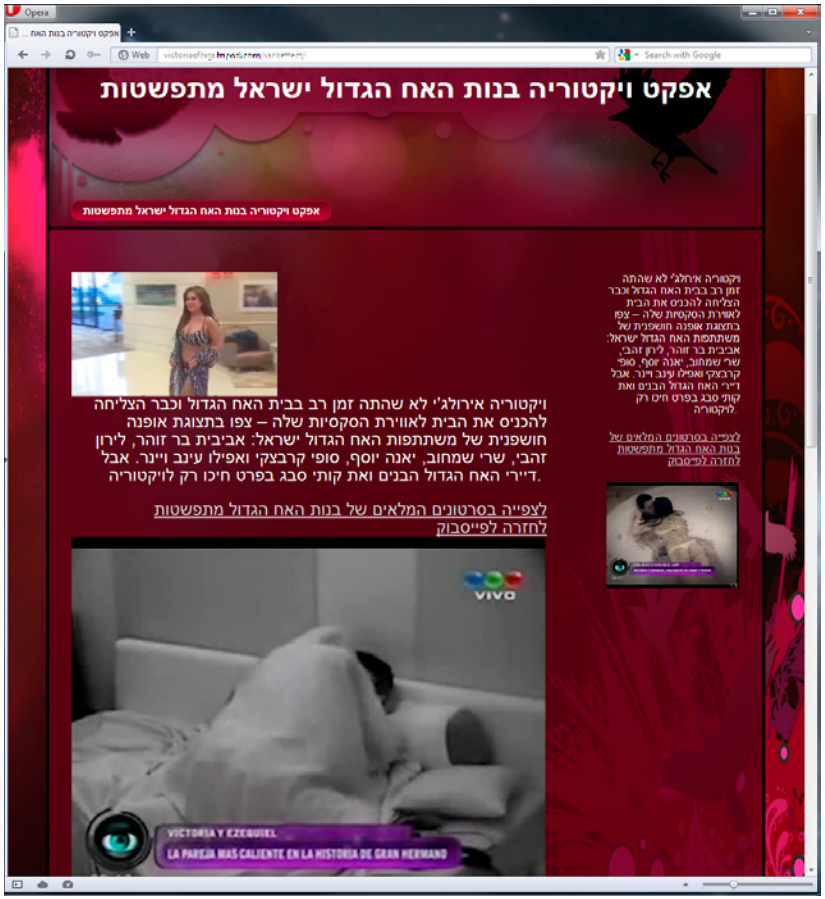
The purpose of this functionality is to direct other Facebook users (i.e. the friends of the users whose logon details have already been stolen) to a fake Facebook log-in site, in order to phish their credentials as well.

The task sent to the bot, apart from a Facebook user name and password, also contains a URL (sent in an encrypted form) and possibly some accompanying text for the post (we haven't observed this feature being used by the botnet, however). The Trojan, having logged in to the Facebook account, publishes the decrypted link on the Facebook user's wall.

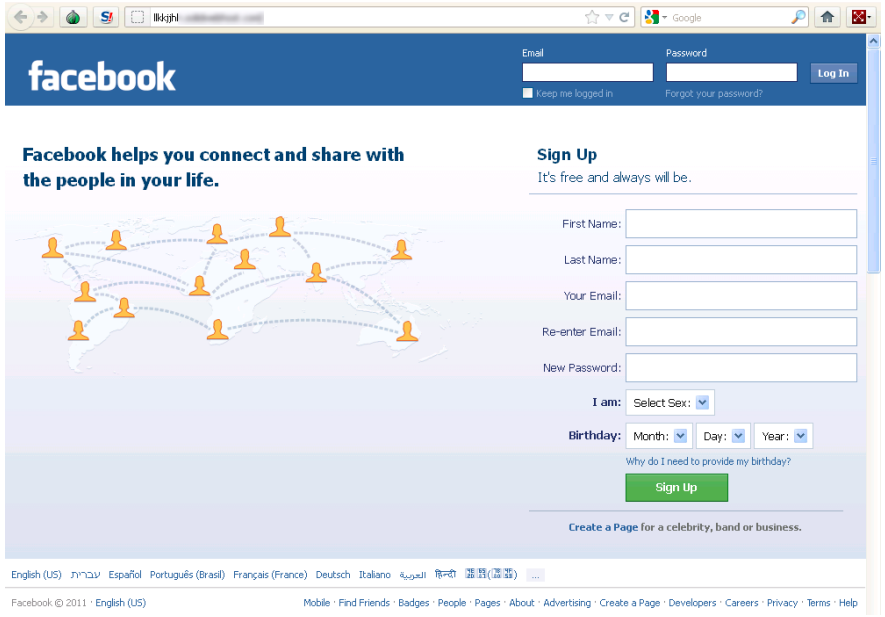
Here are a few examples:



