Hacking for ISIS:
The Emergent Cyber Threat Landscape

By Laith Alkhouri, Alex Kassirer, & Allison Nixon
Introduction

As the Islamic State (ISIS) has grown over the past two years, so too has its media machine, global support, and online channels. This unprecedented expansion has now come to include capabilities to inflict damage over the Internet, which came to light when its supporters began coordinating and organizing cyber attacks on Western targets. Highlighting this newfound desire to cause virtual harm was the brief 2014 takeover of Twitter accounts run by US CENTCOM and Newsweek.

In the wake of the aforementioned Twitter takeover, which was claimed by an ISIS-supportive hacking collective called the “Cyber Caliphate,” two implications that would prove to further change an already evolving jihadi landscape unfolded. Firstly, the hacking attacks launched in support of ISIS generated global attention and afforded ISIS increased publicity. Secondly, like-minded individuals and groups found new ways to target Western interests. As such, new concerns regarding ISIS’s cyber capabilities emerged.

At the center of the conversation has been whether ISIS’s cyber prowess is a real threat or exaggerated. Given the attacks that resulted in the CENTCOM and Newsweek Twitter accounts being compromised, it appears that ISIS’s supporters maintain somewhat of an existing coordinated cyber campaign that aims at launching attacks on targets of opportunity, typically those that are considered low-hanging fruit. Nonetheless, the group’s overall capabilities are neither advanced nor do they demonstrate sophisticated targeting; however, the severity of cyber attacks supporting ISIS will likely not remain at this level of relative unsophistication.

For the vast majority of its existence, the pro-ISIS hacking landscape was composed of at least five distinct groups that launched campaigns in support of the terror group. Although operating under different appellations for nearly a year and a half, there was evidence that these groups, and the individuals who constitute them, overlapped or coordinated with one another in certain campaigns, pooling their resources and manpower. This culminated in the April 4, 2016, announcement of a “United Cyber Caliphate” following the formal merger of several groups. However, as these groups have operated as individual entities for the majority of their existence, this paper will reflect that history, first exploring the most prominent actors on an individual basis, followed by a look into the nascent “United Cyber Caliphate” collective.

Regarding this coordination, however, it is important to note that because the pro-ISIS hacking effort is still an unofficial endeavor, neither acknowledged nor claimed by ISIS itself, it is still poorly organized (and likely under-resourced), which often leads to conflicting messaging among the relevant actors. This inconsistency is best illustrated by the way these groups identify themselves in claims of credit, a trend that this paper will explore in more detail.
Spearheaded by a Lone ISIS Fighter

Efforts to launch, grow, and improve the “Cyber Caliphate” brand, and thus the ISIS community’s cyber reputation, were led by a British actor named Junaid Hussain (a.k.a. Abu Hussain Al Britani). Formerly “TriCk” of TeamPisson fame, Hussain fled the UK to join ISIS in 2013, after serving a prison sentence for hacking Tony Blair. Armed with the technical knowledge and relevant experience, Hussain utilized his position as a member of ISIS to recruit hackers and cultivate his “Cyber Caliphate,” all while on the ground in ISIS’s self-proclaimed capital, Raqqa.

Despite his background, the hacking collective supporting ISIS under Hussain’s direction—until he was killed in an August 2015 drone strike in Raqqa—was still unsophisticated and less productive than what might be expected of an effort led by a former Western hacking group leader. This is in part due to Hussain’s inability to provide the ISIS cyber community with a network of other hackers; Hussain’s prior contacts largely were unsympathetic to his increasingly radical ideology, leading to the dissolution of his “hacking rolodex.”

Obtaining Sensitive Documents

The data provided by the hackers on the potential compromise of a Fusion Center demonstrate that the actors had access to some number of “UNCLASSIFIED/FOR OFFICIAL USE ONLY” and “LAW ENFORCEMENT SENSITIVE” products as recently as November 26, 2014. It is possible that this data was stolen from associated email addresses receiving law enforcement bulletins.

Data thus far provided, however, is not sufficient enough to establish the full compromise of the Fusion Center.

Nonetheless, this group demonstrated at least a basic level of credibility and capability, proving to have the capacity to launch follow-on attacks against the same or similar organizations weeks after the original compromise.

Post-Junaid Hussain

Although Junaid Hussain was targeted and killed in an August 2015 drone strike, temporarily slowing ISIS supportive hacking activities, the group’s notoriety is something future jihadists will likely capitalize on to launch further cyber attacks.

