AnonGhost Team

The AnonGhost Team is a fluid international network of hackers that targets government, corporate and private websites around the world to bring attention to its extremist-inspired agenda. The network’s ability to consistently attack its targets with pro-terror and anti-Semitic messages places them at the forefront of ideologically motivated cyber-threats.

For several years, the AnonGhost Team's activity has primarily involved defacing websites with anti-western, anti-Israel and anti-Semitic messages. In recent months, the network has been particularly unambiguous about its support for the Islamic State in Iraq and Syria (ISIS), declaring on its Facebook profile, “Long Live ISIS... we support all Mujahideens who defend Islam... we support ISIS 100%!”

The network’s cyber-attacks on behalf of ISIS augment the terrorist organization's broader online propaganda efforts by helping bring its message directly to targets in the U.S.

In addition to cyber-attacks, the network has launched a number of software tools designed to enable users to conduct their own cyber-attacks against their targets of choice. For example, in March 2015, AnonGhost alerted its supporters through its social media profiles about software it created enabling users to initiate denial of service (DOS) attacks.

While the actual number of hackers affiliated with the AnonGhost Team is unclear, the nature of the group's ongoing attacks in the U.S. and elsewhere highlights its own development and underscores broader emerging cyber-threats.
Targeting the U.S.
The AnonGhost Team has launched several cyber-attacks against various
government targets in the U.S., often explaining its actions as acts of resistance
against a long list of alleged violations committed by the U.S. government.

In June 2015, AnonGhost claimed to have defaced a White House website with a
statement that read:

\[
\text{we have witnessed your unjust laws. you have abused human rights, creating}
\begin{align*}
\text{ Wars, Financial Crisis, bombings, arresting innocent people, assassinating,} \\
\text{ using media propaganda to spread your lies, to justify your corrupt act. After} \\
\text{ all, we're aware! you are the real terrorists!} [sic]
\end{align*}
\]

It released a similar message in April 2015, when it announced on YouTube
#OpUSA, one of several campaigns it has launched to target the U.S. The group
first used the #OpUSA moniker in 2013 when it published a list of more than 700
websites it claimed to have defaced.

In the past year, AnonGhost has claimed responsibility for at least four cyber-
attacks on U.S. law enforcement affiliated websites, including the Wayne County
(Indiana) Sheriff’s Department, the Rapides Parish (Louisiana) Police Jury, the
Larimer (Colorado) Sheriff’s Office and the Sheriff’s Office in Piatt County (Illinois).

The Rapides Parish Police Jury site was defaced with the seal of AnonGhost and
the slogan “Death to Israel... Viva Hamas, Qassam.” The Wayne County Sheriff’s
Office was also defaced with the seal of AnonGhost and a message that read “Stop
Killing Muslims” along with a list of several countries worldwide. The vandalized
website also included images of civilian casualties in Gaza and images of
American soldiers abusing Iraqi civilians.

The network has also carried out several cyber-attacks in the U.S. on behalf of
ISIS. In a March 27, 2015, statement posted to the file sharing website Pastebin, a
prominent AnonGhost hacker claimed to have hacked into the Pentagon Federal
Credit Union and leaked personal data [this claim has not been confirmed]. The statement written in English and Arabic read in part, “Long Live ISIS and Death to USA,” “the Islamic State will remain in spite of America” and “Death to America.”

University websites around the country have also been attacked on multiple occasions by AnonGhost. The attacks have often targeted subdomains of university sites, which tend to have vulnerabilities that enable hacks to occur more easily. While these sites may be targets of opportunity, the messages left are similar to the ones AnonGhost leaves on government sites and are part of the network’s effort to spread its messages broadly.

In June 2015, the group claimed on its official Facebook page that it hacked the website of the University of Arizona and shared recordings of what appears to be a defacement of a number of university’s website subdomains. The group posted messages on the defaced websites that denounced Israel and Zionism stating, “Our main target is Zionisme and israhell [sic]”

In November 2014, the group claimed credit for hacking several other university websites in the U.S. with anti-Semitic and pro-terror messaging. The hackers succeeded in redirecting visitors of some of the websites to pages playing a recording of the Quran and featuring a message in English that starts with an anti-Semitic pro-terror statement, “Death to All Jews...Viva Hamas, Qassam.”