The link would lead to a webpage like the one on the screenshot below. During our botnet monitoring, we have observed different landing pages being used. Both from our telemetry and from the text on these websites we see that the attacks were mainly targeting Israeli Internet users. The pages featured tabloid topics, which a user could be curious to click on.



Regardless of the topic of the "redirect page", they all had one thing in common – every picture or link was an HTML link to a fake Facebook login website as seen below. Again, different URLs were used over time.



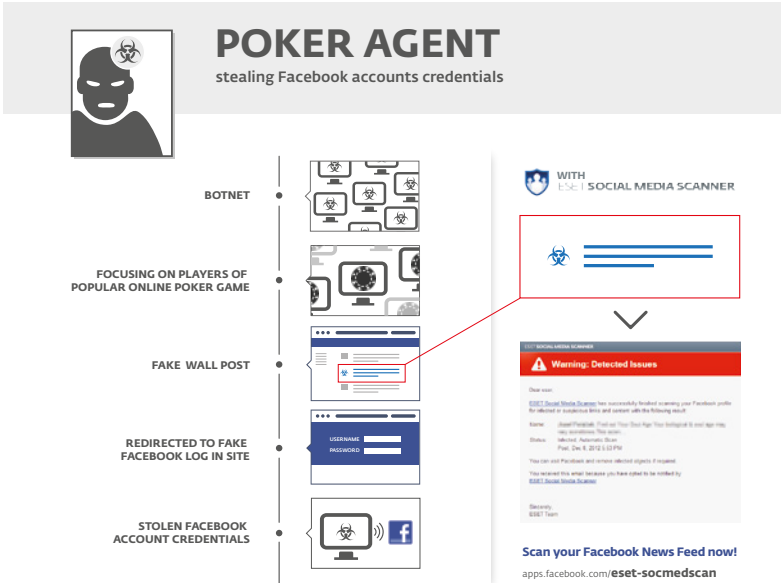
Unsurprisingly, when a victim fills in the log-in form on this counterfeit Facebook page, their credentials are sent to the attacker.

Analysis of the source code also reveals an interesting feature of the Trojan's programming logic. The code contains a function called ShouldPublish, which determines whether the phishing links should be posted to the user's wall. That depends on whether the victim has any credit cards linked to their account and their Zynga Poker ranking. Apparently, if one of these conditions is met, the attacker considers it a success. If not – no payment details and low Poker ranking – the Trojan seeks other victims.

```
private bool ShouldPublish(string finance, string urank)
{
    return this.mLocalTest || (
                                (finance == null || finance.Equals("0")) &&
                                (urank == null || (
                                                    !urank.Equals("5M+")  &&
                                                    !urank.Equals("20M+") &&
                                                    !urank.Equals("1M")   &&
                                                    !urank.Equals("10M+") &&
                                                    !urank.Equals("50M+")
                                                  )));
}
```

Attack Overview

It should be noted that, unlike other Trojans we often see spreading through Facebook, this Trojan does not log into or in any way interfere with the Facebook account of the user that is infected (In fact, they may or may not even have a Facebook account.) The botnet serves rather as a proxy, so that the illegal activities (the tasks given to bots) are not carried out from the perpetrator's computer.



