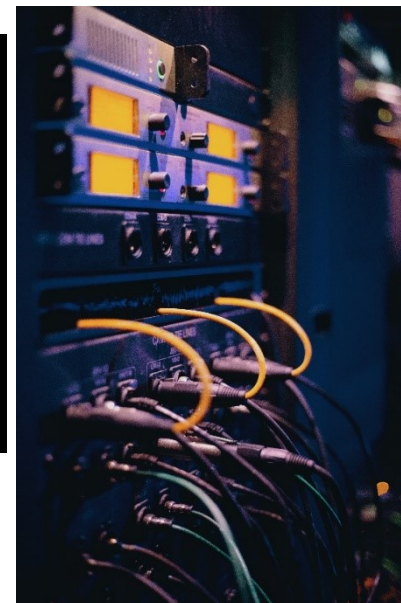




מושגי ייסוד בהגנת סייבר – חלק ב



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: yosish@gmail.com , yosish@sviva.gov.il





FOX 13


5:00 77°

LINDA HURTADO

CYNTHIA SMOOT

מה עשו? 100ppm ← 11,100ppm

איך עשו? השתלטות על ה-HMI דרך TeamViewer



<https://www.ynet.co.il/news/article/HJYZtAyZ00>

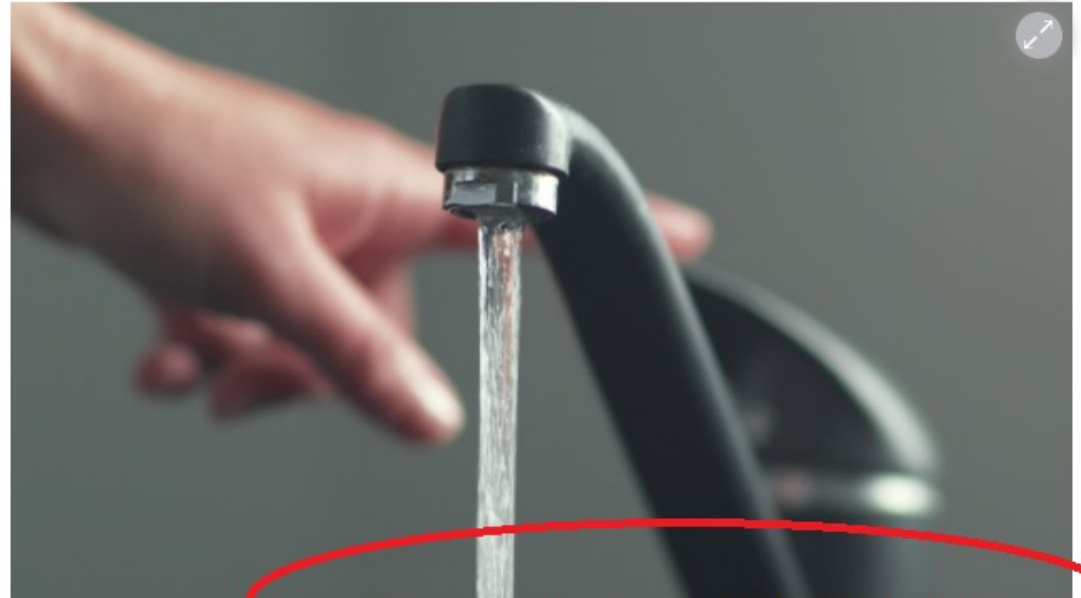
האקרים ניסו להרעיל את המים בעיר בפלורידה

פחות משנה אחרי הפריצה למתקני המים בישראל, מתקפה דומה בארה"ב: האקרים השתלטו מרחוק על המחשב במתקן בעיר בת 15,000 תושבים, והעלו לגובה מסוכן את רמת הנתרן ההידרוקסידי במי השתייה. פקח הבחין בעכבר זז מעצמו וסיכל את הפריצה: "קריאת השכמה"



סוכנויות הידיעות פורסם: 09.02.21, 12:03

האקרים הצליחו להשתלט על מערכת הניהול מרחוק של מתקן המספק מים לעיר בת 15,000 תושבים בפלורידה - וכמעט הצליחו להרעיל אותם. כך חשפו אמש (ב') הרשויות במחוז פינלס הסמוך לטמפה, תוך שהן מדגישות כי הניסיון הזה התגלה במהירות על ידי אחד הפקחים במתקן שנפרץ - וסוכל.



מ-100 חלקיקים למיליון ל-11,100. האקרים ניסו להרעיל, וכמעט הצליחו (צילום: shutterstock)

Open


Holocaust 2nd Gen Rights

Center for Documentation

NIOSH Pocket Guide

[Sodium hydroxide](#)

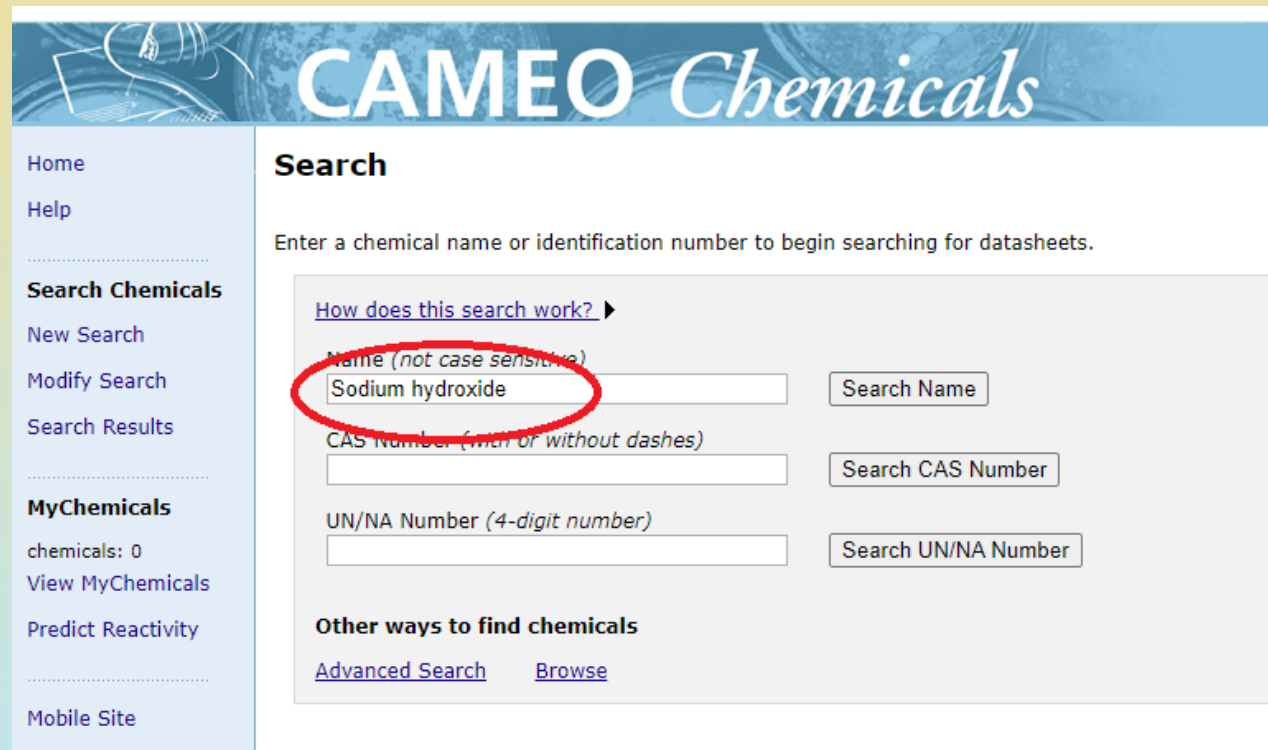
NFPA 704

| Diamond | Hazard | Value | Description |
|--|--------------|-------|---|
|  | Health | 3 | Can cause serious or permanent injury. |
| | Flammability | 0 | Will not burn under typical fire conditions. |
| | Instability | 1 | Normally stable but can become unstable at elevated temperatures and pressures. |
| | Special | | |

(NFPA, 2010)

PACs (Protective Action Criteria)

| Chemical | PAC-1 | PAC-2 | PAC-3 |
|------------------------------|-----------------------|---------------------|----------------------|
| Sodium hydroxide (1310-73-2) | 0.5 mg/m ³ | 5 mg/m ³ | 50 mg/m ³ |



CAMEO Chemicals

Home
Help

Search

Enter a chemical name or identification number to begin searching for datasheets.

[How does this search work?](#)

Name (*not case sensitive*)

CAS Number (*with or without dashes*)

UN/NA Number (*4-digit number*)

