Featured Articles 10.14.15

The Ottoman Hackers? Middle Eastern and Eastern European Exploit Exchange Program

BY NORSE LABS (http://darkmatters.norsecorp.com/author/norse/)

https://norsecorp.com (https://norsecorp.com)

[illegible] Eastern European and Middle Eastern hacking groups looking to [illegible] Threat Intelligence Analysis Team has iden[illegible] located in the Middle East [illegible] ideologically-motivated hacks.

And this trend is not just your average script kiddy begging for N-day exploit proverbial scraps; rather, it's an established pattern of direct and continuous contact between Middle Eastern hackers traveling to Europe to obtain training and experience, then either staying or returning home to begin politically-motivated attacks on global targets.

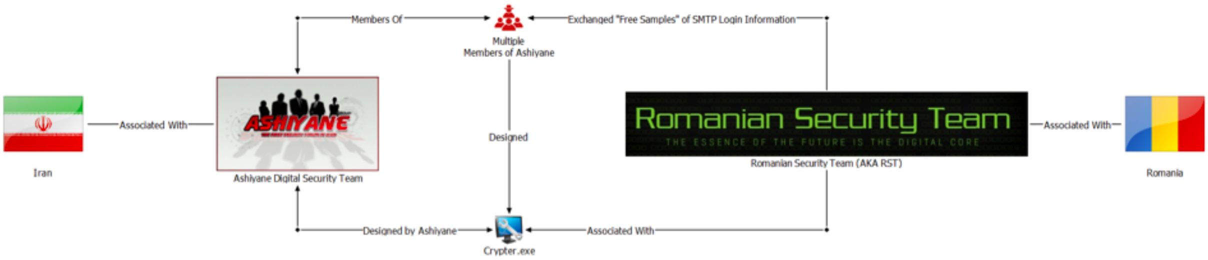
The following cases provide some of the evidence collected by Norse analysts to support this theory*:

CASE 1: ASHIYANE DIGITAL SECURITY TEAM (ADST) AND THE ROMANIAN SECURITY TEAM (RST)

Members of the Ashiyane Digital Security Team (ADST), one of Iran's most notorious hacking groups, and the Romanian Security Team (RST), the largest online hacker community based in Romania, have been exchanging exploit and target data.

A series of posts on the RST forum announced a list of compromised Simple Message Text Protocol (SMTP) systems. Six months later, a large volume of the same compromised systems appeared in a post on the ADST forum from a hacker known to operate in France. Some of the compromised SMTP systems were identified by Norse as used in phishing campaigns as well as other malicious activity.

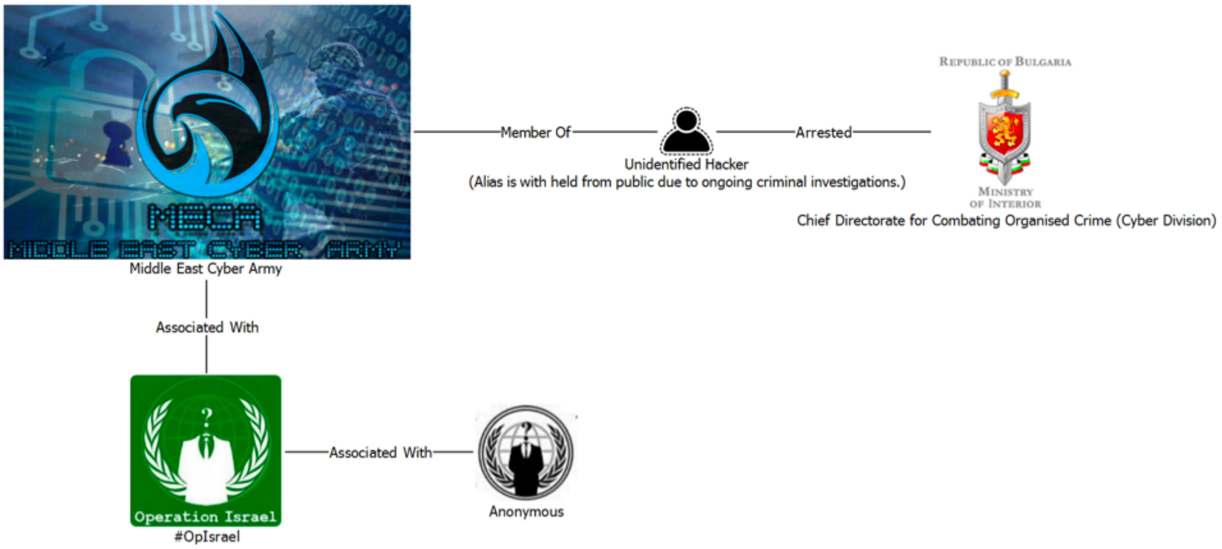
Is this a coincidence, or evidence that supports behind-the-scenes sharing of information between typically unrelated hackers?



