Xtreme RAT Strikes Israeli Organizations Again

Tweet
4
5

by Aviv Raff on January 27, 2014 omment
Filed under Industry News, Rese nd 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.

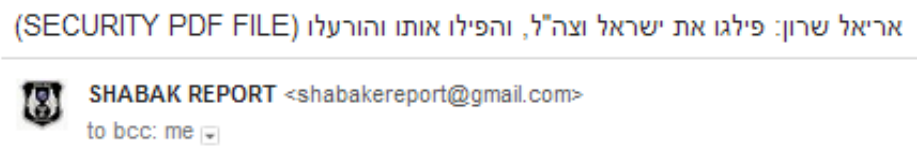
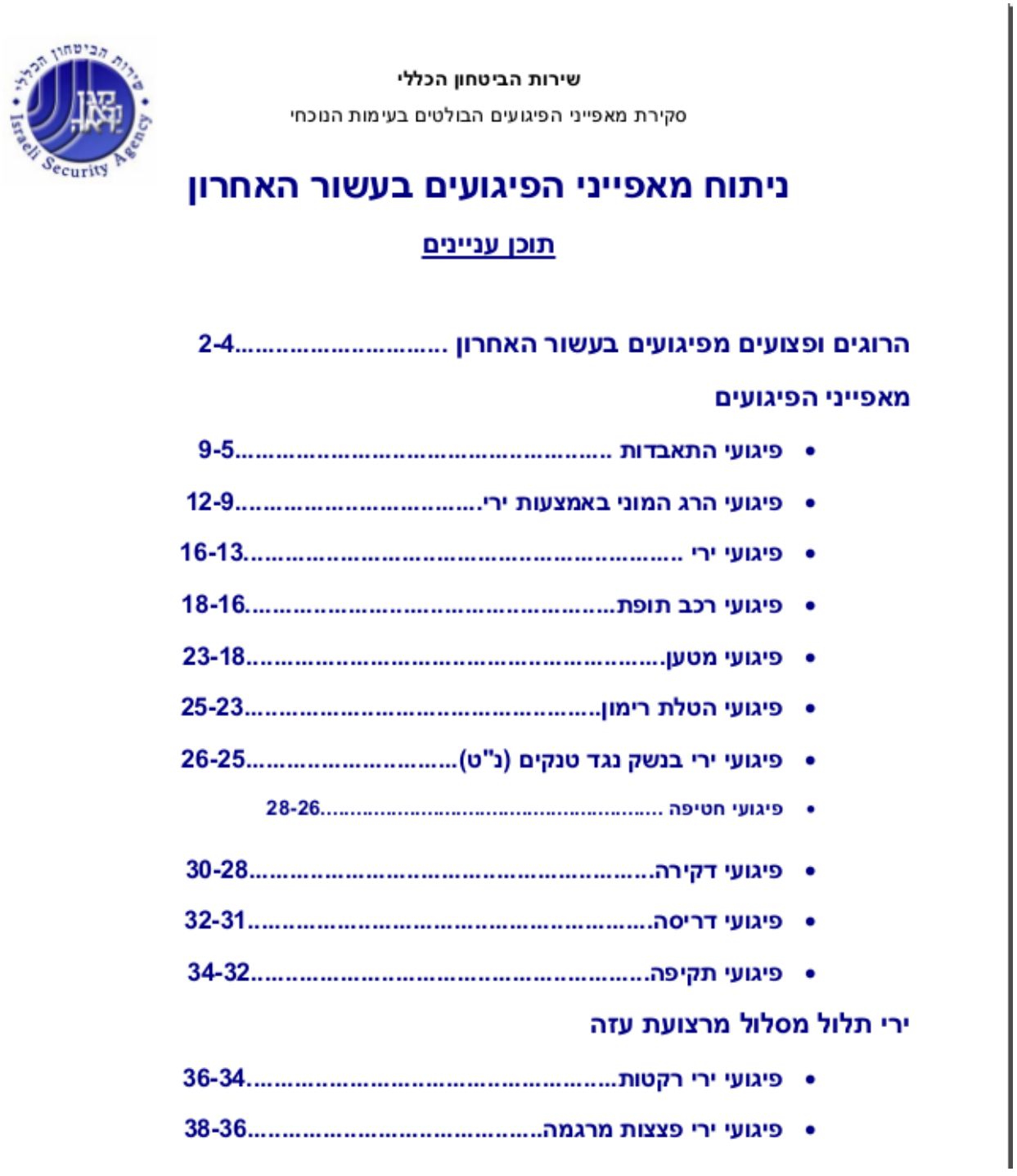


Figure 1: Screenshot of spear phishing email. Image used is the agency's international logo.



