



מבוא למודיעין איומי סייבר (CTI)

הצגה ל-SOC

TLP:RED

German Simkin

June 2022

על מה נדבר?

- הצגת Mandiant
- מבוא למודיעין ו-CTI
- מודלים בניתוח CTI
- מעגל המודיעין
- אנליסט AIA
- APT, TEMP, UNC וביניהם
- מבוא לקבוצות תקיפה



A photograph of two men in business suits shaking hands in a high-rise office at night. The background shows a city skyline with lights visible through the large glass windows. The scene is dimly lit, with the primary light source being the city lights outside.

Mandiant Overview

Mandiant



Solutions that enable every security team in the world to easily **augment** and **automate** our intelligence and expertise into their environment, regardless of the controls they have deployed.


Formerly a part of FireEye Inc., it was incorporated into FireEye in 2013 and separated in 2021. Multiple companies joined during that period, adding technology and/or capabilities.


Services

Advantage Platform

 Security Validation

 **Threat Intelligence**

 Automated Defense

 Attack Surface Management



Incident Response



Strategic Readiness



Technical assurance



Our Collection Universe

MACHINE INTELLIGENCE

- 15,000 network sensors
- 18M endpoints
- Tens of millions of malware detonations per hour
- 65M emails processed a day

OPERATIONAL INTELLIGENCE

- 4 Security Operation Centers
- Human and data science analysis
- 50B+ events investigated per month

The logo features a dark red circular background. Inside, a stylized map of the world is composed of a network of red lines connecting white dots, representing a global grid. The text "Mandiant Intelligence Grid" is centered over the map in white.

Mandiant Intelligence Grid

EXPERTISE

- 14+ years of investigative expertise
- 26 countries with consultants
- 400+ Red Team exercises per year

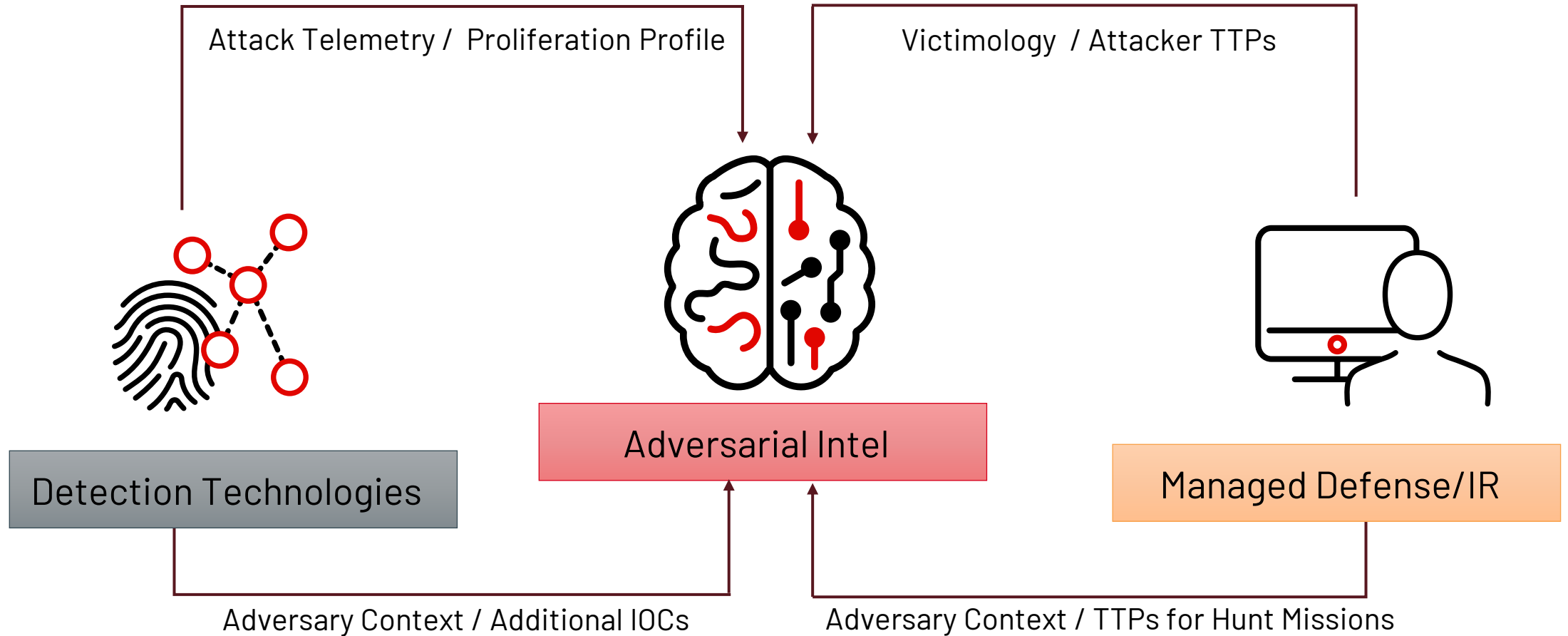
ADVERSARY INTELLIGENCE

- 24+ countries
- 30+ languages
- 300+ analysts and researchers
- 30K intelligence reports per year

