Demystifying the Dark Web
Through Automated Data Monitoring, Collection & Intelligence Production
Who We Are

- Founded 2014
- Headquartered in Israel
- Led by veterans of the Israeli cyber defense and intelligence communities
- 25 Employees

Demystifying the Dark Web Through Automated Data Monitoring, Collection & Intelligence Production
Dark Web Awareness

Demystifying the Dark Web Through Automated Data Monitoring, Collection & Intelligence Production
Today’s Cybersecurity Approach is Incomplete

Spending on Cybersecurity in billions of U.S. dollars

Number of Records Exposed (in millions) by Year

Source: Statista 2018 TIA; 2010 to 2015
Why is this happening?
And why now?
Everyone and Everything is Connected
The Dark Web

Cyber Attack Sources

WORLD WIDE WEB
Only 4% web content available via search engines such as Google

DEEP WEB
96% of web content inaccessible by Google crawlers.

DARK WEB
Anonymous and encrypted network, home base for cybercriminals.
Its Not All Bad...

www.torproject.org
The Dark Web as a Haven for Crime

• “The Tor Network plays a role because it hides criminals. I know it was not the intention, but that’s the outcome....

From the BBC’s *Inside the Dark Web*, 2014
Dark Web Markets Close...
Demystifying the Dark Web Through Automated Data Monitoring, Collection & Intelligence Production

Other Dark Web Markets & Vendor Sites Boom..

July 2017

July 2018
A Crowdsourcing of Bad Guys

Dark Web Research is the Earliest Stage of Attacker Detection, Monitoring and Profiling
Challenge

To bring actionable intelligence in the shortest time when much of its sources reside in the dark web where it is encrypted and anonymous

- Vast amounts of information
- Need to differentiate between data, information and Intelligence
Cyber Intelligence
What we Look For - IOC

**WHEN**
Was the IOC first recognized? When will the attack be launched?

**WHERE**
Is the attacker/s located and where will the attack take place?

**WHAT**
Is the profile of the attacker? What is the extent of his capabilities? What type of attack is planned?

**HOW**
Does the attacker/s typically operate? How will he/they?

**WHY**
Is the attack being planned? What is the objective?

**WHO**
Is the attacker or organization behind the IOC?
Sixgill Approach - Threat Intelligence Model

**SOURCES RECRUITMENT**
Automated and analyst-based identifying for sources

**RAW DATA COLLECTION**
Dark Web: forums, marketplaces, pastebin sites, IRC chatrooms
Deep Web: Telegram
Surface Web: Twitter, Redditt

**CLASSIFICATION & CATEGORIZATION**

**ANALYSIS**
Threat actor analysis
Alert prioritization
Forensics
Threat Actor Analysis

The Dark Web is a Social Network

THE MAPPING OF THE DARK WEB AS A SOCIAL NETWORK ALLOWS FOR THE FASTEST PROVISION OF ACTIONABLE INTELLIGENCE
Mitigating Threats in a Variety of Sectors

Fraud

SCADA/ICS

Aviation

Healthcare

Terror

Hacking Medical Devices - DPA
Kelvinsecurity has had the experience to visit the hospital and dialysis areas to carry out research on "hardware in medicine" to then bring to sale in its new product the FDA in charge of protecting public health to use the hardware that have developed companies to lead a better life and make all the diagnoses quickly.

Demystifying the Dark Web Through Automated Data Monitoring, Collection & Intelligence Production
Thank You!

Come see us at 2205

www.cybersixgill.com
barry@cybersixgill.com

Barry Spielman, VP Marketing
Use Cases/Case Studies
**Canadian Bank X Hack:**

**First Alert:** Nov. - Dec. 17’ (6 months before hack)

**Second Alert:** May 10 ,18’ (2 weeks before hack)

- **2017-2018 Intense chatter about CA Banks**
- **10/5/18 Extreme peak in Bank X CC for sale**
- **26-28/5/18 Bank X receives a ransom note**
MyEtherWallet

- Russian speaking threat actor offered services to redirect traffic to phishing site
- Posted on three dark web markets
- $17.5 million in Ethereum stolen from MyEtherWallet
Sixgill’s CVE Prioritization: Prioritize CVEs by “Severity”:
Chatter on the Darknet + POCs on GitHub

Web Based Miners?