(http://2qmqcd3mz3ky1jsgqh2yivq8.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/Romanian-Security-Team.png)

CASE 2: MIDDLE EAST CYBER ARMY (MECA) MEMBER CAUGHT BY BULGARIA'S CHIEF DIRECTORATE FOR COMBATING ORGANIZED CRIME (CDCOC)

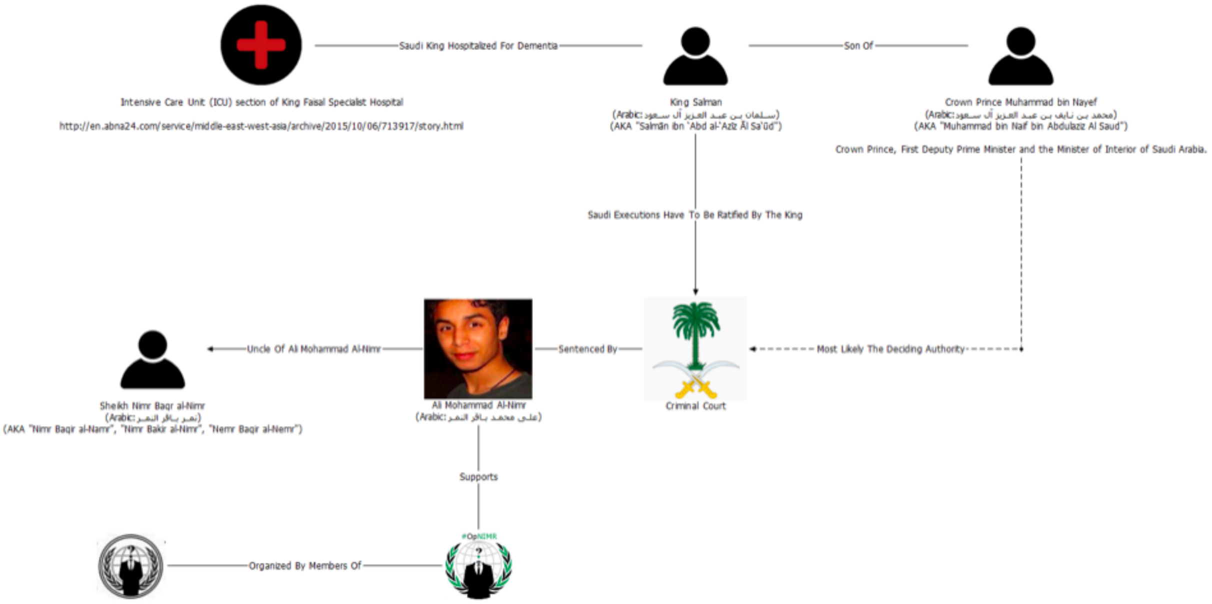
A suspected member of the Middle East Cyber Army (MECA) alleged to have attacked more than 3,500 websites, including government and corporate websites, was brought down by the Bulgarian Chief Directorate for Combating Organized Crime (Cyber Division) on 15JUL2015. The authorities confiscated computer systems, laptops, and external media that contained a wealth of specialized hacking tools. The suspect is believed to be a 21 year old Syrian hacktivist that was studying in Bulgaria while also carrying out ideologically motivated cyber-attacks. The question remains as to who may have been training this person.



(http://2qmqcd3mz3ky1jsgqh2yivq8.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/Middle-East-Cyber-Army.png)

CASE 3: GLOBAL ANONYMOUS MEMBERS ACTIVELY INVOLVED IN POLITICAL/RELIGIOUSLY-MOTIVATED HACKTIVISM

Anonymous has created a hacktivist campaign for the release of Ali Mohammed al-Nimr called #OpNimr. Ali, is a 21-year-old boy sentenced to a beheading then crucifixion by the Saudi Arabian government for acts committed while he was a minor. Ali was arrested in 2012 when he was only 17 for taking part in a protest. According to the anti-death penalty organization reprieve, he was tortured and forced to sign a confession in 2012 and, after two years, he was sentenced to death on May 2014. Anonymous is comprised of a global membership, however a large contingent of active members comes from Europe as well as the Middle East.


