סקירת אירוע סייבר בחברת שירביט 1.12

תקציר

בתאריך 30.11.2020 נפתחו חשבונות טוויטר וטלגרם בשם Black Shadow. בעלי החשבונות פרסמו בהם הודעה על פריצה לחברת שירביט וצרפו תמונות וקבצים של פוליסות ביטוח, רישיונות נהיגה ותעודות זהות של לקוחות החברה. בשלב זה אין לנו יכולת לשייך את התקיפה לתוקף מסוים. חקירה ראשונית אותה ביצענו על מתווה חדירה אפשרי, דרך ביצוע ההדלפה והפרסום שנלווה אליו מצביעה על כך שמטרת התוקפים לא הייתה רק רווח כספי. הפרסום נועד, להערכתנו, לייצר אפקט פסיכולוגי שבו מודגשת הפגיעה בחברת שירביט עם רמזים למבצעי OpIsrael ואולי לנקמה בישראל על ידי קבוצת תקיפה איראנית.

אין לנו מידע מוצק בשלב זה על היקף הנזקים שנגרמו למערך המחשוב של החברה, אך מאיסוף מידע ממספר מקורות, נראה שנגרם נזק רב למערך המחשוב של חברה כולל שרתים וגיבויים שנמחקו.

נכון ל 1.12 בשעות הערב, כלל השרתים שהיו מחוברים לאינטרנט, לא מגיבים ונראה שבוצע ניתוק יזום של רשתות החברה מהאינטרנט.

ההדלפה הראשונה של התוקפים כללה קובץ PST של עובד, שככל הנראה עזב את הארגון בשנת 2015 אך תיבת הדואר שלו לא נסגרה והמשיכה לקבל מיילים כלליים לעובדי החברה שאפשרה לנו לבצע מחקר על מועד ההדלפה האפשרי של המידע.

במחקר שביצענו ב VT מצאנו קובץ נוזקה המשויך על ידנו בסבירות בינונית לתקיפה. אינדיקטורים מצורפים לידיעה.

ניתוח התקיפה:

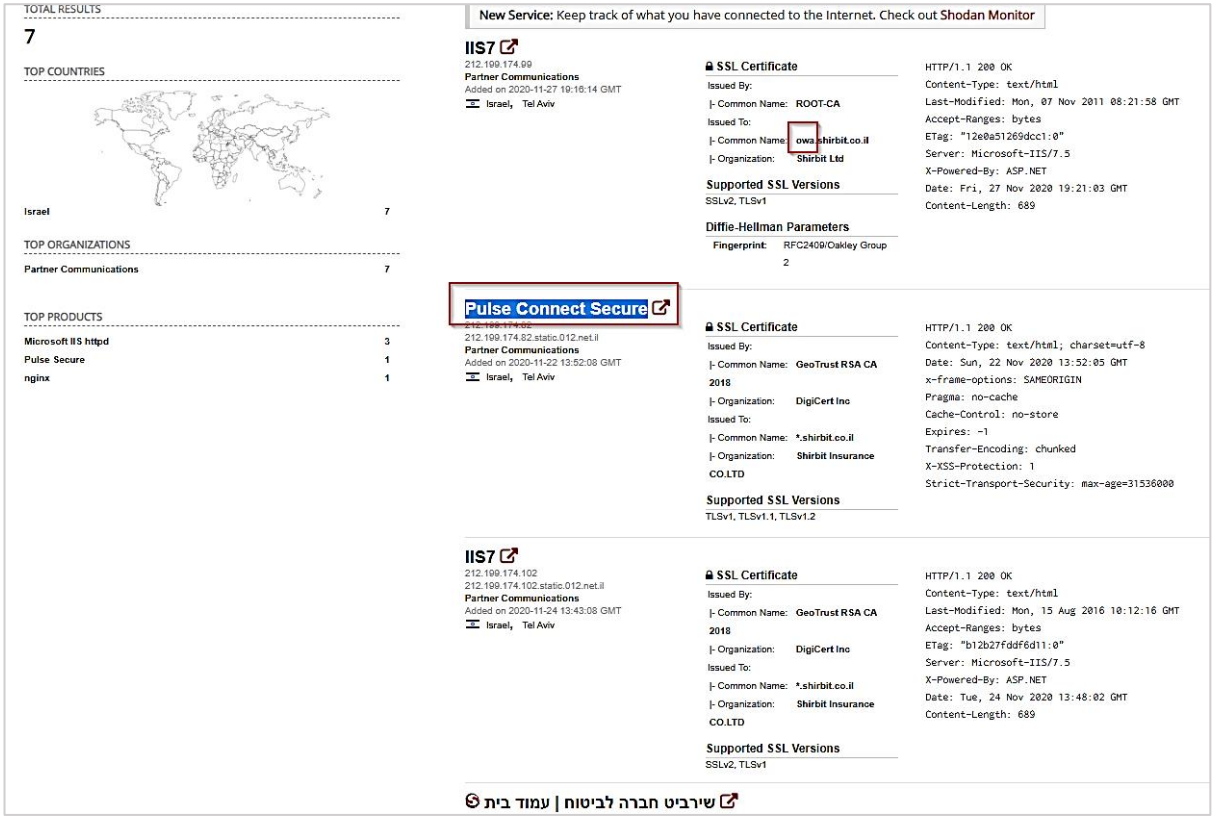
לחברת שירביט הייתה תשתית שרתים ודומיינים רחבה המקושרת לאינטרנט.