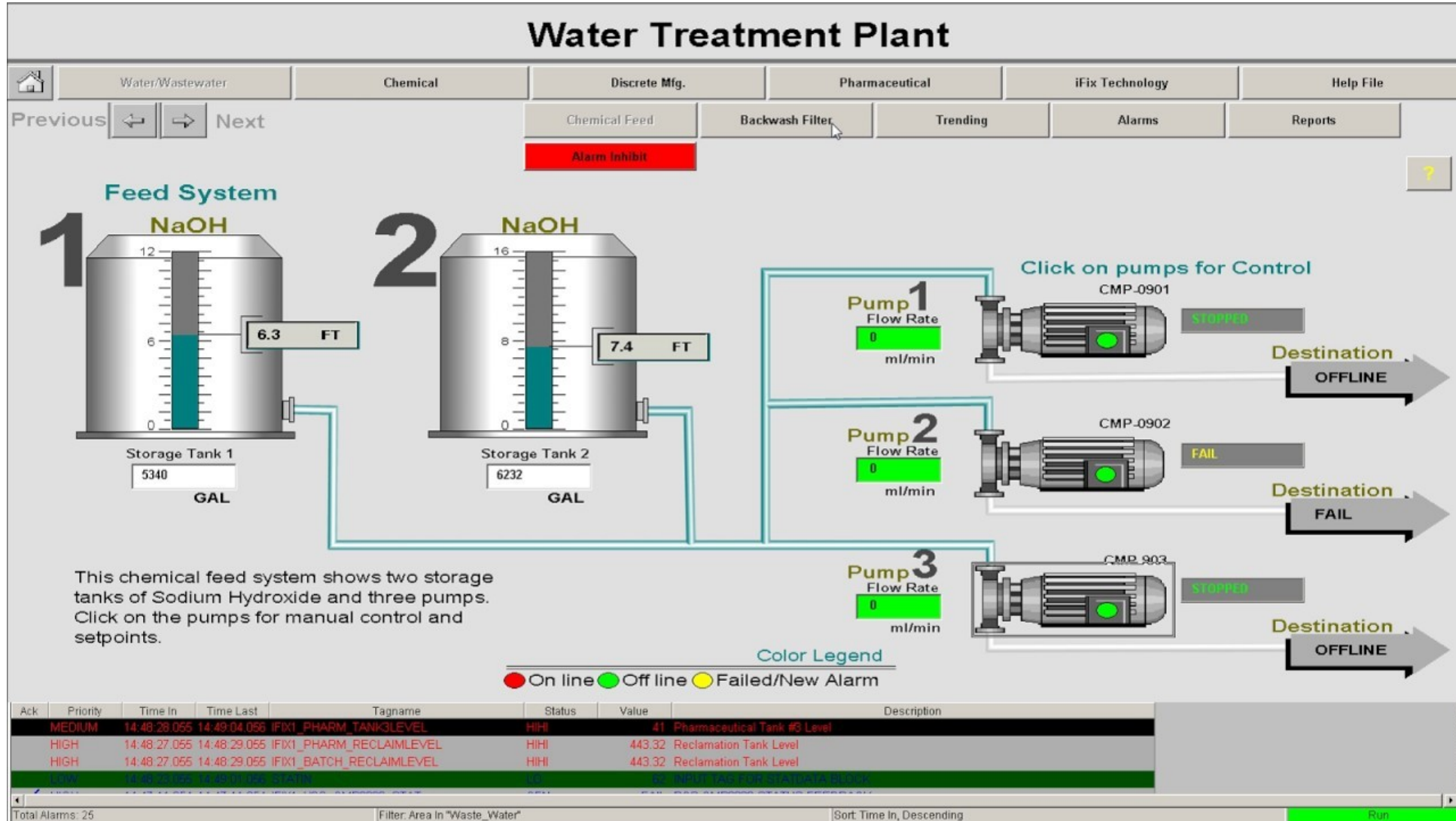
Other ways to find chemicals

[Advanced Search](#) [Browse](#)

Search Chemicals
 New Search
 Modify Search
 Search Results

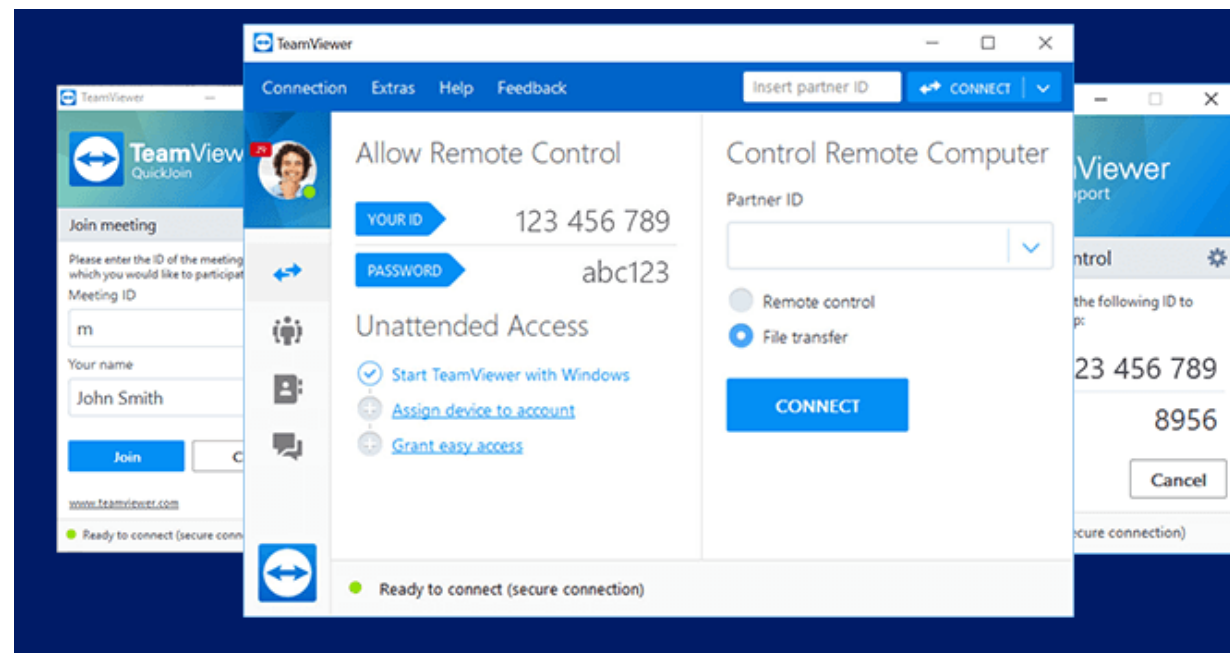
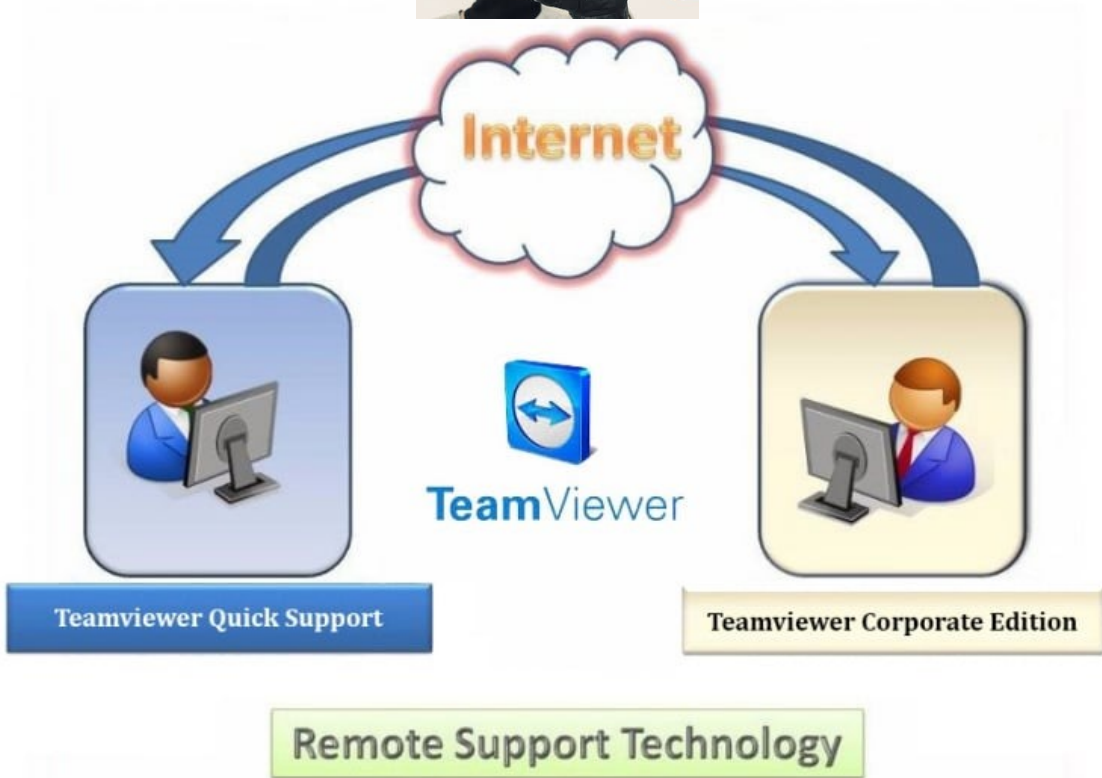
MyChemicals
 chemicals: 0
 View MyChemicals
 Predict Reactivity

Mobile Site



איך עובד TEAM-VIEWER?

השתלטות ממחשב
השתלטות מטל סלולרי



The screenshot shows a Windows desktop environment. At the top, there is a browser window with tabs for 'index1' and 'translate - Google Search'. The desktop background is a map of Israel with several yellow and green callout boxes containing Hebrew text: 'מאגר בית יואב', 'גובה מים מעבר', '14 | 18 | 46', 'מתח סיקוד 24 וולט תקין', 'תקין N.V.R. 230', '5.900 meter', 'מכונת שדה יואב', 'מסך תקלות', 'גרפיקס בית ניר', and 'גרפיקס שדה יואב'. A Bandicam window is open in the foreground, displaying the 'Options' tab. The 'Output folder' is set to 'C:\Users\Administrator\Documents\Bandicam'. Other options include 'Bandicam window always on top', 'Start Bandicam minimized to tray', and 'Run Bandicam on Windows startup'. The 'Scheduled Recording' section shows 'There are no scheduled recordings.' and the 'Auto Complete Recording' section shows 'Disable'. A large watermark '@Unidentified_TM' is overlaid on the center of the screen.



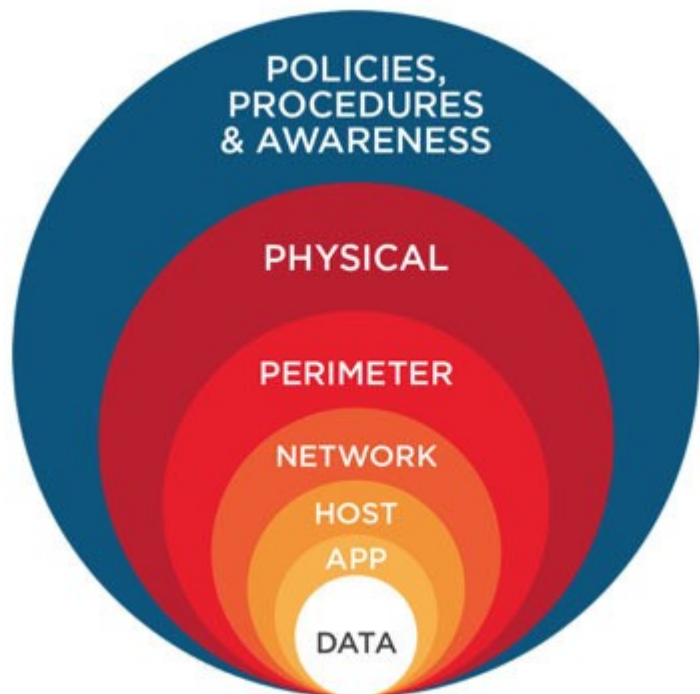
נושאי הלימוד

- מודל "הגנה בשכבות" (Defense in Depth) 📖
- התקפות ZERO DAY ודרכי התגוננות 📖
- התקפת DOS , DDOS 📖
- הגנה על האפליקציה – WAF 📖
- הגנה על בסיס הנתונים – DAF 📖
- הגנה על הכנסת רכיבים זרים לרשת – NAC 📖
- הגנה על זליגת מידע – DLP 📖

סוגי התקפות ויישום הגנות



העיקרון: הגנה על כל רכיב כאילו הוא לבד.



