



NAVIGATING THE DIGITAL FRONTIER:
Cyber Threats in the
Israeli-Palestinian War



Introduction.....	3
Groups and Parties in Cyber Conflict.....	5
Pro-Israel Groups and Supporters.....	6
<i>Examples of Attacks by Pro-Israel Groups and Supporters.....</i>	<i>7</i>
<i>Attack Tactics and Techniques Used by Pro-Israel Groups and Their Supporters.....</i>	<i>19</i>
Pro-Palestinian Groups and Supporters.....	20
<i>Examples of Attacks by Pro-Palestinian Groups and Supporters.....</i>	<i>22</i>
<i>Attack Tactics and Techniques Used by Pro-Palestinian Groups and Supporters.....</i>	<i>46</i>
Threat Actor Groups Active in CyberWar.....	48
Malware Active in the Cyber War.....	49
Techniques of Attacks Taking an Active Role in Cyber War.....	50
Size of Firms Actively Targeted in the Cyber War.....	51
What Awaits Us in the Future in the Israel-Palestine War?.....	52
Conclusion.....	53
Indicator of Compromise List.....	54



Introduction

In this report, we provide data on over **200,000 attack vectors** detected by the [ThreatMon Advanced Intelligence Platform](#) during the Cyber War in Israel and Palestine between **5th October and 13th October 2023**. This information is from the Threat Feed feature within the ThreatMon Advanced Intelligence Platform. Our Cyber Threat Intelligence Analysts at ThreatMon have carried out extensive analysis processes to present this data to you.

The conflict between Israel and Palestine continues to affect the regional and global agenda for years. However, rather than just the military and political dimensions of the conflict, cyber warfare has played an increasing role in recent years. This report aims to examine the cyber warfare dimension beyond the Israeli-Palestinian conflict and to reveal a less visible but highly influential aspect of this conflict.

By examining the cyber warfare capabilities and strategies of Israel and Palestine, this report aims to analyse how cyber warfare between these two sides began, how it has evolved and possible future trends.

It will also address the political, military and economic consequences of cyber warfare and how it is perceived around the world. The Israeli-Palestinian conflict is a complex issue that affects not only the two sides, but also the region and international relations. The rising role of cyber warfare in this conflict further complicates it and complicates the search for a solution.

Therefore, we hope that this report will shed light on this important issue and be a useful resource for all parties involved.



ThreatMon

Experience an Advanced Threat Intelligence Platform for free



Get customizable threat intelligence feeds.



Receive instant notifications for new vulnerabilities.



Minimize risks and keep your organization safe.

30-Days Free Premium Access



Groups and Parties in Cyber Conflict

The Israeli-Palestinian conflict has become a battlefield that has attracted the attention of not only military and political actors, but also the cyber world. Within this cyber war, there are a number of cyber groups and supporters who support both sides of the conflict or prefer to remain neutral.

Pro-Israel Groups and Supporters: Cyber groups that support Israel are known as Pro-Israel groups and are on the Israeli side of the conflict. These groups strengthen Israel's cyber defence strategies and engage in various cyber activities to protect the interests of the Israeli government.

Some pro-Israel groups and supporters include well-known names such as "GlorySec", "Indian Cyber Force", "UCC Team", "Garuna Ops", "SilentOne", and "IT ARMY of Ukraine".

Pro Palestine Groups and Supporters: Pro Palestine groups are cyber actors that support Palestine and advocate for the Palestinian side in the conflict with Israel. These groups defend Palestinian cyber security and Palestinian interests by conducting various cyber operations. Pro-Palestinian groups' cyber attacks against Israel usually target various sectors. These attacks can cover a range of different sectors, from the Israeli government and military infrastructure to financial institutions, the energy sector and healthcare. Government departments and critical infrastructure are one of the most frequently targeted areas for cyber espionage and DDoS attacks. Such attacks can negatively impact Israel's public services and military operations. In addition, critical infrastructure such as financial institutions and the energy sector are also frequent targets. By attacking these sectors, pro-Palestinian groups seek to create a digital impact against Israel and convey their political messages.

Pro-Palestinian groups include "KillNet", "Anonymous Sudan", "UserSec", "Anonymous Russia", "Ghosts of Palestine", "Team Azrael Angel of Death", "Dark Strom Team", "Pakistani Leet Hackers", and many others.

Neutral Groups: Neutral groups are cyber actors who prefer to remain independent from the conflict. These groups are usually concerned with the consequences of cyber warfare and do not support or attack the parties to the conflict, such as "ThreatSec", "Cyber Army Of Russia", and "DUNIA MAYA TEAM".

These cyber groups play different roles in the cyber dimension of the Israeli-Palestinian conflict. Their activities and influence have a significant impact on the development and outcomes of the conflict.



Pro-Israel Groups and Supporters

GonjeshkeDarande	Indian Cyber Force
Team UCC Operations	SilentOne
Garuna Ops	Kerala Cyber Xtractors
AnonyMiss	Gaza Parking Lot Crew
Termux Israel	Silencer of Evil
Israel Cyber Defence	It Army of Ukraine
Cyber Club (Support)	Anonymous Israel
Team NWH Security	Anonymous India
Dark Cyber Warrior	GlorySec
Kerala Cyber Thunders	Indian Darknet Association

ThreatMon Cyber Threat Intelligence Team detected a total of 20 pro-Israel groups. In this process, every action taken by threat actors is actively monitored by us 24/7.


RansomedVC, one of the Ransomware groups actively monitored 24/7 through [ThreatMon Advanced Ransomware Monitoring](#), announced its support for Israel on its website and social media platforms and announced that it will purchase access information for Palestine and Gaza. RansomedVC is a ransomware group that emerged in 2023 and began its attacks by announcing its partnership with Stormous, another ransomware group. The group is known for targeting organisations in Middle Eastern countries more, but it should not be overlooked in its attacks on organisations in other countries.



Examples of Attacks by Pro-Israel Groups and Supporters

- 1) In the activity detected by our team via Telegram, it was determined that the Palestinian health sector was targeted. It was determined that a total of 1,647,837 records, patient laboratory test results, appointment reports and dead patients etc. list were shared from 2 Part containing 16.2MB and 13.3MB files.

The Archivists Domain

 **Palestine Healthcare Dump - 1.3kk.7z**
16.2 MB

Some, think they are too mighty to fall.
However this is often a facade, now laid bare before you.
Now, let me be the flame that burns Icarus and show that even the gods **can bleed**.


I present to you, a dump of Palestine's entire healthcare system.

Contents:
 1,166,252x NCD Nursing Records (Split into 1,2 or 6 month chunks)
 65,589x Nurse Visit Reports
 30,990x NCD Reports
 29,370x NCD Screenings
 7,852x Child Hemoglobin Tests
 2,879x Emergency Nursing Records
 1,391x Mental Health Screenings
 1x Statistics Report

Total count - 1,304,324 Records (For context, the total population of Palestine is ~4.9 Million people)

~ With love, The Archivist

The Archivists Domain

 **Palestine Healthcare Dump - Part 2 - 1.6kk.7z**
13.3 MB







You are, all of you, vermin. Cowering in the dirt, thinking... what?
That you might escape the coming fire?
Your world will burn until its surface is but glass!
- Prophet of Truth

I present to you, part 2 of Palestine's healthcare system dump.

Contents:
 1,637,255x NCD Patients Lab Test Results
 7,269x Appointment Reports
 3,313x NCD Dead Patients List

Total count - 1,647,837 Records (For context, the total population of Palestine is ~4.9 Million people)

~ With love, The Archivist

 Statistics Report	 4.0 KIB folder	Tuesday
 Nurse Visit Reports	 4.0 KIB folder	Tuesday
 NCD Screenings	 4.0 KIB folder	Tuesday
 NCD Reports	 4.0 KIB folder	Today
 NCD Nursing Records	 4.0 KIB folder	Today
 Mental Health Screenings	 4.0 KIB folder	Today
 Emergency Nursing Records	 4.0 KIB folder	Today
 Child Hemoglobin Tests	 4.0 KIB folder	Today
 README.txt	 646 bytes plain text document	Tuesday



ThreatMon

- 2) The activity detected by our team on Telegram claimed that more than 200 network devices, including schools and hospitals in Palestine, were hacked and messages were left by a threat actor named "Indian Cyber Force".

INDIAN CYBER FORCE

SIEMENS Wireless Basic Settings

Wireless Interface	Network Name (SSID)	Hide Name
WLAN1	zafra0013	<input checked="" type="checkbox"/>
WLAN2		<input type="checkbox"/>
WLAN3		<input type="checkbox"/>
WLAN4		<input type="checkbox"/>

DNSlytics Server IP: AS1203

Reverse DNS (PTR) - no PTR record
AS number: AS1203
AS name (ISP): Pakistani Telecommunications Company (PTCL)
IP range/subnet: [redacted]
Network tools: [redacted]
Location: Gaza, Gaza Governorate, Palestine (PS)

ThreatMon

Palestinian more than 200+ Network Device's has been Hacked.

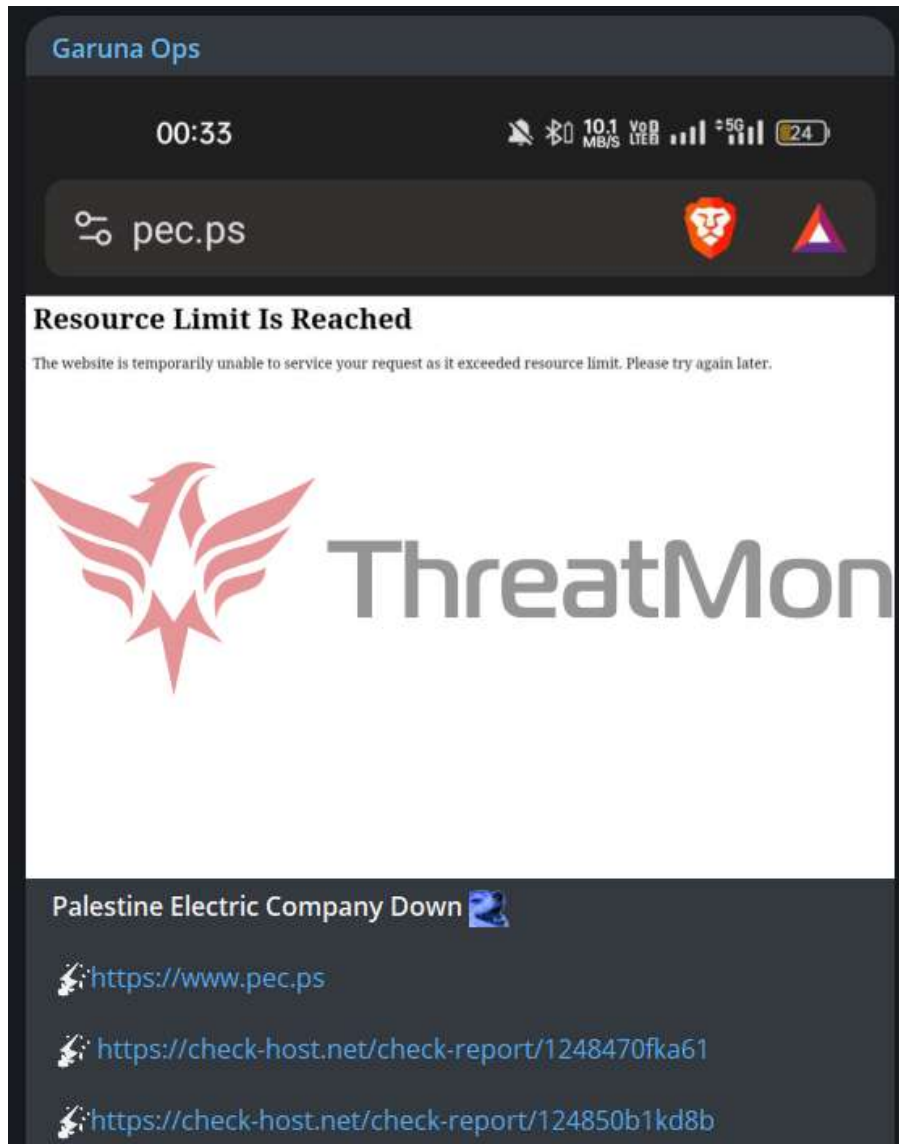
Included School,Hospital, etc.

Message to Palestinian Terrorists:
If you consider yourself a true man, Fight with Real Men face to face instead of hiding behind the shield of women and kids like you Terrorists always do.



ThreatMon

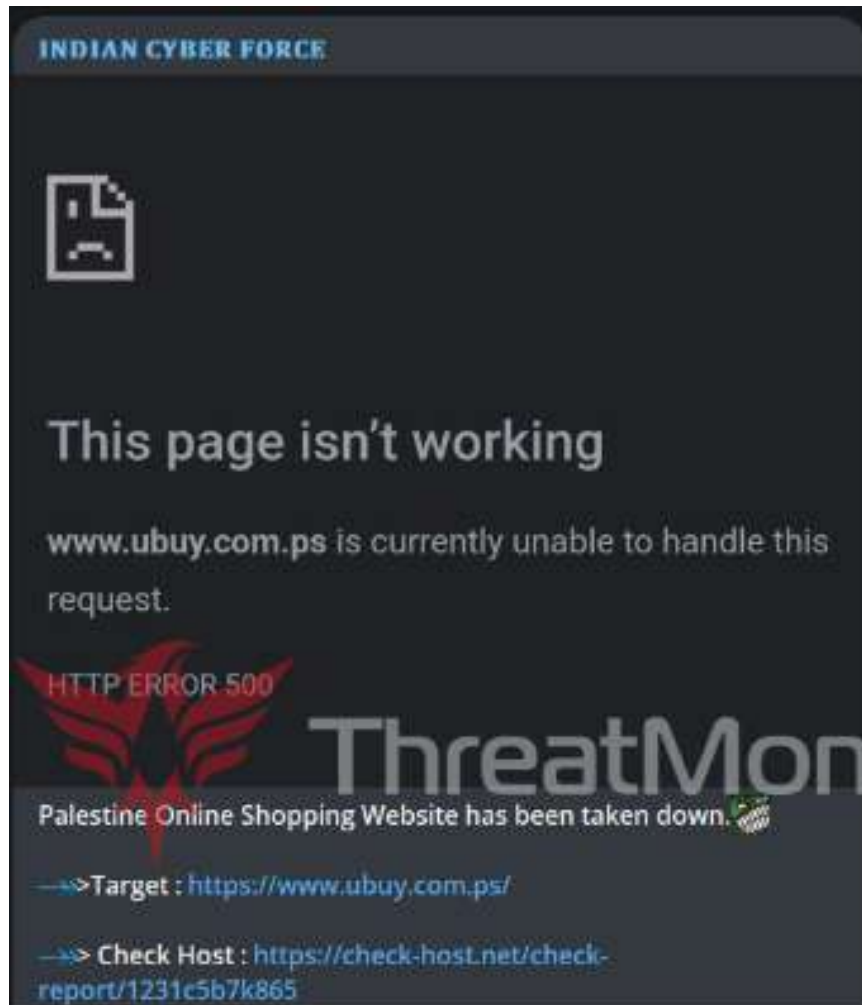
- 3) In the activity detected by our team on Telegram, the Palestinian electricity company Palestine Electric was targeted. As a result of a DDoS attack carried out by a threat actor named "Garuna Ops", the websites could not be accessed.





ThreatMon

- 4) In the activity detected by our team on Telegram, the international e-commerce company "ubuy" was targeted. It was unavailable for a while as a result of a DDoS attack by a threat actor called Indian Cyber Force.