Subdomains	
agnt.shirbit.co.il	212.199.174.69
www.shirbit.co.il	212.199.174.68
int.shirbit.co.il	212.199.174.90
med.shirbit.co.il	212.199.174.68
campaigns.shirbit.co.il	185.70.251.126
qaweb.shirbit.co.il	212.199.174.90
ibay.shirbit.co.il	212.199.174.126
qa.shirbit.co.il	212.199.174.85
bit.shirbit.co.il	212.199.174.66
ark.shirbit.co.il	212.199.174.102
mail4.shirbit.co.il	212.199.174.72
safe.shirbit.co.il	212.199.174.70
mail3.shirbit.co.il	212.199.174.71
ssl.shirbit.co.il	212.199.174.100

לרשת החברה מחובר שרת OWA חשוף לאינטרנט שלו מספר חולשות ידועות ששימשו תוקפים רבים, כולל איראנים לחדור לחברות בישראל.

לרשת החברה מחובר שרת Pulse VPN חשוף לאינטרנט. למוצר זה פורסמו שתי חולשות קריטיות בשנת 2019. CVE-2019-11510 CVE-2019-11539

להלן מתוך Shodan :



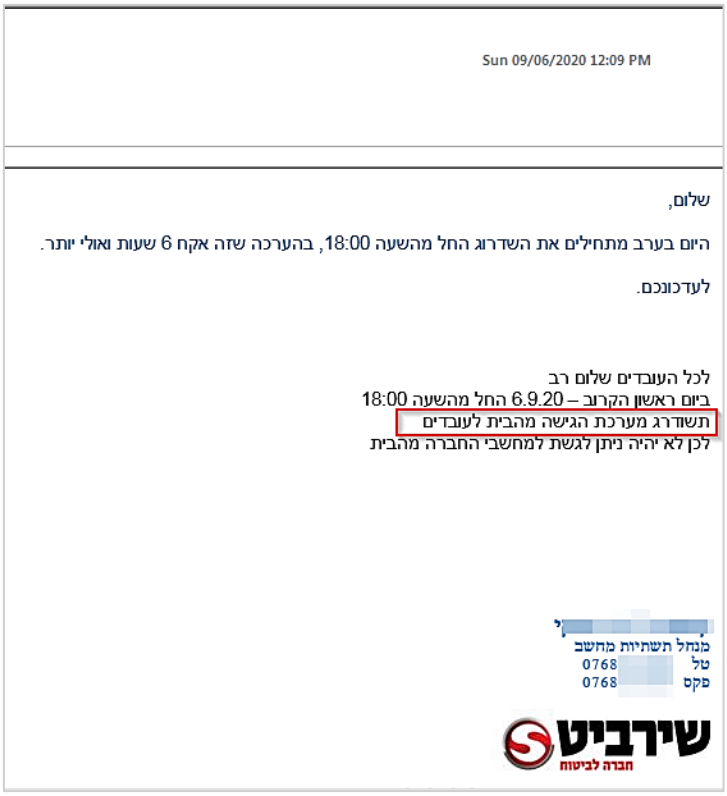
חקירת ההדלפות

התוקף הדליף בנוסף לתמונות, תיבת אימייל מלאה מתוך הארגון. מבדיקה שלנו מדובר בתיבה השייכת לעובד\ת בשם ירדן אלגואר.

לפי הערכתינו העובד הפסיק לעבוד בשירביט בשנת 2015 והתיבה נשארה "כתיבת רפאים" במערכת, שקיבלה אימיילים שנשלחו לתפוצת כלל החברה:

From	Subject	Date/Time
<FILTER>	<FILTER>	<FILTER>
@shirbit....	שדרוג מערכת	Sun 09/06/2020 12:09 PM
@shirbit....	שדרוג מערכת	Wed 09/02/2020 11:01 AM
@shirbit....	חידוש סיסמת הכניסה	Tue 09/01/2020 10:05 AM
@shirbit....	מערך השירות המשרדרג - איך זה הו...	Thu 12/05/2019 13:28 PM
@shir...	תשרמת ליבכם - נרזקה חדשה במכשי...	Tue 12/03/2019 16:50 PM
@shir...	ברוכים הבאים למערך השירות המשר...	Tue 12/03/2019 15:01 PM
@shir...	תזכורת - כיבוי מחשבים לצורך ביצו...	Sun 11/10/2019 13:12 PM
@shirbit....	קישור למערכת דיווח שעות	Tue 06/11/2019 09:25 AM
@shir...	הפעלת מערכת סריקת קבצים במייל	Wed 06/05/2019 15:27 PM
@shirbit....	תיקון שעון במחשב	Mon 03/26/2018 08:02 AM
@shirbit...	הדלקת נרות בשירביט	Sun 12/13/2015 16:51 PM

שלושת האימיילים האחרונים בתיבה שהודלפה הם מחודש ספטמבר 2020.



Sun 09/06/2020 12:09 PM

שלום,

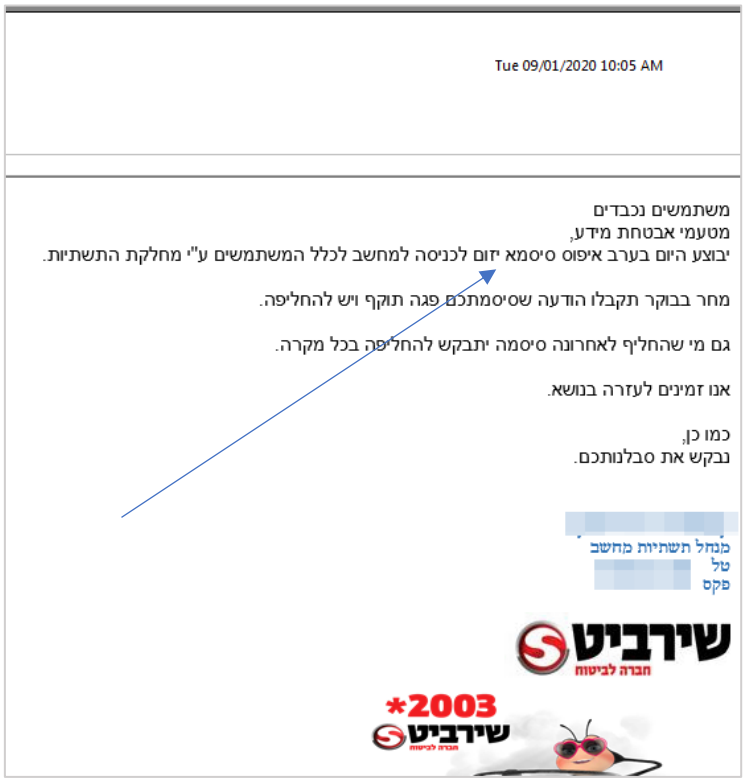
היום בערב מתחילים את השדרוג החל מהשעה 18:00, בהערכה שזה אקח 6 שעות ואולי יותר.