Saudi King Hospitalized For Dementia
Intensive Care Unit (ICU) section of King Faisal Specialist Hospital
http://en.abna24.com/service/middle-east-west-asia/archive/2015/10/06/713917/story.html
King Salman
(Arabic: سلمان بن عبد العزيز آل سعود)
(AKA "Salmān ibn 'Abd al-'Azīz Āl Sa'ūd")
Son Of
Crown Prince Muhammad bin Nayef
(Arabic: محمد بن نايف بن عبد العزيز آل سعود)
(AKA "Muhammad bin Naif bin Abdulaziz Al Saud")
Crown Prince, First Deputy Prime Minister and the Minister of Interior of Saudi Arabia.
Saudi Executions Have To Be Ratified By The King
Uncle Of Ali Mohammad Al-Nimr
Sentenced By
Most Likely The Deciding Authority
Sheikh Nimr Baqr al-Nimr
(Arabic: نمر باقر النمر)
(AKA "Nimr Baqir al-Namr", "Nimr Bakir al-Nimr", "Nemr Baqir al-Nemr")
Ali Mohammad Al-Nimr
(Arabic: علي محمد باقر النمر)
Criminal Court
Supports
#OpNIMR
Organized By Members Of

(http://2qmqcd3mz3ky1jsgqh2yivq8.wpengine.netdna-cdn.com/wp-content/uploads/2015/10/global-anonymous-members.png)

Based on current indications, we expect to see continuing increases in skill development and hacktivism from Middle Eastern hackers training in Europe. As their numbers, interests and skills grow, the dangers also increase the likelihood of a natural evolution from Website Defacement and Denial of Service (DoS) activities to truly worrisome Cyber-Terrorism activities capable of destroying infrastructure and putting real lives at risk.

The ever-increasing technical capabilities empowered by Eastern European training combined with the political uncertainties in various parts of the region enables a clear and significant threat to local governments, their allies, and other entities that fall within their crosshairs.

---

* Further detail withheld to protect sources.

SOC Team

YOU MIGHT ALSO LIKE:

THE UPSIDE OF ACCIDENTALLY HIRING A HACKER (HTTP://DARKMATTERS.NORSECORP.COM/2014/09/26/THE-UPSIDE-OF-ACCIDENTALLY-HIRING-A-HACKER/)

REVEALING THE AWESOME TRUTH ABOUT HACKERS (HTTP://DARKMATTERS.NORSECORP.COM/2014/09/18/REVEALING-THE-AWESOME-TRUTH-ABOUT-HACKERS/)

DARKWATCH UNCOVERS THOUSANDS OF PREVIOUSLY UNKNOWN THREATS

DARKWATCH UNCOVERS THOUSANDS OF PREVIOUSLY UNKNOWN THREATS (HTTP://DARKMATTERS.NORSECORP.COM/2014/07/31/DARKWATCH-UNCOVERS-THOUSANDS-OF-PREVIOUSLY-UNKNOWN-THREATS/)

THE NEW REALITY IN SECURITY: OFFENSE ALWAYS WINS AND DEFENSE ALWAYS LOSES (HTTP://DARKMATTERS.NORSECORP.COM/2014/11/10/THE-NEW-REALITY-IN-SECURITY-OFFENSE-ALWAYS-WINS-AND-DEFENSE-ALWAYS-LOSES/)

Norse Labs

▶ MORE POSTS (2) (http://darkmatters.norsecorp.com/author/norse/)

TOPICS: ADST, ALI MOHAMMED AL-NIMR, ASHIYANE DIGITAL SECURITY TEAM, CDCOC, CYBER-ATTACKS, HACKERS, HACKTIVISM, HACKTIVIST, IRAN, MALICIOUS ACTIVITY, MECA, MIDDLE EAST CYBER ARMY, MIDDLE EASTERN HACKERS, NORSE INTELLIGENCE ANALYSIS TEAM, OTTOMAN HACKERS, PHISHING, RST, SIMPLE MESSAGE TEXT PROTOCOL, SMTP, TACTICS, THE ROMANIAN SECURITY TEAM, TTP,