Our
Website is

C - L - MING
SOON


Meanwhile feel free to explore our
global presence in **190+ countries.**



ThreatMon

- 5) In the activity detected by our team on Telegram, targeted National Bank, the second largest bank in Palestine, which provides comprehensive financial services for the corporate, retail, investment and microfinance sectors. As a result of the DDoS attack, the bank's website became unusable for a while.

INDIAN CYBER FORCE




This site can't be reached

www.tnb.ps took too long to respond.

Try:
Checking the connection

ERR_TIMED_OUT

ThreatMon

Palestine National Bank website Has Been Taken Down 

<Target: <https://www.tnb.ps/en>

<Check Host: <https://check-host.net/check-report/122c80f2k5ed>



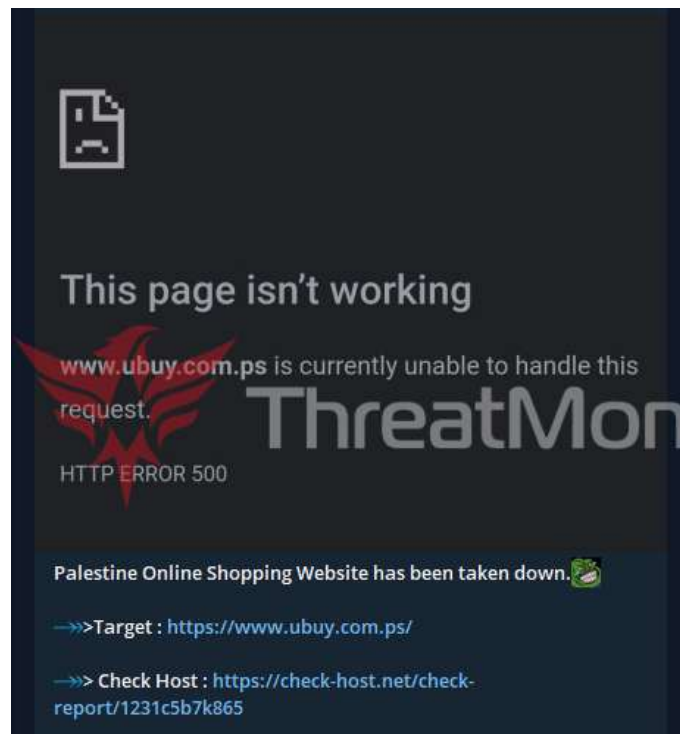
ThreatMon

- 6) In the activity detected by our team in Telegram, Palestinian Government was targeted by the threat actor "SilentOne". As a result of the DDoS attack on the official websites, access to the websites was restricted.

The image shows a Telegram chat interface. At the top, there is a header for a channel named "Silent One (कट्टर हिन्दू)" with a red play button icon. Below this is a screenshot of a web browser displaying an error message: "This site can't be reached" for the URL "query.gov.ps". The error message states "query.gov.ps unexpectedly closed the connection" and provides troubleshooting steps: "Checking the connection", "Checking the proxy and the firewall", and "Running Windows Network Diagnostics". A "Details" button is visible. A large, semi-transparent "ThreatMon" watermark is overlaid on the screenshot. Below the screenshot is a text message in a dark grey background with white text. The message reads: "QUERY WEBSITE OF GOVT OF PALESTINE", "SITE : <https://query.gov.ps/>", "PROOF : <https://check-host.net/check-report/12408288k13c>", "#OpPalestine #IStandWithIsrael #Indian", "#SilentOne #IAF #MoonGod #IndianHackerGroup", "#JaiShreeRam", and "#SilentOne".



- 7) In the activity detected by our team in Telegram, the threat actor named "INDIAN CYBER FORCE" targeted the Palestinian e-commerce site. As a result of the DDoS attack on the website, the site became unusable for a while.

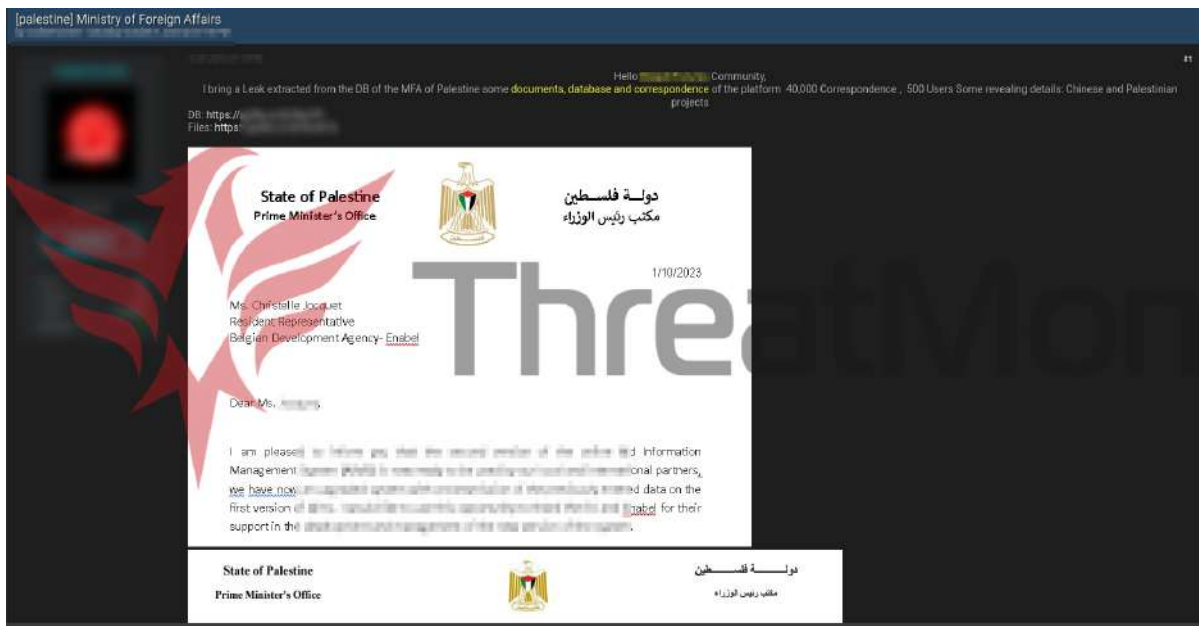


- 8) A threat actor named "Two2", identified by our team in a Dark web forum, has leaked user data of the Palestinian Ministry of Higher Education Scientific Research and the Ministry of Interior National Security. The leaked data includes URL, Username/Mail, Password information.

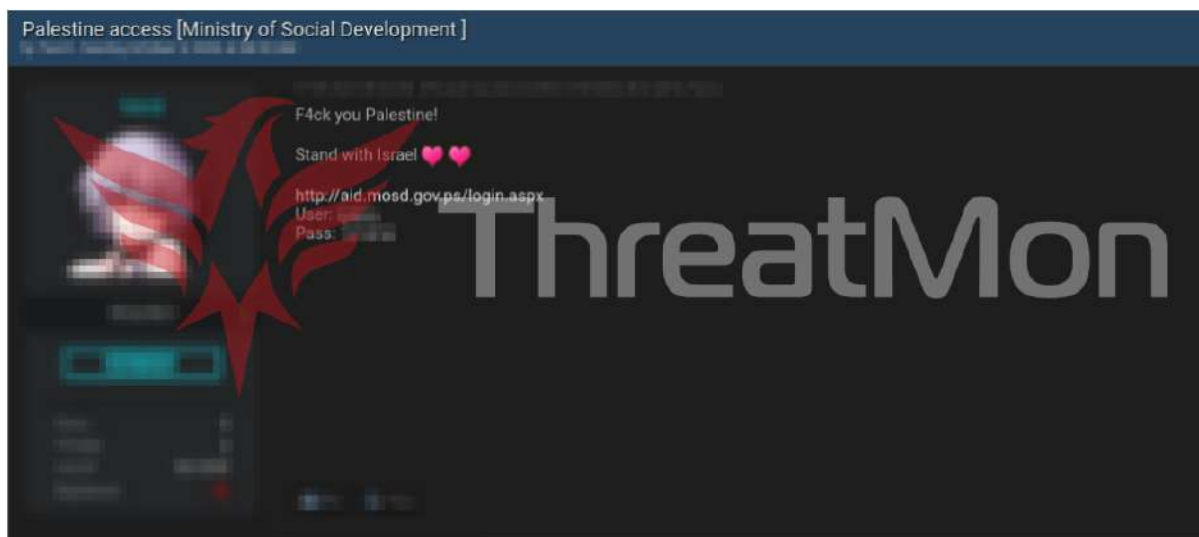




- 9) A threat actor named "Two2", detected by our team, leaked Palestinian Ministry of Higher Education Scientific Research and Ministry of Interior National Security user data, according to the post shared on the dark web forum. The leaked data includes URL, Username/Mail, Password information.



- 10) A threat actor named "Two2", identified by our team, posted on a dark web forum and announced that he had access to the user account of the Palestinian Ministry of Social Development. The threat actor publicly leaked the access. The relevant leak data consists of URL, username/email, password content.



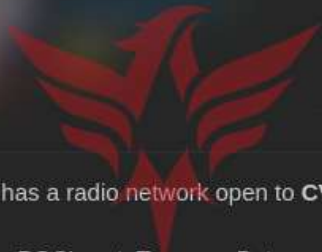


ThreatMon

- 11) In the post shared by the threat actor named "eVeeVendetta" on the dark web forum, he claimed that Palestine is a radio network vulnerable to CVE-2023-42119.

CVE-2023-42119 : It is an out-of-bounds read bug found in Exim within the SMTP service. An attacker could use this in combination with other vulnerabilities to execute arbitrary code in the context of the service account.

CVE-2023-42119



ThreatMon

Palestine has a radio network open to CVE-2023-42119

Not seeing POC's yet. Too new. But something exists somewhere.

#StopTerrorism



ThreatMon

- 12) In the post shared by the threat actor named "batnet" detected by our team in the dark web forum, he announced that he wrote a Palestinian donation script and shared this script publicly. The script is claimed to be compatible with telegram bot and mobile devices.

Öncelikle bu tarz bir şey yapıp yapmamak arasında kalmıştım,
Ta ki twitterda havlayan irtica kuklalarının Filistin tarafına saf tutarak terör övücülüğü yaptığını görene kadar.

Bu Script:
Filistin bölgesine doğrudan bir zarar vermez.
Amacım ülkemizdeki şeriat yanlısı kerkenezlerin cebel.
Duyar kısmak isteyen dostlarım, bimecell çıkıp garibanın 30-40 lirasına göz diken elemanlara ulaşsın.

Script telefona bir android cihazlar için uyumludur,
gereki yinlendirmesi onay adı dosyasında mevcuttur.

KULLANIM VIDEOSU:
TIKLAYIN
İNDİRME LINKİ:
TIKLAYIN
ŞİFRE: [ipn: batnet04](#)

#ÖzgürFilistin

FİLİSTİN İRTİVAÇ LİSTESİ

**FİLİSTİN YARALI
#UZAT ELİNİ**

İHTİLLER VE SAĞİP AMANLAŞTIRILAN

Adı	Adres	Telefon	Banka	Para
1. İsmail	5.000.000 TL
2.	8.563.800 TL
3.	5.431.000 TL
4.	11.350.000 TL
TOPLAM				59.091.961 TL

KART BİLGİLERİ

Kart Sahibi *
Muhammet Doğru

Bağış Tutarı *
3005

Kart Türü *
Yatılı

Kart Numarası *
412 427 1221 7221

Ben Kullanım Tarihi
08/11/2025

CVV *
4444

3D Secure Kullan (sistemdeki kartın ipn. zorunlu değildir)

Bağış Tamamla

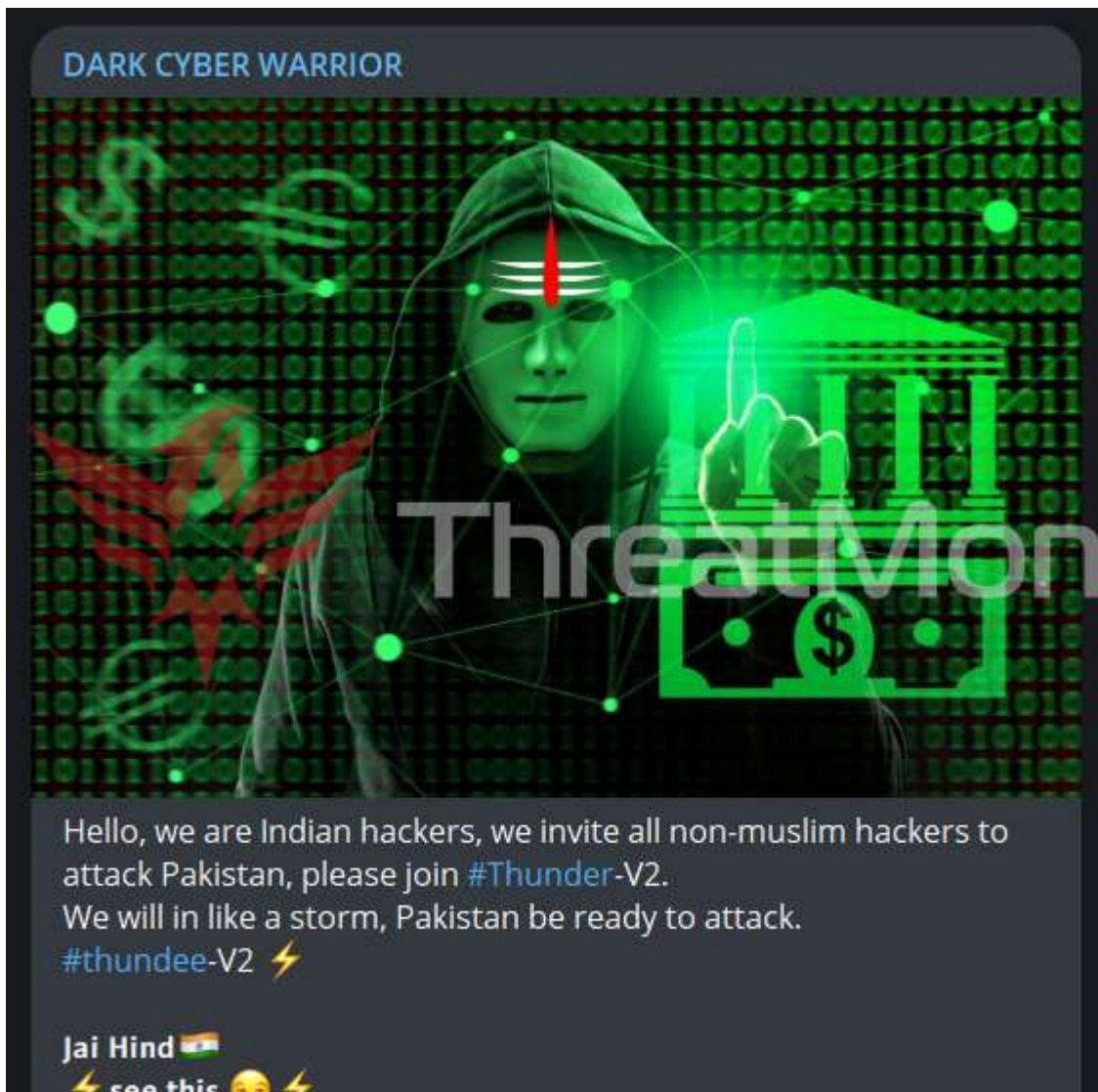
#ÖzgürFilistin

© 2023 Tüm Hakları Saklıdır | Dünya Yardım Derneği

VISA 3D



- 13) The Indian threat actor "Dark Cyber Warrior", which our team identified on Telegram, invited non-Muslim hackers to attack Palestine. They left the message "We will enter like a storm, Pakistan should be ready to attack".