לעדכונכם.

לכל העובדים שלום רב
ביום ראשון הקרוב – 6.9.20 החל מהשעה 18:00
תשודרג מערכת הגישה מהבית לעובדים
לכן לא יהיה ניתן לגשת למחשבי החברה מהבית

מנהל תשתיות מחשב
טל 0768
פקס 0768

שירביט
חברה לביטוח



Tue 09/01/2020 10:05 AM

משתמשים נכבדים
מטעמי אבטחת מידע,
יבוצע היום בערב איפוס סיסמא יזום לכניסה למחשב לכלל המשתמשים ע"י מחלקת התשתיות.

מחר בבוקר תקבלו הודעה שסיסמתכם פגה תוקף ויש להחליפה.

גם מי שהחליף לאחרונה סיסמה יתבקש להחליפה בכל מקרה.

אנו זמינים לעזרה בנושא.

כמו כן,
נבקש את סבלנותכם.

מנהל תשתיות מחשב
טל
פקס

שירביט
חברה לביטוח

*2003
שירביט
חברה לביטוח

ייתכן והסיבה להחלפת הסיסמאות הכללית בחודש ספטמבר היה אירוע אבטחת מידע בחברת שירביט, אך ייתכן ומדובר בהחלפת סיסמאות כללית המתבצעת אחת לתקופה.

במידה והתוקפים הצליחו להשיג גישה לשרת הדואר ולהוציא משם את כל תיבות האימייל יתכן והתוקפים הצליחו להשיג מידע רגיש כמו פרטי אשראי של לקוחות שנשלחים ב clear text באימייל:


From: Mtar-Tours [mailto:z[redacted]com]
Sent: Wednesday, July 22, 2015 11:56 AM
To: ירדן אלגואר
Subject: RE: קבוצה

4580-[redacted]-4027
תוקף- 07-19
על שם [redacted] מטר
ת"ז- 1 [redacted]
שלוש מספרים בגב הכרטיס 297

בתאריך ה 01.12.2020 התוקף עדכן בערוץ טלגרם שהוא מחפש כתבים, כנראה במטרה לספר את סיפור התקיפה מנקודת מבטו, או שמטרתו להשיג אפקט פסיכולוגי מקסימלי לתקיפה.

לאחר הפנייה לכתבים התוקף פירסם מסמכים של חברת שירביט מתאריך 29.11.2020


29/11/2020 -נכון ל

סוכן : 6031 - מקורות - לא נ
מספר רישוי: 27847001
ח.ר./ח.פ. : 57749988

דיווח על תביעות ב[redacted] 3 השנים האחרונות :

ח על עסקי ביטוח, הננו [redacted]עך כי עד לתאריך הדפסת מכתב זה
ידך או בשמך תביעות בגין [redacted] שניתן בפוליסה להלן במשך :

תקופת ביטוח: 26/11/2017 עד 31/10/2018-מקיף

מצב	סכום שולם(בש"ח)	סוג תביעה	מועד מקרה ביטוח	

בכבוד רב
שירביט חברה לביטוח בע"מ

ייתכן שהתוקף חדר לרשת הארגון לפני מספר חודשים, הדליף במשך התקופה מידע מבסיסי הנתונים בחברה ואתמול החליט מטעמים שונים לבצע פעולת הרס.