BREACH INTELLIGENCE

- 1,000+ engagements per year
- 200K+ hours per year responding to attacks

Mandiant Cyber Threat Intelligence Cycle



Intelligence

Intro





מודיעין

הגדרות בסיס

- מידע מעובד וממוין
- רלוונטי
- נאסף ונצבר ממקורות מהימנים
- מדויק, מלא ככל האפשר
- הוצלב לטובת דיוק
- עדכני
- עבר הערכה ופרשנות על ידי מנתחי מודיעין מיומנים
- ניתן לפעולה

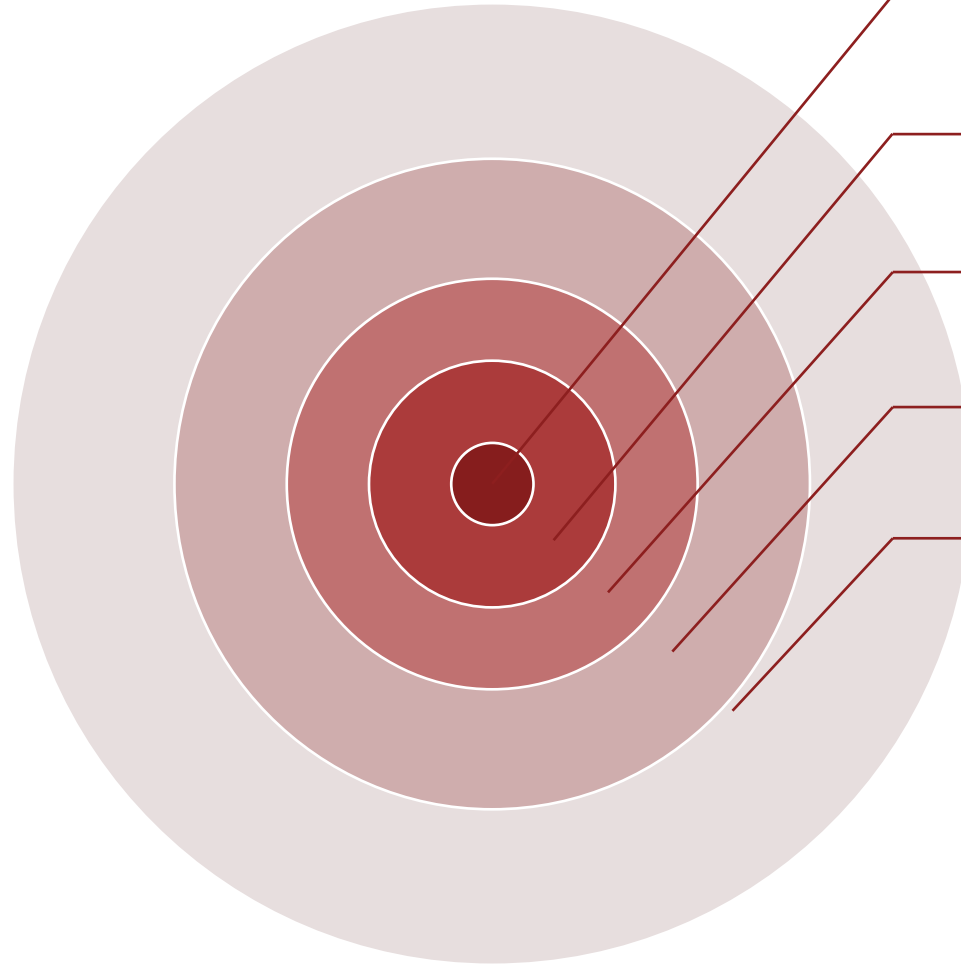
Cyber Threat Intelligence (CTI)

- ידע מבוסס עובדות על היריב – על המניעים שלו (למה?); הכוונות (מה?); היכולות, הסביבות המאפשרות והמבצעים (איך?); תוך התמקדות באירוע, סדרה של אירועים או טרנדים המאפשר **יתרון בקבלת החלטות** (Gartner Research)
- המגן זקוק למידע עדכני, מדויק ומפורט ("מודיעין לפעולה") על האיומים הפוטנציאליים, ועל האופן שבו המוטיבציה והיכולת של היריב עשויה להשפיע על מצב האבטחה של הארגון.
- יתרון בקבלת החלטות – התוצר הסופי מטרות להבין כיצד ניתן להציג את האיומים והדרכים הפוטנציאליים להתמודדות. ההבנה מאפשרת להניע ולשפר את הערכת האיום בסייבר וקבלת החלטות, ניהול.