שירות הביטחון הכללי

סקירת מאפייני הפיגועים הבולטים בעימות הנוכחי

ניתוח מאפייני הפיגועים בעשור האחרון

תוכן עניינים

הרוגים ופצועים מפיגועים בעשור האחרון 2-4

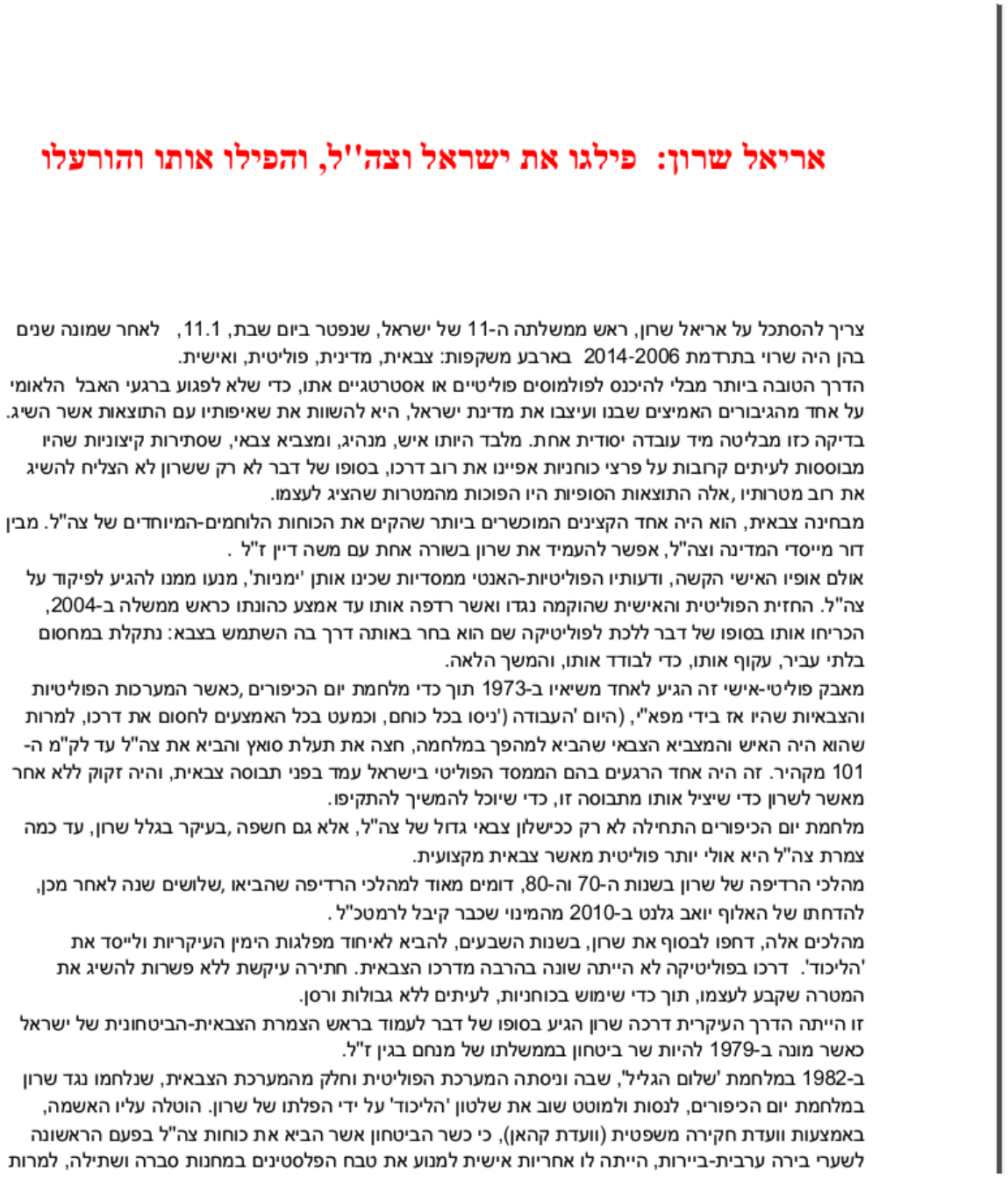
מאפייני הפיגועים

- פיגועי התאבדות 5-9
- פיגועי הרג המוני באמצעות ירי..... 9-12
- פיגועי ירי 13-16
- פיגועי רכב תופת..... 16-18
- פיגועי מטען..... 18-23
- פיגועי הטלת רימון..... 23-25
- פיגועי ירי בנשק נגד טנקים (נ"ט)..... 25-26
- פיגועי חטיפה 26-28
- פיגועי דקירה..... 28-30
- פיגועי דריסה..... 31-32
- פיגועי תקיפה..... 32-34