Proving this desire to carry on without its former leader, it is now evident that the group replaced Hussain with British-educated businessman and computer expert, Siful Haque Sujan, a 31-year-old Bangladeshi whose role was brought to light after he too was targeted and killed in an American drone strike in Raqqa, Syria, on December 10, 2015.

Hussain’s Legacy Continues

Further exemplifying Hussain’s legacy is his wife, Sally Jones (aka Umm Hussain Britaniya). Attempting to carry on her late husband’s mission, she maintains a prolific and violent social media presence; for instance, she released, “the address & details of US Military target no.2 also one of America’s most decorated soldiers,” Sgt. 1st Class Dillard Johnson on October 8, 2015. Making very clear why she released the information, Britaniya proclaimed, “Once again I leave these details online to cause havoc in his life & for my brothers and Al-Qaeda in the U.S to eventually hunt him down & kill him.”

Cyber Caliphate (Caliphate Cyber Army CCA)

The first of the pro-ISIS hacking groups emerged after ISIS declared its Caliphate in the summer of 2014. In addition to the aforementioned hijacking of Newsweek and CENTCOM’s Twitter accounts, the group identifying itself as the “Cyber Caliphate” claimed credit for a string of attacks that generated global publicity. On January 6, 2015, for instance, the group launched cyber attacks on a number of US targets, including the city of Albuquerque, New Mexico; the Facebook and Twitter profiles for the Albuquerque Journal; WBQC News (which serves the Delmarva Peninsula in Delaware, Maryland, and Virginia); and a Fusion Center in Tennessee, although that allegation was not fully substantiated.
Hussain’s Legacy Continues

Further exemplifying Hussain’s legacy is his wife, Sally Jones (aka Umm Hussain Britaniya). Attempting to carry on her late husband’s mission, she maintains a prolific and violent social media presence; for instance, she released, “the address & details of US Military target no.2 also one of America’s most decorated soldiers,” Sgt. 1st Class Dillard Johnson on October 8, 2015. Making very clear why she released the information, Britaniya proclaimed, “Once again I leave these details online to cause havoc in his life & for my brothers and Al-Qaeda in the U.S to eventually hunt him down & kill him.”
The August 11 dump included the names, departments/divisions, emails, passwords, locations, and phone numbers of nearly 1,500 military and government personnel, including individuals from the Air Force, various foreign embassies, the Marines, NASA, USAID, and the NY Port Authority. The hack also included the credit card information of several State Department officials, as well as screenshots of private Facebook messages between US servicemen.

Ferizi, who is believed to be the leader of hacking collective "Kosova Hacker’s Security," hacked a target located in the US and subsequently stole thousands of individuals’ personal information. He then allegedly provided the information of more than 1,000 American government personnel to Junaid Hussain, representing ISIS, for public release. Hussain subsequently branded it an Islamic State Hacking Division (ISHD) dump on August 11.

Alongside the data dump, Hussain proclaimed, "O Crusaders, as you continue your aggression towards the Islamic State and your bombing campaign against the Muslims, know that we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands! So wait; we too are waiting." The message also specified the target as the "United States Government and Military – The Head of the Crusader Coalition."

On October 15, 2015, federal prosecutors unsealed a criminal complaint charging Kosovo citizen Ardit Ferizi, aka "Th3Dir3ctorY," with providing material support to ISIS and committing “computer hacking and identity theft violations in conjunction with the theft and release of personally identifiable information (PII) of US service members and federal employees.”

Although the Islamic State Hacking Division (ISHD) claimed responsibility for the August 11 dump, maintaining that they had hacked into sensitive databases. Flashpoint analysts believe the information came from unclassified systems and that no military servers were in fact compromised. The same is likely true of ISHD’s other claimed attacks, including the alleged “hack” of several military servers in Italy on June 1, 2015, after which the group leaked the purported personal information of 10 Italian army officers.

The still nascent and unofficial nature of the ISIS cyber landscape has created inconsistent, and often conflicting, messaging. One of the primary examples of this is the Islamic State Hacking Division’s self-identification. Since it first emerged as “the Islamic State Hacking Division,” subsequent hacks supporting ISIS have identified a contributing actor with the different name, “the Islamic State Hack Division.” Although only a slight discrepancy, the title is nonetheless different and, without self-generated actor profiles, it is difficult to ascertain whether ISHD evolved into this new title since Junaid Hussain’s death, or if it is a completely different collective. So is the case with the former Cyber Caliphate, which assumed the title “Caliphate Cyber Army” following Hussain’s death. Nonetheless, without an official statement from the group, it is unclear whether the same individuals involved in Hussain’s former collective rebranded themselves, or if an entirely different group of actors assumed the group’s identity.