- ✓ הגנה על בסיס הנתונים
- ✓ הגנה על האפליקציות
- ✓ הגנה על המחשבים
- ✓ הגנה על הרשת
- ✓ הגנה פיסית על חדרי השרתים
- ✓ בקורות גישה בתוך הארגון
- ✓ הגנה היקפית של הארגון (גדרות, מצלמות, שומרים)
- ✓ מודעות עובדים
- ✓ נהלים ופרוצדורות עבודה

התקפה על האפליקציה

Vulnerability – חולשה

Exploit – ניצול חולשה

אנלוגיה לעולם המיחשוב:

חולשה: באג בתוכנת דפדפן אקספלורר של מיקרוסופט המאפשר פריצה אל המחשב שלנו

ניצול החולשה: תוכנות שהאקרים כתבו ופרסמו באינטרנט על מנת ל"התנקס" בחברת מיקרוסופט

מי מנצל: כל מי שמוריד את התכנה



התקפת DOS , DDOS



התקפת Denial of Service – DOS

התקפת Distributed Denial of Service – DDOS

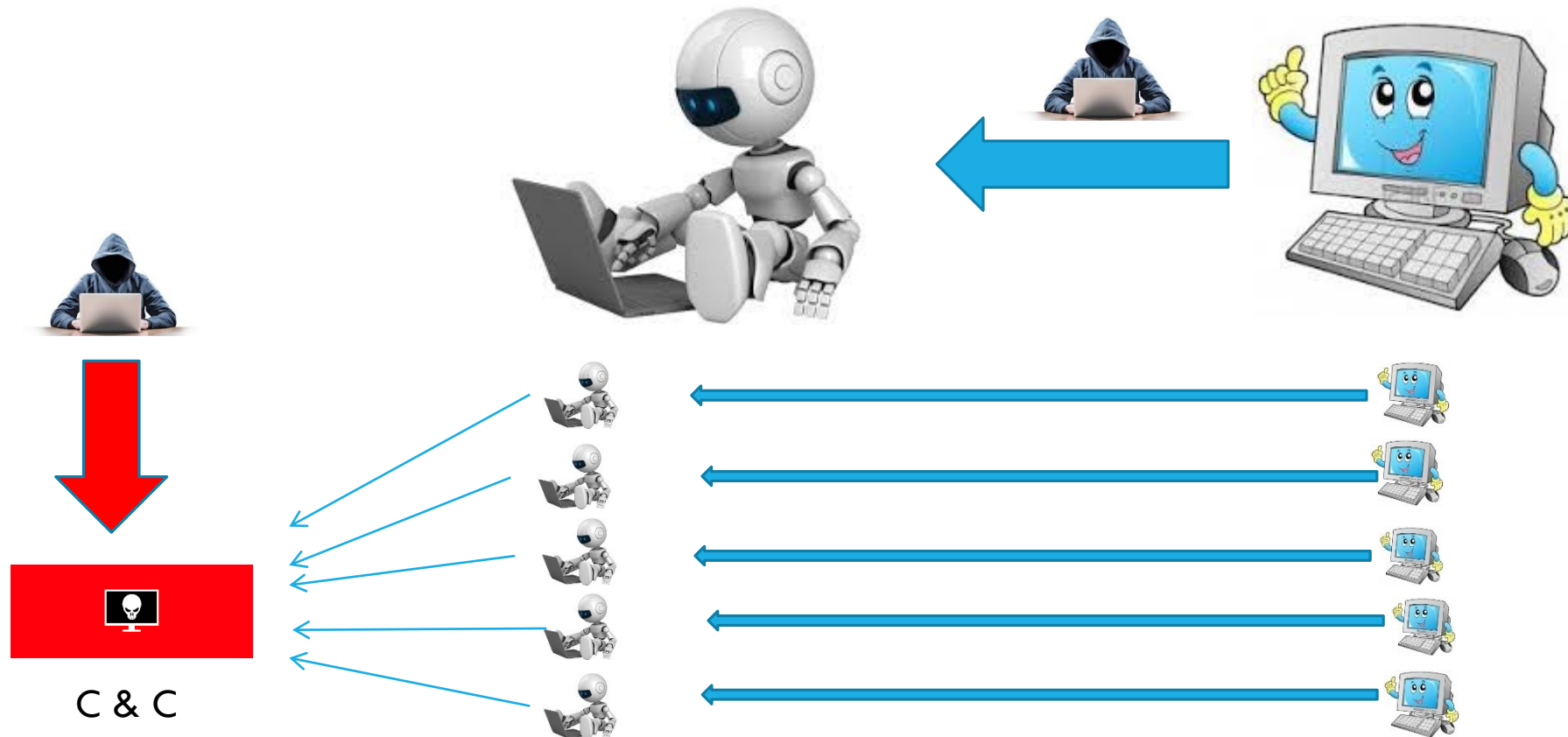
הרכיבים המעורבים:

- אתר אינטרנט כלשהו שנפרץ (למשל hotels.com)
- מחשב הקורבן שהופך לבוט
- מחשב התוקף
- תחנת ניהול הבוטים שמקים התוקף

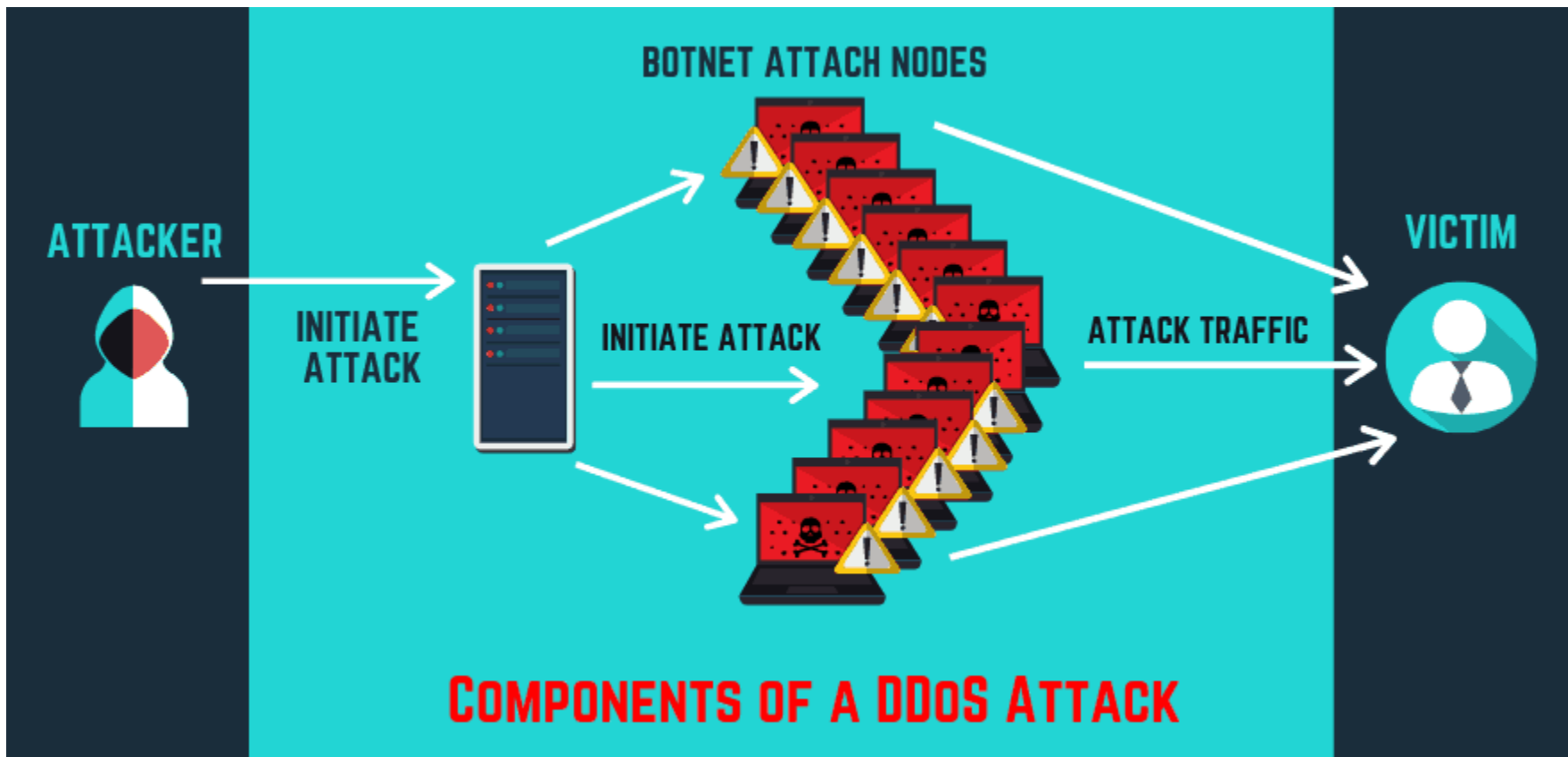
בוט – מחשב שנמצא תחת שליטה חסויה של האקר

שלבי ההתקפה בהתקפת DOS

התוקף הופך מחשב ל-BOT



לאחר "איסוף" צבא הבוטים ביצוע ההתקפה



אפשר גם לקנות התקפות מוכנות באינטרנט

<http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html>

How much costs a DDoS attack service? Which factors influence the final price?

March 26, 2017 By [Pierluigi Paganini](#)

How much costs a DDoS attack service? Kaspersky Lab published an analysis on the cost of a DDoS attack and services available in the black markets.