ThreatMon


14) In the activity detected by our team in Telegram, Paltel Group, operating as a telecommunications company in Palestine, was targeted. As a result of the DDoS attack by the threat actor named "INDIAN CYBER FORCE", access to websites was restricted.

INDIAN CYBER FORCE



This site can't be reached

The web page at <https://www.paltel.ps/en/home> might be temporarily down or it may have moved permanently to a new web address.



ThreatMon

Palestine Telecommunication Company Has Been Taken Down 🌐

➡>Target: <https://www.paltel.ps>

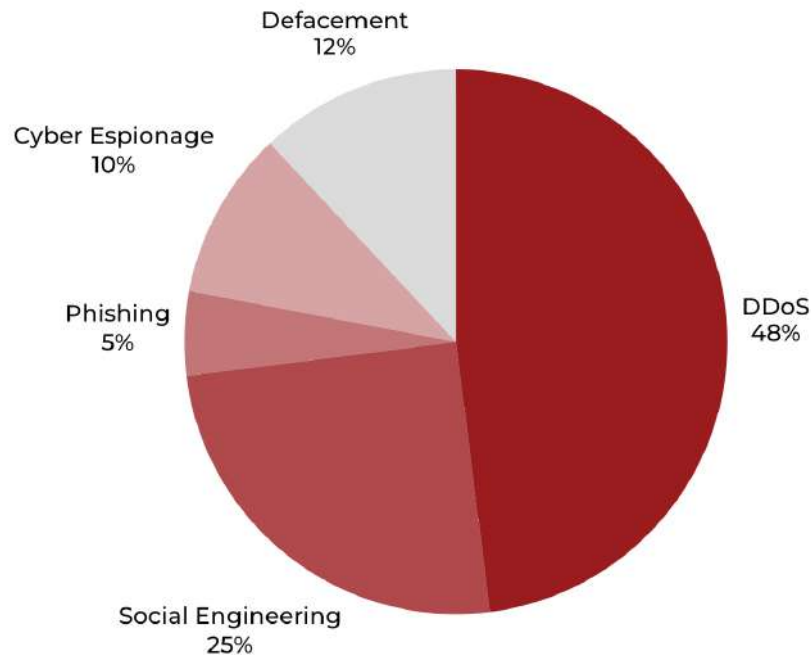
➡>Check Host: <https://check-host.net/check-report/122c6cf1k12c>

Duration: 4 hrs

#StandWithIsrael



Attack Tactics and Techniques Used by Pro-Israel Groups and Their Supporters



- **DDoS Attacks (%48):** Pro-Israel groups frequently use Distributed Denial of Service (DDoS) attacks against Israeli online services. These attacks involve sending massive traffic to make targeted websites temporarily inaccessible.
- **Social Engineering and Ransomware (%25):** Pro-Israel groups use social engineering tactics to achieve their goals. They may also use ransomware to harm their targets or steal information.
- **Web Site Defacement (%12):** Groups supporting Israel can use page modification tactics to convey their political messages by changing targeted websites.
- **Cyber Espionage and Information Gathering (%10):** Pro-Israeli groups could carry out cyber espionage to gather sensitive data from specific individuals or organizations.
- **Phishing Attacks (%5):** In certain instances, Pro-Israel organisations might resort to phishing attacks as a means to procure sensitive information from targeted groups or individuals. These statistics demonstrate the breakdown of methods employed by Pro-Israel groups in their cyber attacks.

These tactics and techniques reflect the diversity of cyber operations of groups supporting Israel when the attack tactics and techniques used are analysed.



Pro-Palestinian Groups and Supporters

KillNet	Anonymous Sudan
Anonymous Russia	UserSec
Ghost of Palestine	Team Azrael Angel of Death
Pakistani Leet Hackers	DarkStrom Team
Sylhet Gang - SG	Team_insane_Pakistan
Garnesia Team	Hacktivism Indonesia
Blackshieldcrew MY	Gb Anon 17
Ghost Clan Malaysia	Anonymous Morocco
Mysterious Team Bangladesh	Ganosec Team
Ghost Clan	Moroccan Black Cyber Army
Eagle Cyber Crew	Muslim Cyber Army
Kerala Cyber Xtractors	YourAnon T13x
SynixCyberCrime MY	Team Herox
Panoc Team	4 Exploitation
Moroccan Defenders Group	Team R70
The White Crew	Stucx Team
TYG Team	Hizbullah Cyb3r Team
StarsX Team	Electronics Tigers Unit
1915 Team	WeedSec
Storm-1133	Dragonforce Malaysia
Cyb3r Drag0nz	End Sodoma
Khalifah Cyber Crew	Teng Korak Cyber Crew



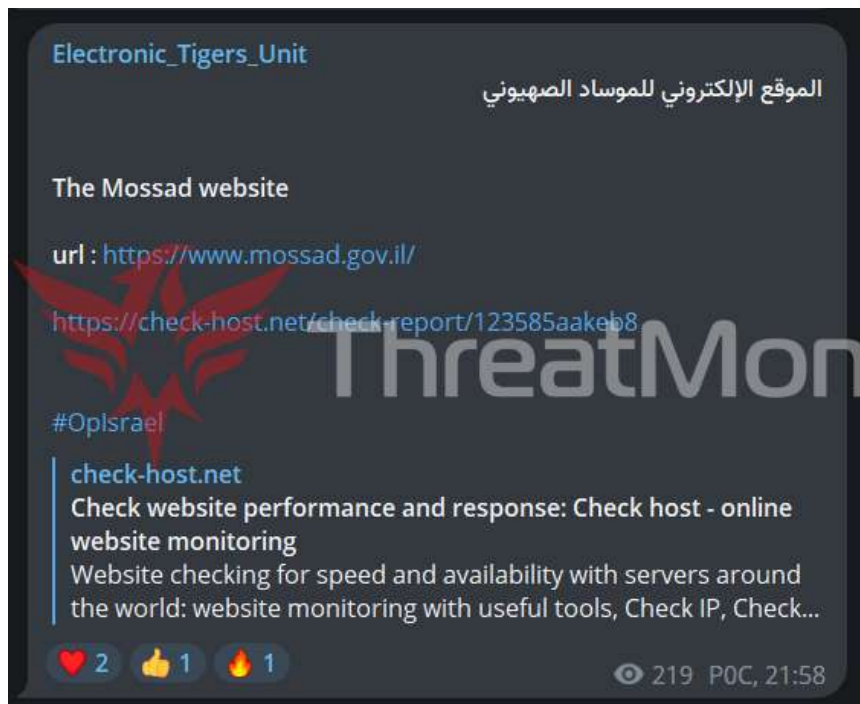
Skynet	ACEH About Hacked World
DevilAttacks	Boom Security
./TeaParty	./CsCrew
JATIM RedStorm Xploit	ASKAR DDOS
Anonghost	Yemen Legions Team
Arab Anonymous Team	Russian Tools
Islamic Cyber Team Indonesia	Bangladesh Civilian Force
KEP Team	Pakistan Cyber Hunter
Jateng Cyber Team	Systemadminbd Official (BCF)
AnonHamz	Anonymous 070
Kingman World Official	Black Security Team
Islamic Hacker Army	Malaysia Cyber Defacer
Team Anon Force	SiegedSec
VulzSec	Cyber Error Team
CyberActivism	GhostSec
Anonymous Indonesia	Khan Cyber Army

As ThreatMon Cyber Threat Intelligence team, we have detected a total of 76 pro-Palestinian groups. In this process, every action taken by threat actors is actively monitored by us 24/7.



Examples of Attacks by Pro-Palestinian Groups and Supporters

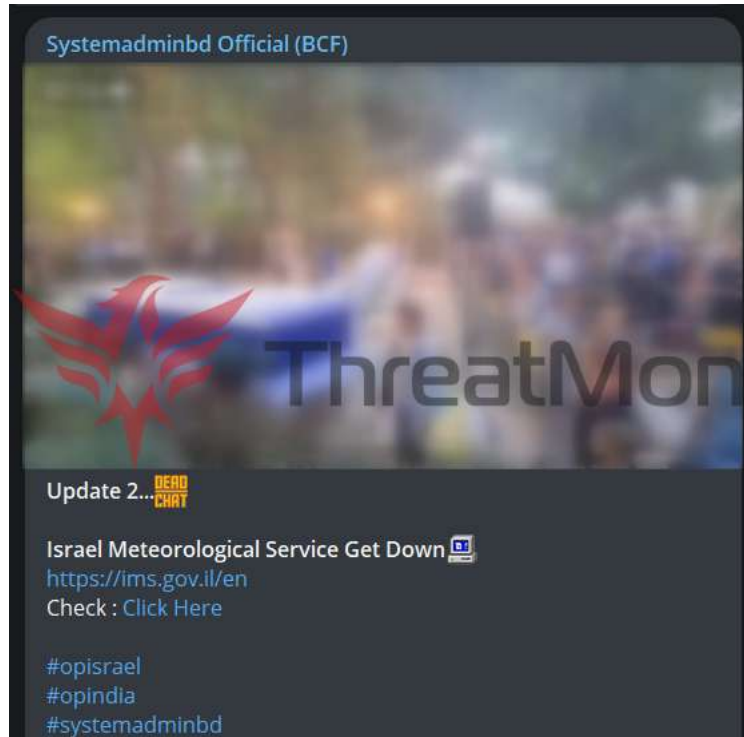
- 1) In the activity detected by our team on Telegram, the threat actor named "Electronic_Tigers_Unit" disabled the official website of the Mossad for a while with a DDoS attack.





ThreatMon

- 2) In the activity detected by our team on Telegram, the threat actor named "Systemadminbd Official" targeted the Israel Meteorological Service. As a result of the DDoS attack carried out by the threat actor, access to the websites could not be provided for a while.



- 3) In the activity on Telegram detected by our team, the threat actor named "ACEH ABOUT HACKED WORLD" targeted the Israeli Ministry of Finance. As a result of a DDoS attack on their website, it became unusable for a while.





- 4) The activity detected by our team on Telegram, targeted the Israeli Army Radio Broadcast, Ministry of Foreign Affairs, News Sites, Israel Nuclear Research, Ben Gurion Airport. As a result of a DDoS attack carried out by a threat actor named "YourAnonT13x", the websites could not be accessed.

GHOSTS of Palestine TM
Israeli Sites Attacked

Ministry of Foreign Affairs
Israeli Army Radio Broadcasting
Breaking News Online Newspaper Infrastructure News Website i24
Israel Nuclear Research Website Ben Gurion Airport Website

אתרים שתקפנו את ישראל משרד החוץ של משרד החוץ שידורי הרדיו של
הצבא הישראלי חדשות חדשות עיתון מקוון תשתיות חדשות אתר i24
ישראל למחקר גרעיני אתר נמל התעופה בן גוריון

المواقع التي هاجمناها إسرائيل وزارة الخارجية إذاعة الجيش الإسرائيلي أخبار عاجلة
صحيفة إلكترونية أخبار البنية التحتية موقع i24 موقع الأبحاث النووية الإسرائيلية
موقع مطار بن غوريون

سایت هایي که ما به آنها حمله کردیم
وزارت امور خارجه اسرائیل
راديو ارتش اسرائیلخبرش اخبار فوری
زیرساخت های روزنامه آنلاین
وبسایت خبری i24 اسرائیل
وبسایت تحقیقات هسته ای
وبسایت فرودگاهی بن گوریون

Sitios que atacamos Ministerio de Asuntos Exteriores de Israel
Ejército israelí Radiodifusión Noticias de última hora Periódico en
línea Sitio web de noticias de infraestructura Sitio web de
investigación nuclear de i24 Israel Sitio web del aeropuerto Ben
Gurion

By Operation Israel Hackers



ThreatMon

- 5) In the activity on Telegram detected by our team, the threat actor named "YourAnonT13x" targeted the Diplomat Culinary, 103fm, Gefeno, Canaanite, The bouncer, bhol.co.il. As a result of a DDoS attack on their website, it became unusable for a while.

The image displays two screenshots of Telegram messages from the threat actor 'YourAnonT13x'. The left screenshot shows a message with a graphic of the Israeli flag crossed out with a red 'X' and a hooded figure in the background. The text includes the following information:

- Hashtags: #OpIsrael #FckIsrael, #FreePalestine #StandWithPalestine
- Announcement: 5 websites belonging to the Israeli have been #TangoDown by @YourAnonT13x
- Targets and links:
 - <https://www.diplomat-culinary.co.il/> | Culinary Diplomat Website
 - Check-host: <https://check-host.net/check-report/12338ddck79c>
 - <https://103fm.maariv.co.il/> | Radio station 103fm
 - Check-host: <https://check-host.net/check-report/1233822bk64>
 - <https://www.gefeno.co.il/> | Gefno Website
 - Check-host: <https://check-host.net/check-report/12338735k168>
 - <https://hacnaanit.co.il/> | The Canaanite Restaurant
 - Check-host: <https://check-host.net/check-report/12338901k3e6>
 - <https://www.extrasport.co.il/> | Extra Sport Website
 - Check-host: <https://check-host.net/check-report/12026068k712>

The right screenshot shows a message with a hooded figure in the background and the following information:

- Announcement: Behaderi News Website has been #TangoDown by @YourAnonT13x
- Target and link:
 - <https://www.bhol.co.il/> | Behaderi News Website
 - Check-host: <https://check-host.net/check-report/12338056k67d>
- Signature: Expect Us. We are YourAnonT13x Group
- Hashtags: #Anonymous #YourAnonT13x #OpIsrael #FreePalestine



ThreatMon

- 6) In the activity on Telegram detected by our team, the threat actor named "Sylhet Gang" targeted the Israeli Patent Search Portal and the Tel Aviv Medical Centre. As a result of a DDoS attack on their website, it became unusable for a while.