The Islamic State Hacking Division (ISHD) emerged in early 2015 and appears to be inspired by, and loosely affiliated with, the Cyber Caliphate. Both are linked by the common thread of Junaid Hussain’s leadership.
Inconsistent Branding

The still nascent and unofficial nature of the ISIS cyber landscape has created inconsistent, and often conflicting, messaging. One of the primary examples of this is the Islamic State Hacking Division’s self-identification. Since it first emerged as “the Islamic State Hacking Division,” subsequent hacks supporting ISIS have identified a contributing actor with the different name, “the Islamic State Hack Division.” Although only a slight discrepancy, the title is nonetheless different and, without self-generated actor profiles, it is difficult to ascertain whether ISHD evolved into this new title since Junaid Hussain’s death, or if it is a completely different collective. So is the case with the former Cyber Caliphate, which assumed the title “Caliphate Cyber Army” following Hussain’s death. Nonetheless, without an official statement from the group, it is unclear whether the same individuals involved in Hussain’s former collective rebranded themselves, or if an entirely different group of actors assumed the group’s identity.
Targeting “Crusaders”

The statement urged “all supporters hackers to join us and work with us to target Crusader alliance electronically,” adding, “hurry up to support your ISLAMIC STATE.”

Discussing its targeting, the group stated, “we also announce for RAID soon targets the Crusader coalition forces electronically, targeting everything…ranging from accounts of recruited, to their banks and their airports. To their nuclear bases.”

Directing a message to “the infidels America and their alliance, [we] will not forget your crimes and your war on Islam, and we will not let you forget our war on you and the blessed Battle of 11 September and the hit of Sheikh-ul-Mujahideen Osama that blow you.”

Focus on the US

In a final threat, ICA declared, “O disbelievers Your Fate will be killing, homelessness and misery know that…this [is] only the beginning and [we] will slaughter your necks over your land soon.” The statement concluded by quoting Osama Bin Laden: “America will not enjoy security and safety until we live it…”

Islamic Cyber Army

On September 10, 2015, the self-proclaimed “Islamic Cyber Army” (ICA) hacking group tweeted its first official statement proclaiming, “the hackers Supporters of the Mujahideen configure under the banner of unification in the name of Islamic Cypher [sic] Army to be …[the] working front against the Americans and their followers to support the ISLAMIC STATE Caliphate with all their forces in the field of e-jihad.”

Further exemplifying the US as its focus, ICA was most active in the days preceding, and including, the 14th anniversary of the September 11 attacks. On September 8, 2015, for instance, the group issued a countdown proclaiming, “Two days and 24 hours left,” with the hashtags #IslamicCyberArmy and #AmericaUnderAttack.

Under the same #AmericaUnderAttack campaign, on the eve of the 9/11 anniversary, ICA also claimed credit for hacking the data of White House personnel,” stating, “[We’re] in your home Obama.” The supposed data leak included the alleged names and contact information of a list of US legislative personnel.

The #AmericaUnderAttack campaign also consisted of a list containing “300 FBI Agents emails hacked.” However, as purported FBI emails/passwords are a staple of low-level hacker dumps, Flashpoint analysts cross-checked the data and found that the list was a duplicate of a LulzSec leak from 2012.

Non-Discriminatory Targeting

Lacking sophistication, ICA resorted to attacking any low-hanging fruit in its anti-American campaign, regardless of target relevance. On September 10, 2015, for instance, the group claimed credit for defacing the website of AmrahBank, an Azerbaijani bank. The defaced page included ISIS’s banner, ICA’s logo, a photo of Osama bin Laden, and the World Trade Center, with the symbolism attempting to tie the attack back to its US focus. The following anti-American statement was included:

“This is a message to the crusaders…WE ARE BACK, We would like to remind you of the holy 911 attack…and will soon be a double…we will not leave you alone until you leave us alone and you will not see peace until we witness it in our Muslim countries, We will appear everywhere and anywhere, you will find us everywhere you go we will hack your details websites pc’s credit cards information and even your cell phones, This is your worst nightmare, it started and it will never end and this is just the beginning, And if you’ve killed Osama R.A its never the end of our Jihad WE ARE ALL OSAMA and will 9/11 you over and over again…We hacked many of your banks, government and military websites, serious and sensitive information and we will publish some, If you wont stop we will publish all data later. FINAL Warning, we define you 7 days notice that if you didn’t stop your War we will post information would threaten the security of your countries…-

ISLAMIC CYBER ARMY.”
“hacking the data of White House personnel,” stating, “[We’re] in your home Obama.” The supposed data leak included the alleged names and contact information of a list of US legislative personnel.

