National Cybersecurity and Communications Integration Center

201303270800

Tunisia Cyber Army

Changes/Updates

Version	Change	Section	Analyst
201303130800 – v.1	Original	NA	SPL/CLF
201303131200-v.2	Added Indicators & New Twitter Post	Indicators & New Post	SPL
201303150800-v.3	Redaction	Attack Methodology/Recent Attacks	SPL
201303270800-v.4	Additional Attack Claims & Capabilities	Attack Methodology/Recent Attacks	SPL
201304041500-v.5	New Twitter Posts	Social Media	SPL

Executive Summary

(U//FOUO) Recent attacks targeting the Pentagon, Department of State (STATE), Customs and Border Protection, and the Office of Personnel Management have all been claimed by the Tunisian Cyber Army (TCA) under #OpBlackSummer. This operation, which features input from the Tunisian Cyber Army as well as an Al-Qaeda related persona, is slated to start on 31 May 2013 and last until 11 September 2013. The attacks currently taking place against U.S. entities are likely in efforts to attain the data that will supposedly be leaked from May to September.

(U//FOUO) This product is a brief roll-up of activity related to the TCA.

Attack Methodology

(U//FOUO) The Tunisian Cyber Army's modus operandi seems to be SQL Injection and cross-site scripting (XSS) exploits. However, regional activity and access could allow the TCA and affiliates to grow their cyber capabilities. According to Zone-H, the TCA only has a few hundred documented defacements, but possible individual members, such as Tn_Scorpion have over 21,000 website defacements including 2,284 single IP defacements and 19,172 mass defacements.[1] This could suggest that he (and other TCA members) have exploited vulnerabilities within ccTLD's in the past, which is a common occurrence with other regional actors.

Recent Attacks using SQL Injection and XSS Vulnerabilities:

- In the past 60 days TCA has used SQL or XSS vulnerability to target entities including, but not limited to:
  - 6 separate US government entities
  - 6 different US financial establishments
  - 2 US telecommunications companies
  - 1 transportation/service company

Additional Attacks:

- 2 Feb 2013 – TCA actors found SQL Injection vulnerability on the British Chamber of Commerce for Luxembourg website and successfully defaced the main page. They also harvested and dumped account data on Pastebin under the #OpMali operation.[2] The leaked data posted included usernames, addresses, phone numbers, emails and plain text passwords from the chamber of commerce and other major British financial giants like Barclays bank and ATC Group.
- 2 Feb 2013 – TCA claimed to have compromised a number of French websites belonging to the Ministry of Sport and Jeunesse (drdjs-basse-normandie.jeunesse-sports.gouv.fr)[3]. They followed the exact same TTP as with the British Chamber of Commerce website and leaked account information such as usernames and passwords onto Pastebin.[4]
- 30 January 2013 – TCA uses SQL Injection vulnerabilities within the French Chamber of Commerce website (www[.]cci[.]fr) to deface their website.[5]

(U//FOUO) The majority of the attacks announced in the past month against USG agencies and US financial sector targets have not been successful. The only "success" has been their compromise of Kemteck, which is a web hosting and social media company that specializes in real estate marketing in Minnesota. TCA claimed to have "hacked" Central Bank in Minnesota, but the leaked data suggests that it was actually obtained through Kemteck. The date of this leak was 11 February 2013.

Capabilities:

(U//FOUO) As noted above, their capabilities are limited and seem to revolve around the use of XXS and SQL attacks to retrieve sensitive information. These actions have been demonstrated in the past by posting the information onto forums such as Pastebin. It is possible as their notoriety begins to grow that they could receive resources from other like-minded actors.

Affiliations

(U//FOUO) Recent tweets, claims, and operational focuses have indicated that the TCA is being influenced and/or assisted by other nefarious actor sets. For example, the two most recent attacks targeting the Pentagon and STATE involved the Al-Qaeda Electronic Cyber Army. There appears to be no open source history of this particular sub-set of Al-Qaeda. There is very little evidence to show that the Al-Qaeda Hacker Team has been active prior to the past 60 days or so.

(U//FOUO) On Friday, 8 March 2013, the TCA posted the following tweets pertaining to #OpBlackSummer:[6]

- We and al qaida anonce that #opblacksummer will start on 31may and will end on the 11 of september with a gift to the usa on the virtual and the real life.
- They also tweeted about collaborating with Al-Qaida to leak 4430 logins (NFI).

(U//FOUO) **NCCIC Comment**: *It is possible that the 4,430 logins they are claiming to have may be from a 4 February 2013 incident, during which Anonymous leaked account data for approximately 4,000 US bank executives.[7] Cyber actors reposting or, in this case, re-leaking already leaked information and claiming it as their work is not uncommon. They claim the actions of others for themselves often in order to develop a reputation and gain credibility.*

(U//FOUO) After the attempts against STATE's website and the possible attack on Pentagon websites, TCA members stated that they were also collaborating with unspecified Chinese actors in order to target a number of identified vulnerabilities within USG entities.[8] While it is possible that Chinese actors are influencing the TCA in one fashion or another, collaboration is unlikely. Historically, Chinese threat

actors have been more interested in cyber espionage, rather than website defacements and data leakage for embarrassment or to propagate additional campaigns.