Check website <https://israelpatents.justice.gov.il/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more [asa.net](#)

Permanent link to this check report | Share report on [Twitter](#)

Checked on Mon Oct 09 08:48:14 UTC 2023 | [Check again](#)

Location	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C. Brno	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Hong Kong, Hong Kong	OK	1.181 s	200 (OK)	142.251.2.111
Iran, Tehran	Too many open files			
Israel, Tel Aviv	OK	0.040 s	200 (OK)	142.251.2.111
Italy, Milan	Connection timed out			
Japan, Tokyo	Connection timed out			
Korea, Seoul	Connection timed out			
Poland, Warsaw	Connection timed out			
Russia, Moscow	Connection timed out			
Spain, Barcelona	Connection timed out			
Switzerland, Zurich	Connection timed out			
Turkey, Istanbul	OK	0.457 s	200 (OK)	142.251.2.111
USA, New York	Connection timed out			
USA, Los Angeles	Connection timed out			

Website Down

Target:<https://israelpatents.justice.gov.il/>

Check website <https://ichilov-clinic.gov.il/>

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more [asa.net](#)

Permanent link to this check report | Share report on [Twitter](#)

Location	Result	Time	Code	IP address
Austria, Vienna	Connection timed out			
Brazil, Sao Paulo	Connection timed out			
Bulgaria, Sofia	Connection timed out			
Czechia, C. Brno	Connection timed out			
Finland, Helsinki	Connection timed out			
France, Paris	Connection timed out			
Germany, Frankfurt	Connection timed out			
Germany, Nuremberg	Connection timed out			
Hong Kong, Hong Kong	Connection timed out			
Iran, Tehran	Too many open files			
Iran, Karaj	Connection refused			
Iran, Shiraz	Connection timed out			
Italy, Rome	Connection timed out			
Iran, Tehran	Connection refused			
Israel, Tel Aviv	Connection timed out			
Italy, Milan	Connection timed out			
Japan, Tokyo	Connection timed out			
Kazakhstan, Karaganda	Connection timed out			
Lithuania, Vilnius	Connection timed out			
Moldova, Chisinau	Connection timed out			
Netherlands, Amsterdam	Connection timed out			
Poland, Poznan	Connection timed out			
Poland, Warsaw	Connection timed out			
Portugal, Viana	Connection timed out			
Russia, Ekaterinburg	Connection timed out			
Russia, Moscow	Connection timed out			
Russia, Moscow	Connection timed out			
Russia, Saint Petersburg	Connection timed out			
Serbia, Belgrade	Connection timed out			

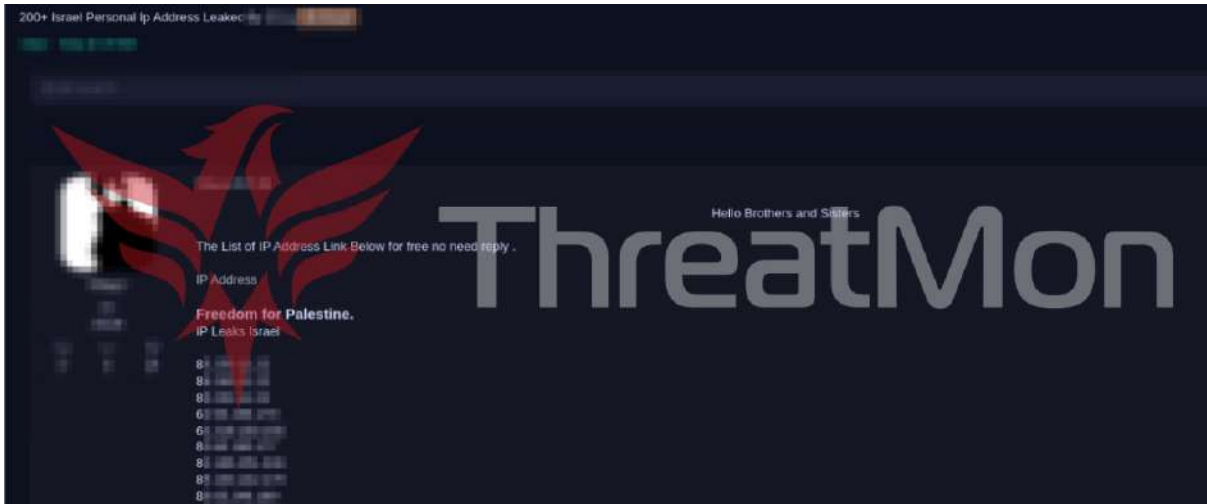
Tel Aviv Medical Center

<https://ichilov-clinic.gov.il/>



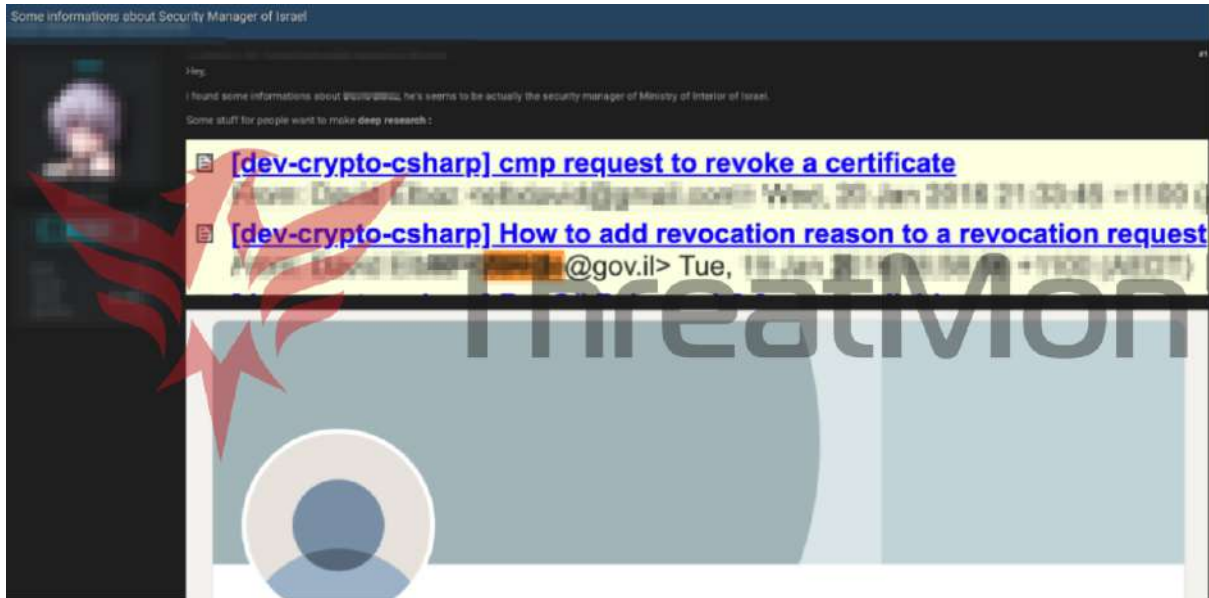
ThreatMon

- 7) According to a post shared by a threat actor named "Oday" detected in a dark web forum, it was observed that he leaked more than 200 Personal IP Addresses located in Israel.





- 8) According to the post shared by the threat actor named "xsod", which was detected in the dark web forum as a result of the scans made by our team, it is seen that he shared the Personal E-mail, Business E-mail, Skype account information of the Security Manager of the Israeli Ministry of Interior.





ThreatMon

- 9) The threat group "Anonymous Sudan", about which we presented a detailed [research report](#) a few months ago and which was identified by our team, shared its cooperation with KillNet, one of the most well-known Russian hacktivist groups, with the message "Victory to the Palestinian Resistance!".





ThreatMon

- 10) As a result of our scans in Telegram, the threat group named "Legion (Cyber Spetsnaz)", known for its cyber activities against NATO and government resources in Ukraine, launched DDoS attacks against major financial institutions in Israel in cooperation with the threat actor named "KILLNET".

00:01 🔊

ЛЕГИОН
КИБЕР СПЕЦНАЗ

И СТЕНЫ ТОЖЕ ПЛАЧУТ

ThreatMon

Банк Дисконт
<https://discountbank.co.il/>
<https://check-host.net/check-report/122edcedk22f>

Банк Меркантиль Дисконт
<https://mercantile.co.il/>
<https://check-host.net/check-report/122edf5ak76e>

Банк Иерусалима
<https://bankjerusalem.co.il/>
<https://check-host.net/check-report/122ee0d8k25e>



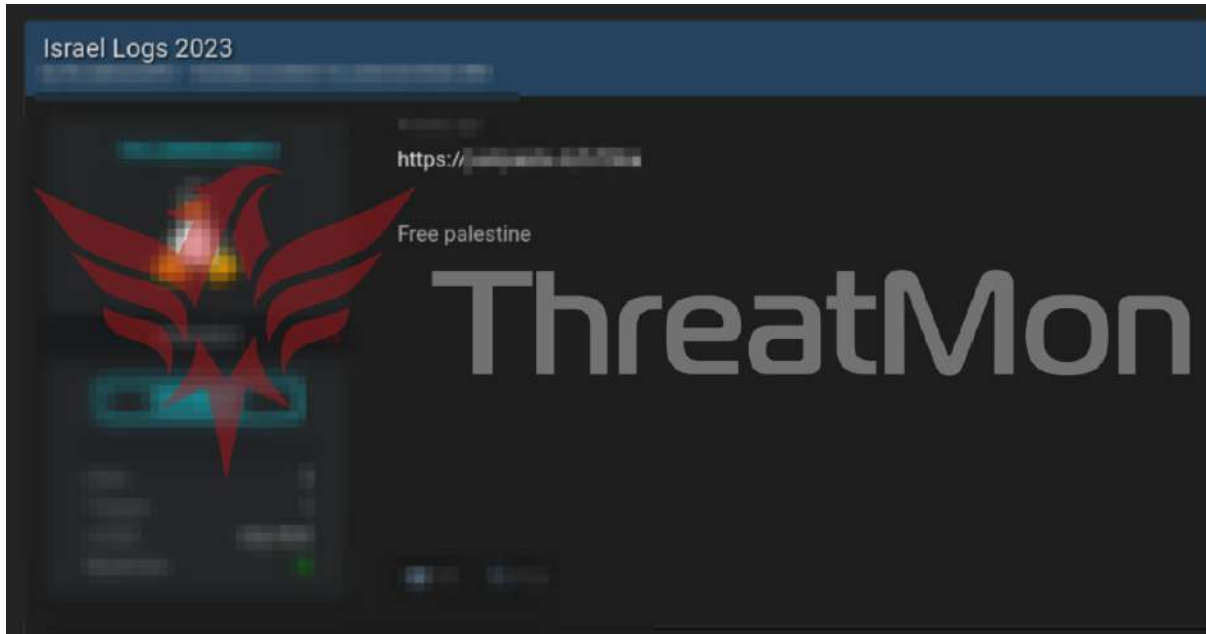
11) According to a post shared by a threat actor named "RRR", identified by us on a dark web forum, he claimed to have leaked 2 Million registered databases belonging to the Israeli transport operator Bus[.]co[.]il.

Bus.co.il 2M Israeli transportation operators

1	2	3	4	5	6	7	8	9	10	
1	תו	פרטי	משפחה	כתובת	ישוב	מיקוד	לידה	טלפון	אב	דירה
2	2675	הדרת	מאהל נפול	12	השמה	34752	1986		יוסף	01
3	276	החוס	כלי	א	השמה	34752	38	Apr-82	מואל	01
4	276	ההובל	הכליך	12	השמה	34752	19	04-8348640	יוסף	01
5	277	הנה	הסאר	9	השמה	11894	38		השה	01
6	281	הה	השפר	80	השמה	34752	19	04-8241968	דב	01
7	286	ההלי	העברי	6	השמה	34752	19	04-8345752	הודה	01
8	286	ההון	היוקס	68	השמה	34752	19	04-8241813	החיה	01
9	295	ההב	הדתם	72	השמה	11445	19		העון	01
10	304	ההחל	הלי	56	השמה	34752	19	04-8241358	הרט	01
11	310	ההחיד	ההקלר	21	השמה	34752	19	04-8251302	הואל	01
12	317	ההחיה	ההסאר	9	השמה	34752	19		היש	01
13	321	הההרה	ההורץ	12	השמה	34752	19	04-8258832	השה	01
14	332	ההח	ההגלית	12	השמה	34752	19	04-8323101	הההרון	01
15	333	הההים	הההפלס	12	השמה	34752	19		הד	01
16	124	ההההה	ההההה	54	השמה	34752	38		הצבי	01
17	380	הההה	ההההה	12	השמה	34752	19		ההההה	01
18	391	הההה	ההההה	12	השמה	34752	19		ההשה	01
19	395	הההחל	ההההה	15	השמה	34752	19	04-8247445	הההה	01
20	396	ההההה	ההההה	52	השמה	34752	19	04-8241261	הההה	01
21	409	הההה	ההההה	12	השמה	34752	19		ההההה	01
22	426	הההה	ההההה	א	השמה	34752	19		ההצבי	01
23	148	הההה	ההההה	12	השמה	34752	19	Apr-82	הההה	01
24	446	הההה	ההההה	12	השמה	34752	19		הההה	01
25	470	ההההה	ההההה	60	השמה	34752	19	04-8241528	הההה	01



- 12) It has been observed that the threat actor named "lol_babasanfor", who was detected by us in a dark web forum, shared logs that he claimed to belong to Israel and the year 2023, according to the post he shared in support of Palestine with the message "Free Palestine" after the war started.

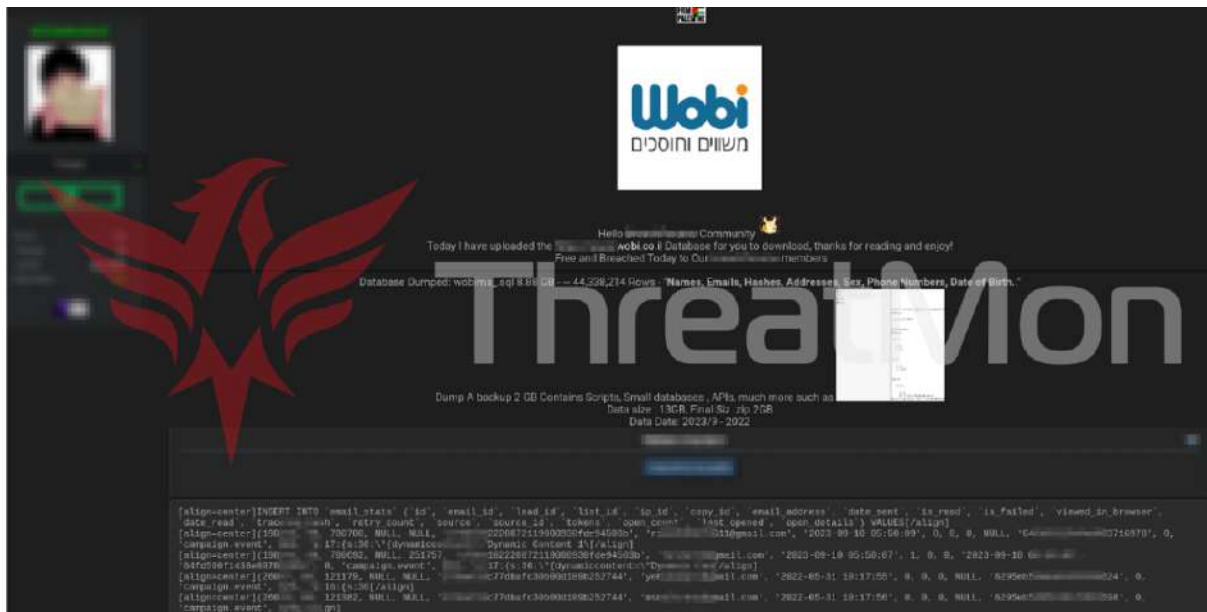


https://accounts.google.com/: [redacted]@gmail.com:maywai [redacted]
https://account.next.co.il/: [redacted]1516: [redacted]79
https://www.npmjs.com/: [redacted]09:s [redacted]79
https://www.twitch.tv/:A [redacted]1:sl [redacted]25
https://www.matific.com/:n [redacted]1: [redacted]89
https://login.live.com/login.srf:[redacted]@gmail.com:m [redacted]31
http://online3.talpiot.ac.il/login/index.php:[redacted]349: [redacted]62
http://projects.telem-hit.net/SnakesandLadders/welcome.aspx:s [redacted]man:[redacted]79
https://www.amazon.com/ap/signin:[redacted]16:[redacted]34
https://wordpress.com/start/user:[redacted]man:s [redacted]79
https://www.thinglink.com/register:[redacted]@walla.co.il:[redacted]
https://www.sefereshet.org.il/users: [redacted]l:[redacted]79
https://www.amazon.com/ap/register:[redacted]an:[redacted]30
https://pisga.tik-tak.co.il/webPro/hishtalmuyot/student/index.asp:UNKNOWN:[redacted]49
https://accounts.google.com/AddSession/identifier:[redacted]@gmail.com:[redacted]10
https://accounts.google.com/signin/v2/challenge/pwd:[redacted]@gmail.com:[redacted]16
https://www.epicgames.com/id/login:[redacted]@gmail.com:[redacted]12
https://account.gov.il/sspr/public/newuser:UNKNOWN:[redacted]55
https://login.gov.il/nidp/idff/sso:[redacted]49:[redacted]@100
https://ps.btl.gov.il/:UNKNOWN:[redacted]079
https://my.account.sony.com/central/signin/:UNKNOWN:[redacted]30
https://www.harel-group.co.il/Pages/default.aspx/:UNKNOWN:[redacted]10
https://lgn.edu.gov.il/nidp/wsfed/ep:[redacted]: [redacted]3
https://www.amazon.com/ap/signin:[redacted]@gmail.com:[redacted]2020
https://apps2.education.gov.il/EduLogin/setpassword.aspx:[redacted]@gmail.com:[redacted]2020
https://accounts.google.com/: [redacted]@gmail.com:[redacted]1980
http://yesodotarts.tikshuv.org/: [redacted]: [redacted]4Y4h4y