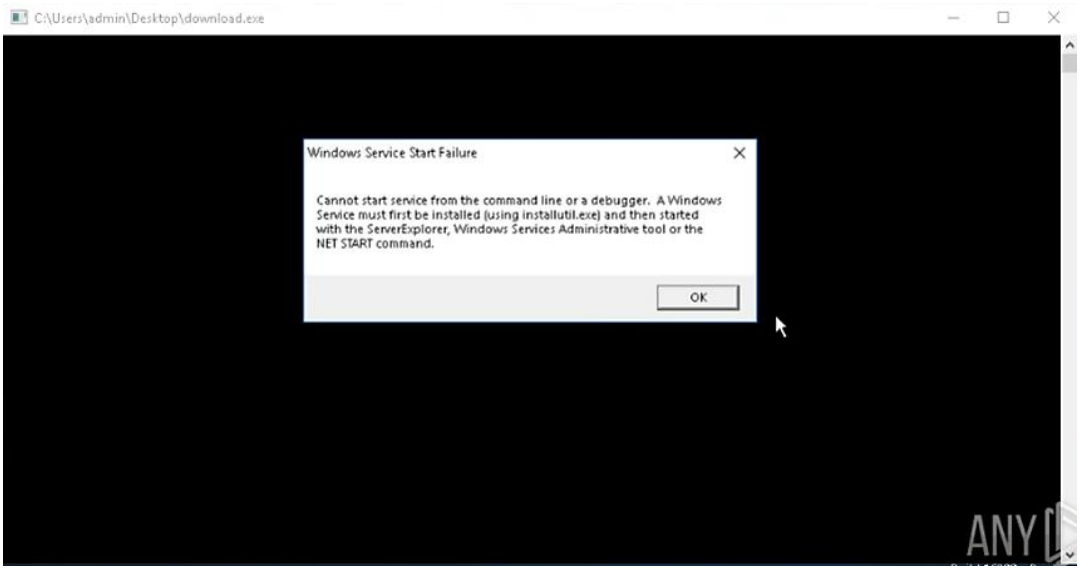
מחקר לאיתור הנוזקה שהופעלה בחברת שירביט ב Virus Total

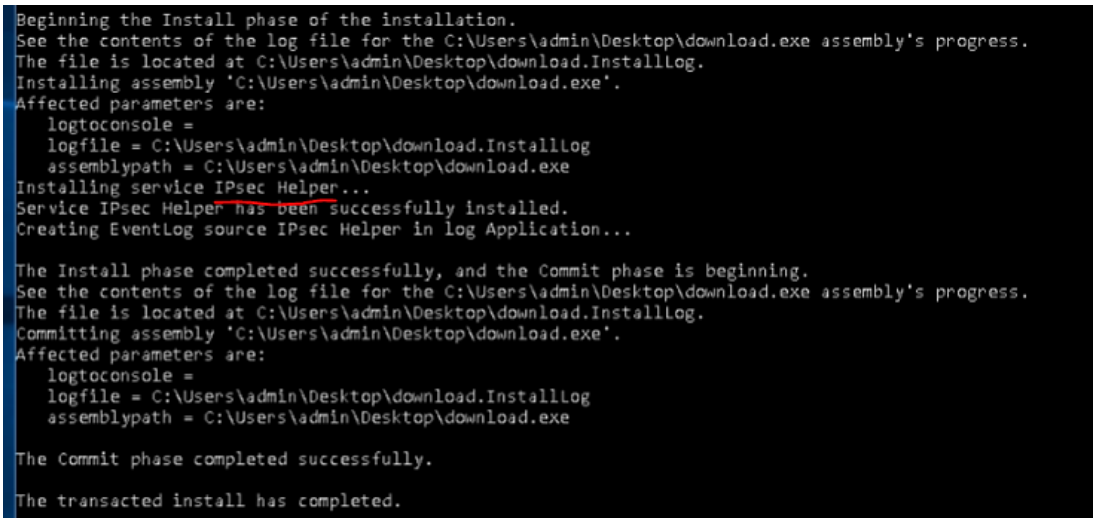
במחקר שביצענו ב VT מצאנו קובץ ששייכנו בסבירות בינונית לתקיפה על שירביט.