The #AmericaUnderAttack campaign also consisted of a list containing “300 FBI Agents emails hacked.” However, as purported FBI emails/passwords are a staple of low-level hacker dumps, Flashpoint analysts cross-checked the data and found that the list was a duplicate of a LulzSec leak from 2012.

**Non-Discriminatory Targeting**

Lacking sophistication, ICA resorted to attacking any low-hanging fruit in its anti-American campaign, regardless of target relevance. On September 10, 2015, for instance, the group claimed credit for defacing the website of AmrahBank, an Azerbaijani bank. The defaced page included ISIS’s banner, ICA’s logo, a photo of Osama bin Laden, and the World Trade Center, with the symbolism attempting to tie the attack back to its US focus. The following anti-American statement was included:

“This is a message to the crusaders...WE ARE BACK, We would like to remind you of the holy 911 attack...and will soon be a double...we will not leave you alone until you leave us alone and you will not see peace until we witness it in our Muslim countries, We will appear everywhere and anywhere, you will find us everywhere you go we will hack your details websites pc’s credit cards information and even your cell phones, This is your worst nightmare, it started and it will never end and this is just the beginning. And if you've killed Osama R.A its never the end of our Jihad WE ARE ALL OSAMA and will 9/11 you over and over again...We hacked many of your banks, government and military websites, serious and sensitive information and we will publish some, If you wont stop we will publish all data later. FINAL Warning, we define you 7 days notice that if you didn’t stop your War we will post information would threaten the security of your countries...- ISLAMIC CYBER ARMY.”

This claim, as well as others, were released under the hashtag #AmericaUnderHacks.

**Hacking For ISIS**
Laying Foundation as Anti-US Hackers, Reasserting Focus Via Media “Campaign”

On March 31, 2015, the group issued a message indicating that within ten days it would launch an online anti-American terror campaign under the hashtag #WeWillBurnUSAgain. The campaign included the distribution of English-language ISIS propaganda, including videos showing operations against US forces in Iraq, the beheadings of US nationals, as well as messages from Osama bin Laden and other prominent Al-Qaeda leaders to America.

The campaign also included English phrases and threats promising attacks on America to “terrorize its people,” also inviting them to Islam.

Continuing its preparation for what was to come, the group also worked to mobilize ISIS’s online supporters and translators, via designated Twitter accounts.

Personal Information of Americans Distributed

Following its March 31 promise for an anti-US terror campaign, on April 10, 2015, Rabitat Al-Ansar released a statement claiming credit for “pulling the data of 2000 individuals, most of them are Americans.” The group indicated that “Rabitat Al-Ansar Hackers” conducted the purported cyber attack and added, “The data includes their names, the city in which they live, the country they are from, their emails, phone numbers, and home phone numbers.”

The group released a sample dump including 400 of the 2,000 targeted individuals. It also vowed more attacks, proclaiming, “What will come will be worse and more bitter.” The group indicated that the rest of the data, which also included information on Canadian, Norwegian, and Australian citizens, would be released within 24 hours.

It remains unclear whether the group obtained the information by hacking systems or instead was just gathered from open sources. If the group indeed conducted cyber attacks, the provenance of the data is unknown.

“Message to America” Video


The video began with claims of responsibility for previous hacking attacks that purportedly targeted American and Australian websites, including claims of personal information of Americans.
credit made by the “Cyber Caliphate.” Rabitat Al-Ansar’s boasting of a Cyber Caliphate attack further exemplifies the fluidity between pro-ISIS cyber actors, seeing each other’s victories as an extension of their own.

The group added, “We send this message to America and Europe; we are the hackers of the Islamic State, the electronic war has not begun yet. What you have seen before is just a preface for the future. [We] were able until this moment to hack the website of the American leadership and the website of the Australian airport, and many other websites despite paying billions to secure your electronic websites; however, it became easier to hack your websites in a short time. Thus, your security information is in our hands; you do not have the power to fight the Islamic State.”