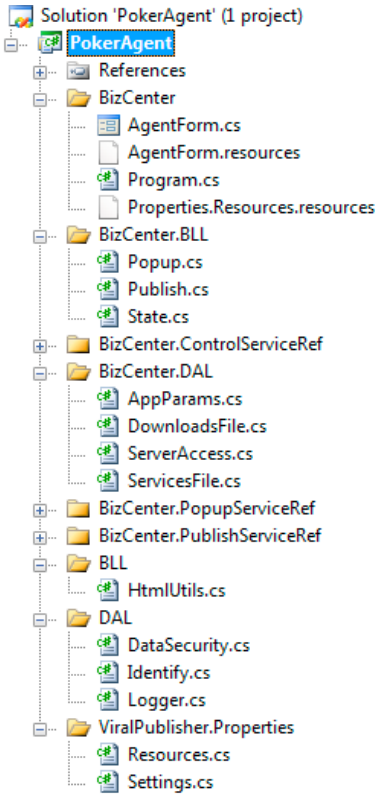
Having said that, the aforementioned facts lead us to the conclusion that the purpose of the botnet is to:

1. **Expand the database** of stolen Facebook usernames and passwords
2. Update the database: **pair the credentials** with information on the user's Zynga Poker stats and their saved credit cards

We can only speculate how the attacker further abuses these harvested data. The code suggests that the attacker seeks out Facebook users who have something of value, worth stealing - determined by the Poker stats and credit card details saved in their Facebook account. Later, the attacker can simply abuse the credit card information themselves or they may sell the database to other criminals.

Additional Technical Details

The analyzed samples were written in C# and could therefore be decompiled into source code that's very close to the code written by the programmer. The PokerAgent application is object-oriented and class-based, and while it isn't particularly advanced or low level coding, the source codes suggest an author with previous programming experience.



In the screenshot of the source files, we can see that the code is quite extensive (The BizCenter.ControlServiceRef, BizCenter.PopupServiceRef and BizCenter.PublishServiceRef folders are collapsed with many more source files inside).
In the following text, we will cover some of the more interesting parts of the code, including the botnet communication mechanism and payload implementation.

Without getting into unnecessary details, the classes where the main Trojan functionality is executed are called *Popup* and *Publish*. *Popup* tasks get a numerical Facebook ID as an input, and return the Zynga Poker stats for that account. *Publish* tasks require a Facebook user name, password and phishing URL to log into the account and check the amount of linked credit cards and to post the phishing links to the victims' Facebook wall.

C&C communication

The communication with the C&C server is implemented through SOAP[1].

The Trojan binary contains two hardcoded arrays of DES-encrypted primary C&C URLs (these varied across different Trojan versions):

- one for downloads – updating to a new version, downloading a new configuration file, etc.
- a second one for commands – executing tasks regarding stolen Facebook credentials

The primary URLs hardcoded in the binary, in fact, only led to the download of the actual C&C URLs. These were seen hosted on different domains. This two-step URL method added extra flexibility to move to different C&C hosts.

The table below shows the commands supported by the C&C.

Class	Command	Note
Control	Connect	Initial message sent by the bot. Identifies itself using the computer's MAC address and bot version. The server assigns the bot a machineID.
	IAmAlive	Second message sent by the bot. The server replies with a list of configuration parameters.
Popup	GetNextPopupTask	The server sends the bot a userID (in his own database of stolen Facebook credentials) and Facebook user ID pair.
	UpdateUser2	The bot sends the server Zynga Poker stats (gender, points and rank) for the current Facebook user.
Publish	GetNextTask	The server sends the bot a userID, Facebook user name, password, encrypted phishing URL and (possibly) accompanying text for Wall post.
	UpdateUser1	The bot sends a report to the server whether or not the current Facebook account has attached payment methods.
	WrongPassword	Send error message – wrong Facebook credentials
	SuccessNotification	Send success message
	ErrorNotification	Send error message

Sample GetNextTask response:

