Xtreme RAT Campaign – The Next Phase

by Aviv Raff on November 17, 2012 | Leave a comment
Filed under Research Lab and tagged IDF, Malware, News, Operation Pillar of Defense, RAT, remote access trojan, spear phishing.

Two weeks ago, an APT attack against the Israeli Police was reported. The attackers used a Remote Access Trojan called "Xtreme RAT", and caused the Israeli Police to disconnect their entire network from the internet, in order to further investigate the persistency of the attack.

A week ago, Snorre Fagerland, security researcher at Norman, confirmed the persistency of the "Xtreme RAT" attack. According to his report, the attackers initiated the campaign over a year ago, targeting both Palestinian and Israeli entities.

Today, the same attackers sent an email to an Israeli political candidate, Jonathan Klinger, who was kind enough to provide Seculert with a sample of the email, including the email headers (Read here an initial report by Jonathan, in Hebrew).

Analyzing the headers (see Figure 2) reveal that an IDF Spokesperson officer's gmail account got hacked, and used to send the spear-phishing email to the victims (see Figure 1).

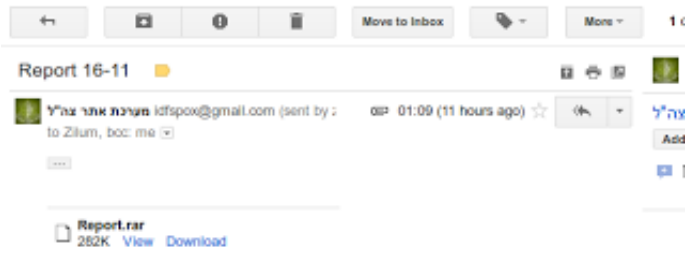

Figure 1: Spear-phishing email sent by hacked account of IDF Spokesperson (Courtesy of J.K.)

Figure 2: Spear-phishing email headers (Courtesy of J.K.)

When the victim opens the attached archived report (see Figure 3), the “Xtreme RAT” malware executes and then automatically opens a Word document of an article (see Figure 4), describing the recent events which lead to “Operation Pillar of Defense”. The malware then starts communicating with the Command & Control server, currently located in the U.S. (see Figure 5).

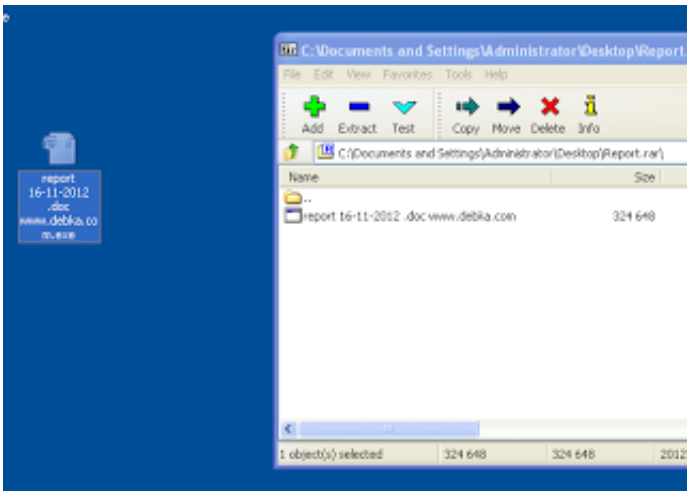

Figure 3: Report.rar attachment archive with a fake Word document file

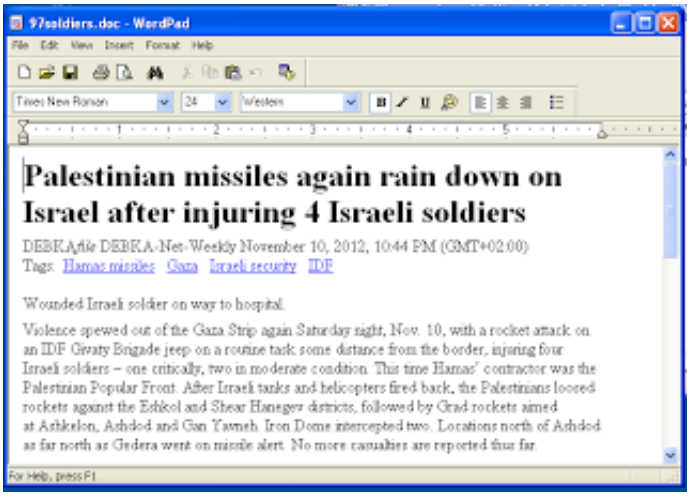

Figure 4: Fake Word document file with an article describing recent events

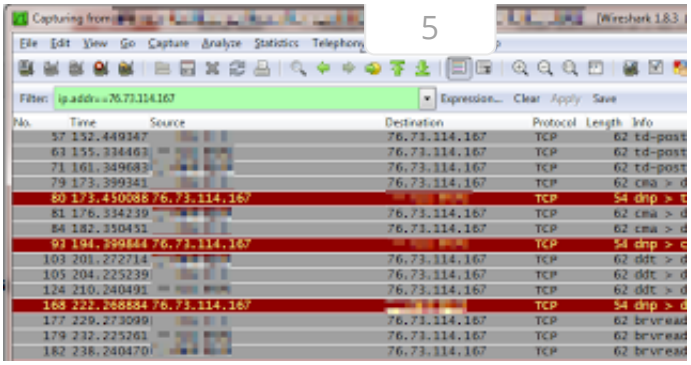

Figure 5: Xtreme RAT communicates with C&C hosted in the U.S

It is very common to see attackers use recent political events as part of spear-phishing attacks. It is less common to see them actually attack relevant players, and use them as a social-engineering proxy for the attack.

It seems as if this persistent attack is getting to an “Advanced” level quicker than we thought.

Is your network compromised? Take a free trial of Seculert and discover threats your other security solutions have missed.

FAQ

News & Media

In the Media

Press Releases

About Seculert

Management

Board of Directors

Follow Us

Resources

Blog

Contact Us

UP NOW!
RE OR HARDWARE