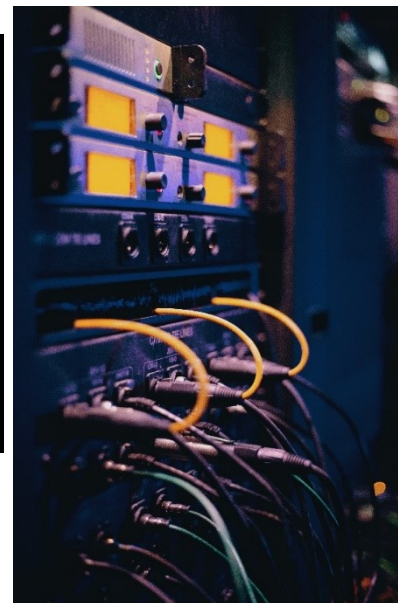


# מושגי ייסוד בסייבר – חלק ג



Yosi Shavit MBA, CISO, CISM, CDPSE - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: [yosish@gmail.com](mailto:yosish@gmail.com) , [yosish@sviva.gov.il](mailto:yosish@sviva.gov.il)



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

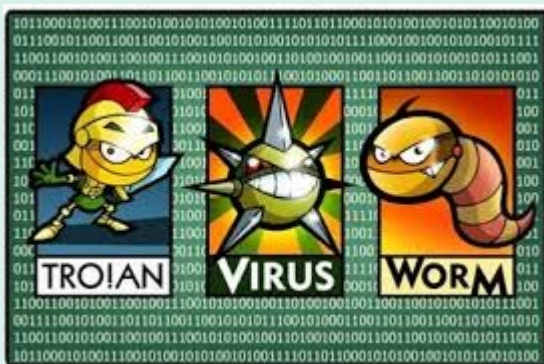
התולעים פועלים באופן עצמאי ומטרתם העיקרית היא להתפשט בכל המחשב ולהביא לקריסתו התולעת משכפלת מפיצה את עצמה ממחשב ומגיעה לנפחים אדירים.

## 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

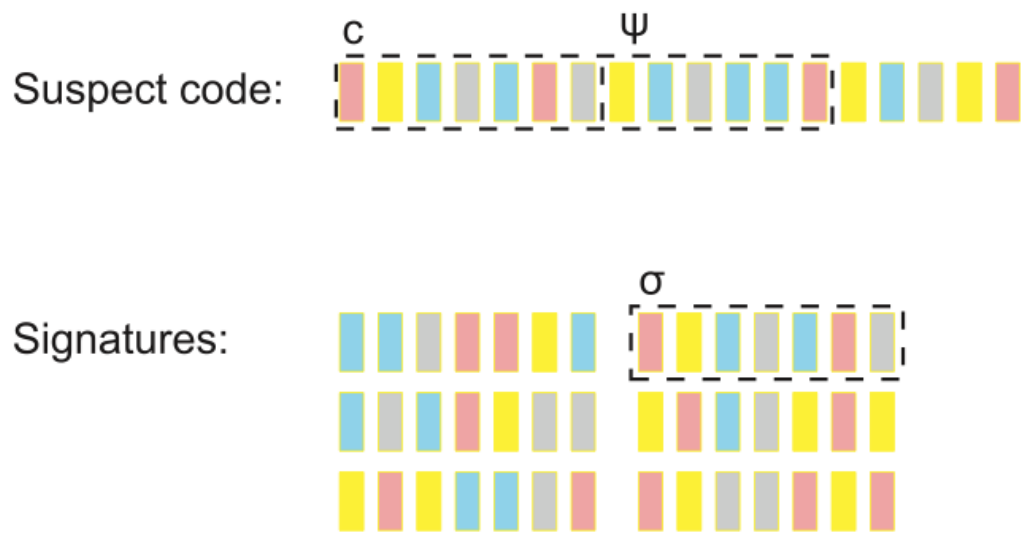
וירוסים אלו מתחבאים בתוך מסמכים סטנדרטיים כמו וורד או אקסל. וירוסים אלו יכולים לגרום למחיקת קבצים או הרס מערכת ההפעלה