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:xsi="http://www.
    <soap:Body>
        <GetNextTaskResponse xmlns="http://tempuri.org/">
            <GetNextTaskResult>true</GetNextTaskResult>
            <userID>334893</userID>
            <user>[redacted]</user>
            <pass>[redacted]</pass>
            <links>
                <string>MTum2+exoWr+y88FvhSmZR//LGr2NiMKdaIWSYpya3e1nGOLbpHP0g==</string>
                <string />
            </links>
        </GetNextTaskResponse>
    </soap:Body>
</soap:Envelope>
```

[1] In fact, older versions, which we were able to capture during our tracking of this threat, use a different approach by accessing the attacker's database directly. In this text, we only describe the functionality of the most recent version.

Facebook-related functions

The malware writer tried to make the Trojan quite foolproof, which makes sense as he would want to take as much advantage of the stolen Facebook login credentials as possible. The code keeps track of the state for the currently executing task and reports to the server in case an error happens during its execution.

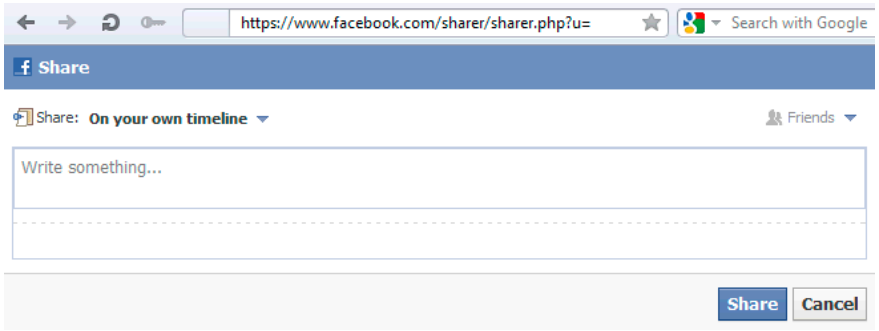
The C# code uses instances of the Browser component to navigate to Facebook webpages as if it was done by the victim himself. The Trojan then parses the HTML, fills in text and simulates clicks as necessary.

When logging into the Facebook account, the Trojan can also handle scenarios such as Facebook warning that the user has logged in from an unknown device. The code excerpt in the following figure shows this functionality.

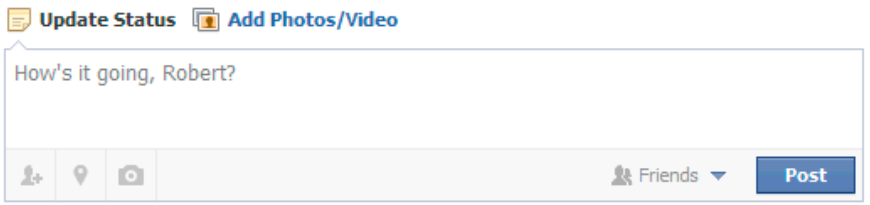
```
Logger.Instance.WriteLine("HandleLogin: " + this.mUser);
if (this.mBrowser.Url.AbsolutePath.Equals("/checkpoint") && "https".Equals(this.mBrowser.Url.Scheme))
{
    HtmlElement htmlElement = HtmlUtils.LookupName(this.mBrowser.Document.GetElementById("content"), "submit[Continue]");
    if (htmlElement == null)
    {