That same month, another group of university websites were hacked to direct visitors to a page featuring anti-Israel images and playing a pro-Qassam anti-Semitic song with the lyrics, “Teach the son of the Jewish woman how many times we will conquer him.”

**OpIsrael**

In addition to defacing sites in the U.S. and elsewhere with anti-Israel messages, AnonGhost often engages in cyber-attacks directly targeting Israel and Israelis. Indeed, there are strong indications that AnonGhost replaced Anonymous in
spearheading the 2015 “OpIsrael,” an annual anti-Israel cyber-attack campaign previously led by Anonymous and timed to coincide with Holocaust Remembrance Day.

While anti-Semitic themes existed in previous OpIsrael campaigns, it had been primarily billed as a response to the Israeli-Palestinian conflict. AnonGhost’s tactics in the 2015 campaign highlighted the centrality of anti-Semitism in the campaign.

During OpIsrael, AnonGhost claimed it acquired a large amount of personal information about over 200 Israelis, including phone numbers supposedly associated with WhatsApp as well as Facebook accounts, and made it available to other hackers.

It then directly targeted Israeli individuals by hacking their personal information and sending them anti-Semitic and threatening text messages on their phones and through other texting platforms such as Facebook Chat and WhatsApp messages.

Muhammed Nazmi (a.k.a. DonNazmi), one of the leaders of AnonGhost, posted images of what appear to be samples of messages he sent to Israelis. According to one image, he initiated a conversation with an Israeli and once the Israeli responded, Nazmi sent a threatening message which included an image of an ISIS fighter with the caption, “We are coming O Jews to kill you.” Under the image, a message reads, “I am Donnazmi [blurred] from AnonGhost Team. Send This Msg to your GOV Israel you better get ready to be prepared #opIsrael 07/04/2015 is coming.”

Another image posted by Nazmi shows a message that includes what appears to be a personal family picture sent to a father with his children circled in red and a caption that reads, “I’ll stick a knife in their throats.”
Other AnonGhost hackers have also shared images of threatening messages they sent to Israeli citizens using WhatsApp. “All your Private confidential details are in our hands, including your phone number/Your Home....we will kill you all of the Jews/Israeli. [sic]” another message reads.

AnonGhost and Anonymous have occasionally taken opposing sides on several issues, including the position on ISIS, and competed over leadership positions among hacker groups. The rivalry between the two groups has often resulted in them launching cyber-attacks against each other.

Leadership

The AnonGhost Team appears to be headed by Mauritania Attacker. In an online interview with a hacker’s blog in 2013, Mauritania Attacker claimed to be a 25 year old male from Mauritania who started hacking at a young age by joining TeaMp0isoN and ZCompany Hacking Crew (ZHC), two hacking groups known for their attacks of high-profile targets such as NATO, NASA, the UN, Facebook and the personal email account of former British Prime Minister Tony Blair.

Mauritania Attacker’s social media accounts are strongly influenced by ISIS propaganda, often including statements, videos and photos glorifying ISIS and its leadership. On May 21, 2015, he posted a comment in reference to the advancement of ISIS fighters in Iraq on Twitter stating, “Congratulations of the supporters of #the Islamic State in America for the victories.”

The comment also included a link to a YouTube video of what appears to be an audio message of an ISIS supporter in Michigan. The video recording starts with a statement by the speaker saying, “We are the supporters of the Islamic State in America, State of Michigan. We would like to send you our congratulations for such a great victory; the victory of conquering Ramadi.”

His current Twitter profile image features the Jihadi John, the British ISIS fighter who appeared in several ISIS beheading videos. Additionally, at one point he gave
his location on his Twitter profile as “Wilayat Khorasan,” a name given by ISIS to the Muslim region in parts of Asia.

Another prominent leader in AnonGhost who appears to have a high level of technical skills is Ungku [“Prince” in Bahasa Malaysia], a.k.a., Muhammad Nazmi, a Malaysia-based male hacker who also expresses radical Islamist views in support of ISIS on his Facebook page. For example, the cover photo of his Facebook profile, he uses an image depicting ISIS flag in a battle against the rest of the world flags.