**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"

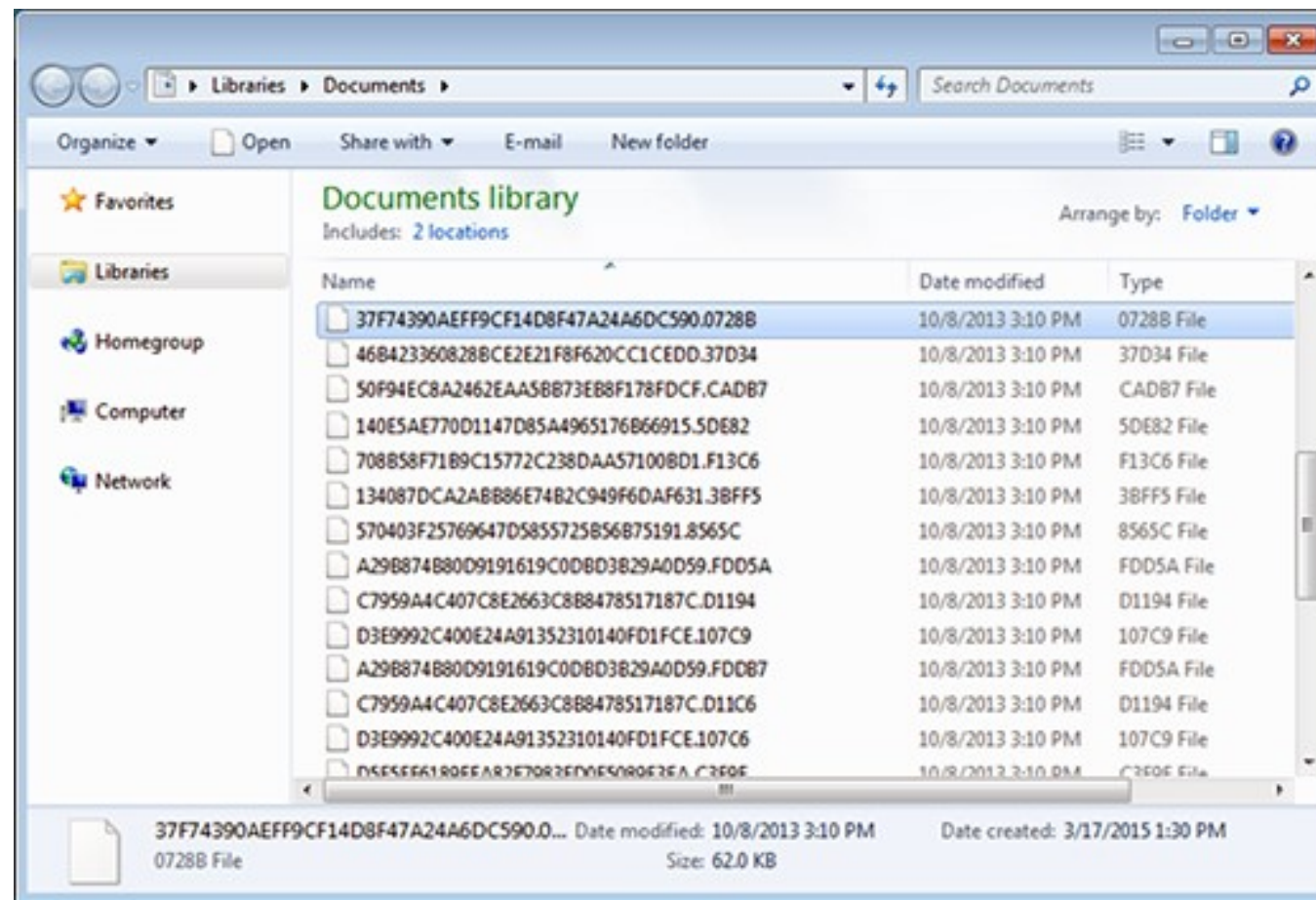
✓ הדרכה לרכישת ביטקוין

✓ המלצה להסיר אנטי-וירוס כדי שהכופרה לא תמחק

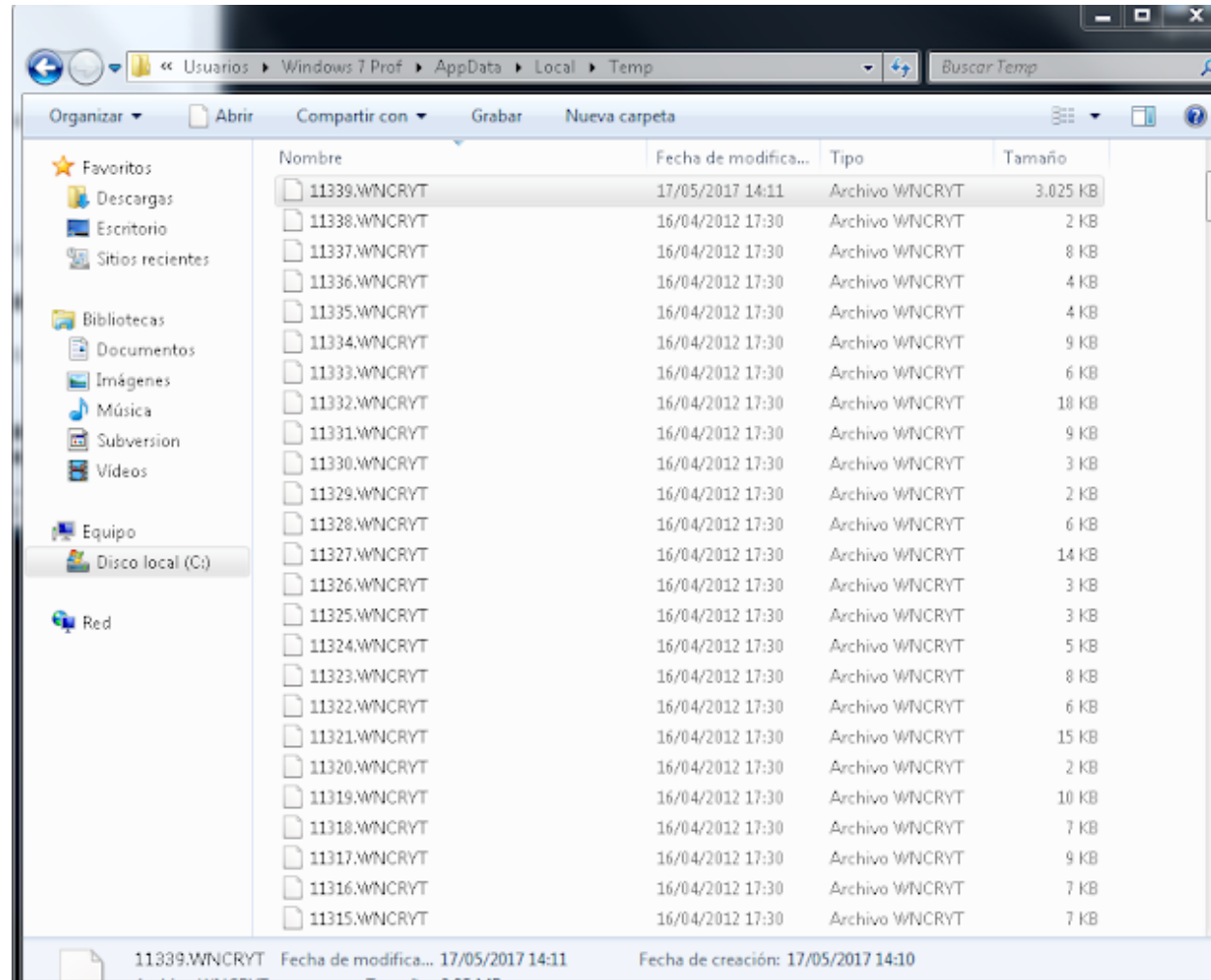
✓ אופציה להצגת המסמכים המוצפנים

# דוגמאות ל- ZERO DAY

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