American Banks as Targets

Further demonstrating coordination among pro-ISIS cyber actors, on September 4, 2015, Rabitat Al-Ansar tweeted a threat saying they, “will penetrate to the banks and US government sites on September 11,” warning “expect us.” The tweet included an image that featured a hooded, faceless individual sitting at a laptop that bears ISIS’ logo. The photo included text that read, “ELITE ISLAMIC STATE HACKERS,” specifically including a hacking collective known as Hacker Aldmar, which is part of Rabitat Al-Ansar.

Furthermore, on July 13, 2015, Rabitat Al Ansar’s subgroup Hacker Aldmar claimed to have obtained “American Visa and MasterCard” accounts, asking followers to use the information “for whatever Allah has made permissible.” It is worth noting, however, that after Flashpoint analysts attempted to verify the actors’ claims, the findings suggested that the allegedly leaked data may have been sourced from the so-called “Scarfaze Hack Store,” at scarfaze[.]com, calling into question the legitimacy of the group’s capabilities.
In its first video release, with less than impressive graphics and production, titled “Flames of Ansar” – or “Flames of Supporters” – SCA claimed credit for hacking more than 15,000 Twitter and Facebook accounts.

The amateurish video began with excerpts featuring security experts that speak about existing vulnerabilities and the rise in ISIS’s cyber capabilities. The video also indicated that SCA took down Twitter’s official website, including media clips reporting that the website was unavailable for two hours. This service interruption allegedly took place on February 4, when Flashpoint analysts noticed that Twitter was experiencing service issues for a short period of time. Flashpoint analysts closely watched SCA’s activities as the initial service interruptions were observed and, although it did not explicitly claim credit, SCA insinuated that it was responsible.

Threat to Twitter and Facebook Founders

The video, which was preceded by a teaser poster featuring images of Twitter and Facebook founders, Jack Dorsey and Mark Zuckerberg engulfed in flames, shows the group’s alleged hacking attacks on various Facebook and Twitter profiles. The group claimed that it hacked and compromised 10,000 Facebook accounts, 150 Facebook groups, and 5,000 Twitter accounts.

Threat Assessment

As Flashpoint analysts believe that this group is affiliated, or synonymous, with what is known as the Caliphate Cyber Army (a.k.a. Cyber Caliphate), the first pro-ISIS hacking collective to emerge, the emergence of SCA as a subgroup further underscores the increasing interest in cyber capabilities among ISIS’ supporters.

The footage ended with a message that read, “To Mark and Jack, founders of Twitter and Facebook, and to their Crusader government, you announce daily that you suspended many of our accounts, and to you we say: is that all you can do? You are not in our league. If you close one account, we will take 10 in return and soon your names will be erased after we delete your sites.”

Social Media Target Emphasis

Further demonstrating the constantly evolving pro-ISIS cyber landscape, a group called Sons Caliphate Army emerged in early January 2016. Even before a later April 4 announcement of a merger with the Caliphate Cyber Army (CCA), SCA appeared to be closely affiliated with CCA, especially as SCA’s establishment was first advertised on CCA’s private Telegram channel. Following that introductory message, CCA and SCA consistently shared each other’s statements and claims of credit on their respective Telegram channels, exemplifying coordination seemingly more structured than that between other groups. This strong relationship between SCA and CCA continued, as they are two of the four groups now constituting the United Cyber Caliphate.
A United Front

The announcement came after CCA claimed via its private Telegram channel that it hijacked a Twitter account, which the group frequently does, to then broadcast a message. After gaining control of the Twitter account, CCA tweeted, “incorporation between Islamic State Hackers Teams #CaliphateCyberArmy #SonsCaliphateArmy #KalashnikovTeam new #Team. #UnitedCyberCaliphate.”

Simultaneously, CCA released a message on its Telegram channel saying, “After relying on Almighty Allah and by his grace, incorporation between Islamic State Hackers Teams...To expand in our operations. To hit ‘em deeper. We announce our new #Team #UnitedCyberCaliphate.”

Shortly thereafter, the newly established “United Cyber Caliphate” launched its own private Telegram channel. The statements were released in English, Arabic, Russian, and French.

Given that SCA’s establishment was first announced on CCA’s Telegram channel and the two groups subsequently shared each other’s material on their respective channels, it is likely the two groups are affiliated. However, this statement is the first explicit announcement of their formal alliance.