ThreatMon

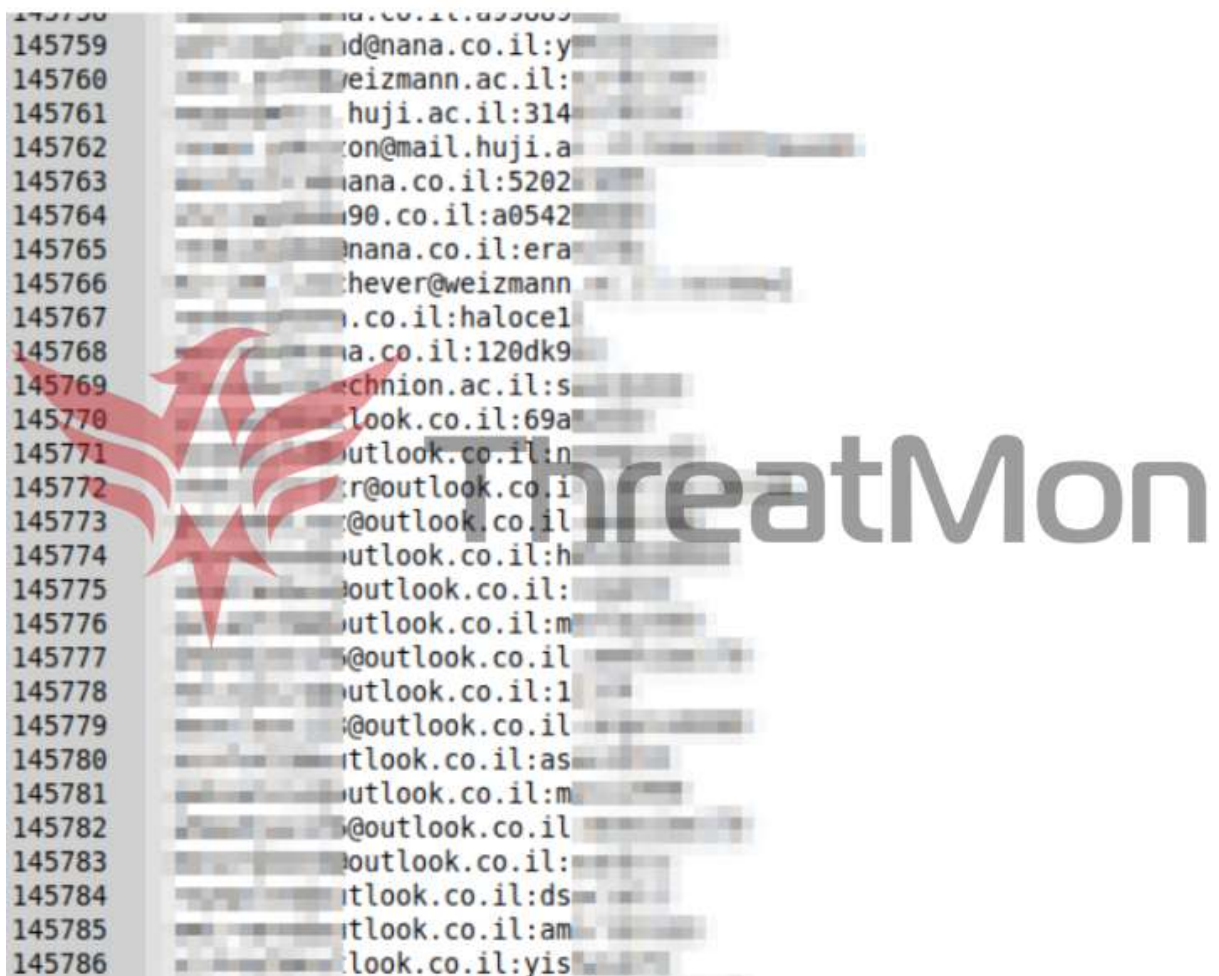
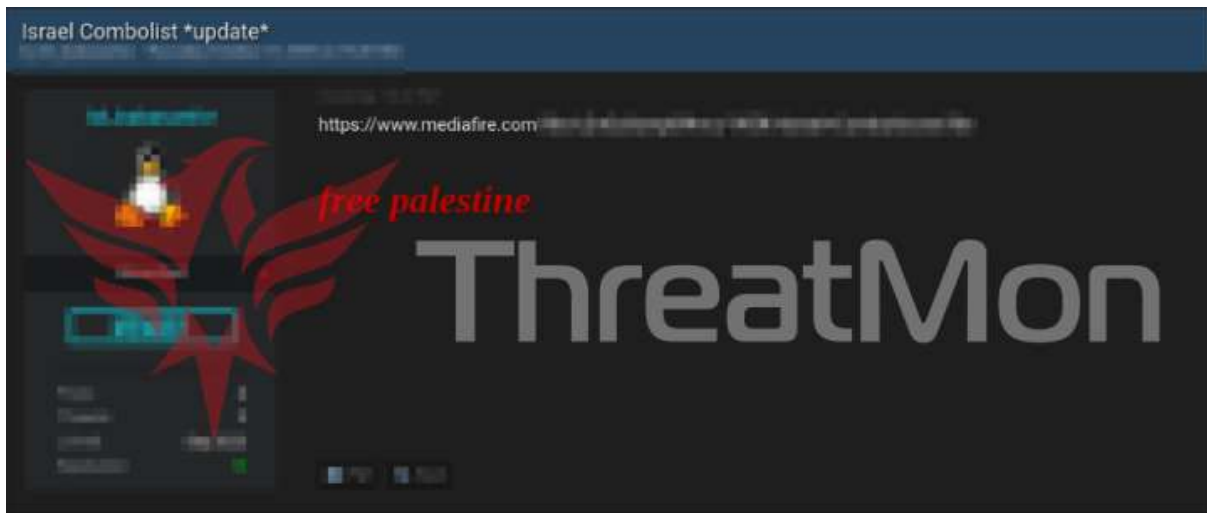
- 13) According to the post shared by the threat actor named "Ddarknotevil", which was detected in the dark web forum in the scans made by our team, it was revealed that he claimed to have hacked Wobi, an Israeli insurance company, and captured its database. According to the threat actor's claim, the database contains columns such as Names, Emails, Hashes, Addresses, Gender, Phone Numbers, Date of Birth. The total data file size appears to be 13 GB.



```
[redacted]INSERT INTO email_stats (id, email_id, lead_id, list_id, ip_id, copy_id, email_address, data_sent, is_read, is_failed, viewed_in_browser, data_read, [redacted] FROM [redacted] WHERE [redacted] ORDER BY [redacted];
```



14) According to the claim of the threat actor named "lol_babasanfor" detected in the dark web forum in the scans made by our team, 145K Israel combolist was leaked. When the leaked file is examined, there is a 5.09 MB file in .TXT format. The file contains e-mail and password data.





- 15) In the activity detected by our team in Telegram, the threat actor named "Cyber Error System" announced that India is helping Israel to attack Palestine in the cyber world and that they will fight them to the end for Palestine.

CYBER ERROR SYSTEM



#OpIndia #OpIsrael #OpAmerica

India has Helped Israel Attacks Palestine in Cyberspace.

America Has Helped Israel, Sending Various Weapons to the Israeli Army, to kill Hamas troops.

we will fight for Palestinian independence, in cyberspace.

[#SavePalestine](#)
[#OpIsrael](#)
[#OpAS](#)
[#OpIndia](#)



ThreatMon

- 16) In the activity on Telegram detected by our team, the threat actor named "Cyber Error System" targeted the Madhu Vachaspati Institute of Engineering and Technology. As a result of a DDoS attack on their website, it became unusable for a while.

CYBER ERROR SYSTEM



Madhu Vachaspati Institute India
HACKED BY CYBER ERROR SYSTEM

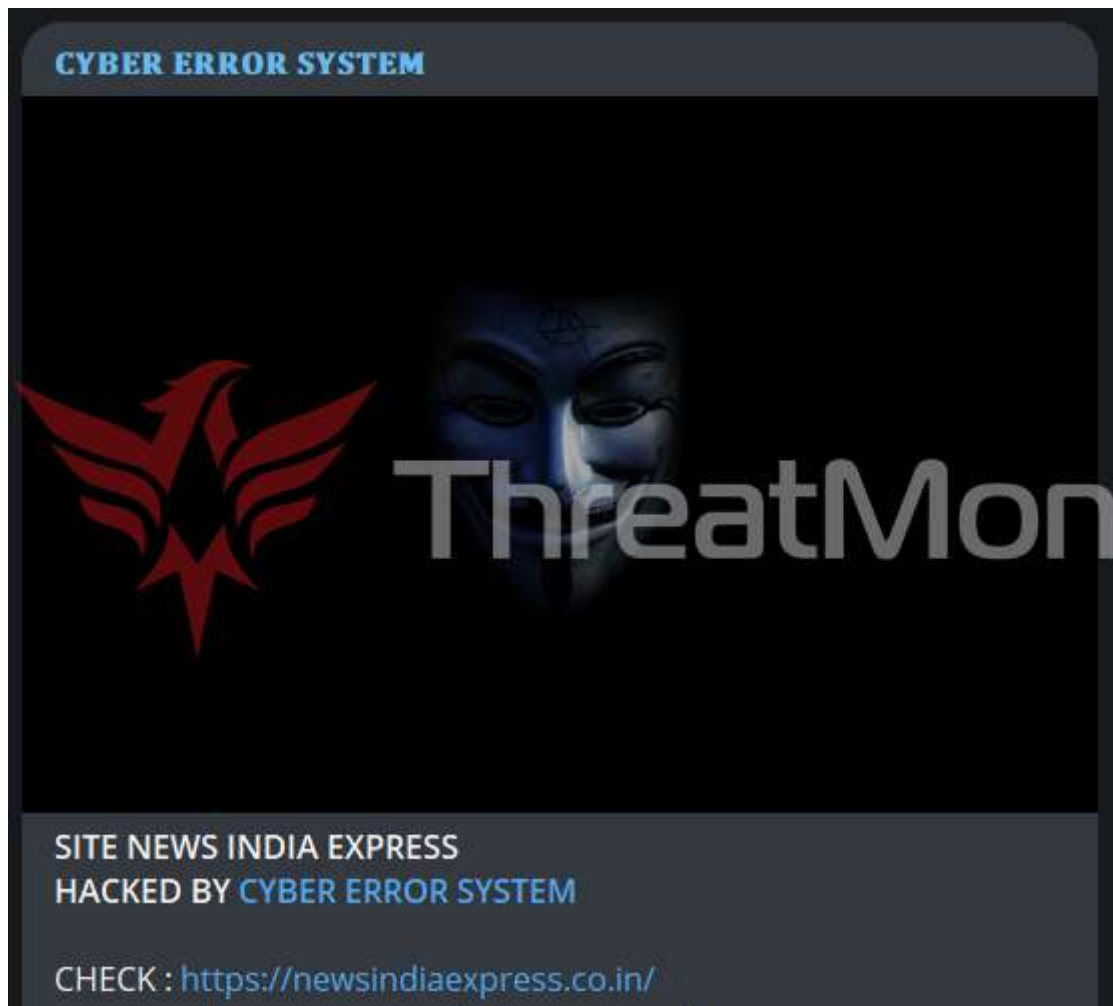
SITE : <https://www.mviet.co.in/>

#Cybererrorsystem
#ganosecteam
#hisbullahcyberteams
#hacktivistindonesia
#gbanon17
#garudasecurity
#SavePalestine
#OpIndia
#OpIsrael
#OpUs



ThreatMon

- 17) In the activity on Telegram detected by our team, the threat actor named "Cyber Error System" targeted websites. As a result of a DDoS attack on their websites, it became unusable for a while.





- 18) In the activity on Telegram detected by our team, the threat actor named "Ghosts of Palestine" claimed that they would target NATO countries (except Türkiye) and India for supporting Israel and remaining passive on Palestine/Gaza.

GHOSTS of Palestine TM



#Update:

Nato member countries will be face an cyber attack by us for supporting Israel and being silent about Palestine/Gaza.

Turkey excluded.

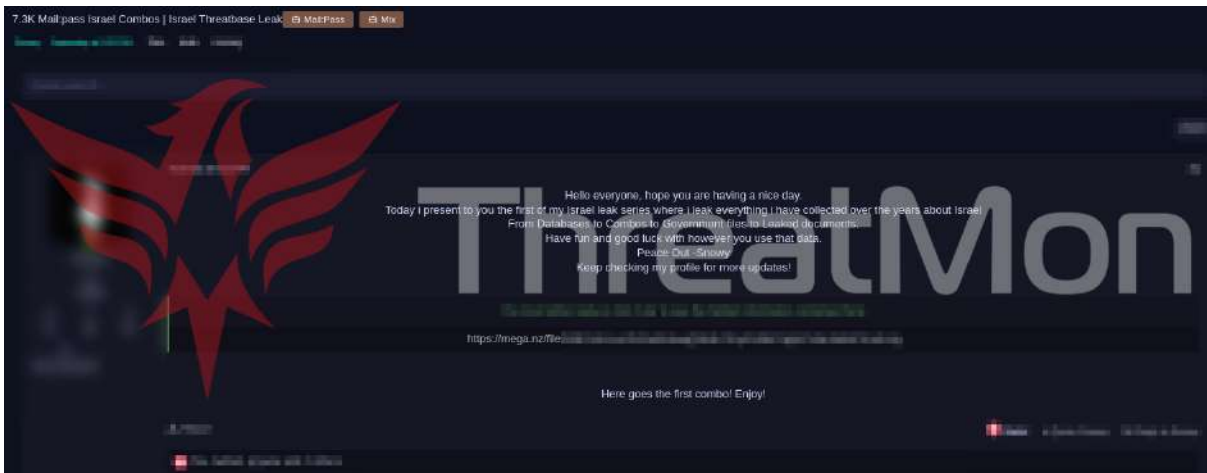
Asian Country - India will be attacked soon.

If they support Zionism you better secure your site because we are coming.

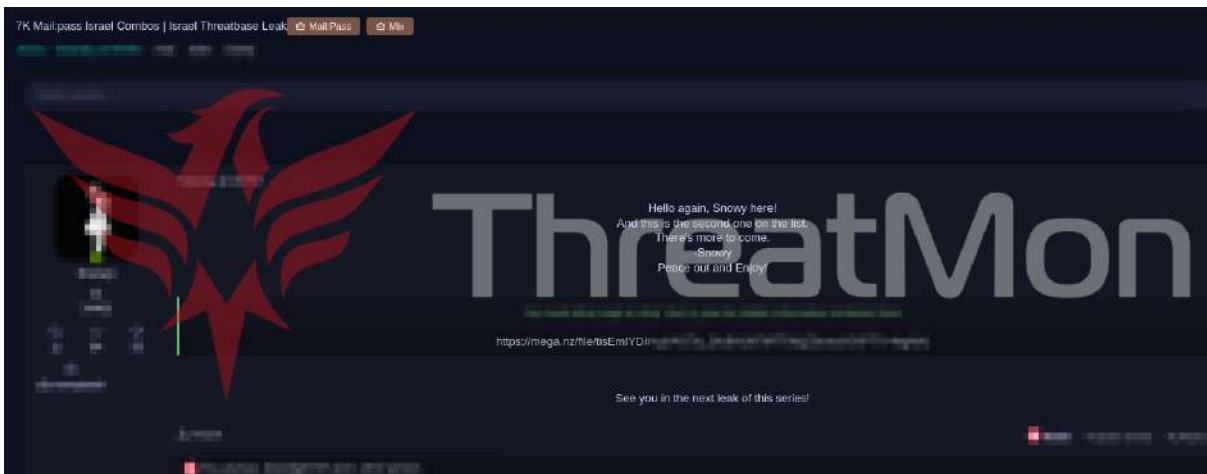


ThreatMon

- 19) On 12 October 2023, a threat actor named "Snowy" was detected posting data on a dark web forum with the statement "I present the first in my Israel leak series, leaking everything I have collected about Israel over the years". The threat actor stated that he would publish everything from databases and combinations to government files and leaked documents. Then, without slowing down, he published 7.3K lines of combolist data.