להלן ניתוח ראשוני של הקובץ: IPsec Helper שאיתרנו ב VT
96cc69242a7900810c4d2e9f3f55aad8edb89137959f4c370f80a6e574ddc201[1]

1
https://www.virustotal.com/gui/file/96cc69242a7900810c4d2e9f3f55aad8edb89137959f4c370f80a6e574ddc201/detection

מדובר בשירות שיש לבצע עבורו התקנה בעזרת הכלי installutil ואז להפעילו בעזרת net start.





השירות מותקן בשם IPSec Helper ולאחר כשהוא מופעל הוא נכנס למצב המתנה לטווח זמן של כחמש דקות לאחר מכן הוא מבצע חיבור לשרותי Microsoft לבדוק שקיים חיבור אינטרנט מהמחשב המודבק

לאחר שחיבור זה נוצר בהצלחה, הקובץ מנסה להתחבר לכמה שרתי שליטה ובקרה בכתובות IP הבאות:

5.2.73[.]67

185.142.97[.]81

185.142.98[.]32

הקובץ מתחבר בעזרת User Agent מיוחד לשרתי שליטה ובקרה:

POST /Panel/new/File/css/boot.php

User-Agent: Mozilla/4.0 (compatible;MSIE 7.0; Windows NT 5.1; EmbeddedWB 14.52 from: http://www.google.com/ EmbeddedWB 14.52;...NETCLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1; .NET CLR 1.0.3705; .NET CLR 3.0.04506.30).

Referer: https://www.google.com/

נוסף לכך הנוזקה מייצרת קובץ בתיקיית ההרצה המקורית שממנו הורצה הנוזקה בשם <Filename>.dat המכיל בתוכו הגדרות שונות שכנראה הנוזקה משתמשת בהן.

```
<?xml version="1.0" encoding="utf-16"?>
<ConfigModel xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <EmbedId>ltQTLPxCdaCY_El]jb!B</EmbedId>
  <InternetNeeded>true</InternetNeeded>
  <LogEnabled>false</LogEnabled>
  <UseCache>false</UseCache>
  <Interval>10</Interval>
  <Relays>
    <string>B7hjekKVJ0XdjRrnQ8vx32FhSUcLv6M99LDK05lzvqN8b8i/yjsGuQqroZrcH5uqpc9lwYG38MiQC9R8CE2gpA==</string>
    <string>Hs/9KdISz1jCUYR1zb1URAnuNH4zQN5XkD4uANpa7ICrPfHpKC2/1bju6hxm6RnCxapXyIO2rNA3LaV0gn6s4Q==</string>
    <string>IL9PHeTnOzn/H1XIEVWe9CjSjGv/TYmBu3YY5nwuvEvnB8f0sqFdlIpzDqgqVBiBdIt1miI0hybnhpF5cU1VUw==</string>
  </Relays>
  <Servers />
  <DeviceIdSalt>k+xpGkuWOF5JRREJudQkd3tU6F+rzW24BEaryEl70WH3YUKTM1FxELCie7Xbpg82y4UrjPWh5zkKmMXWF5hU4g==
</DeviceIdSalt>
  <PublicKeyToken>e5VtH3ptjMofUBfncDnwUpzYqLB/Z+3DOpVUw7n8Mr4=</PublicKeyToken>
  <SessionKey>eOL1awi41Bl2FW5pqSKFLvO3aHpVeaE0befM7sYJ718=</SessionKey>
</ConfigModel>
```

הנוזקה נוגעת במפתחות Registry בניתוב הבא:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\<originalfilename>_RASMANCS

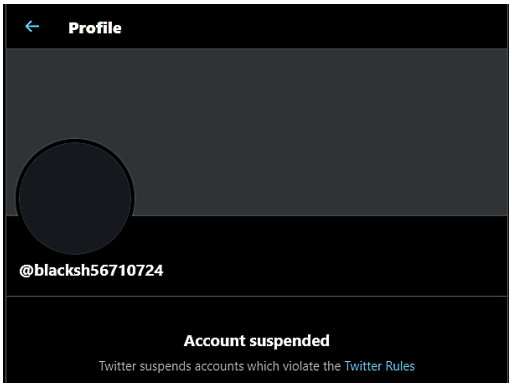
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\< originalfilename >_ RASAPI32

המפתחות שהנוזקה עורכת קשורים לשירות חיבור מרחוק של Windows ונראה שהנוזקה מכבה את הניטור של השירות הזה.