Furthermore, there have been other signs of coordination between these groups, and other pro-ISIS collectives, on an individual basis in the past, primarily in the form of claim of credit posters in which multiple groups are mentioned. Nonetheless, this is the first occasion in which online groups supporting ISIS, of which there are several, announced a formal merger and subsequent creation of an umbrella organization.

First Claim of Credit and Expanding Focus

United Cyber Caliphate released its first statement on April 5, claiming credit for defacing the website of Indonesia Embassy in France. The defacement included a picture of a fallen Eiffel Tower as well as a message that said, “Now our fighting has come! We don’t negotiate except with cannon, we don’t have dialogues except with guns, we will not talk except strength. And we will not stop the fighting until we make Athan [call for prayer] and pray in Rome by Allah’s will in a conquest, as a promise from Allah, and Allah does not break his promise.”

The unification of these groups also means that the scope of the united team has expanded. In addition to the focus on hacking attacks launched by groups like CCA and SCA, the growing relevance of other groups like Kalashnikov Team joining UCC demonstrates that the united group is placing an increased emphasis on educating the online jihadi community on encryption and other technology, including VPNs, proxies, and website vulnerabilities.

Evolving but Still Flawed

Because today’s groups that engage in cyber attacks on behalf of ISIS are neither acknowledged nor claimed by ISIS itself, a poorly organized landscape of these actors exists which has often led to conflicting messaging among the many actors. This
The announcement came after CCA claimed via its private Telegram channel that it hijacked a Twitter account, which the group frequently does, to then broadcast a message. After gaining control of the Twitter account, CCA tweeted, “incorporation between Islamic State Hackers Teams #CaliphateCyberArmy #SonsCaliphateArmy #KalashnikovTeam new #Team. #UnitedCyberCaliphate.” Simultaneously, CCA released a message on its Telegram channel saying, “After relying on Almighty Allah and by his grace, incorporation between Islamic State Hackers Teams...To expand in our operations. To hit ‘em deeper. We announce our new #Team #UnitedCyberCaliphate.”

Shortly thereafter, the newly established “United Cyber Caliphate” launched its own Telegram channel.

The statements were released in English, Arabic, Russian, and French.

Given that SCA’s establishment was first announced on CCA’s Telegram channel and the two groups subsequently shared each other’s material on their respective channels, it is likely the two groups are affiliated. However, this statement is the first explicit announcement of their formal alliance.

Furthermore, there have been other signs of coordination between these groups, and other pro-ISIS collectives, on an individual basis in the past, primarily in the form of claim of credit posters in which multiple groups are mentioned. Nonetheless, this is the first occasion in which online groups supporting ISIS, of which there are several, announced a formal merger and subsequent creation of an umbrella organization.

First Claim of Credit and Expanding Focus

United Cyber Caliphate released its first statement on April 5, claiming credit for defacing the website of Indonesia Embassy in France. The defacement included a picture of a fallen Eiffel Tower as well as a message that said, “Now our fighting has come! We don’t negotiate except with cannon, we don’t have dialogues except with guns, we will not talk except strength. And we will not stop the fighting until we make Athan [call for prayer] and pray in Rome by Allah’s will in a conquest, as a promise from Allah, and Allah does not break his promise.”

The unification of these groups also means that the scope of the united team has expanded. In addition to the focus on hacking attacks launched by groups like CCA and SCA, the growing relevance of other groups like Kalashnikov Team joining UCC demonstrates that the united group is placing an increased emphasis on educating the online jihadi community on encryption and other technology, including VPNs, proxies, and website vulnerabilities.

Evolving but Still Flawed

Because today’s groups that engage in cyber attacks on behalf of ISIS are neither acknowledged nor claimed by ISIS itself, a poorly organized landscape of these actors exists which has often led to conflicting messaging among the many actors. This inconsistency is exemplified by the way in which groups identify themselves, often using variations of the same name without explanation, such as the Islamic State Hacking Division, which at times was referred to as the Islamic State Hack Division. Despite this apparent effort to coordinate, such as the creation of United Cyber Caliphate, there continues to be some remaining inconsistency. For instance, in the multiple Telegram and Twitter messages announcing this merger, one of the members was called “Ghost Caliphate Section” as well as simply “Ghost Caliphate.” Another member was referred to as “Kalashnikov Team” as well as “Kalashnikov E-Security Team.”