A little later, in a second post, he announces that he has shared a 7K combolist file by saying "And this is the second one on the list".





ThreatMon

The data leaks are followed by 5K combolists, and another 5K combolists, 2.3K combolists and finally 2K combolists, ending the combolist posts. It is seen that the next targeted leak content was on Israeli phone numbers. It is seen that he leaked a total of 570K phone number data.





ThreatMon

The last move of the threat actor was to leak the database of 420K Israeli Business. When the leaked file is examined, there is a file in .CSV format with a size of 86.63 MB. The database contains ID, Cat, Company Name, E-mail, Address, City, State, Postcode, Telephone Number, Fax Number, Sic Code, Sic Description, Web Addresses.

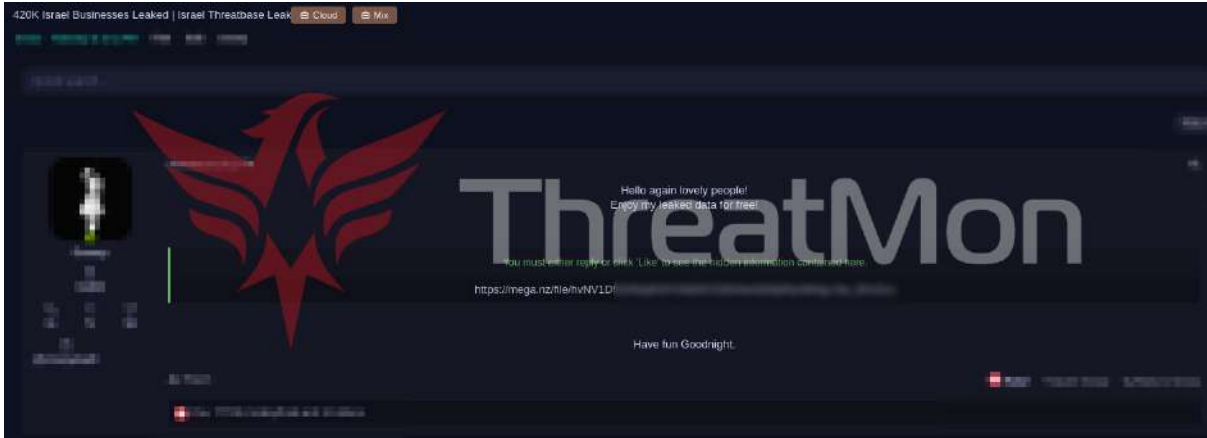


Table of 420,000 Israeli business records. Columns include ID, Cat, Company Name, E-mail, Address, City, State, Postcode, Telephone Number, Fax Number, Sic Code, Sic Description, and Web Addresses. The table is partially obscured by a large 'ThreatMon' watermark.



ThreatMon

20) According to the post shared by the threat actor with the code name "0xv3v1L" in the dark web forum activity detected by our team, Mondial telecommunications company located in Israel was targeted. The threat actor unauthorisedly changed the appearance or content of the website with a deface attack. As a result of this attack, he posted a "zone log" on "archive.is" and "ownzyou" platforms as evidence. The threat actor leaked domain and user information in the forum.

The image shows a defaced website and its archive.today capture. The top part is a screenshot of the defaced site, which has a blue header with the text "Operasyon FCK ISRAEL mondial telecom owned" and a "mondial telecom owned" button. Below the header is a large red phoenix logo and the text "ThreatMon". A list of URLs is provided: <http://mondialtelecom.co.il/>, <https://archive.is/trwT2>, <https://ownzyou.com/zone/186770>, and <https://www.instagram.com/mondial.telecom/>. Below the URLs is the text "buda domain panel bilgileri" and a URL: <https://domain.internic.co.il/index.php> followed by "telecom.co.il:" and "508".

The bottom part is a screenshot of the archive.today capture of the website. The header shows "archive.today Saved from http://mondialtelecom.co.il/" and "8 Oct 2023 16:30:58 UTC". Below the header is a red phoenix logo and the text "ThreatMon". Below the logo is the text "Owned By 0x" and "FUCK ISRAEL".

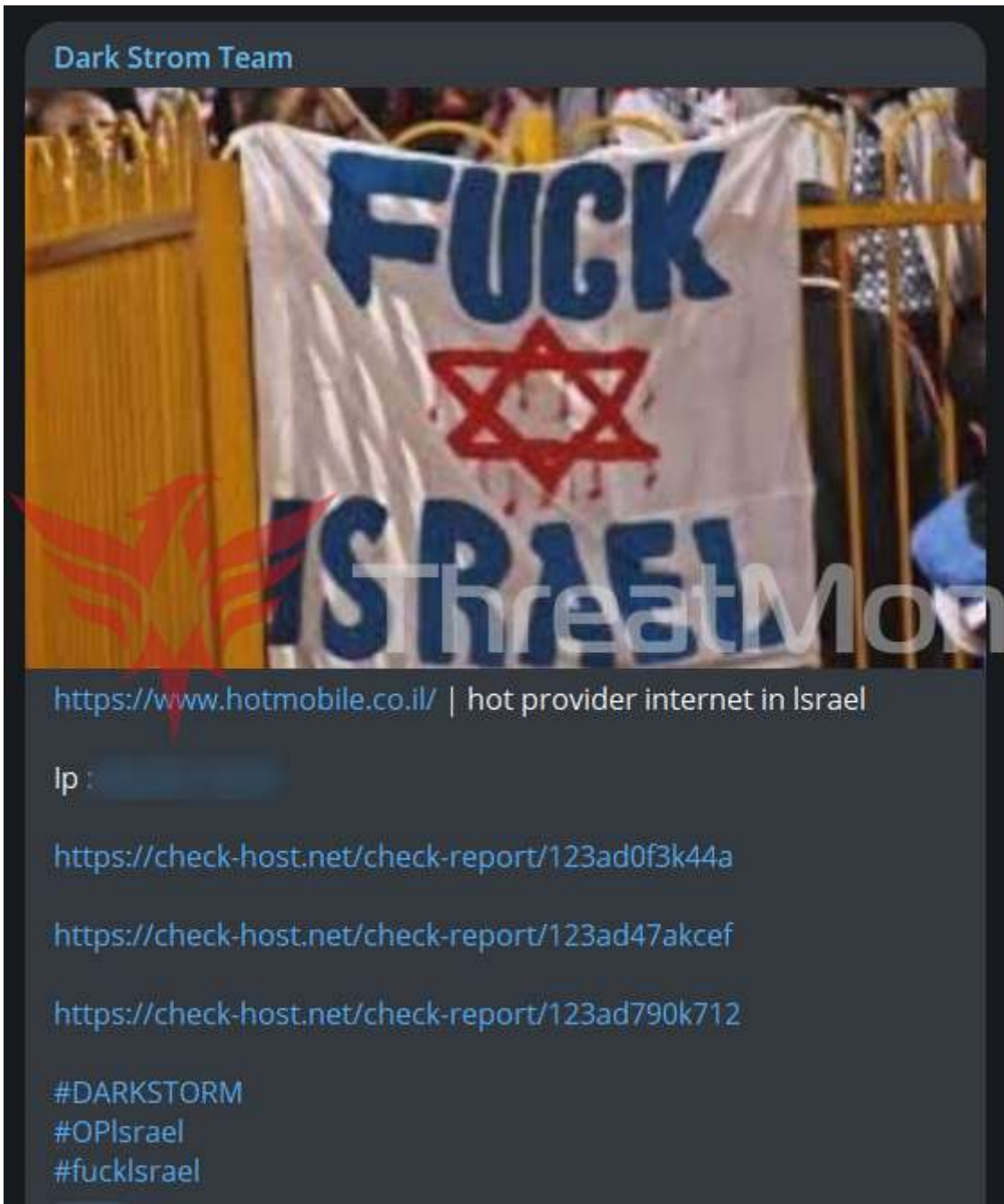


21) In the activity detected by our team in Telegram, Israel's first online website, "Walla!", a part of the Teletel Communications Ltd. company, was targeted. Communications" was targeted. When the .rar's shared by the "Mujahideen_2023" group were analysed, it was found that sensitive information of the employees of Walla!.

01/05/1998	@walla.com	5231
23/09/1998		5445
04/06/1998	@walla.com	5066
15/02/1988		5432
02/12/1996	@walla.com	5065
09/11/1997		5589
14/05/1997		5497
29/09/1997		5239
14/10/1998		5272
30/09/1998		5098
07/11/1997		5064
05/09/1997		5044
17/03/1998		5327
16/05/1998		5033
13/04/1997	@walla.com	5435
02/10/1997	@walla.com	5026
24/04/1997		5477
14/09/1997		5423
10/09/1997	@gmail.com	5092
22/02/1997		5487
23/03/1997		5448
08/03/1997	@gmail.com	5256
01/05/1998	@gmail.com	5431
17/07/1997	@gmail.com	5452
16/08/1998	@walla.com	5494
12/07/1998		5491
02/01/1998	@gmail.com	5226
11/10/1997	@gmail.com	5862
08/09/1998		5254
05/03/1998	@gmail.com	5499
18/05/1997	@gmail.com	5092
05/01/1998	@walla.com	5428



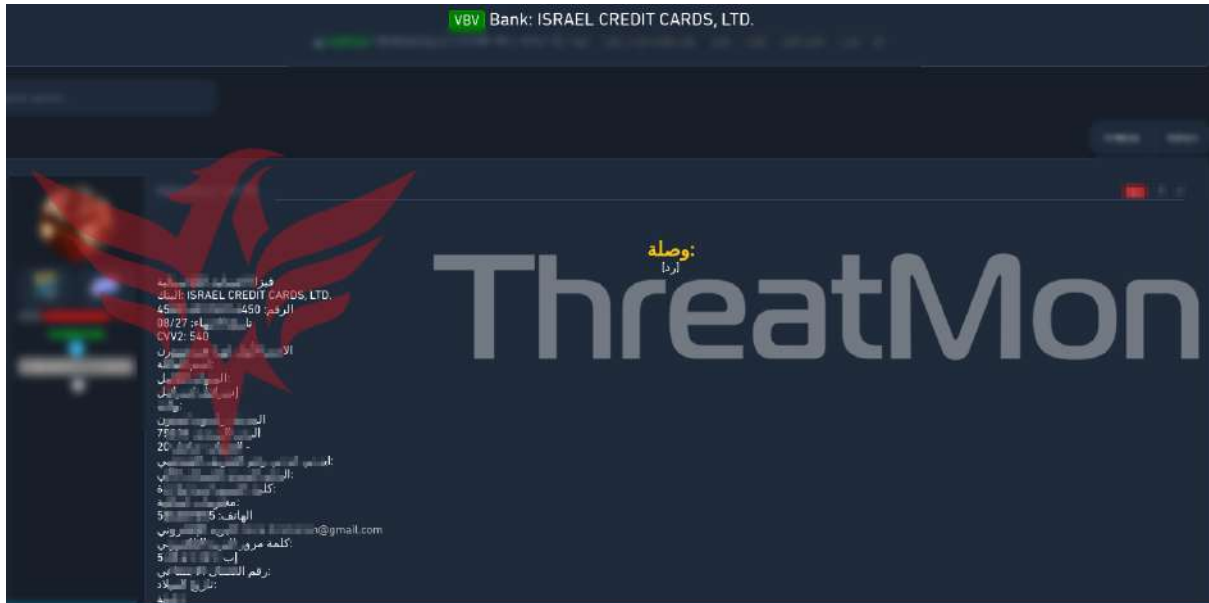
22) In the activity detected by our team in Telegram, Israel-based wireless telecommunications company "Hot Mobile" was targeted. As a result of the DDoS attack by the threat group called "Dark Strom Team", it could not be used for a while.





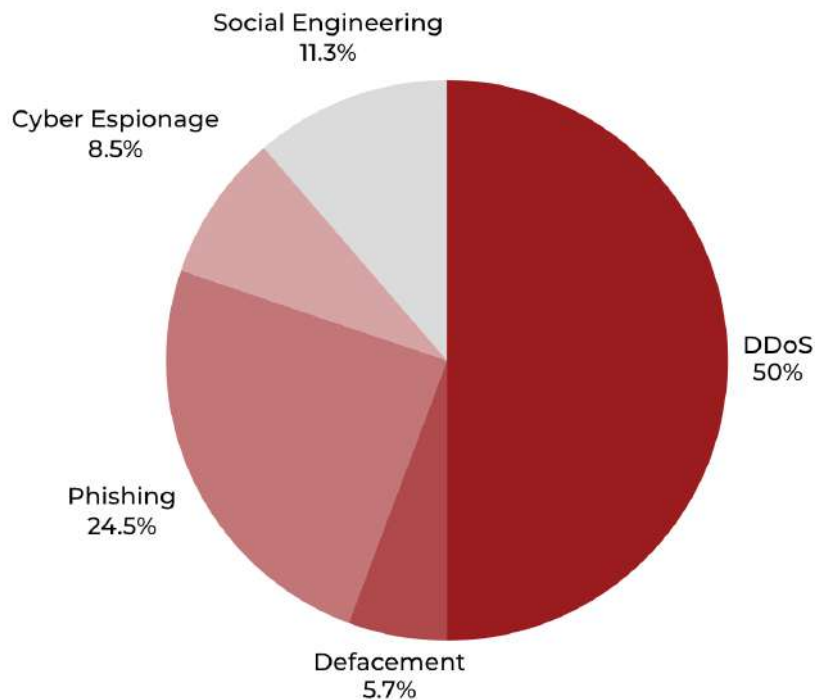
ThreatMon

- 23) A threat actor named "naseemalz", identified by our team on a dark web forum, appears to have leaked all bank account information data of an Israeli Credit Card user. The leaked data includes bank, number, expiry date, cvv2, name, city, address, telefon, e-mail, IP, etc.





Attack Tactics and Techniques Used by Pro-Palestinian Groups and Supporters



- **DDoS Attacks (%50):** Pro-Palestinian groups use DDoS attacks as the most common and effective cyber attack tactic against Israel. This tactic involves sending massive traffic to make Israel's online services temporarily inaccessible.
- **Phishing Attacks (%24.5):** The second tactic used by pro-Palestinian groups is phishing attacks. These attacks involve deceiving targeted individuals in order to gain access to sensitive information or harm their targets.
- **Socail Engineering (%11.3):** Social engineering tactics are another method of attack used by pro-Palestinian groups. These tactics include social manipulation techniques to achieve their goals.
- **Cyber Espionage and Information Gathering (%8.5):** Pro-Palestinian groups can use a variety of techniques to gather sensitive information and harm their targets, using cyber espionage activities used against Israel.
- **Web Site Defacement (%5.7):** The last tactic is changing the targeted websites. This tactic can be used to convey political messages or as a symbolic act.