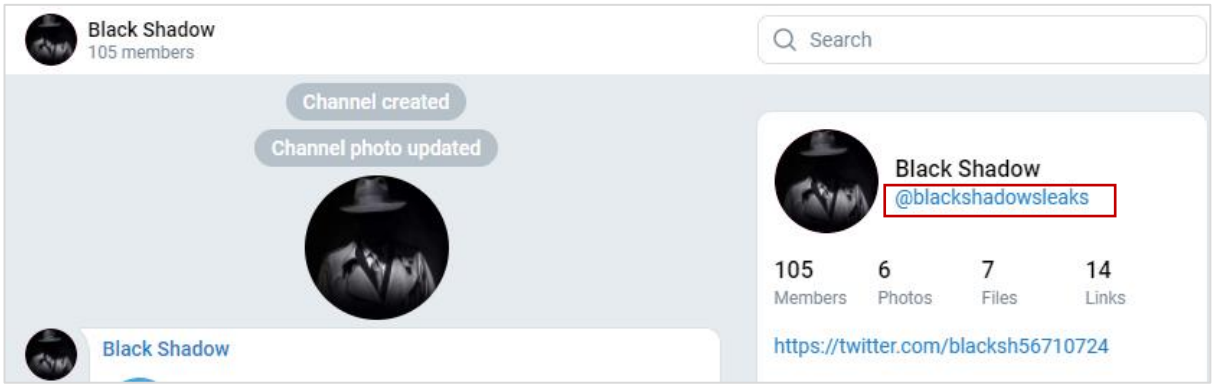
ניתוח הקבוצה והדמויות

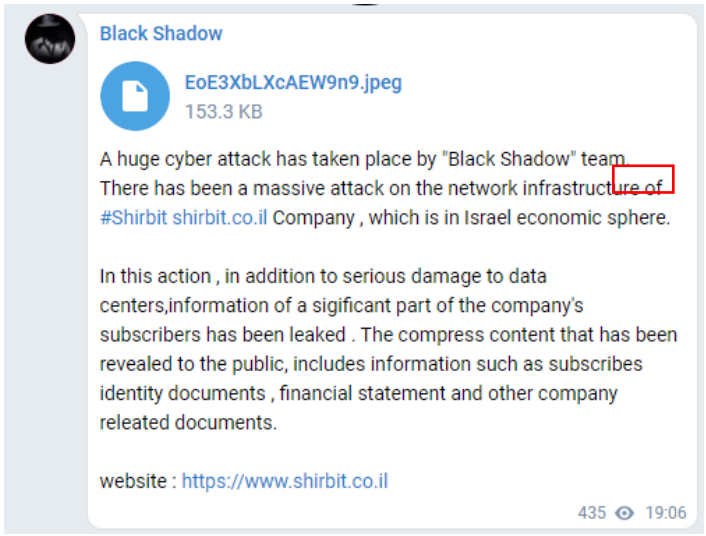
בתאריך 30.11.2020 Black Shadow פרסמו בטוויטר מספר תמונות של פוליסות ביטוח, רישיונות נהיגה ותעודות זהות של לקוחות חברת הביטוח שירביט.