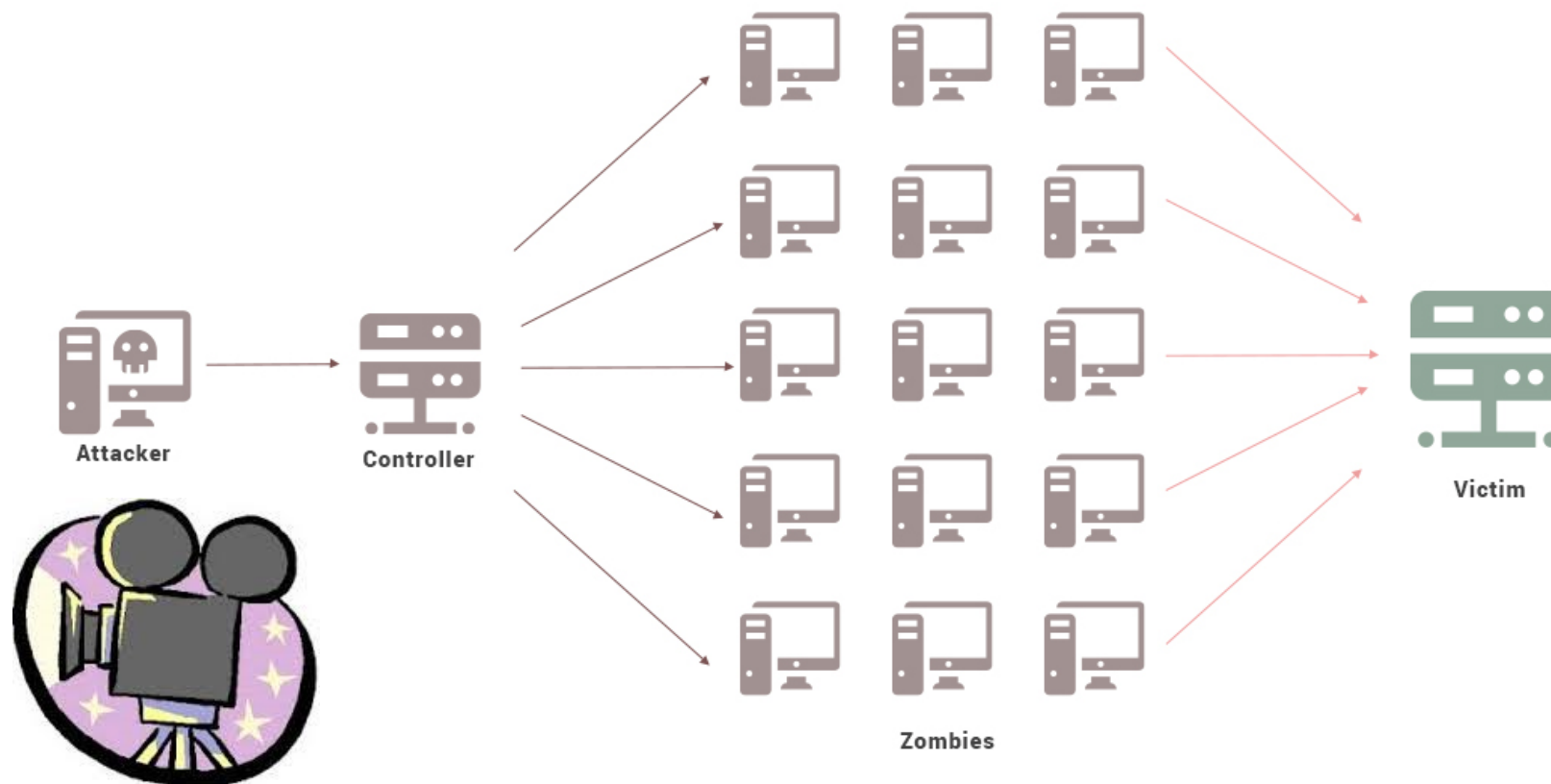
Kaspersky Lab has published an interesting analysis on the cost of DDoS attacks. The experts estimated that the cost to power a DDoS attack using a **cloud-based botnet of 1,000 desktops is about \$7 per hour**. A DDoS attack service typically goes for \$25 an hour, this means that the expected profit for crooks is around $\$25 - \$7 = \$18$ per hour.

Our Pricing

| 1 Month Basic | Bronze Lifetime | Gold Lifetime | Green Lifetime | Business Lifetime |
|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
| 5.00€ /month | 22.00€ Lifetime | 50.00€ Lifetime | 60.00€ Lifetime | 90.00€ lifetime |
| 1 Concurrent + | 1 Concurrent + | 1 Concurrent + | 1 Concurrent + | 1 Concurrent + |
| 300 seconds boot time | 600 seconds boot time | 1200 seconds boot time | 1800 seconds boot time | 3600 seconds boot time |
| 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity |
| Resolvers & Tools | Resolvers & Tools | Resolvers & Tools | Resolvers & Tools | Resolvers & Tools |
| 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support |
| Order Now | Order Now | Order Now | Order Now | Order Now |

התקפת DDOS - סרטון

התקפת DDOS - סרטון



ה

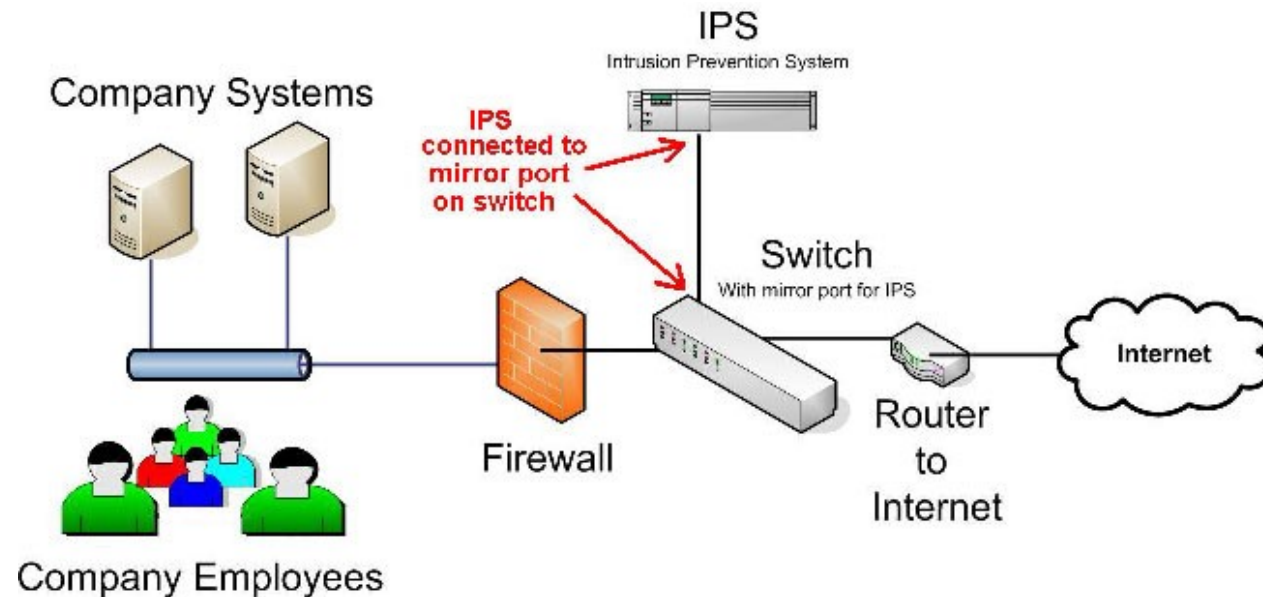
IDS , IPS - הגנה כנגד התקפות

IDS = INTRUDER DETECTION SERVICE

IPS = INTRUDER PROTECTION SERVICE

IDS - במקרה של התקפה על הארגון - מתריע בלבד

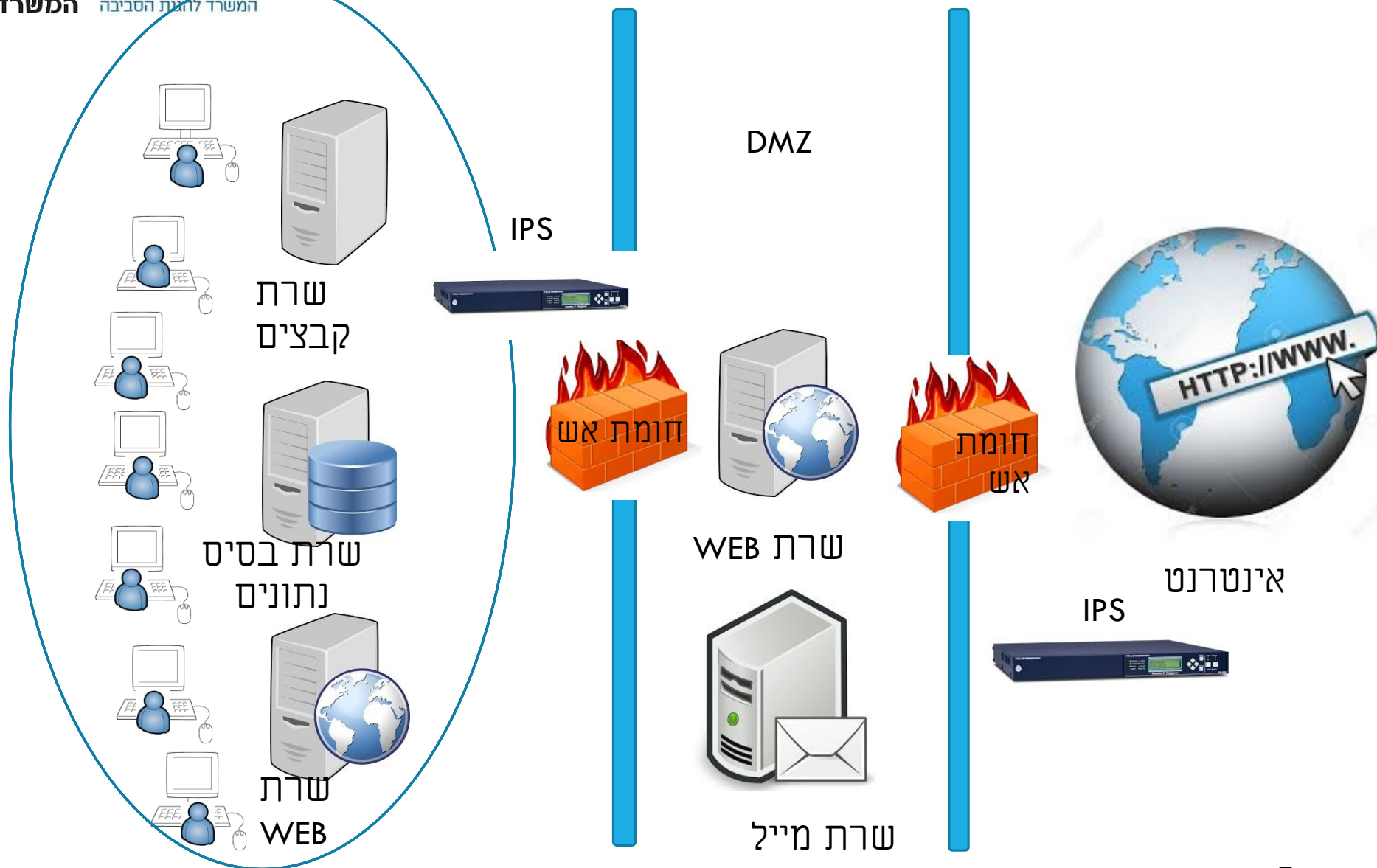
IPS - מתפקד כ-IDS ובמידת הצורך, אם קינפגנו אותו כך - יכול לחסום התקפות בצורה אקטיבית



הצורך:

- חסימת התקפות מחוץ לארגון
- חסימת התקפות מתוך הארגון

מיקום IPS ברשת ארגונית



בעיות בחסימת התקפות

ב-IPS יש לקחת בחשבון **חסימת תעבורה לגיטימית***

| מצב חסימה | סוג התעבורה | מצב |
|-----------------|---------------------|-----|
| מאפשר | לגיטימית | 1 |
| 1 בעיה חוסם | לגיטימית | 2 |
| 2 בעיה מאפשר | לא לגיטימית (התקפה) | 3 |
| חוסם | לא לגיטימית (התקפה) | 4 |

מי יותר גרוע לארגון ??