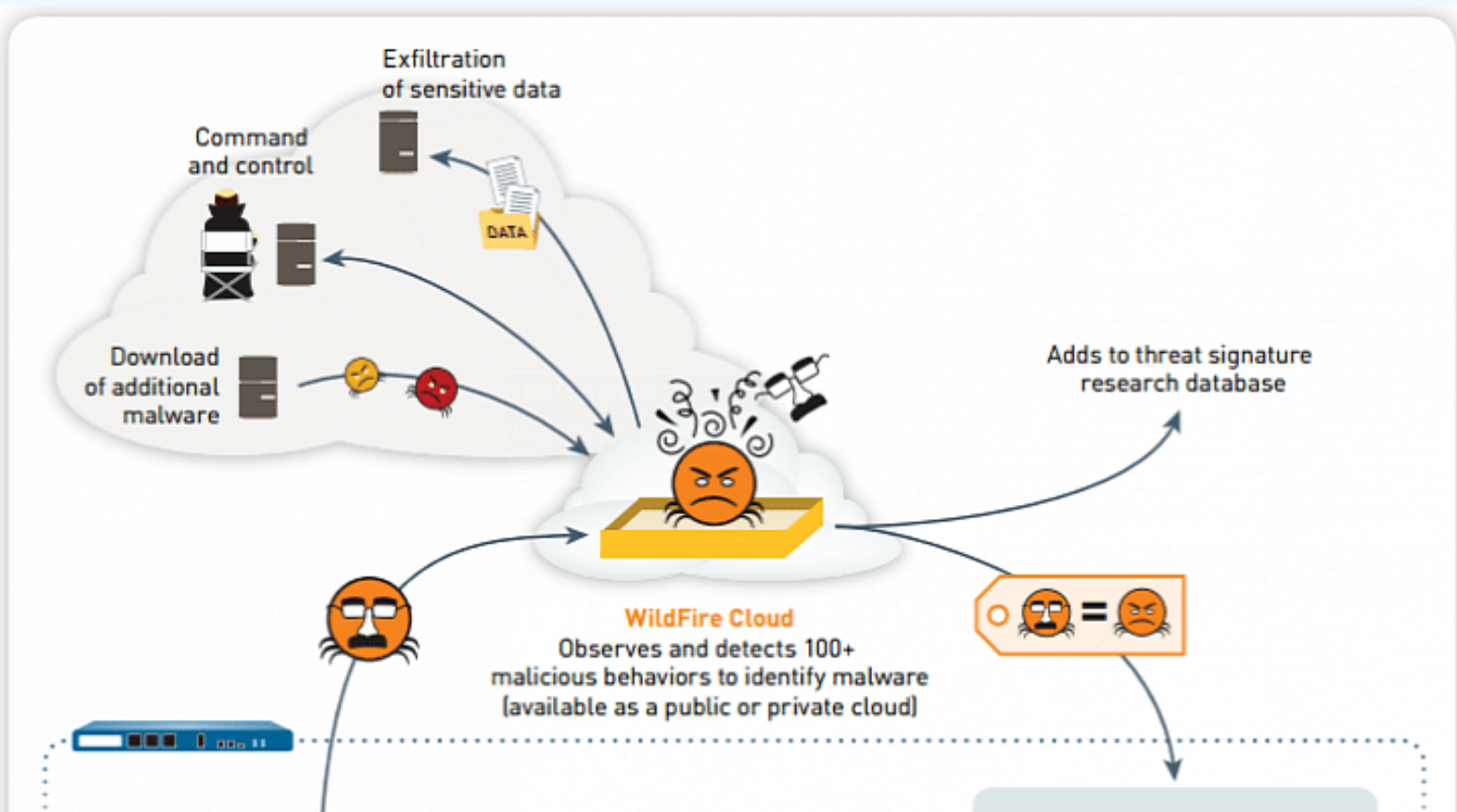


# איך מגינים בפני ZERO DAY ?

## SAND BOX – ארגז חול



# איך מגינים SAND BOX – חול



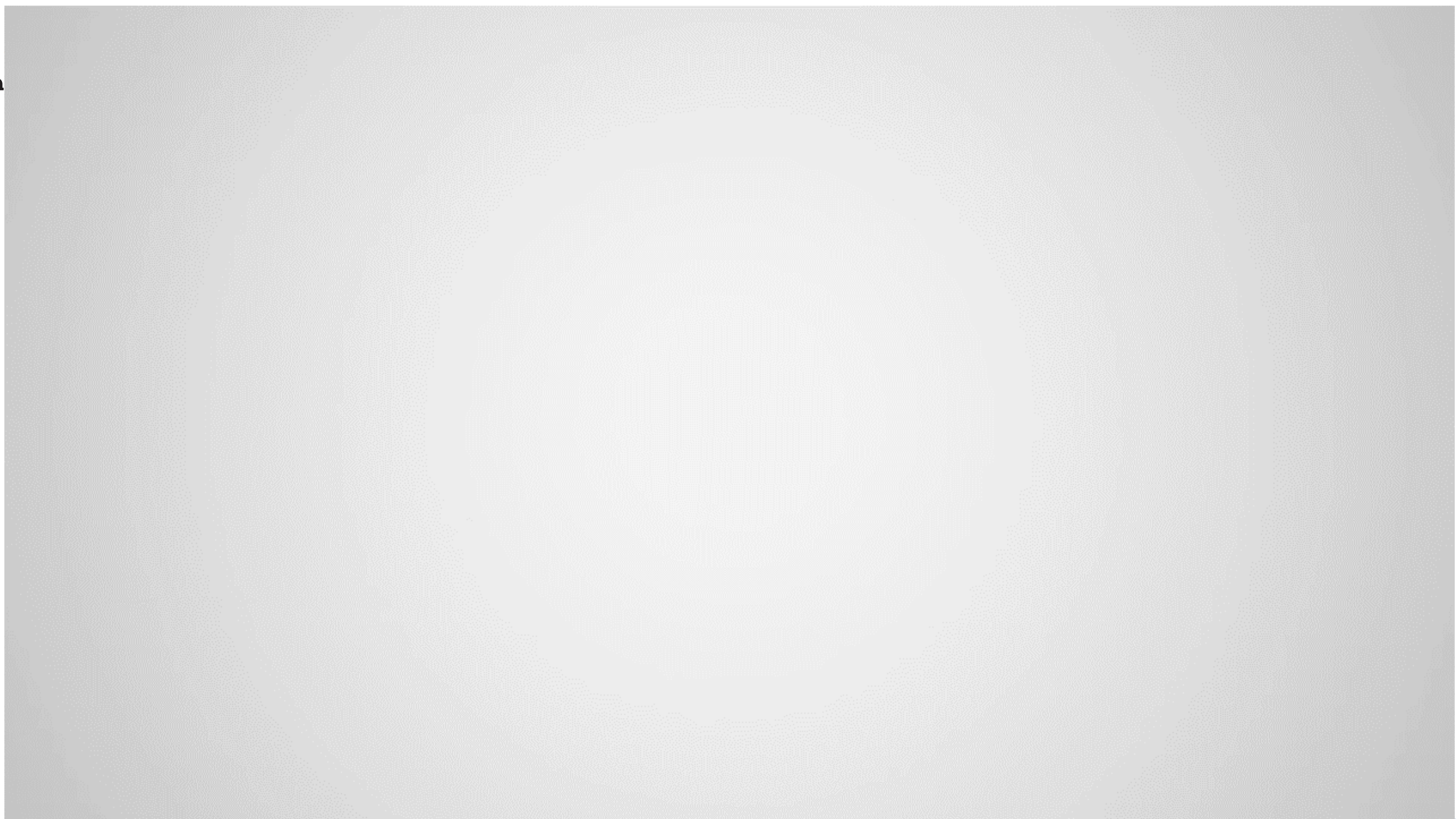
מאפיינים חשובים:

- 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

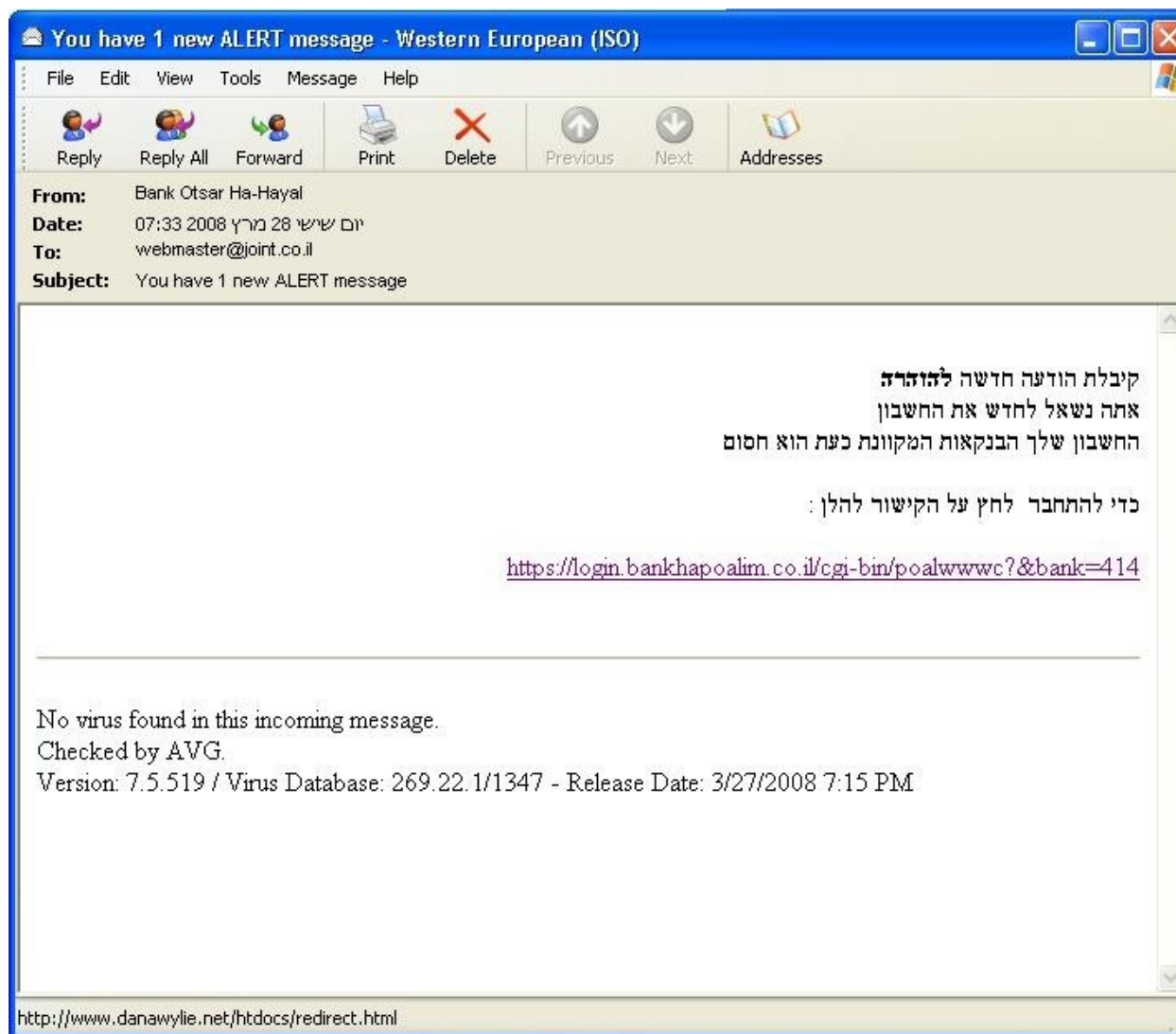
## SAND BOX – ארגז חול

כיצד דפדפן כרום עושה שימוש בארגז חול – סרטון





# התקפות פישינג



אתם מקבלים דוא"ל:

# ואז מתקבל הדף הבא.....

תמיכה לשירותך

בנק אוצר החייל

**ברוכים הבאים לאוצר באינטרנט**

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

קוד משתמש : ?  
ת.ז. : ?  
סיסמא : ?