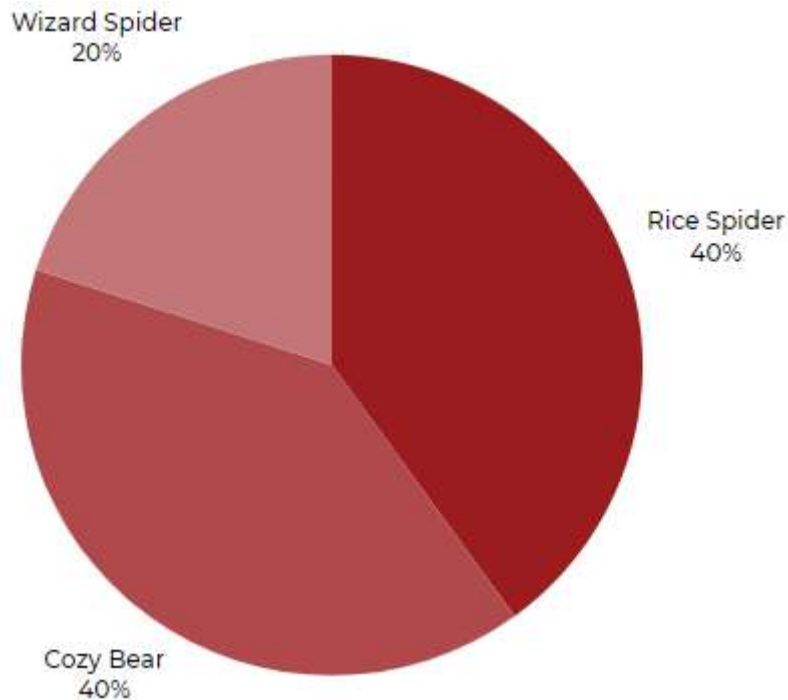


ThreatMon

These statistics show the cyber-attack tactics and techniques used by pro-Palestinian groups against Israel. As can be seen, DDoS attack techniques are used intensively. In addition, it is clear that cyber espionage is targeted with the knowledge gained through phishing and social engineering attacks. These tactics reflect the groups' efforts to be effective in the digital arena in the conflict with Israel.



Threat Actor Groups Active in CyberWar



As a result of the studies conducted on more than 200,000 attack vectors centred on Israel and Palestine through the Threat Feed area of the ThreatMon Advanced Threat Intelligence platform, three different threat actors were traced, as indicated in the graph above.

All of these attacks of APT Groups were detected on Israel. The reason for this is that the electricity and internet infrastructure of Palestine has been cut since the day the war started. Therefore, the attack could not be realised.

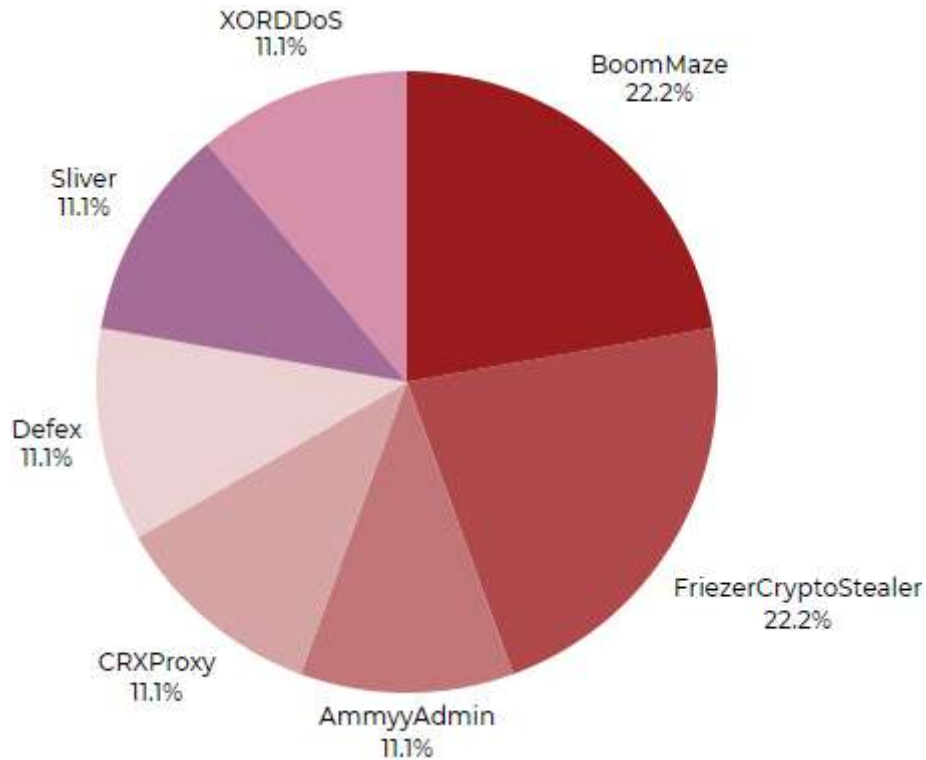
When we proceed through the graph above, there are 3 APT groups whose attacks are actively detected. All of these APT groups are Russia-based APTs.

The important factor here is that the increase in the attacks of APT groups politically is that Russia supports Palestine and therefore is against Israel.

As a result of all these attacks, the purpose of APT groups has been observed as cyber espionage and information leakage through Israel-based systems. As ThreatMon, we predict that with the prolongation of the war, APT attacks will increase and the cyber war environment will become more chaotic.



Malware Active in the Cyber War



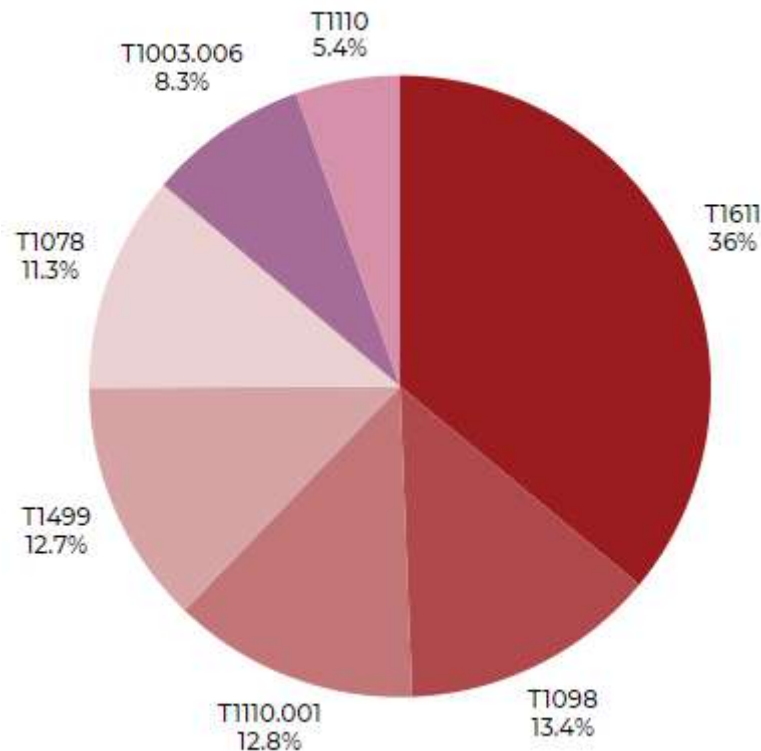
As a result of the studies conducted on more than 200,000 attack vectors centred on Israel and Palestine through the Threat Feed area owned by the ThreatMon Advanced Threat Intelligence platform, as indicated in the graph above, traces of malware distributed by many different threat actors were found.

Here, the malware that play an active role in the cyber warfare environment are shown on the graph.

At the end of the research and analysis processes on these malware, it was observed that most of them are malware designed to work connected to Botnet networks. The important point here is that although the types of malware traced in the cyber warfare environment are different, their objectives are the same.

These detected malware are especially malware with information leakage and ransomware capabilities.

Techniques of Attacks Taking an Active Role in Cyber War



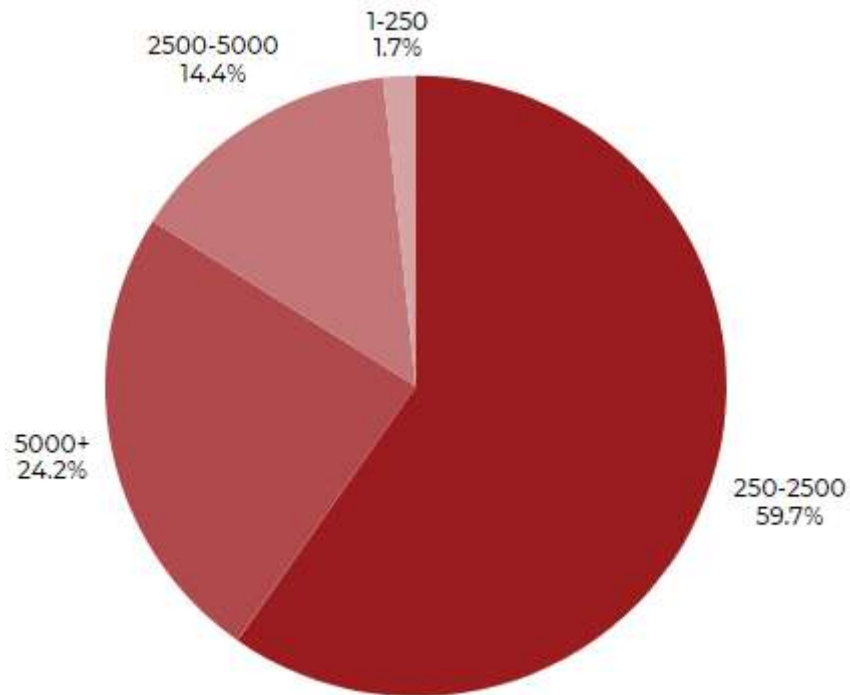
When the techniques of all of these attacks detected by ThreatMon are analysed, the most important and most common techniques in the cyber warfare environment are indicated in the graph in accordance with MITRE ATT&CK standards.

When the "T1611" technique, which has the highest share on the attacks when proceeding through the graph, is examined, the technique with the name "Escape to Host" is given in the graph with a share of 36%.

In addition, this technique is followed by "Account Manipulation", "Brute Force" and "Endpoint Denial of Service" techniques. When it is inferred from this, T1611, which has the largest share in attacks, aims to access the system from Docker containers on servers. "Account Manipulation" and "Brute Force" aim to access systems on users. And finally, "Endpoint Denial of Service" attacks, which are preferred by the most threat actors and are a relatively easy attack technique, are among the attacks detected especially in the attacks on Israel.



Size of Firms Actively Targeted in the Cyber War



Based on all these attacks detected by ThreatMon and through the extended information obtained through the attacks, the size of these companies are listed on this graph, as well as the attacks on Israel-based companies in the cyber war environment of the war between Israel and Palestine.

Through the data given on the graph, as ThreatMon, our inference is that the size of the companies targeted in the attacks consists of companies with values between 250 and 2500 employees with the largest share. These companies, which can be considered as Small-Medium scale, are composed of companies with more than 5000 employees, which we can characterise as Large. These companies are the second-sized companies targeted in attacks. The rest of the list consists of Medium-Large sized companies and Small sized companies with the smallest share.

Here, considering that the digital assets of the companies targeted in the attacks are developing and growing companies, the size of the targets can be measured statistically through these graphs on the cyber warfare environment.



What Awaits Us in the Future in the Israel-Palestine War?

It is a fact that in this war environment, which started on October 6, 2023 and continues from past to present, the war between Ukraine and Russia is not limited to military operations only, but also moves to cyber war environments.

However, currently, in the cyber war environment between Israel and Palestine, there are 76 threat actors supporting Palestine and 20 threat actors supporting Israel. These threat actors are the number of threat actors who have publicly declared their support and are actively attacking the institutions and organisations they target.

In addition, malware belonging to APT groups, which have not publicly declared their support but are known to carry out attacks on both Palestine-based and Israel-based systems, have also been observed. These APT activities are malware distributed by threat actors that specifically target the telecommunications industry.

Since October 6, 2023, the most common attack type on Israel-based systems has been malware distributed via e-mail addresses. It has been observed by ThreatMon that this increase is a 30% increase compared to last week. Methods frequently used by threat actors, such as Ransomware activities and Botnet activities, continue without an increase for either side in this cyber war environment.

In the future, in this war environment, when countries and their leaders declare their political support in the adapted and expected scenarios of the cyber war between Ukraine and Russia for the Middle East and the Palestine-Israel war, the attacks of the threat actors in those countries will increase, regardless of the size of the opposing party. An increase is expected in attacks, especially in the Infrastructures, Citizenship Systems, Telecommunications, Logistics, and Healthcare sectors.



Conclusion

This report has been prepared to examine the cyber warfare dimension of the long-standing conflict between Israel and Palestine. The Israeli-Palestinian conflict is not limited to its military and political dimensions, it has increasingly come under the influence of cyber warfare.

The cyber war between Israel and Palestine reflects a complex situation in which both sides continue the conflict in the digital sphere using their cyber capabilities. Both parties are openly supported by threat actors and are carrying out cyber attacks. These attacks are particularly focused on critical infrastructure sectors and pose a major threat to sustainable social life.

The political, military and economic consequences of cyber war threaten not only Israel and Palestine, but also companies in various sectors serving the region. Such attacks make conflict resolution difficult and create new security threats.

In the future, cyber warfare is expected to become even more sophisticated. Cyber attacks, especially those similar to the Ukraine-Russia war, may increase in the Middle East and especially in the context of the Israeli-Palestinian conflict. Cyber attacks may increase further in areas such as infrastructures, citizenship systems, telecommunications, logistics and healthcare sectors.

In addition, detailed analyses of the cyber warfare environment through the statistical data given above are shared in the report.

By scaling these analyses with your own company, you can work on strengthening your security systems by considering the Israeli-Palestinian war scenarios in the cyber war environment.

It is hoped that this report will shed light on this important issue and be a useful resource for all companies in the relevant region.

Whenever you have any questions or requests for additional information, do not hesitate to contact us. We will be happy to assist you.



Indicator of Compromise List

As ThreatMon, we care about your security in this cyber war environment. By providing the necessary integration of the list to the security products through the SHA-256 Hash values in the IoC list below, 200 IoC data carefully selected from Israel and Palestine based data sources from 6 October 2023 to today are listed below in this period between Israel and Palestine, where various threat actors show activity on a global scale.

Important Notice: The hash values listed here in SHA-256 format are not guaranteed to be used as an attack vector in an attack or malware in the cyber war between Palestine and Israel. These hash values are the hash values of files containing malware activity seen in Israel and Palestine since 6 October 2023.