בעיה 1 או בעיה 2?

בעיות בחסימת התקפות במערכת IPS



בעולם ה-זו – השבתת גישה למערכת מידע

בעולם ה-זס – פס ייצור **מושבת!!**

איך להתגבר על החסרון? הפעלת IDS ולאחר קבלת התראה שיקול דעת אנושי מה לחסום בפועל



מה זה וירוס?

וירוס זה תוכנה העשויה מקוד מסוים שהיא בתוך קובץ הרצה מסוים ויש לו יכולות שכפול.

2 סוגים עיקריים:

- ❑ וירוס אקטיבי-וירוס שעובר ממחשב למחשב
- ❑ וירוס פאסיבי-שנשאר רק במחשב אחד.

פעולות לדוגמא שמבצעים וירוסים:

- ❖ וירוס שיכול למחוק את הקבצים במחשב או לשנות אותם
- ❖ וירוס ששולח מידע מהמחשב לעמדת הבקרה של ההאקר
- ❖ וירוס שמאפשר שליטה מרחוק על המחשב

1. תולעים

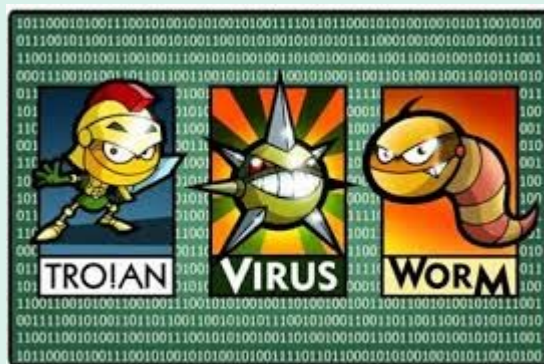
התולעים פועלים באופן עצמאי ומטרתם העיקרית היא להתפשט בכל המחשב ולהביא לקריסתו התולעת משכפלת מפיצה את עצמה ממחשב ומגיעה לנפחים אדירים.

2. סוס טרויאני

סוס טרויאני הוא תוכנה שיכולה לשנות קבצים או למחוק אותם או לגנוב באמצעות שליטה מרחוק ע"י מחשב מרוחק.

3. פצצות לוגיות

פצצות לוגית היא וירוס שפועל ע"פ תאריך/יום/שעה. הפצצה הלוגית עושה פעולה כלשהי שגורמת נזק למחשב.



4. תוכנת רוגלה (SPYWARE)

זוהי תוכנה אשר מסוגלת להציג למישהו במחשב מרוחק מידע על המחשב שתוכנה זו נכנסה אליו. בניגוד לסוס טרויאני, תוכנה זו לא מסוגלת לשנות או למחוק קבצים.



5. וירוסי מאקרו

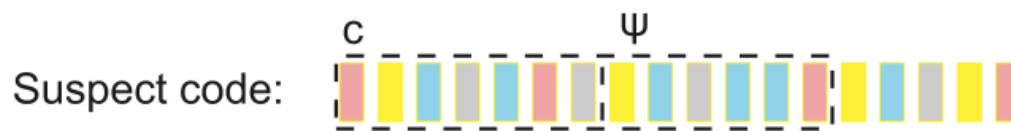
וירוסים אלו מתחבאים בתוך מסמכים סטנדרטיים כמו וורד או אקסל. וירוסים אלו יכולים לגרום למחיקת קבצים או הרס מערכת ההפעלה

איזה סוג של וירוס לא הזכרנו כאן ?? !!!



איך מתגוננים ?

חברות אבטחת מידע מייצרות חתימות לוירוסים הידועים



חתימות:



מה החסרונות: מוגנים בפני וירוסים ידועים בלבד



ZERO DAY



מהו וירוס ZERO DAY?

וירוס לא ידוע לחברות האנטי וירוס ולכן לא מופיע בקובץ החתימות של האנטי וירוס המותקן במחשבינו.

איך מייצרים וירוס ZERO DAY ?

2 אפשרויות:

1. יוצרים וירוס חדש לגמרי שלא מוכר עדיין (לכן נקרא ZERO DAY כי זה היום הראשון שלו בחוץ)

2. לוקחים וירוס קיים ויוצרים ממנו "מוטציה" לעיתים מזוהה ע"י קובץ החתימות של ה-AV ולעיתים לא

דוגמאות ל - ZERO DAY

וירוסי כופרה שונים



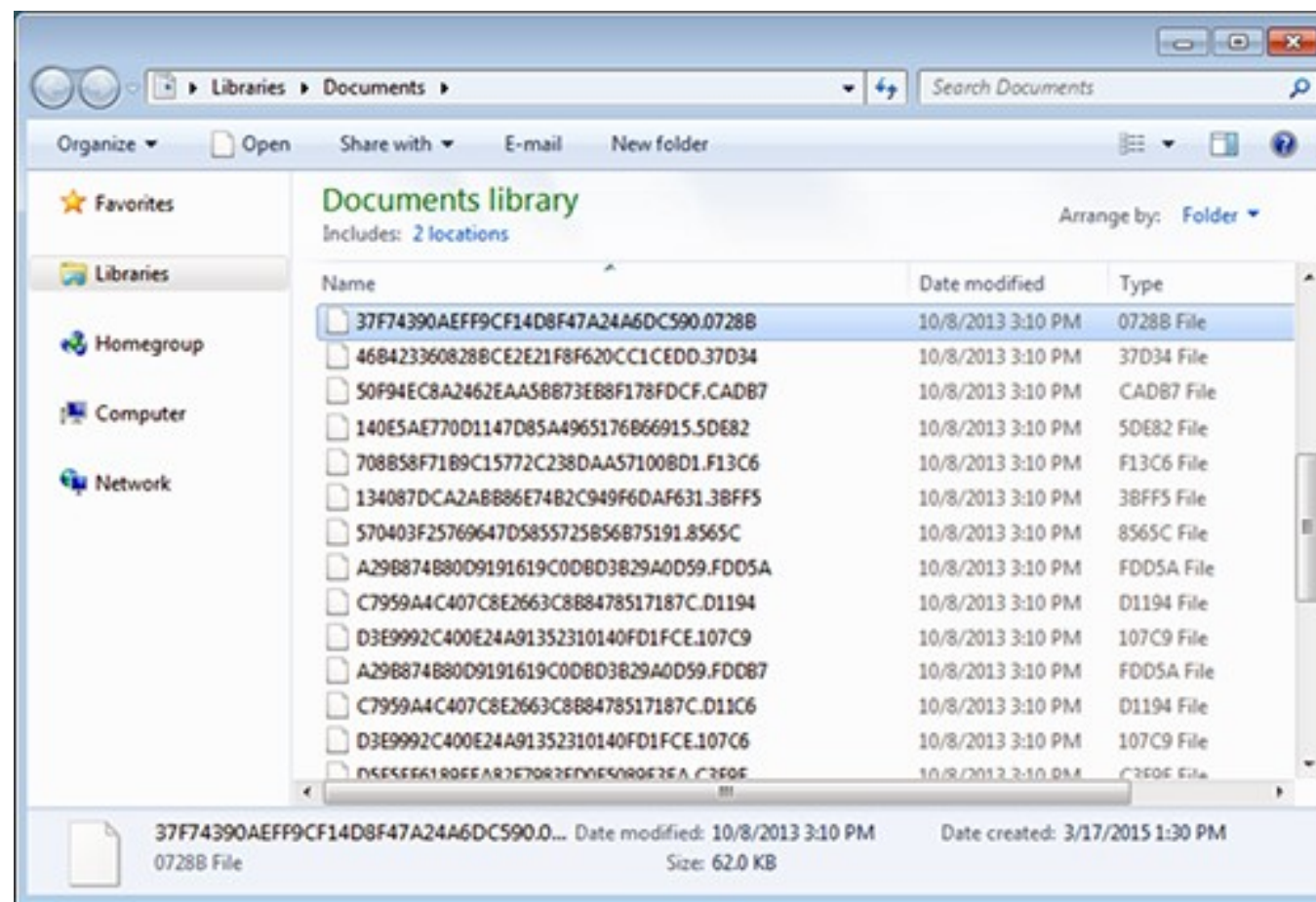
✓ קיים "שירות לקוחות"