נחסמה/ שכחת סיסמתך? [כניסה לחשבוןך](#)

אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר. לחצ'י 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 :

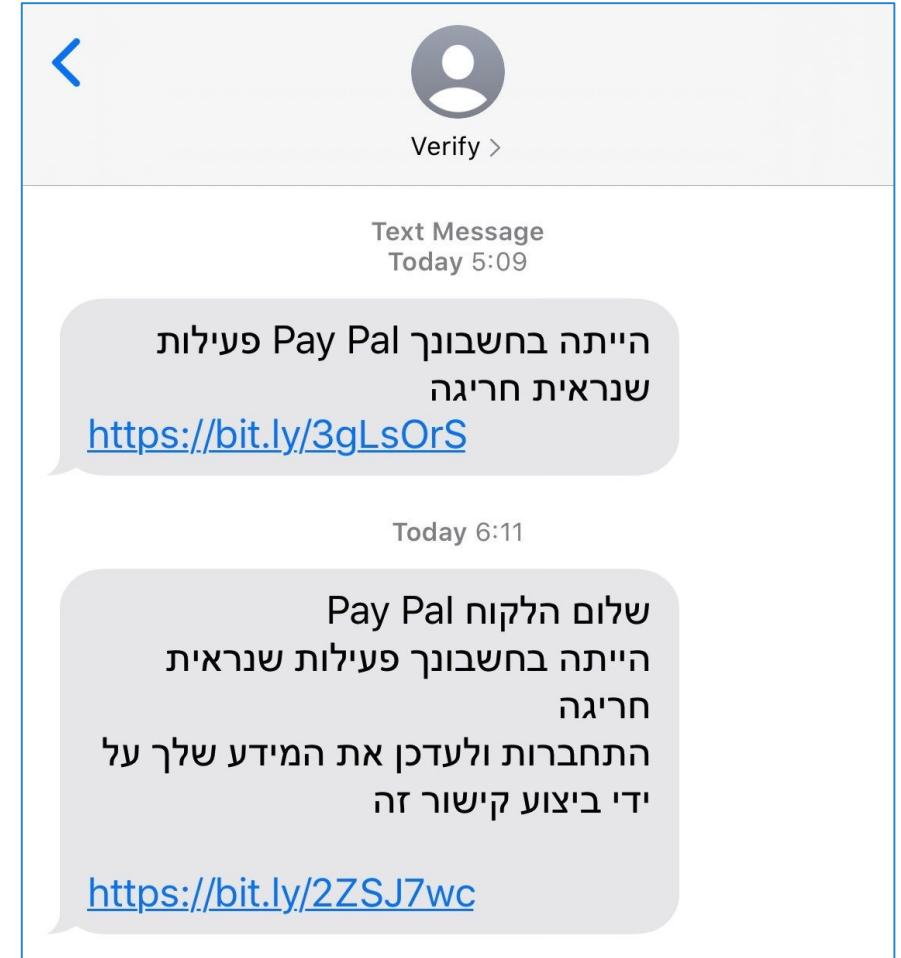
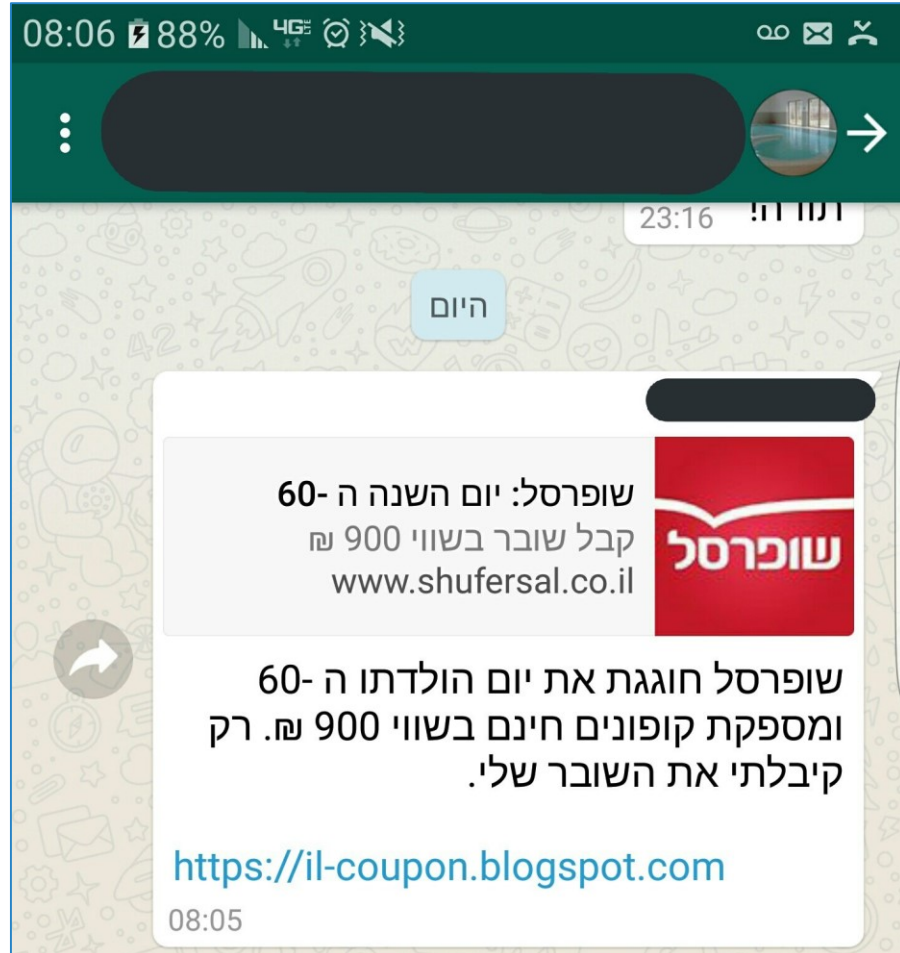
אתר זה מאובטח בשיטות אבטחת המידע המתקדמות ביותר.

