Xtreme RAT Strikes Israeli Organizations Again

by Aviv Raff on January 27, 2014 | Leave a comment
Filed under Industry News, Research Lab and tagged RAT, xtreme rat.

You may remember the targeted attack from November 2012, where attackers used a Remote Access Trojan called “Xtreme RAT” to compromise the Israeli Police network, causing them to disconnect from the internet. And this wasn’t the first time this malware had reared it ugly head. Now, 2 years later, it seems that this same group of presumably Palestinian hacktivists are at it again.

On January 15, the experts in Seculert’s Research Lab identified a new targeted attack that used Xtreme RAT. This latest attack used spear phishing emails to target Israeli organizations and deploy this nasty piece of advanced malware. To date, 15 machines have been compromised including ones belonging to the Civil Administration of Judea and Samaria. This is especially disconcerting as the Administration is responsible for entry and work permits from the West Bank to Israel.

We know that the cybercriminals behind the attack used multiple attack vectors in order to accomplish their goals. Spear phishing emails presumably from the Israeli Shin-Bet (Shabak), but are actually from shabakreport@gmail.com (Figure 1) contained a malicious attachment. One email contained a document that was a publicly available Shin-Bet report summarizing a decades worth of terrorist attacks (Figure 2). And the email’s attachment was related to former Prime Minister Ariel Sharon (Figure 3). Both reports were in Hebrew and the second was sent within in days of the prime minister’s passing. Closer examination of the spear phishing emails revealed that the attackers are not native Hebrew speakers and most likely copied and altered incomplete text to create the subject of the email. Evidence shows that the word “poisoned” was then added with incorrect grammar to the end of this phrase as seen below.
Figure 1: Screenshot of spear phishing email. Image used is the agency’s international logo.

Figure 2: Shin-Bet report on terrorist attacks from 1999-2009
The files delivered by the spear phishing emails contained a malicious executable masquerading as a PDF document. Once the attachment was opened, the malicious executable was deployed in the background. The malware used HTTP protocol over port 1863 to communicate with the attackers. This port is usually used by instant messaging applications, but in this situation it gave the hackers access to the network remotely.

Our experts have determined that in the case of this targeted attack, the command and control server (C&C) is located in the United States.

This isn’t the first and it most definitely won’t be the last time we see Xtreme RAT used by cybercriminals, hacktivists or nation-states. In terms of this particular targeted attack, the nature of the compromised organizations could have implications outside cyberspace.
Seculert customers are automatically protected from this threat. Using automatic traffic log analysis Seculert detects the abnormal communications created by this malware. Seculert’s technology recognizes these behavioral anomalies and automatically enhances customer’s on-premises devices.

Seculert notified the relevant authorities about this threat.

Learn more about advanced threat protection, visit www.seculert.com.