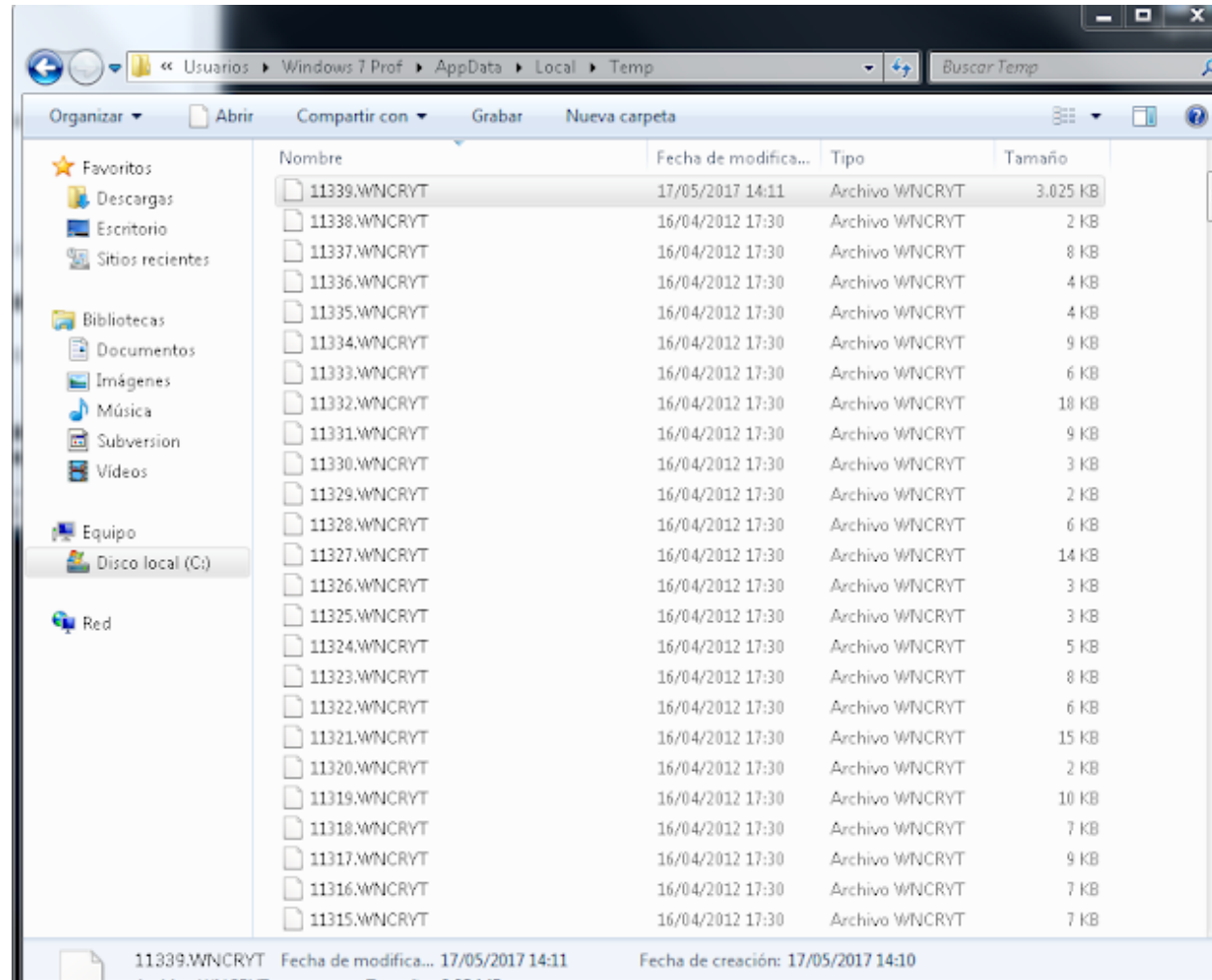
✓ הדרכה לרכישת ביטקוין

✓ המלצה להסיר אנטי-וירוס כדי שהכופרה לא תמחק

✓ אופציה להצגת המסמכים המוצפנים

לאחר הצפנת הקבצים ע"י וירוס כופרה הם נראים כך:



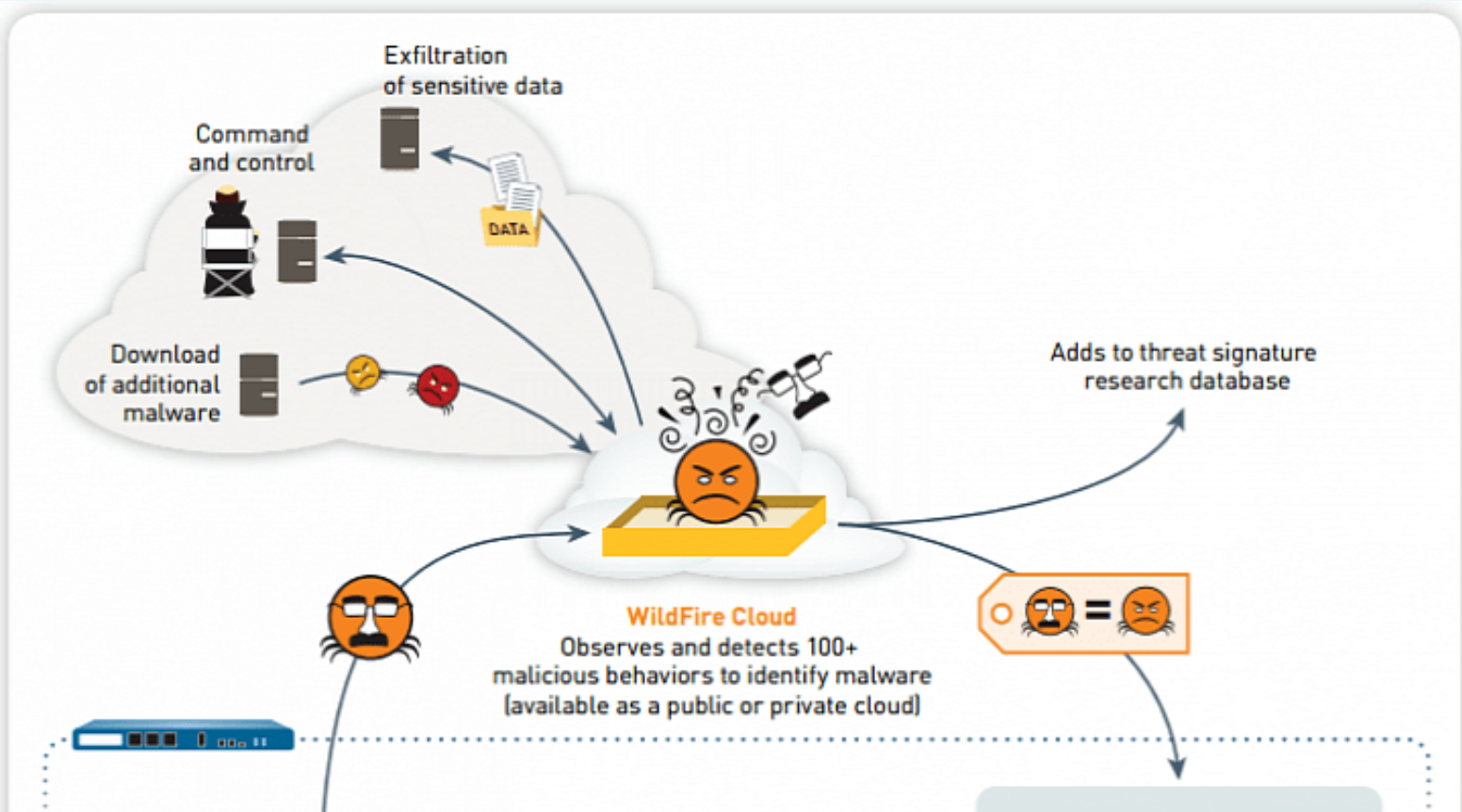


איך מגינים בפני ZERO DAY ?

SAND BOX – ארגז חול



איך מגינים SAND BOX – חול



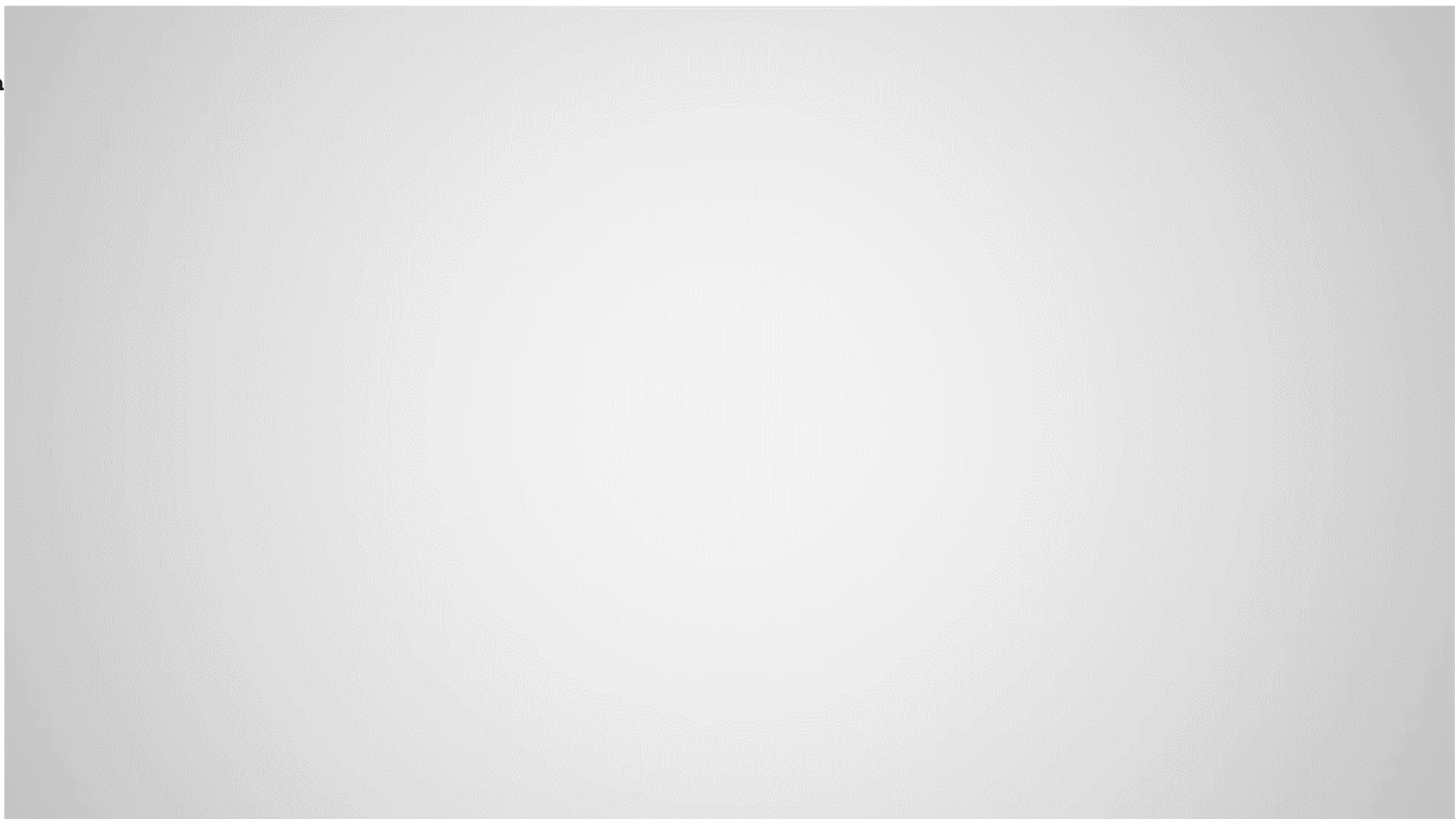
מאפיינים חשודים:

- העברת מידע מחוץ לארגון
- תקשורת עם C & C
- הורדת קבצים פנימה לארגון
- שינוי ערכים ב-REGISTRY
- נגיעה / שימוש / שינוי בקבצי מערכת
- התנהגות שלא מתאימה לקובץ המדובר

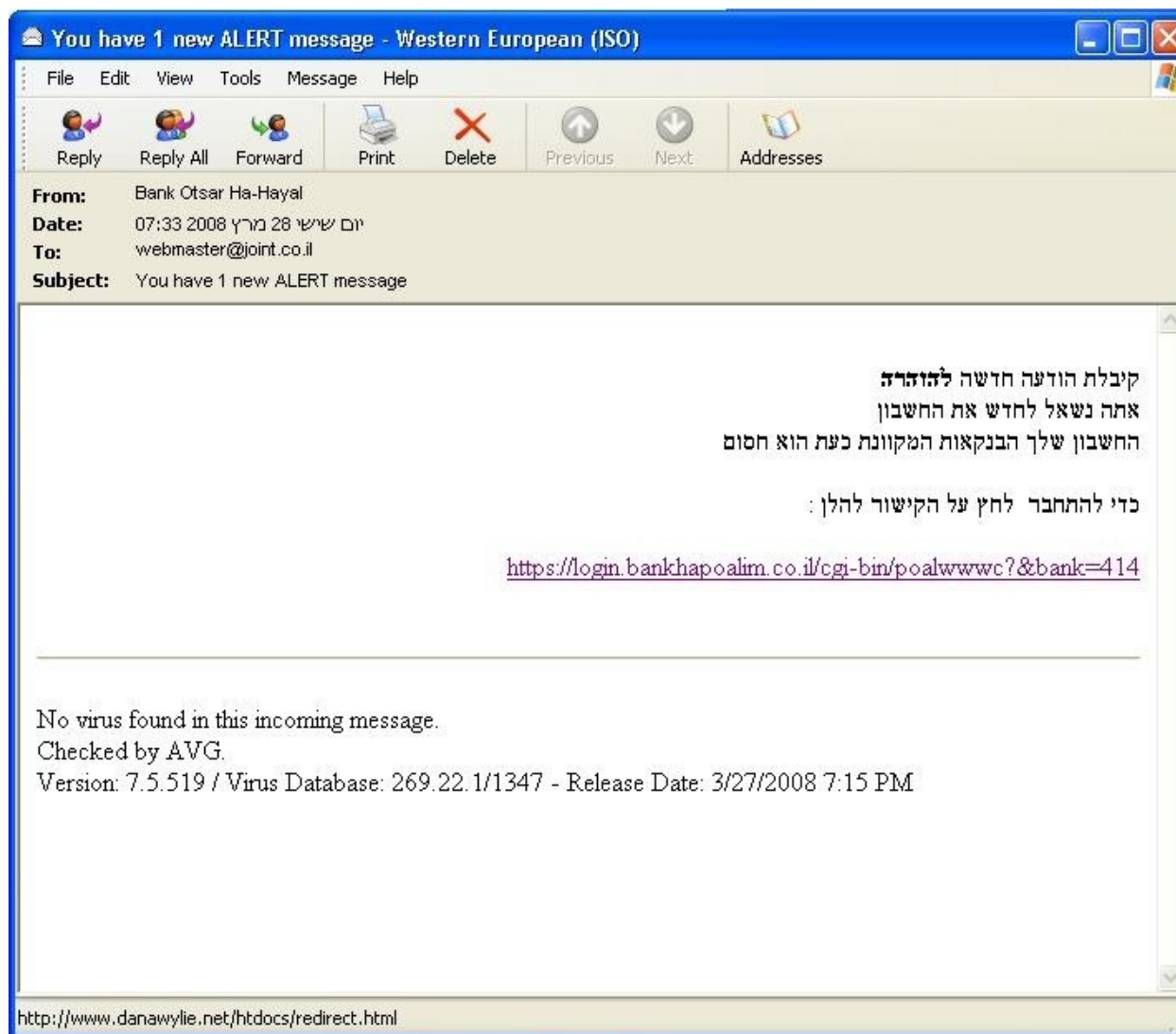
SAND BOX – ארגז חול

כיצד דפדפן כרום עושה שימוש בארגז חול – סרטון





התקפות פישינג



אתם מקבלים דוא"ל:

ואז מתקבל הדף הבא.....

תמיכה לשירותך

בנק אוצר החייל

מידע למגוי חדש

הדגמות

הצטרפות לשירות

הטבות באינטרנט

ברוכים הבאים לאוצר באינטרנט

לצורך כניסה לשירות יש להקליד את הפרטים המזהים וללחוץ על "כניסה לחשבוןך".

קוד משתמש : ?

ת.ז. : ?

סיסמא : ?

כניסה לחשבוןך

נחסמה/ שכחת סיסמתך?

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

לחצו כאן לפרטים נוספים.

© כל הזכויות שמורות לבנק הפועלים תנאי גישה

תמיכה לשירותך

בנק אוצר החייל

מידע למנוי חדש

הדגמות

הצטרפות לשירות

הטבות באינטרנט

ברוכים הבאים לאוצר באינטרנט

טופס און-ליין עבור חידוש השירותים
נא לספק את המידע להלן. מילוי כל המידע חובה, פרט למקרה בו קיימים הנחיות במובן של

שם מלא :

כתובת :

יישוב :

כתובת דוא"ל :

מספר כרטיס :

תוקף הכרטיס :

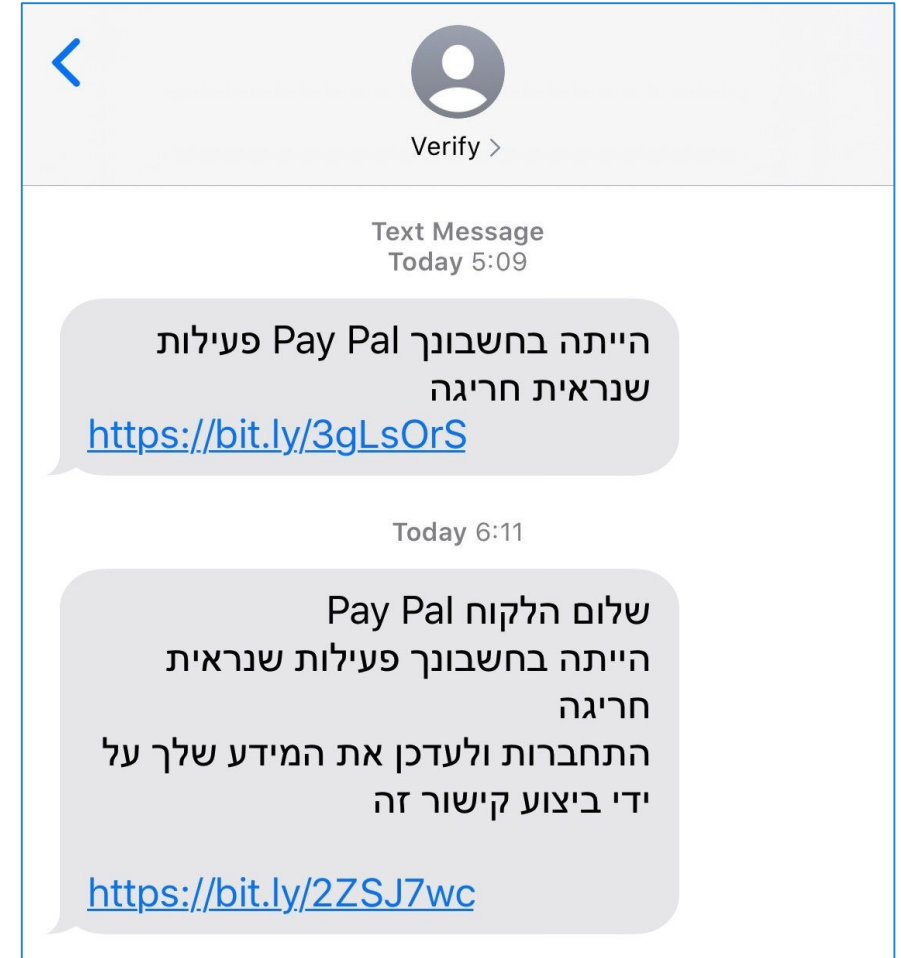
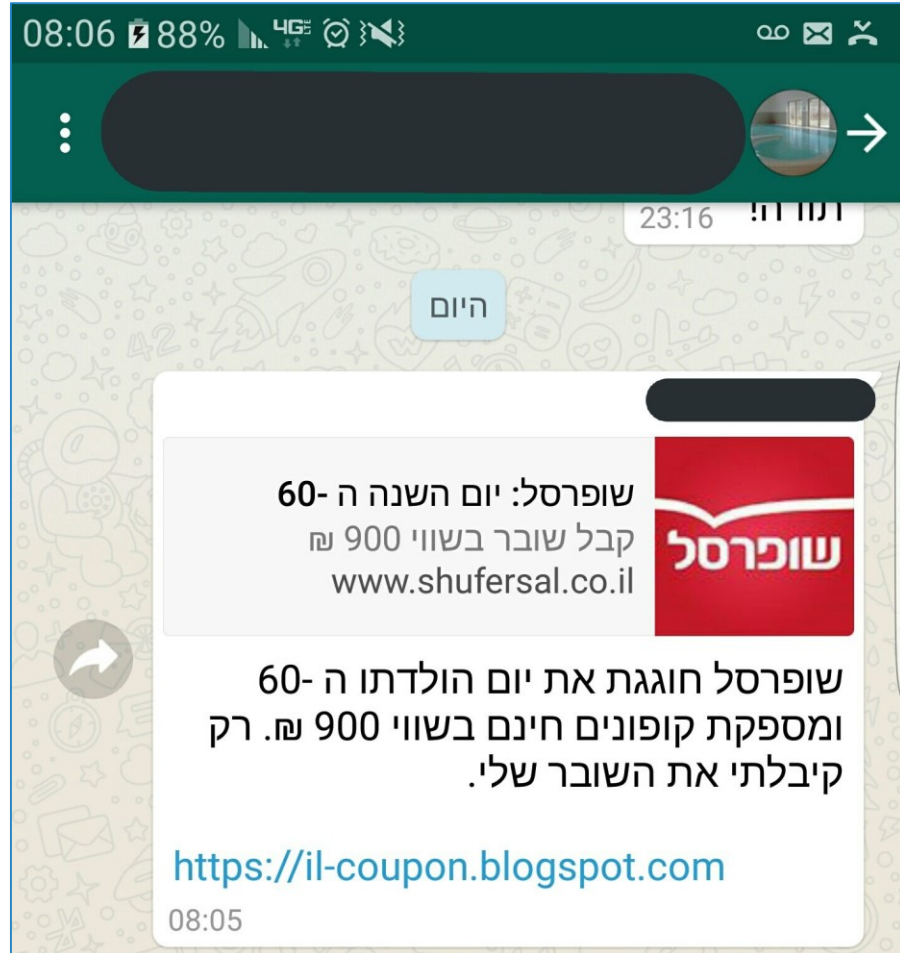
מספר זהות אישי :