Despite this lingering inconsistency, the establishment of UCC will likely create a more organized pro-ISIS hacking force. It remains to be seen, however, whether the individual members will continue operating on their own or if the new umbrella group will replace all CCA, SCA, Ghost Caliphate, and Kalashnikov Team specific activities.
Although it is difficult to ascertain what techniques, tactics, and procedures (TTPs) ISIS’s supporters employ, based on the groups’ “successful” cyber attacks thus far, the following is what Flashpoint analysts believe pro-ISIS hackers depend on (but not limited to):

Integration of Technology

Pro-ISIS hackers appear to coordinate their campaigns in private - likely using encrypted communications platforms - before launching a media campaign teasing forthcoming attacks. In many cases, the actors declare their intent to launch a hacking attack on social media, such as Twitter, using hashtags to galvanize support for the intended actions.

Patterns

The timing of attacks can be pegged to certain dates of significance - such as the September 11 anniversary. These dates are highly significant for jihadi hackers, as they guarantee a substantial level of media attention and security frenzy, which helps to drum up support by allowing the actors to capitalize on high social media traffic.

We believe that while private communication between hackers takes place, they rely heavily on social media to generate support for their campaigns. Pro-ISIS hackers continuously utilize Twitter hashtags to garner support from like-minded jihadists. In this way, Twitter is essential in their campaigns.

Tools Assessment

In regards to communication tools, Flashpoint analysts have seen examples of security-savvy jihadists, but not necessarily hackers, using encrypted online platforms for communication, such as Surespot and Telegram.

While it is difficult to ascertain the precise methods of attack used to perpetrate these alleged hacks claimed by pro-ISIS groups, a number of techniques and tools could have been used, assuming these hacks were indeed legitimate.

Assessing these groups’ capabilities requires consideration of whether these actors utilize custom-made hacking tools developed in-house, or whether they are relying on pre-made tools and software that are available in the Deep & Dark Web. These types of tools can be divided into two overall groups: hacking tools used to infiltrate systems externally and malware used to compromise systems from the inside.

Hacking tools are almost invariably going to be taken from publicly available open source projects because of the ease of obtaining such tools along with the fact that they can often be used successfully. Developing proprietary tools would require significant effort and resources to create a completely private toolset that is on par, or better than, what is already available publicly. Of course, actors may modify this publicly available software or writing simple scripts, but it is unlikely these groups are currently building software from the ground up for their supporters to use.
Hacking Tools Vs. Malware

Pro-ISIS cyber actors are likely to download hacking tools from publicly available sources and are likely to utilize both off-the-shelf and custom malware. In underground markets, where malware is commonly sold, hacking tools are not as frequently available because it is widely understood in the black market that paid malicious products cannot compete with the free open source products that already exist.

One example of custom malware being deployed by pro-ISIS elements occurred in late 2014 when a malicious fake slideshow was distributed to Twitter users who were critical of ISIS. The executable was a customized malware, yet was extremely simple in its function. Even though it was not complex or sophisticated, it was enough to identify and geolocate the infected machines and their owners. In other words, pro-ISIS cyber threat actors have a record of distributing malware via social media.

Potential Use of Malware

Malware usage has a different calculus than hacking tools. Malware does not require a significant amount of effort to build another password stealer or remote access trojan (RAT). The sticking point with malware is its detectability with antivirus. Publicly available malware is highly detectable with antivirus products, and obfuscation tools (i.e. crypters) may be able to extend the lifetime of a sample. But to ensure stealth, writing custom malware and maintaining very narrow targeting is the only way to keep it out of the hands of antivirus companies. Even despite these incentives, we still see many nation state actors who continue to use off-the-shelf malware products. Due to the differing barriers to entry of these categories of attack tools, an emerging hacking group will likely use custom malware before it uses custom hacking tools.

Targeting

ISIS cyber threat actors appear to have two primary macro targets - as professed by at least one pro-ISIS hacking collective: “governmental and economic” targets. According to the aforementioned claims of responsibility, financial institutions are among the primary targets for ISIS cyber actors as well.

Given the previous focus of hacking attacks, we assess that ISIS cyber threat actors will continue targeting financial institutions in the future.

Pronounced Targets

To date, ISIS cyber actors have launched attacks on primarily government, banking, and media targets. These entities appear to be not only what these actors are focused on, but also what generates the most publicity for the groups behind them, likely contributing to the focus on such targets.

In addition, ISIS cyber actors have launched a campaign inciting similar attacks on non-American targets, including those in Russia. This development unfolded after Russia began its military engagement in Syria.