חשבון הטוויטר הושעה ולא פעיל:



המשתמש פתח במקביל ערוץ טלגרם באותו תאריך:

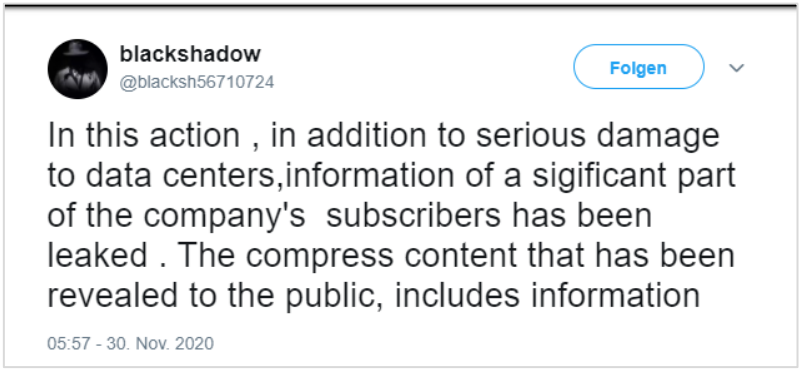




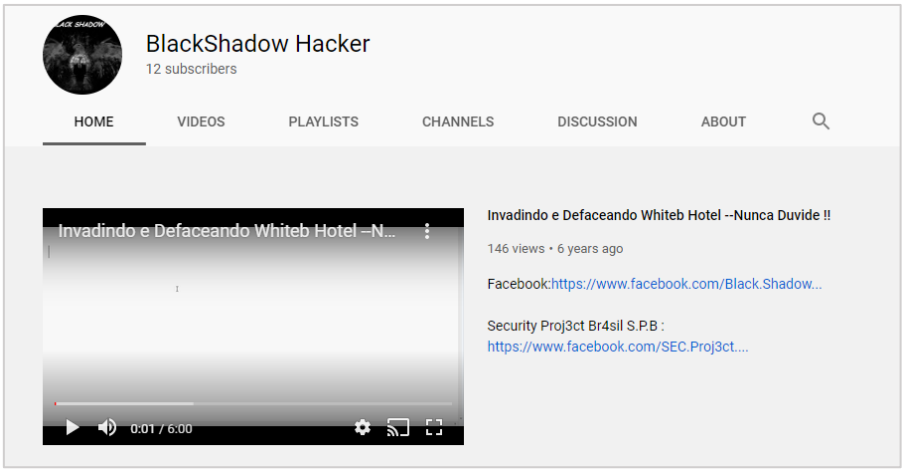
בערוץ הטלגרם מצויים עדיין כל הקבצים שהודלפו בטויטר. שם החשבון הוא blackshadowS עם הסופית S שמשמעותה רבים באנגלית. בהודעות בערוץ נרשם שמדובר בקבוצה "team".

בבדיקה שערכנו כשחשבון הטוויטר היה פעיל, המשתמש שפתח את החשבון עקב אחר חשבונות שמזוהים עם פעילות האקטיביסטית של ארגון אנונימוס וביניהם לדוגמא Lorian Synaro שהוא אחד ההאקרים האקטיביסטים המובילים בארגון אנונימוס, פעיל מתחילת 2018 והוביל מספר קמפיינים של OpIsrael.

פרט מידע נוסף שיכול להעיד שהתוקפים הינם הקטיביסטים הינו תיוג שהם עשו לרשתות תקשורת עולמיות בכוונה לפרסם את המידע וכן "ניפוח" של ההישגים.



בבדיקה שערכנו נמצא ערוץ יוטיוב של האקר עם שם דומה מלפני 6 שנים.



לא ניתן לקשר את הערוץ לדמות הנוכחית בוודאות. בערוץ יוטיוב השפה הינה פורטוגזית. בתמונת אבטר של המשתמש ישנו הסמל של קבוצת אנונימוס. בערוץ ישנם 2 קישורים לפייסבוק, שניהם כבר לא פעילים. הלינק הראשון היה כנראה לפרופיל של התוקף והשני לקבוצה שהוא משתייך אליה. שם הפרופיל שהיה בפייסבוק: "Black.Shadow.anony".

לקבוצה יש עדיין חשבון טוויטר פעיל:

אינדיקטורים:

5.2.73[.]67

185.142.97[.]81

185.142.98[.]32

IPsec Helper[.]exe

96cc69242a7900810c4d2e9f3f55aad8edb89137959f4c370f80a6e574ddc201