ירי תלול מסלול מרצועת עזה

- פיגועי ירי רקטות..... 34-36
- פיגועי ירי פצצות מרגמה..... 36-38

Figure 2: Shin-Bet report on terrorist attacks from 1999-2009



אריאל שרון: פילגו את ישראל וצה''ל, והפילו אותו והורעלו

צריך להסתכל על אריאל שרון, ראש ממשלתה ה-11 של ישראל, שנפטר ביום שבת, 11.1, לאחר שמונה שנים בהן היה שרוי בתרדמת 2006-2014 בארבע משקפות: צבאית, מדינית, פוליטית, ואישית.
הדרך הטובה ביותר מבלי להיכנס לפולמוסים פוליטיים או אסטרטגיים אתו, כדי שלא לפגוע ברגעי האבל הלאומי על אחד מהגיבורים האמיצים שבנו ועיצבו את מדינת ישראל, היא להשוות את שאיפותיו עם התוצאות אשר השיג.
בדיקה כזו מבליטה מיד עובדה יסודית אחת. מלבד היותו איש, מנהיג, ומצביא צבאי, שסתירות קיצוניות שהיו מבוססות לעיתים קרובות על פרצי כוחניות אפיינו את רוב דרכו, בסופו של דבר לא רק ששרון לא הצליח להשיג את רוב מטרותיו ,אלה התוצאות הסופיות היו הפוכות מהמטרות שהציג לעצמו.
מבחינה צבאית, הוא היה אחד הקצינים המוכשרים ביותר שהקים את הכוחות הלוחמים-המיוחדים של צה"ל. מבין דור מייסדי המדינה וצה"ל, אפשר להעמיד את שרון בשורה אחת עם משה דיין ז"ל .
אולם אופיו האישי הקשה, ודעותיו הפוליטיות-האנטי ממסדיות שכינו אותן 'ימניות', מנעו ממנו להגיע לפיקוד על צה"ל. החזית הפוליטית והאישית שהוקמה נגדו ואשר רדפה אותו עד אמצע כהונתו כראש ממשלה ב-2004, הכריחו אותו בסופו של דבר ללכת לפוליטיקה שם הוא בחר באותה דרך בה השתמש בצבא: נתקלת במחסום בלתי עביר, עקוף אותו, כדי לבודד אותו, והמשך הלאה.
מאבק פוליטי-אישי זה הגיע לאחד משיאיו ב-1973 תוך כדי מלחמת יום הכיפורים ,כאשר המערכות הפוליטיות והצבאיות שהיו אז בידי מפא"י, (היום 'העבודה ('ניסו בכל כוחם, וכמעט בכל האמצעים לחסום את דרכו, למרות שהוא היה האיש והמצביא הצבאי שהביא למהפך במלחמה, חצה את תעלת סואץ והביא את צה"ל עד לק"מ ה-101 מקהיר. זה היה אחד הרגעים בהם הממסד הפוליטי בישראל עמד בפני תבוסה צבאית, והיה זקוק ללא אחר מאשר לשרון כדי שיציל אותו מתבוסה זו, כדי שיוכל להמשיך להתקיפו.
מלחמת יום הכיפורים התחילה לא רק ככישלון צבאי גדול של צה"ל, אלא גם חשפה ,בעיקר בגלל שרון, עד כמה צמרת צה"ל היא אולי יותר פוליטית מאשר צבאית מקצועית.
מהלכי הרדיפה של שרון בשנות ה-70 וה-80, דומים מאוד למהלכי הרדיפה שהביאו ,שלושים שנה לאחר מכן, להדחתו של האלוף יואב גלנט ב-2010 מהמינוי שכבר קיבל לרמטכ"ל .
מהלכים אלה, דחפו לבסוף את שרון, בשנות השבעים, להביא לאיחוד מפלגות הימין העיקריות ולייסד את 'הליכוד'. דרכו בפוליטיקה לא הייתה שונה בהרבה מדרכו הצבאית. חתירה עיקשת ללא פשרות להשיג את המטרה שקבע לעצמו, תוך כדי שימוש בכוחניות, לעיתים ללא גבולות ורסן.
זו הייתה הדרך העיקרית דרכה שרון הגיע בסופו של דבר לעמוד בראש הצמרת הצבאית-הביטחונית של ישראל כאשר מונה ב-1979 להיות שר ביטחון בממשלתו של מנחם בגין ז"ל.
ב-1982 במלחמת 'שלום הגליל', שבה וניסתה המערכת הפוליטית וחלק מהמערכת הצבאית, שנלחמו נגד שרון במלחמת יום הכיפורים, לנסות ולמוטט שוב את שלטון 'הליכוד' על ידי הפלתו של שרון. הוטלה עליו האשמה, באמצעות וועדת חקירה משפטית (וועדת קהאן), כי כשר הביטחון אשר הביא את כוחות צה"ל בפעם הראשונה לשערי בירה ערבית-ביירות, הייתה לו אחריות אישית למנוע את טבח הפלסטינים במחנות סברה ושתילה, למרות

Figure 3: Ariel Sharon story from a debka.co.il article

The files delivered by the spear phishing emails contained a malicious executable masquerading as a PDF document. Once the attachment was opened, the PDF document got displayed, and the Xtreme RAT 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 hacktivists 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.

Share: Email Facebook Google +1 LinkedIn Twitter

© 2013 Seculert. All right reserved | Privacy Policy | Terms of Service

UP NOW!
RE OR HARDWARE