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

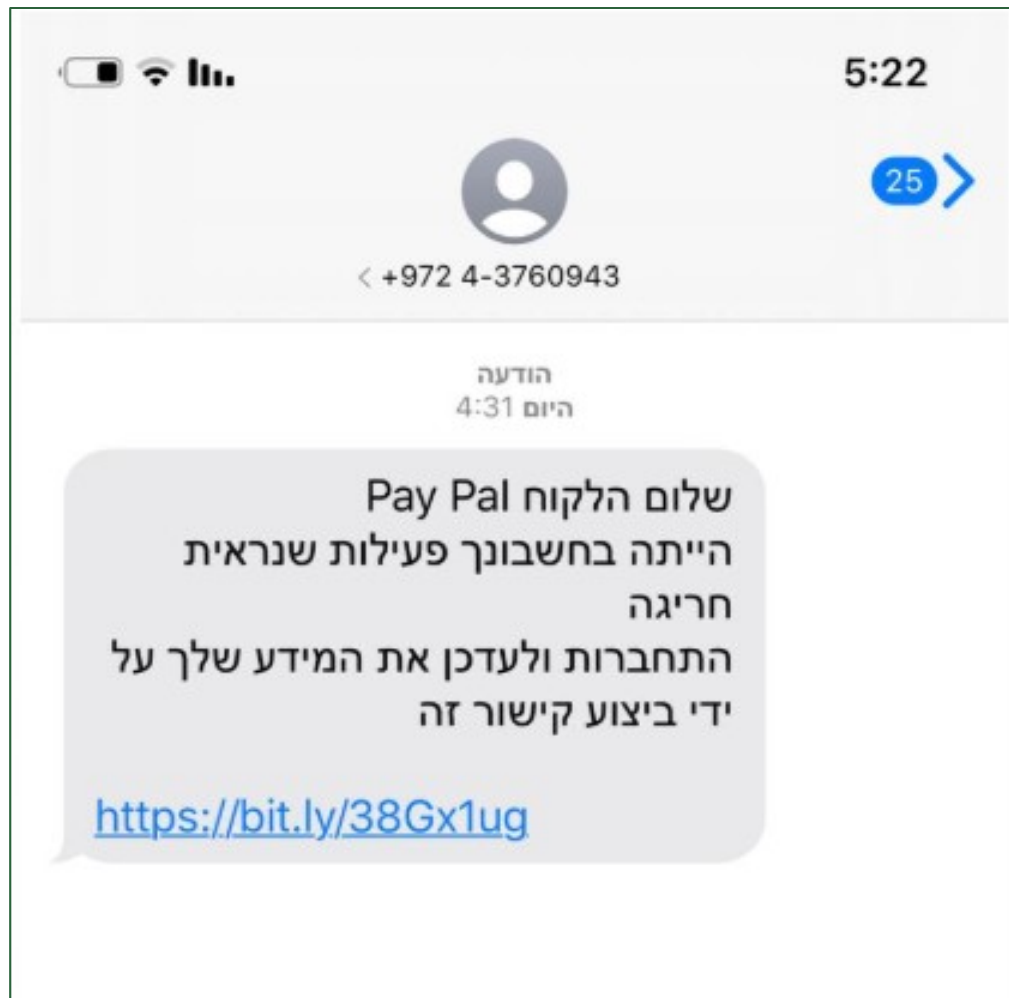
[לחצו כאן לפרטים נוספים...](#)


© כל הזכויות שמורות לבנק הפועלים [תנאי גישה](#)

לאחר שהקורבן מזין את הפרטים גם כאן, הוא מופנה לעמוד שמוסר לו להמתין יומיים עד שהמידע יעודכן.



יום חמישי בבוקר 9.7.2020





Deceptive site ahead

Attackers on **theredgone.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). [Learn more](#)

💡 To get Chrome's highest level of security, [turn on enhanced protection](#)

[Hide details](#) [Back to safety](#)

Google Safe Browsing recently [detected phishing](#) on theredgone.com. Phishing sites pretend to be other websites to trick you.

You can [report a detection problem](#) or, if you understand the risks to your security, [visit this unsafe site](#).

<https://www.virustotal.com/gui/>

VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE URL SEARCH

theredgone.com

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

Want to automate submissions? [Check our API](#), free quota grants available for new file uploads

4 / 79
Community Score

4 engines detected this URL

http://theredgone.com/
theredgone.com

200 Status | text/html Content Type | 2020-07-11 03:10:37 UTC 7 months ago

| DETECTION | DETAILS | COMMUNITY |
|---------------------|-----------|---------------------------|
| CyRadar | Malicious | ESET Phishing |
| Google Safebrowsing | Phishing | Sophos Malicious |
| ADMINUSLabs | Clean | AegisLab WebGuard Clean |
| AlienVault | Clean | Antiy-AVL Clean |
| Artists Against 419 | Clean | Avira (no cloud) Clean |
| BADWARE.INFO | Clean | Baidu-International Clean |
| BitDefender | Clean | BlockList Clean |
| Blueliv | Clean | Botvrij.eu Clean |
| Certego | Clean | CINS Army Clean |
| CLEAN MX | Clean | CRDF Clean |
| CyberCrime | Clean | Cyren Clean |
| desenmascara.me | Clean | DNS8 Clean |

זהירות: ישראלים תחת מתקפת פשינג

משעות הבוקר נרשמו אלפי נסיונות להפיל ישראלים בפח באמצעות הודעות SMS שמדווחות על בעייה כביכול בחשבון הפייפאל שלהם. לפי בדיקת ynet המקור הוא ככל הנראה קבוצה ערבית שמבצעת את המתקפה מאתר בלוב. מה לעשות? כלום. פשוט לא ללחוץ על הקישור



טל שחף פורסם: 11.07.20, 12:27

קיבלתם הודעה על בעייה בחשבון הפייפאל (Paypal) שלכם? אל תלחצו על הקישור! אלפי משתמשי טלפון ישראלים קיבלו מאז שעות הבוקר המוקדמות הודעות SMS שמתריעות כביכול על בעייה בחשבון הפייפאל. מדובר בקמפיין דיג (פשינג), שנועד לגנוב את פרטי חשבונות הפייפאל במסווה של עדכון פרטים בשירות לקוחות. הנסיונות האלה נחסמו במהירות וככל הידוע בשלב זה כבר לא ניתן לגשת לדפים המסוכנים.

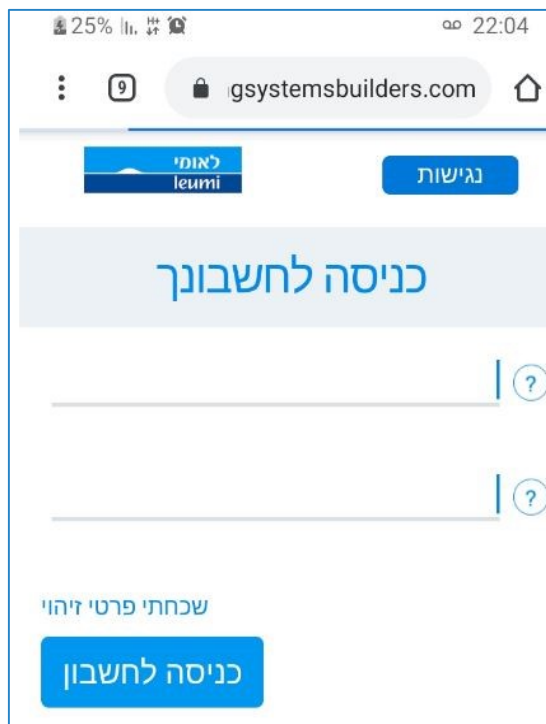
מבדיקה של ynet עולה כי מאחורי המתקפה מסתתרת ככל הנראה קבוצה ערבית או מישהו שמסווה את עצמו כקבוצה כזו. המתקפה כולה נעשית מתוך אתר של ארגון לובי שעוסק באיכות הסביבה, שייתכן שכלל לא יודע שהאתר שלו משמש לעקוץ ישראלים.



האתר שמשמש למתקפת הפשינג בישראל (צילום מסך)

התקפת פשינג דרך אתר איכות סביבה המשמש לעוקץ

איך יוצרים תקיפת פישינג?



✓ הפעלת כלי: SETOOL (כחלק מחבילת כלים שניתן להוריד חינם)

✓ מעתיקים אליו לינק אליו מבקשים הזדהות למשל אתר בנק לאומי

✓ הכלי לוקח את דף ההזדהות של האתר + את דף האתר ויוצר לינק מוכן שמדמה את דף האתר.

✓ שולחים את הלינק ל"תפוצת נאטו" – תפוצה רחבה ככל האפשר בהנחה ש- 1% מהקורבנות מכניס פרטי משתמש וסיסמא

✓ פרטי ההזדהות (שם משתמש וסיסמא) מועברים לכתובת התוקף