        htmlElement = HtmlUtils.LookupName(this.mBrowser.Document.GetElementById("content"), "submit[This is Okay]");
    }
    if (htmlElement == null)
    {
        htmlElement = HtmlUtils.LookupName(this.mBrowser.Document.GetElementById("content"), "submit[Save Device]");
    }
    if (htmlElement != null)
    {
        HtmlElement elementById = this.mBrowser.Document.GetElementById("machine_name");
        if (elementById != null)
        {
            elementById.RaiseEvent("onclick");
            elementById.InvokeMember("click");
            elementById.SetAttribute("value", "Home");
            elementById.InnerText = "Home";
            this.WriteText(elementById, "Home{ENTER}");
        }
        HtmlElement elementById2 = this.mBrowser.Document.GetElementById("remember_computer");
        if (elementById2 != null)
        {
            elementById2.SetAttribute("value", "0");
        }
        htmlElement.RaiseEvent("onclick");
        htmlElement.InvokeMember("click");
```

For the publishing of the phishing links on victims' Facebook walls, the Trojan utilizes one of the two implemented methods outlined below. Their use is determined by a downloaded configuration file.

The first method for Facebook sharing is by means of http://www.facebook.com/sharer/sharer.php?u=.



The second method is through the Update Status form found at the top of the Facebook News Feed (HTML element with id="pagelet_composer").



Distribution vector

Above, we have shown the fake Facebook login page that the attacker uses to lure their victims into giving them their Facebook credentials.

As far as the distribution of the "PokerAgent" Trojan itself is concerned, we haven't been lucky enough to catch 'in the act' of spreading. At the time when we were monitoring the botnet in March 2012, it was no longer spreading actively. What we do know, however, is that the Trojan is downloaded onto the system by another downloader component (of which we have also seen several versions). This downloader component was seen on the web (on various dynamically changing URLs) and the victims have been fooled into downloading it.

Given the nature and techniques used by the Trojan, it's a fair assumption that the Trojan downloader was also distributed through Facebook, making use of similar social engineering tricks.

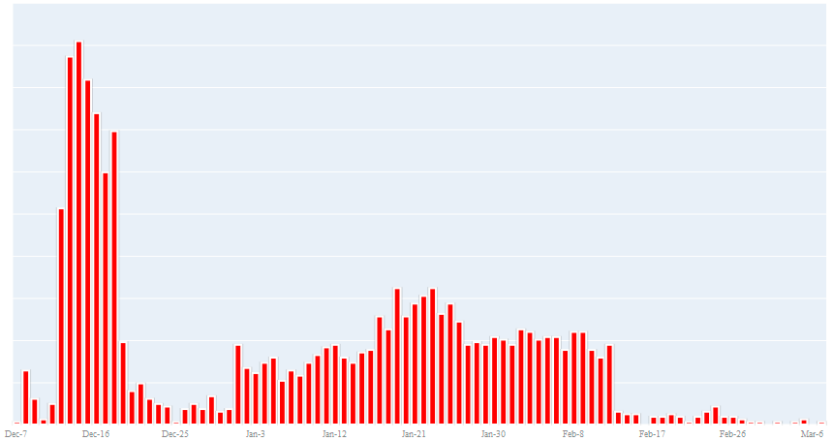
Scale of the attacks and action taken

We have been detecting the Trojan **MSIL/Agent.NKY** since December 3, 2011. Sometime later, we noticed that this was something that deserves more of our attention and conducted an in-depth analysis of the code, started tracking the threat and, after having analyzed its C&C protocol, began monitoring the botnet.

Thanks to our generic detection, we were able to capture both earlier and later versions of the Trojan. We have found 36 different versions of 'PokerAgent' with compilation timestamps from September 2011 to March 2012. MD5 hashes are provided at the end of the document. Thus, we were able to see the malware writer actively developing his project.

Our tracking of the botnet revealed that **at least 800 computers have been infected** with the Trojan and that the **attacker had at least 16194 unique entries in his database of stolen Facebook credentials** by March 20, 2012. Note that this number does necessarily correlate exactly to the number of valid users whose credentials have been stolen, as there could have been more, which we didn't see. However, of those that we did see, not all entries were valid as not all users were tricked by the phishing scheme and have entered details that were obviously fake.