There are currently no statistics that could accurately demonstrate the frequency of pro-ISIS cyber attacks on specific targets.

Nevertheless, Flashpoint analysts have observed a noticeable uptick in the emergence of more pro-ISIS hacking groups since the summer of 2014. There is also an apparent increase in the diversification of the desired targets of pro-ISIS hackers, evolving from an overwhelmingly American target list to one that includes British, Italian, and Russian targets, among others.

Call to Cyber Recruits

The example of Junaid Hussain demonstrates that ISIS has been successful in attracting savvy hackers and will likely continue to do so. While we have not seen ISIS explicitly call for sophisticated hackers, Deep Web forums frequented by jihadists include sections containing both beginner and advanced hacking courses, hacking tools and manuals, as well as ways to communicate with like-minded forum dwellers.

Jihadi Hacker Forum

For example, the Gaza Hacker web forum, the primary Jihadi hacking Deep Web forum, is frequented by all types of jihadists, including pro-ISIS types. The forum offers a variety of hacking courses and manuals.

Members of the forum have previously distributed stolen credit card information as well as manuals on hacking tools and methods. This hub offers jihadists a one-stop shop for everything from learning how to hack, how to improve hacking skills, how to obtain certain hacking software, and more.
The Future of ISIS's Cyber Capabilities

As pro-ISIS cyber attacks and capabilities have gradually increased over time but remained relatively unsophisticated, it is likely that in the short run, these actors will continue launching attacks of opportunity. Such attacks include finding and exploiting vulnerabilities in websites owned by, for example, small businesses, and defacing these websites. Other attacks may include DDoS attacks.

Furthermore, advanced targeting and exfiltration are not far-fetched if the group is able to recruit outside experts into its fold, such as the previous examples of Hussain and Ferizi. The advancement of the cyber capabilities of pro-ISIS actors largely depends on the group’s ability to bring in a technological savvy, diverse group of people with broad technical skills. Hussain, who joined ISIS as a somewhat sophisticated hacker, given his time with TeaMp0isoN, is a good example and set the precedent.
Conclusion

In the past year, several pro-ISIS hacking groups emerged, all of them with the intention of launching electronic attacks on the US and other Western targets, including government, economic, and media entities. Indeed, some have been successful, such as the hacking of US CENTCOM’s Twitter account. These initiatives have afforded ISIS a new layer of notoriety and simultaneously raises concerns regarding its cyber capabilities. This is especially unnerving as one of the hacking group’s leaders, Junaid Hussain, fought in ISIS’s ranks and attempted to recruit overseas talent while stationed in Syria, which he accomplished on at least one occasion when he worked with hacker Ardit Ferizi to obtain information on US servicemen.

Despite the significant amount of attention that ISIS supportive hackers are garnering, it is important to note that their skill level is still low. Nonetheless, these actors are demonstrating a desire to carry on legacy efforts, such as Junaid Hussain’s call to ‘lone wolves’ by leveraging targeting information, and also building upon that foundation.

Whereas Hussain provided targeting information by tweeting the addresses of “wanted” individuals, often using the hashtag #GoForth, CCA and SCA have intensified this effort, issuing “dumps” consisting of hundreds of individuals’ alleged personal information. In March 2016 alone, these groups released the alleged information of New Jersey and Minnesota policemen, US National Guardsmen, US Marines, Saudi Royal Guards, among others. Therefore, pro-ISIS cyber actors are demonstrating an upward trajectory, indicating that they will continue to improve and amplify preexisting skills and strategies.

Such a trend was exemplified by the recent merger of multiple pro-ISIS cyber groups under one umbrella: the United Cyber Caliphate. This willingness to adapt and evolve in order to be more effective and garner more support indicates that while these actors are still unsophisticated, their ability to learn, pivot, and reorganize represents a growing threat.
About Flashpoint

Flashpoint helps companies and individuals understand the threats looming in the Deep & Dark Web in order to help mitigate and prevent both cyber and physical attacks.

We provide data, tools, and expertise to security and intelligence teams across the Fortune 500 and government to help them both obtain actionable intelligence, as well as gain critical awareness of threatening actors and their relationships, behaviors, and networks prone to malicious activity.

Contact

web:  [www.flashpoint-intel.com](http://www.flashpoint-intel.com)
Email:  [info@flashpoint-intel.com](mailto:info@flashpoint-intel.com)