Blog

# Thamar Reservoir – An Iranian cyber-attack campaign against targets in the Middle East

Posted on June 3, 2015 by ClearSky Research Team

This report reviews an ongoing cyber-attack campaign dating back to mid-2014. Additional sources indicate it may date as far back as 2011. We call this campaign **Thamar Reservoir,** named after one of the targets, Thamar E. Gindin, who exposed new information about the attack and is currently assisting with the investigation.

The campaign includes several different attacks with the aim of taking over the target's computer or gain access to their email account. We estimate that this access is used for espionage or other nation-state interests, and not for monetary gain or hacktivism. In some cases, the victim is not the final target; the attackers use the infected computer, email, or stolen credentials as a platform to further attack their intended target.

The attackers are extremely persistent in their attempts to breach their targets.  These attempts include:

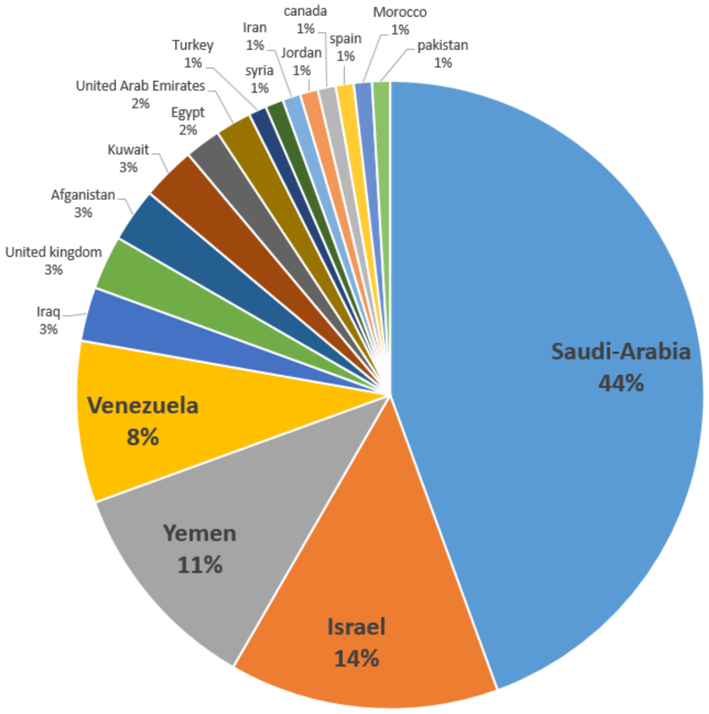
- Breaching trusted websites to set up fake pages
- Multi-stage malware
- Multiple spear phishing emails based on reconnaissance and information gathering.

- Phone calls to the target.
- Messages on social networks.

While very successful in their attacks – the attackers are clearly not technically sophisticated. They are not new to hacking, but do make various mistakes – such as grammatical errors, exposure of attack infrastructure, easy to bypass anti analysis techniques, lack of code obfuscation, and more.

These mistakes enabled us to learn about their infrastructure and methods. More importantly, we have learned of 550 targets, most of them in the Middle East, from various fields: research about diplomacy,  Middle East and Iran, international relations, and other fields; Defense and security; Journalism and human rights; and more.

Below is the target distribution by country (click the image for full size):



Various characteristics of the attacks and their targets bring us to the conclusion that the threat actors are Iranian. In addition, we note that these attacks share characteristics with previously documented activities:

- Attacks conducted using the Gholee malware, which we discovered.
- Attacks reported by Trend Micro in Operation Woolen-Goldfish.
- Attacks conducted by the Ajax Security Team as documented by FireEye.
- Attacks seen during Newscaster as documented by iSight.

Read the full report: Thamar Reservoir – An Iranian cyber-attack campaign against targets in the Middle East

Posted in: Incidents

Search

## Categories

- Campaigns
- cat2
- Crypto
- cyber attack
- Cyber-Crime
- Disinformation
- General
- Incidents
- Threat actors
- Uncategorized

## Archive

- February 2024
- January 2024
- May 2023
- June 2022

- April 2022
- August 2021
- May 2021
- February 2021
- January 2021
- December 2020
- October 2020
- August 2020
- June 2020
- April 2020
- February 2020
- January 2020
- October 2019
- September 2019
- August 2019
- July 2019
- June 2019
- May 2019
- April 2019
- February 2019
- November 2018
- July 2018
- February 2018
- January 2018
- December 2017
- November 2017
- October 2017
- August 2017
- July 2017
- May 2017
- April 2017
- March 2017

- January 2017
- November 2016
- October 2016
- June 2016
- January 2016
- November 2015
- September 2015
- June 2015
- May 2015
- September 2014

## Cyber Solutions

Threat Intelligence

Cyber strategy

Cyber architecture

Pay per report – APT Group research

Cyber Tabletop Exercise

## Contact us

Head office:
HaTa'asiya St 4
Tel Aviv-Yafo
Phone: +972 586 277684
Email: info [at] clearskysec.com

Sitemap xml |