As can be seen from our ESET LiveGrid® detection timeline below, the malware author seemed to have ceased actively spreading the Trojan mid-February 2012.



The attacks are regionally concentrated in only one country. Our telemetry indicates that precisely **99% of all MSIL/Agent.NKY detections** by ESET security products **come from Israel.**

Immediately after we had gathered solid information on these criminal activities, we cooperated with both the Israeli CERT and Israeli law enforcement. The details of the investigation cannot be disclosed for reasons of confidentiality.

Facebook has also been notified and has taken preventive measures to thwart future attacks on the hijacked accounts.

Conclusion

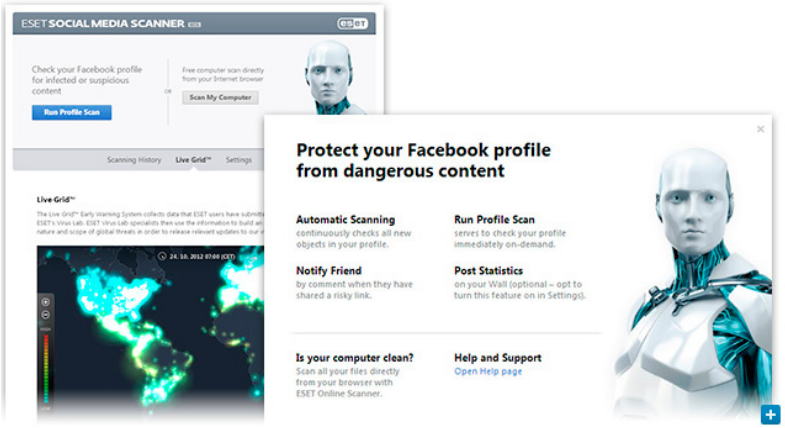
The 'PokerAgent' case represents a successful attack against the users of the largest social network in the world and players of the largest Poker site in the world. There are, however, several security practices – aside from the obvious recommendation to use an updated anti-virus – which would have prevented the perpetrators from being so lucky.

- Not only technical measures, but also user vigilance are important as countermeasures to all attacks that employ social engineering. While visually it's a perfect copy of the real thing, the fake Facebook log-on webpage could easily be recognized as such if the user checked the browser address bar, yet the majority of victims were duped by the phishing scam.

- Facebook has implemented various mechanisms for improving the security of their users. In particular, two-factor authentication would have prevented the infected bots from logging into the victim Facebook accounts.

- We advise careful consideration before allowing a browser or other app to 'remember' passwords for sensitive services and before storing credit card details into any application (not only Facebook!).

- With popular social networks being exploited for malware dissemination, spam, phishing, and other nefarious purposes, it is highly advisable to ensure that you are protected from this attack vector as well. In order to keep your Facebook account clean, ESET has introduced the ESET Social Media Scanner app.



List of MD5s

1A177AD790309F162043557DA2C178B8

2CBE2BA07C5887170FE587C91739F137

82EECB76E4F0EFEA29CE7E790EBFFF99

AEF2313BAAE374CE3AB000AE15046CC5

4988851C88674CE45883141628559C04

4A05B90F662CBC47CC4C826ABEBEBE8F

335864D4E02CEFE9E328043730BA4630

725A34B0F9EE536B63E75913CA17DEC8

538312BDAD9F1EA62D5690E87CABA00F

47AC52B3A13443B061DD293D64142D18

6B51FEF476C48AD121D2543F037CC438

B038A93D36FA9FA82F2C2AD3908F79A9

BB1236655A35D74F43FC1087BA0A6D59

EB4740D54570E847086D863E1FA51C61

1C6689ABD86A1114B50DCF1F809B164D

B1E168DE7E9E495F2C02F73BC0092FE3

C854D298D5A70E89390F55E998682B1A

5E8A0B4EF16B784CA4D78F8036EEC52E

4D3DBFCA81F73F03CE18A848478838CD

4F2BA75830B3470615C9AD66A3B86916

D764E2B23ADDD8156AFE259097713101

10ABB121FF6C6EDC47AEA2263F00DF2E

2E2F62C79F31EFF7A2F4605D6B59455D

82482F49F9E204E48CD68F3A6081162F

911B0EDC23382C8E6BC4684C759FE429

6FF4D77ED54F50EF36348478D71BA490

B29E3ACDF92D665D2B175C60A70C72AC

4E917F6FBB9F4D722018273B0C764B86

F6695F4B63073F059ABD57DFFA397353

5168C1A87AAE174272FD9993B2365ACA

BA15FE1242D471BCB80803A40C30F9EE

3C7485C07D631EB67486A06C9BA6037A

85728B5295F48905E33FF2833AC7A70B

D78ED2A9268068129266F8B28C97C9BA

287E4DEBE7E1F407ADD481ED67897EEC

D21A691EEFBA72113C4B44389A304466