[לחצ'י כאן לפרטים נוספים...](#)

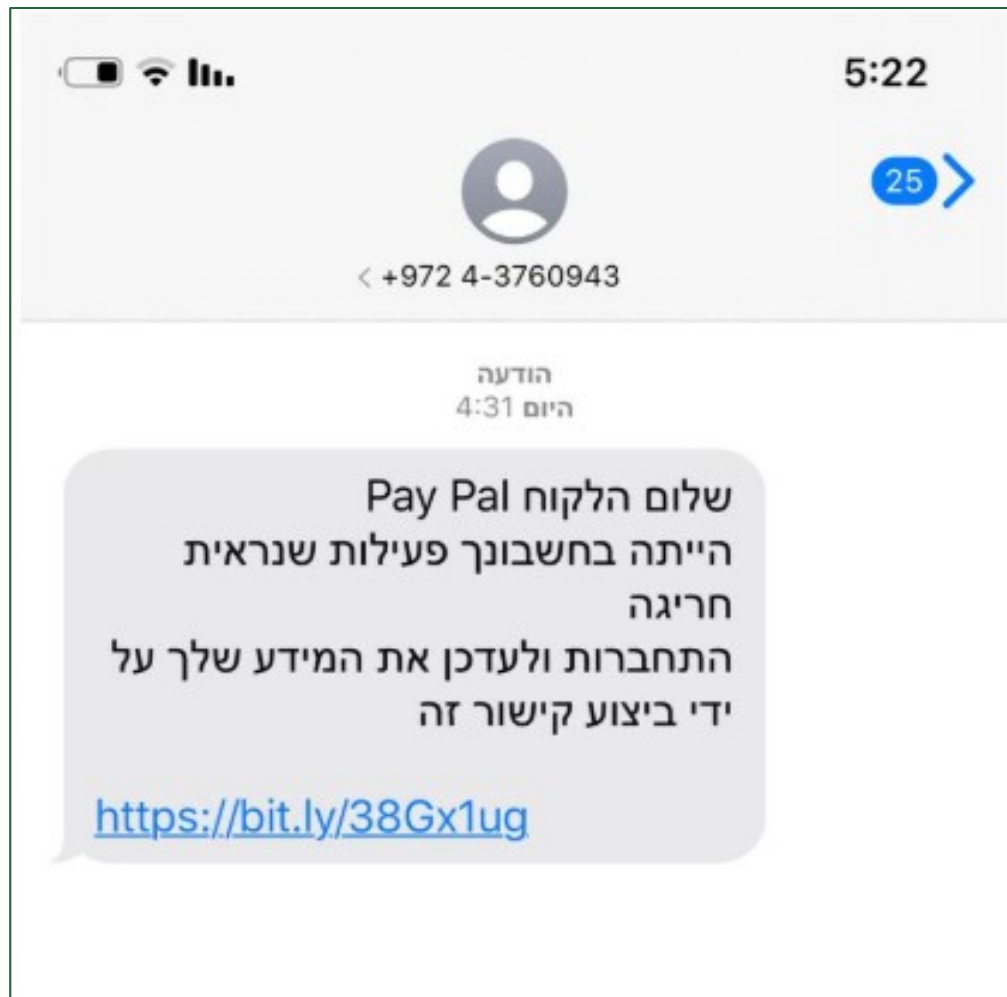
© כל הזכויות שמורות לבנק הפועלים [תנאי גישה](#)


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](#)