(U//FOUO) **NCCIC Comment**: *TCA's claims that Chinese actors are assisting them in the targeting of USG entities could be due to the attention being given to the recently released Mandiant Report. TCA actors may be looking to leverage fear and misattribution while developing credibility and notoriety.*

Social Media

(U//FOUO) Recent Twitter posts from the TCA also indicate that they are going to start potentially targeting the Energy sector as per the direction of AQCEA leadership.

10. 4 hrs TunisianCyberArmy1 @TN_cyberarmy

New #decision from the leader of #AQECA : we know that the us is interested about necluer pow so we know what we will target now...

Expand

17. 11 hrs TunisianCyberArmy1 @TN_cyberarmy

@redsky2727 we actualy do it and now we will let our bro in china play there will be an artical tommorow we target largest petrocompanie

View conversation

TunisianCyberArmy1 @TN_cyberarmy 24 hrs

@RT_com @BBCBreaking #BinGo we and #Electronic-Al-QAEDA got access to one of the most largest american gaz companies #opBlackSummer

Expand

TunisianCyberArmy1 @TN_cyberarmy 24 hrs

#BinGo one of the largest companies on #USA is #Under attack by #TCA & #AQECA #then #chinise hackers will act @EHackerNews @zataz @HackRead

Expand

#prince of #AlQaeda message to first national bank in [redacted]:close your banking service for one week or we will do it #opBlackSummer

– TunisianCyberArmy1(@TN_cyberarmy) March 30, 2013

(U//FOUO) **NCCIC Comment**: *The most recent Twitter post is in Arabic, but roughly translates to the following: "Muslim brothers, please remove your money from [US] banks in Washington, Seattle, and NY [New York] before tomorrow. Friday will be horrible attacks."*

Al-Qaeda Hacker Team/Al-Qaeda Electronic Cyber Army:
(U//FOUO) Neither the Al-Qaeda Electronic Cyber Army nor the Al-Qaeda Hacker Team have much of history and according to Zone-H, the only registered website defacement is the recent targeting of the Wanatah, IN website noted below. That incident is credited to the Al-Qaeda Hacker Team. There are no indications of capabilities on heavily-trafficked exploit download sides (exploit-db.com, etc). The possible Pentagon defacement (noted above) in conjunction with the Tunisian Cyber Army is the first notable incident involving the Al-Qaeda Electronic Cyber Army. It is still unknown if they are one-in-the-same.

Recent Attacks:

- 1 March 2013 – Al-Qaeda Hacker Team in conjunction with an actor using the online moniker "TKL" defaced the Indiana website www[.]wanatah-in[.]gov, which is the Wanatah, Indiana town website.[9]
- 2 March 2013 – The same actors defaced Washington State Community College website. This website has been taken off-line until the vulnerability can be fixed.[10]

Both defacements used the same imagery:

(U//FOUO) **NCCIC Comment**: *It is possible that these defacements are being used in recruiting efforts for the Al-Qaeda Electronic Cyber Army/Al-Qaeda Hacker Team.*

(U//FOUO) TKL has been identified as a member of the Gaza Hacker Team and according to Zone-H has 228 website defacements including 201 mass defacements. Most targets appear to be IP's located in the US, Germany, and Canada. However, the Gaza Hacker Team has over 1,800 website defacements almost exclusively targeting IP's located in Israel IP space. They have a number of social media sites such as Facebook and YouTube. The Gaza Hacker Team also hosts SQL Injection vulnerability exploits on www[.]exploitsdownload[.]com. This site also hosts a number of other exploits authored and hosted by regional actors such as the Emperor Team.[11]

Summary

(U//FOUO) The recent activity surrounding the Tunisian Cyber Army suggests that there is a desire to join forces with other regional actors targeting USG interests and agencies. Furthermore, as they continue to develop relationships with actor sets possessing more potent capabilities, the Tunisian Cyber Army

could increase the frequency and impact of campaigns against US entities. At the moment, they are making a lot of claims and seem to be aggressively working to increase their notoriety and credibility. Because they are such a new actor set, we are not fully aware of their intent, motivations or beliefs. As a greater understanding is developed, future products and information will be assessed and distributed for situational awareness. The NCCIC will continue to monitor for activity related to the Tunisian Cyber Army and their affiliates.

Indicators

IP Address	IP Location
41.228.53.74	Tunet, Tunisia
41.224.0.0 - 41.231.255.255	Tunisia
Attack Vector	
Havij Scanning Tool	

References

[1] www.zone-h.org
[2] http://www.thehackerspost.com/2013/02/british-chamber-of-commerce-luxembourg.html
[3] http://www.ehackingnews.com/2013/02/tunisian-cyber-army-cyber-attack.html
[4] pastebin.com/wSEfbSd9
[5] http://rewired-security.com/2013/01/30/network-of-chamber-of-commerce-www-cci-fr-has-been-hacked-by-tunisian-cyber-army-tn_cyberarmy/
[6] Twitter / *TN_cyberarmy: Al Qaida* electronic *cyber army* ...
[7] http://gizmodo.com/5981396/anonymous-leaked-account-data-for-4000-bank-executives-on-a-government-website
[8] http://hackread.com/tunisian-cyber-army-founds-xss-vulnerability-on-pentagon-website
[9] http://www.thehackerspost.com/2013/03/town-of-wanatah-indiana-usa-site-hacked.html
[10] http://www.hackersnewsbulletin.com/2013/03/wscc-website-hacked-by-al-qaeda-hacker.html
[11] zionops.wordpress.com