Threat Actor looks for a way to monetize botnet

IC
iCub™ | 4/9/2018, 5:46:00 AM

I have around 3,000 websites rooted including their servers that they are hosted on. What can someone tell me about web-based miners and how they would work for me?

Drupalgeddon2

Threat Actor identifies the POC and look to exploit it

IC
iCub™ | 4/18/2018, 12:31:00 PM

Anyone had any luck using the Drupalgeddon2 PoC that was recently released?

CVE-2018-7600 Detail

Current Description

Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and

Proof-Of-Concept for CVE-2018-7600

Base Score: 9.8 CRITICAL
Impact Score: 5.9
Exploitability Score: 3.9

Pretty serious exploit and I'm sure it could be fun to use, but I have had no luck.
<table>
<thead>
<tr>
<th>SITE</th>
<th>DATE</th>
<th>CREATOR</th>
<th>TITLE</th>
<th>CONTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>forum_alphabay</td>
<td>2015-05-13T02:00:00</td>
<td>maestrolive</td>
<td>Important Job</td>
<td>PM me quickly if the following means anything to you: 845237 Server IP, blocking code, operation common code and password/ID available. Need some assistance with an important matter. Contact me only if you know what I am talking about!</td>
</tr>
</tbody>
</table>
Understanding the Threat Actor Maestrolive
Examples of Stolen Information
Example of FULLZ – Full Financial Info
Recent Examples on ISIS on Telegram

A pro-ISIS Telegram channel reports on a UAV attack on a Popular Mobilization Forces [PMF] position in Salah al-Din Province in Iraq.
Recent Examples on Telegram

Dissemination of UAV and Aerial Technology

Some of the top pro-ISIS telegram channels are dedicated to sharing military-related knowledge – including physical training, weapons manufacturing and using tutorials, technology-related material, etc. – with the aim of ISIS supporters around the world will carry out attacks. The military-related material also include instructions to build UAVs and other kinds of aircraft.

https://youtu.be/skevis1gPM

https://youtu.be/lvE1rY7v

http://formech.com/product/686
Sixgill Broke Stories in Press about Telegram-Based ISIS Threats

**Prince George in the UK**

**PRO-ISIS TELEGRAM CHANNEL INCITES TO KILL PRINCE GEORGE IN HIS SCHOOL**

On October 13th, a pro-ISIS Telegram channel, which incites ISIS sympathizers on a regular basis to commit terror attacks against Western targets and provide instructions and tutorials, posted a picture of Prince George, the son of Prince William, along with the school address and the caption:

"Even the royal family will not be left alone... School starts early."

1. The words written on the ISIS figures in the picture are taken from ISIS’s Islamic-inspired songs, and means: “When war comes, the melody of bullets, we demand on others’ bearing regulation.

---

**The Telegraph**

News

**Jihadist who used encrypted app to call for an attack on Prince George has been jailed for life**

[Article Link]

July 19, 2018

Sixgill Broke Stories in Press about Telegram-Based ISIS Threats

• Champions League Finals

• Mondial in Russia

Champions League final
Real Madrid vs Liverpool
TERROR as ISIS promise ‘we WILL be there’

By Henry Hallaway / Published 24th May 2018

Jihadis have warned football fans ‘we will be there’ as they threatened terror attacks while thousands descend on Kiev for the Champions League Final.

Cyber security firm Sixgill – which monitors ISIS activity on the dark web and in encrypted apps – revealed the latest threat in Daily Star Online.

ISIS threatens to behead Ronaldo and Messi at World Cup

IS "러시아 월드컵서 호날두, 메시 참수할 것”

¡Nueva amenaza para el Mundial de Rusia! El grupo terrorista ISIS realizaría ataques con Drones Armados

El grupo terrorista ISIS volvió a su actividad con amenazas fuentes de realizar un atentado durante el Mundial de Rusia.

En esta ocasión utilizaron Telegram para compartir fotos en donde se veían como intentaban a Lionel Messi y Cristiano Ronaldo con el mensaje: “You will not enjoy security until we live in Muslim countries” (No disfrutarás de seguridad hasta que la vivamos en países musulmanes).

ISIS también amenazó a Cristiano Ronaldo con una escuadrilla de drones en la que aparece con un ojo morado a punto de ser atacado por este grupo terrorista.