IoC Type	IoC Value
SHA-256	016a20e198d889b9b65fc938f4285ac0ad728a38a5afc9b6659cedc1b4a759ed
SHA-256	0ff134057a8b2e31b148fedfdd185f5b1a512149499a8c5c0915cf10b10a613e
SHA-256	2dd1fe89eef0ba99f4b72dcbd4a5b874708121480e916e4c88d2dbb8398bef1b
SHA-256	815dcdf0078108bd5afa21c1428d392b423a68e6935676c49102c6f0bea99d6d
SHA-256	f887e04ce6c43da608cfcb45e51398305bb3912ee9d88ac7569c917e245d404a
SHA-256	0e31f55a21fcf8762ab4238c99c923a1995996c5d2375bedeb15ef466514f30b
SHA-256	5d92914acdfb551c237866cc4cce6c80aeceb695e52beecd2613694302c62271
SHA-256	ea8205f225d51e85214845bdf800740a231e15754384511f7a9a93317469180
SHA-256	2ae03f2efcabdb54a38c92ad77cbc9575709f9d76bb7877a02457eca82b3f48e
SHA-256	eefc50ff827c1785a740258d0f18bd87a758a80b6f898c1582f15ff8a0382306
SHA-256	d77fbaa35585f25de3f492e4e3d0bfa6f0f73b053fd6a64058766fef75eca04e
SHA-256	ad441253f8ebe56e6c216d5a95c9107407c911080c57deb9a9aad8973d36a13a
SHA-256	0f898ab1619220fedc066e5ca65fde3ea6740f0ce68d2ba93220688940bb1b7f
SHA-256	2522e04f7abcd7c32d2c73aa0e66d97d0d121e86aefc7e715dd013e8e27a73f3
SHA-256	18df68d1581c11130c139fa52abb74dfd098a9af698a250645d6a4a65efcbf2d



SHA-256	b7c296942c605bea21b5dfa843190e8619286a4b6ea432d872246bae9b346000
SHA-256	9e766f6ac15d73deb5829eb2d5cedd3ac180a5a97fdf19024f55ab01322bf1d3
SHA-256	3d01520d6f211ef408c4fb4bc80ea617da938608b4c8706f7958448e5d7a08bf
SHA-256	607ea1c8b3d09ad76a7f364c21f4b91fe8832ad19fa1efa40e3e6c3881048e71
SHA-256	fd7499214abaa13bf56d006ab7de78eb8d6adf17926c24ace024d067049bc81d
SHA-256	9b1c965430289c82edff635e1b7650abddf9753e6ebe5e66f13770a766375f2e
SHA-256	5e8ddd10a4d9e33d8b2072264a2c0cdb6d7d2502b59710ac70577cab7980764e
SHA-256	83fe6929f55fc4112d73b3fb35bf50d90bf5c1c5bb9a5cf47dd0f1ad140ee630
SHA-256	953cf938a09ddd4db5fcb6ee3439abca6ef47740a8c0f4b062cb8e2bb23be0c3
SHA-256	c1884df08a8753d9b5bf6e403534a5f2a19347da4bf0f016b2a3d792d79d2197
SHA-256	1545ae8cd3c42a4bbe200387caad812e569ffc468c677c671391e69e7d373580
SHA-256	f8f03eb41c0b00aa6131804a787a6cc7a2a75c26539b5859f551dde077f8fc06
SHA-256	bbe4f4e1df9ab0edf1c599780f243c87fcaff76bf7772cdd37511185c802cec2
SHA-256	61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
SHA-256	4a5bdf328d682efaec55979b3e0723db5bb79775c7c133936c779e3bdc03201d
SHA-256	415e04eb340f1b092288cbcc71295a2c95e864fc1bbfcd55d6e3f5aa67099b1a
SHA-256	7d7c9b407e4ecb92c554a8813625f9e27b85231348f0ebbb0ff3531488160878
SHA-256	f3674df3162514f00fa67bd242d5449a359e05df32d3a4316c7951399692836e
SHA-256	e06a094d0bec6020536cdb92f0bd2171e48ca36b3f34b8ffd6da7f52f78436ec
SHA-256	8d0b92e4458a052969add4f23b07e8c05d48bb0868bb650bc58c2cc074f559f2
SHA-256	c83a62bccd3cb73772875dfedd41faf7b1f44118a39abc7e3f65faea8e7ad67e
SHA-256	4d8711055022ac708e1d36687f8884e507b583435cfabafa0d7032072c10373a
SHA-256	d938d80f5f97b1e50c496dca63d5f78ba48c36924946434159c3362c24d2e6d7
SHA-256	b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34
SHA-256	10cf4817ef64c066405db6f601ae00d75935c56ed9d64115488bb429dfffb83d7
SHA-256	fbe8af35d5259c0e9d1a85fc754504c62667cc9d3bcd581e9d36fcb641cb246f



SHA-256	02640e1dd5e7e7ea7a3b89ed9b7691ae934782013cb21b07905dc3b63782dd6a
SHA-256	5db145489890a82d3bbaade586301bc43c22e2a548528ac40f552f5599f1d1c
SHA-256	7cbfb088ca3e6fd64001fd6a12893981cddfa2dbb18f7643fe02d2a13cc329c4
SHA-256	c73620f5bb8767150d7fe143bee059b1608e988c27abecf2d74e5bde29c3c2d9
SHA-256	3a3adf8d0bdcd0e19fe0a094faab539890291da07dfd2ff6248c6cc352d03d4a
SHA-256	e12f8f6ec2389d04dc3d5ab4e0be80fb0aca65dd76abbf3c452e6dee371962d6
SHA-256	b3ba2ee4b97b3e247cca9cb8cdb356cf6ac2fa160ff3cc0e05d65615fe2e1b64
SHA-256	d8911b82b4afe86b6e78d7b52a5ee77f5f879bc98d5ada1d4acfdb4286955791
SHA-256	8b0a5a28132045e3e5ec4584852e690500177a5b2ea4cbc4733a8c6cd7aa3bed
SHA-256	5f4ef152e62ab08f5ef1c4961c4f1d96ee28d8cfb72289856bf42e81d6497e2e
SHA-256	e74c24d70c3ebb75f1767a60024501b072b7404945a76ba8f9a4bb89ea585f7c
SHA-256	3a6233951627ac4b0660e93aadf2cd9bc1ac38c7979b4e70fa54ca3a396ac314
SHA-256	72743f8d18d566745a9132d0bf8cafb00c1dc5d125538f41a651ea5110b73d79
SHA-256	89a34c981357ead140d03c50c6db909498a355b1d510ed558ce242bfc1b5069a
SHA-256	b6d6e0d1dce867836a684a0af278e46ed4a50be49a784ab7bfc3ed59841c9d0
SHA-256	3ae96f73d805e1d3995253db4d910300d8442ea603737a1428b613061e7f61e7
SHA-256	7393097678fe782b7a3fbdf29330eb51fde54cf5c7f8cdd5b7a05075efeade5a
SHA-256	6268d17128de5cca14a8952ac8c8b32d3585e3af3d848e0d117d54c338c88e6e
SHA-256	4c7bade8a3ed1e74d03e0021737f9160c18e62fb85e9cc7eb5f5a21d4e7f1000
SHA-256	1b385604d945f9a600f47439e3673452e0b83642423205403d5d638f85d38b18
SHA-256	84be47f95a3422f33b93fa9549b916885ff113258f21c13aa2ffbab7aea5cfd4
SHA-256	6606a4519d6671cb7d1dbae04154e82002bad86276d801cd2f0c5ab3f5603c27
SHA-256	36f49c52a84e5919fe698a8f0f564af99b1c14726d9ca6b3eb112cb8c022fa2c
SHA-256	51658887e46c88ed6d5861861a55c989d256a7962fb848fe833096ed6b049441
SHA-256	4cc9c11ddf0f4583ec76e8ce266e71367538ebfc7587d53b6cca8274f87bf0f
SHA-256	204b8ecdeb317bcaed5d260387ff0bc9076402d996349c277f6cc89121a5fb37



SHA-256	01505deebc2976bd8d75f2e18dbc242d8c87c1b886eb4b2bcfa32ee25e31584b
SHA-256	e7a6b1823307f1e79b6d3a9fc3da2e44455c768f8e27a4052855390d97a2d1f0
SHA-256	77b9a509d4fa77d6da1186ab3d920532c742fe50273ba97207e89adce91e2e3d
SHA-256	4a5bd17d3ac3bd04f169fd683ace7efdac8828c9eae23186f2cc890fcbc54c17
SHA-256	cb57d1c001114d560ae91116cf23c18e3124a2016ea278f4edc9fd80de42b180
SHA-256	cbd91081616d6be04e5fc17ef72ed805e283c5db1fa1bbb594ad79bac09bfd5f
SHA-256	be7f171061697229768b4991d5cf177dfa71b7cc963fba7f75c0bf7294f02fc
SHA-256	35582950ed05ce5e0a331f68f205b5da5335c2b33f128834c32efd83605b585b
SHA-256	3f180e089c9167eb765bec4cc6859745feede762ae3f329296ece5b707383372
SHA-256	978a686c183fec034955a087b44e23280994c2abce4a416bd34a7b55eda2e6b9
SHA-256	750919c0c291b5c40e2f73c7ee101016d0dd20766d53ee27f368db9bc64a1385
SHA-256	bd84ff36a0ea7f9dd1466efd849adc86ad26a1017bae3660d68851a9350bbb54
SHA-256	5ae9c0ec527ca0b93d23a6d28588ee9651ce921f8c0afb980bda4808b9ce9765
SHA-256	eadb49dd95f7f8b24d48299b574787da19f383a301c44d9099e3b00cd46a6a44
SHA-256	1a891c545774aa81d1365d9f84f1e7528922df6798e13106056405f027ddde7c
SHA-256	b28d0d83c894c144a5f9bc36b936c861b038c7218414e51472e7c9b9e3fd67ea
SHA-256	8ae32bf96105ff433c9c9fbc8b69f09736afbb270bf4ce1d0e7b3f3292097b34
SHA-256	8a819e695c75616a733fc5a3cd4d0efcc8b480b76478600497edc660a7e94342
SHA-256	29f95d959d750352a1dfdaeea315b421195d91d625248a8886420f3173b89368
SHA-256	0562fd7c3fbd49a049c7b9bf9c01ee9250d971f6931d9f5b15a8350b3f8ebb2f
SHA-256	68a989e60b520b311889181ac47e01b0001d51c9161cae980f78c7d30630fdc2
SHA-256	04f5943fc7ec6df0accacf51d3aace0c1e075e2da5e683083b5a6d955a7b5ef2d
SHA-256	fb12f7c1c897888496b23d7a175e3157336b97520a71ee8a9053b70e81aed104
SHA-256	eeb622317f1b4822356c2ddbe0debfa154c39d8be362908fcb613fa740f3ee
SHA-256	8869c44219364f911548cb18da0cc6413b3277d3a8a8df18d0a521b558830d6e
SHA-256	5144e31e94bee71c52347c42b33c2c6ef35dd872d226ffc3a407f3757882413d



SHA-256	a500b238ec483181fc6ec328103c991096a9377a892c28d0c0bb7364c5c152bf
SHA-256	3e95f3c963a2a08efd127f6f26b96d25f100ca2b382c72f1812c90340fd37136
SHA-256	0c88db0f9bbf4525dfd3cd166f5a4e58c6c9ec7d8e567796f91c8fce0c731126
SHA-256	775c38a666d750292c4a2feaf15a492f75f41bcd13e4c076fbf6c2311ddacaf0
SHA-256	3bc8b7528168eee902093ad454a0713fc642493244362c89849446d834ae5e61
SHA-256	d8557a8feb4555c4daa426b0c26881712b4be22610caf924079a454150611736
SHA-256	7852fc7df542592d3935fd5b505f9447080cd1f71f5be6a542bcaaf7a5f7278e
SHA-256	aced782ea8a1621955c6ade07769eab61bacb171a14f77037b2690834e1e742a
SHA-256	2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73
SHA-256	2601047bca99cdfaf23b33d0de884f643547d04a091b3360d7da4cd4f4985445f
SHA-256	9006b7c9428d33596cbad41adbde739ce335f5abb10349305a65548fdb30d0f
SHA-256	cc705f2722f947c2051582caf40fd3218a4a8340f64ca8291f82ea10373dbaea
SHA-256	0d1c6e79d316846fbc2608ad56ee3a2bc0d2ef2604e13daeed2efd4d316002bf
SHA-256	a528ccb23d570a59ed0dc484020dcc66a50983d43bea1ea5b9e04e70714bdedc
SHA-256	12b968c00aa2b3e5998c2c99d7661b3b5e0abc f2103a4abc797a40dfb9c40f4b
SHA-256	7c047d252770298df8c2f50ea8246d9e7127213672dc1dda00b03f31025cb971
SHA-256	667f8c9bfb3fbbe9e22527cc4f4377397b75e0756876af5824c2518e1a343805
SHA-256	f19767e7cac6b1f762d46f8151077923d9d38a25295c809459bd5bb960a75e84
SHA-256	34157cb8213bd46f829cfa3ed04d113ef1ebc52a0e86ce4395c9138d3a1c0c05
SHA-256	0bcb5a66817b23b3bac865bf91ff5607e3ea7766086105ce5a92816e9de278ee
SHA-256	daebf367ce0b1367b552f08ac556ffc377ce92b848ada3d7c59c0eb37cc305d1
SHA-256	2015ab403f108956ab43e6ac7e8f9238e0e253918833a1b7115a0b7e5a61cdc1
SHA-256	4f996f0d6d634d972a75e44b33894525f7a777337a6d385109518f62a0ee884a
SHA-256	654ab3cd000c4b37d256ccb95f5bb7ae4627fb55b00d5c fb610177d7635f226e
SHA-256	267ef390ea3f6605a681787f7ffccaef23e784282287184309eddc46280571c2
SHA-256	aca0b9a33079889e9ace78cc651f097734f74803de2875902cbe3fb2d9e9004a



SHA-256	9a5aa641344c93a41a048392464445091a88e659947e683f4f65de9acacf5d1c
SHA-256	428ef20e3d64dfb1a48fb4034da5f439a9c906baca540f5a39f7e6248f798519
SHA-256	b875051a6d584b37810ea48923af45e20d1367adfa94266bfe47a1a35d76b03a
SHA-256	7e2413fbf54d23d77def054631c3c865afd6e5c76a863246a7ec721b33bab20a
SHA-256	48b45fb770626676c55d437f8fdda1a50de0c2006fa8ada559d6df87a60c90d9
SHA-256	0a0c225f0e5ee941a79f2b7701f1285e4975a2859eb4d025d96d9e366e81abb9
SHA-256	6b7069133c2ae9bf963d44f601f85ad829c20e6f7a7ab3d321297945b81f955f
SHA-256	794b37d03568cedd4452a3fba8a5be05f30196a1f17cd03b2981ba66318ac9a6
SHA-256	6f190afd8cc235345c9615a094aa280a77327a37cb79d0377a2c31698d14d589
SHA-256	83a714fa83e68956295290f9434b2777a0991a3703af0f1fc8f0005928b4abe0
SHA-256	778bd69af403df3c4e074c31b3850d71bf0e64524bea4272a802ca9520b379dd
SHA-256	5de4e2b07a26102fe527606ce5da1d5a4b938967c9d380a3c5fe86e2e34aaaf1
SHA-256	1841c6b8f7bced635a6a24cd7fd913b6f64ffb4e6e60300182b2199b10dbe2cd
SHA-256	78782fd324bc98a57274bd3fff8f756217c011484ebf6b614060115a699ee134
SHA-256	1ef8db7e8bd3aaba8b1cef96cd52fde587871571b1719c5d40f9a9c98dd26f84
SHA-256	200d866f81ea46228de31fc4066cceeefab8e569b0fed0be34fa5a1091f6727c
SHA-256	1cc7c198a8a2c935fd6f07970479e544f5b35a8eb3173de0305ebdf76a0988cb
SHA-256	7ca3065396a815639cd413de0618cbcd6d79c97509f561b58beb87555c59f6e4
SHA-256	27991f7872c075ae4a6eb5d24e739018570f8266c5d46f15661f02621441fdcc

You can access the continuation of IoCs offered free of charge by ThreatMon via the GitHub link below.

[Click here for IoC list!](#)



0101000110100001101001011100110010000000110100101
170010000001110011010101110110110101010010100100
00100110000101101110011001000011011101101101010
1110100011001010111100001110100000100000000
101101001011011100110011100100000000110101
00001101000011001010111001001100100110010
01101111011100100001000000000110001111
0001101001011011100110011001110010