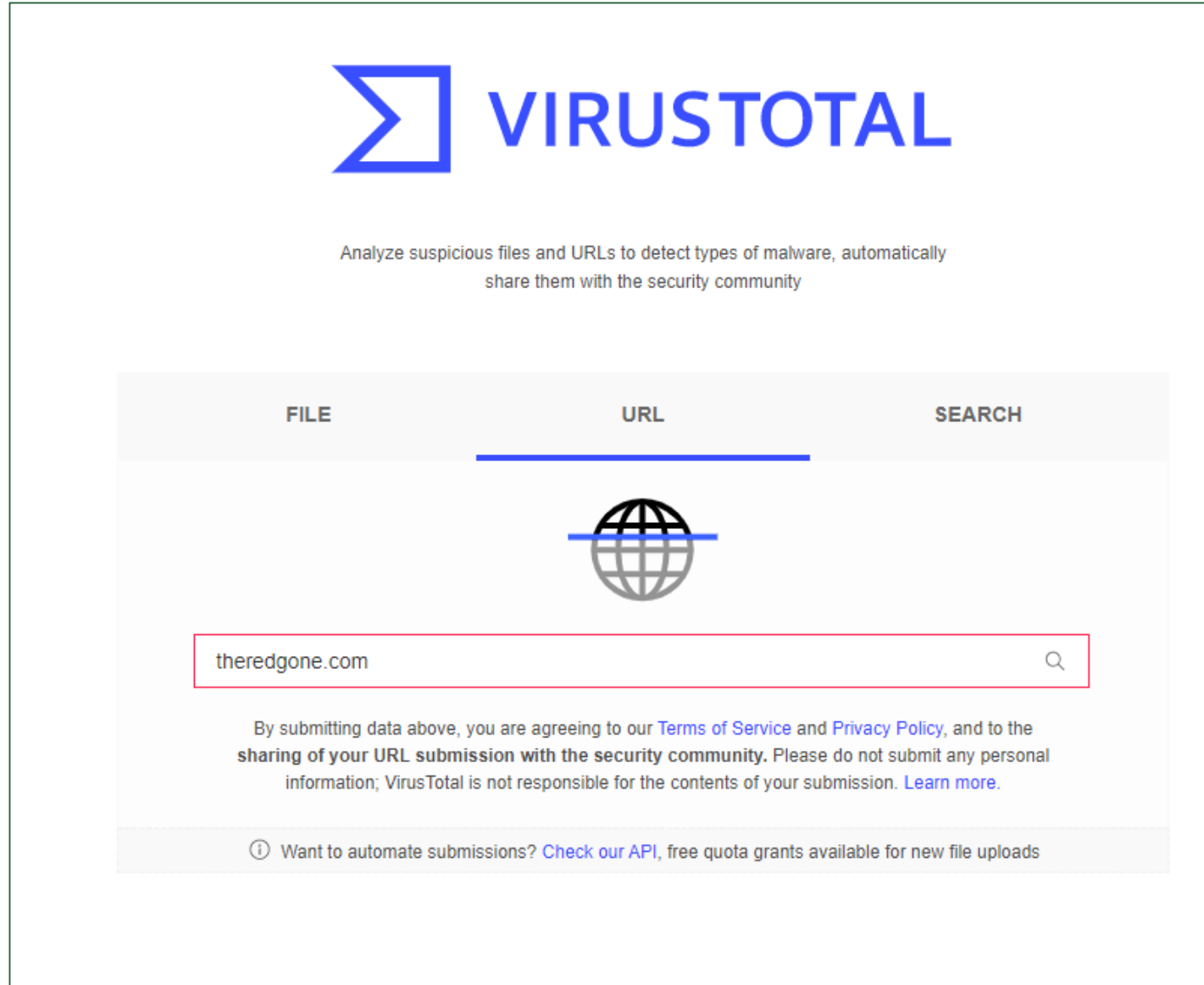
 To get Chrome's highest level of security, [turn on enhanced protection](#)

[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/>



The screenshot shows the VirusTotal website interface. At the top, the VirusTotal logo is displayed in blue. Below the logo, the text reads: "Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community". The interface has three tabs: "FILE", "URL", and "SEARCH". The "URL" tab is selected and highlighted with a blue underline. Below the tabs, there is a search input field containing the text "theredgone.com". Below the search field, there is a disclaimer: "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](#)." At the bottom of the interface, there is a link: "Want to automate submissions? [Check our API](#), free quota grants available for new file uploads".

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

Community Score: ?

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 דיגי (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.

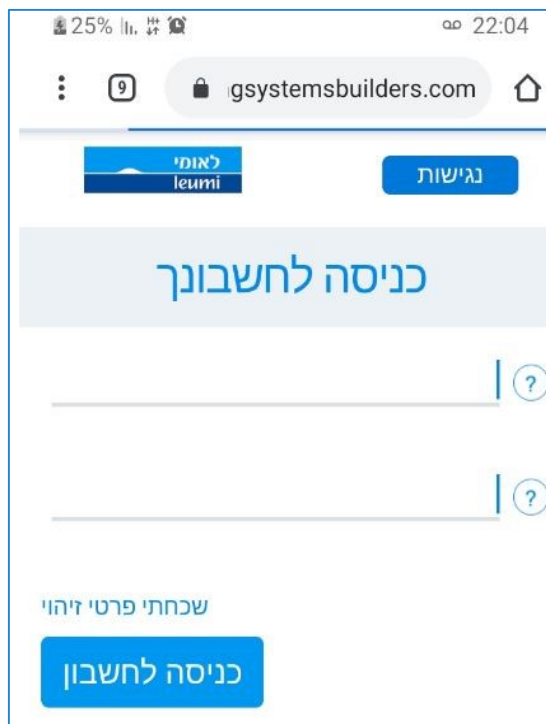
מבדיקה של ynet עולה כי מאחורי המתקפה מסתתרת ככל הנראה קבוצה ערבית או מישהו שמסווה את עצמו כקבוצה כזו. המתקפה כולה נעשית מתוך אתר של ארגון לובי שעוסק באיכות הסביבה, שייתכן שכלל לא יודע שהאתר שלו משמש לעקוץ ישראלים.



האתר שמשמש למתקפת הפשינג בישראל (צילום מסך)

התקפת פשינג דרך אתר איכות סביבה המשמש לעוקץ

# איך יוצרים תקיפת פישינג?



✓ הפעלת כלי: SE-TOOL (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

# WAF – הגנה על האפליקציה

WAF = WEB APPLICATION FIREWALL

ההתקפות על האפליקציה נובעות מחולשה באפליקציית האתר שאליה מחדיר ההאקר נזקה

הבעיה: חומת אש מעבירה כל בקשה לשירות WEB ולא מזהה התקפות אפליקטיביות



הפתרון:



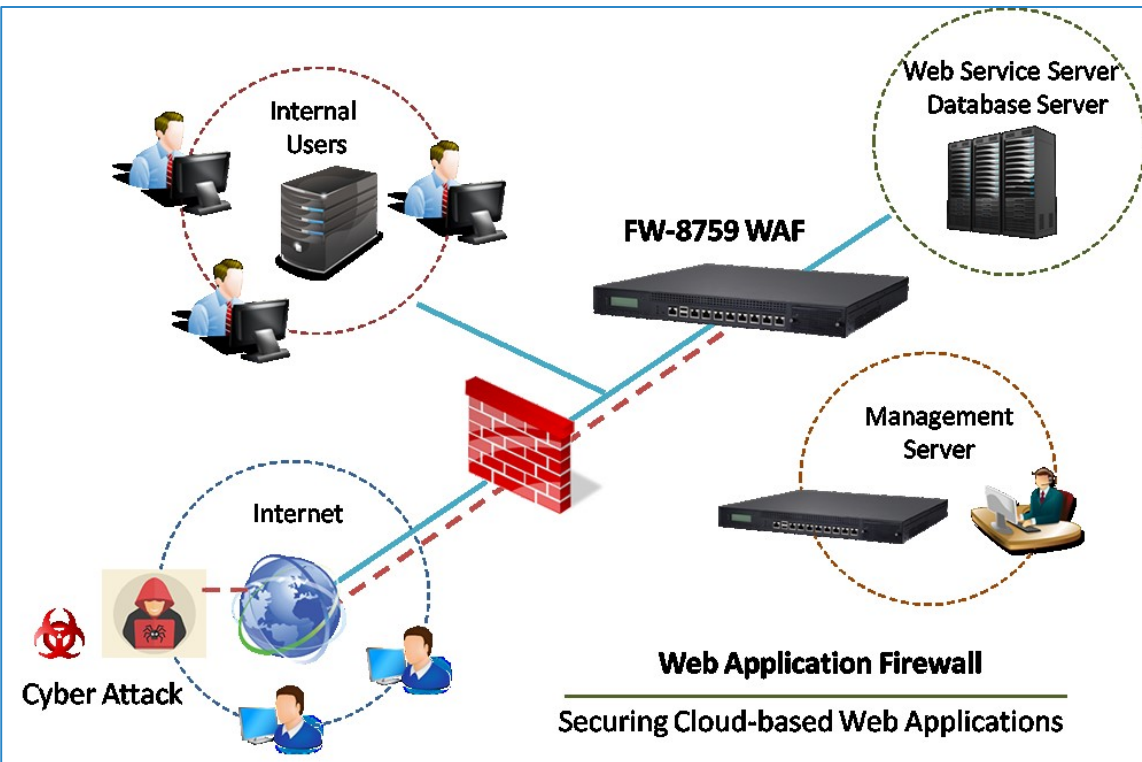
# שלבים ביישום WAF

שלב 1: המוצר לומד את התנהגות המשתמשים (מצב Learning Mode)

שלב 2: חוסם פעילות חריגה

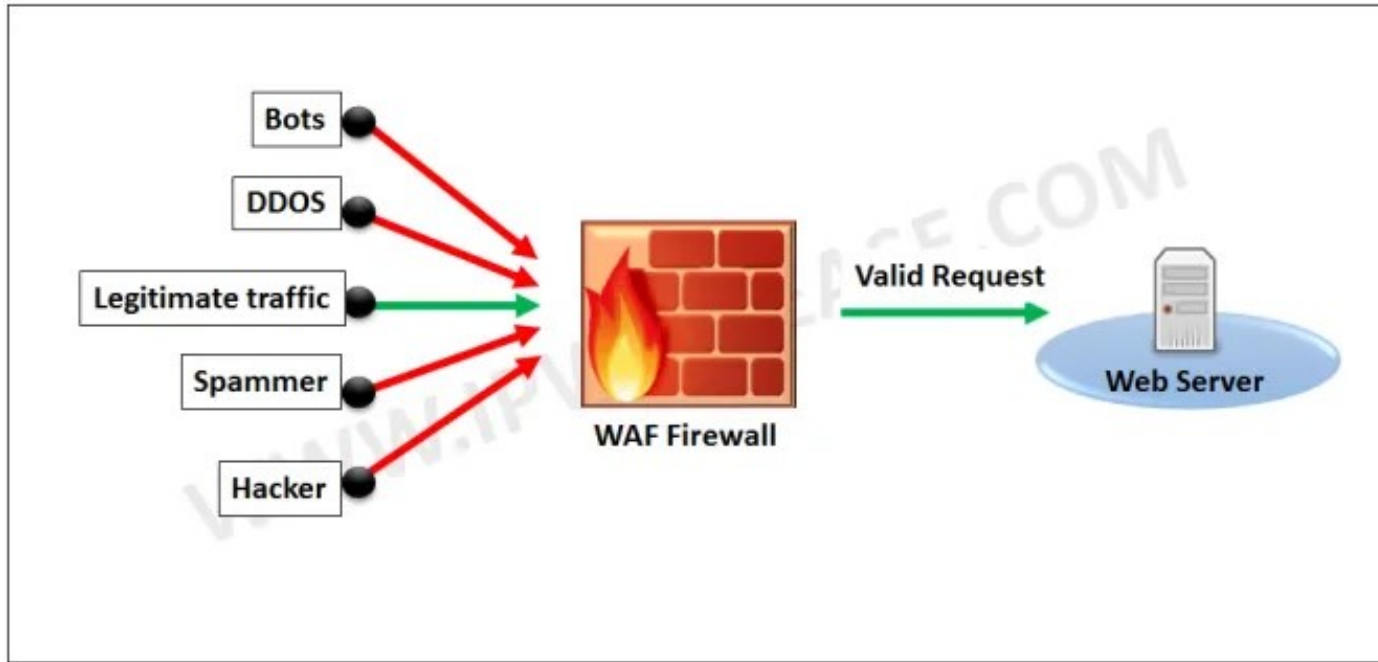
שלב 3: טיוב ידני של המוצר

שלב 4: תחזוקה שוטפת- איש הסייבר מול איש מערכות מידע. כל אתר שנוסף יש להכליל



SOURCE: <https://www.lanner-america.com/network-computing/securing-cloud-based-web-applications-next-generation-waf/>

# ארכיטקטורת WAF



עלינו להיות ערים:

- ❖ יתכנו פניות לגיטימיות שיחסמו
- ❖ יתכנו פניות לא לגיטימיות שיעברו
- ❖ ככל שיעבור זמן, כמות הטעויות תלך ותקטן עקב עקומת למידה של המוצר

SOURCE : <https://ipwithease.com/introduction-to-waf-web-application-firewall/>