“Leveraging intelligence to create
a **proactive** cyber defense posture
while **informing** organizational-wide decisions
to **reduce cyber risk**”

מדוע יש לזהות איומים?

גישה לא מורשית
השמדה
הדלפה
חבלה במידע
DoS/DDoS



- מניעת פגיעה בחיי אדם
- מניעת נזק חומרי
- שמירה על ריבונות
- צמצום פגיעה במוניטין
- תמיכה בצמיחה

מטרות מבצעי סייבר

עבור מעצמות, הסייבר הוא כלי א-סימטרי בו נעשה שימוש בתור צורה של עוצמה רכה להרחבת הכלים הקיימים של המדינות. מבצעי סייבר מבוססים על גישה, וניתן להשתמש בהם למספר מטרות:

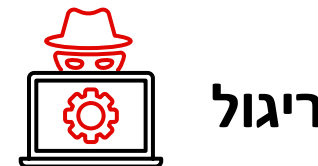


תקיפה

- שיבוש או פגיעה בזמינות של מערכות מחשוב או רשתות
- שיבוש, פגיעה או השמדה של תשתיות קריטיות
- הדהוד או סיוע לבצעי השפעה (IO)



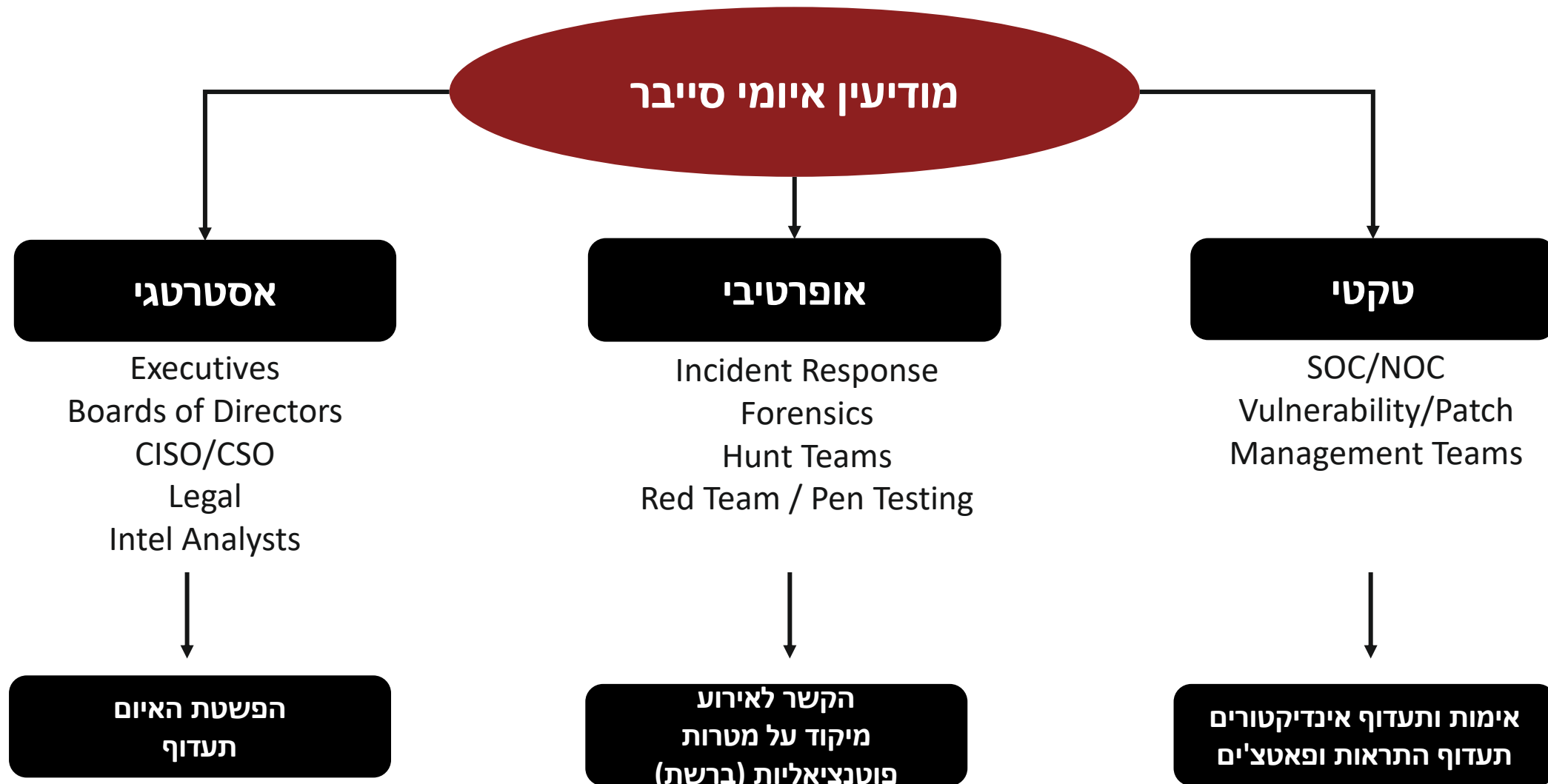
מניע כספי*

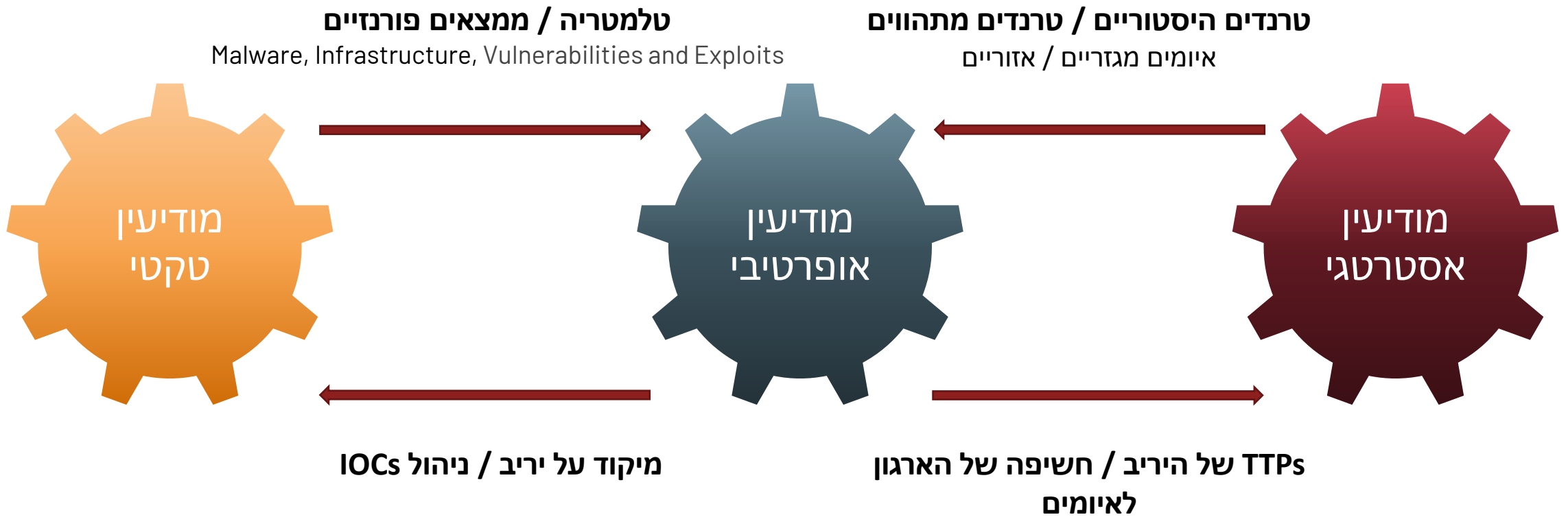


ריגול

- **צבאי**
 - הבנת יכולות היריב, תוכניותיו, תהליך קבלת ההחלטות ודמויות המפתח
- **פוליטי**
 - השגת מידע אודות החלטות ותוכניות ארגוניות
 - קבלת מידע על כוונות במהלך משא ומתן
 - איתור מידע מביך אשר עשוי לשמש בתור "קלף מיקוח"
- **כלכלי**
 - חיזוק התחרותיות
 - מימון קופת המדינה

צרכני המודיעין בארגון





INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems

Cyber Espionage (CE)

Critical Infrastructure (CI)

Fusion (FS)

April 13, 2022 09:12:08 PM, 22-00008528, Version: 3.0

Executive Summary

- Mandiant Threat Intelligence analyzed a set of novel industrial control system (ICS)-oriented attack tools—which we call INCONTROLLER—built to target specific Schneider Electric and Omron devices that are embedded in different types of machinery leveraged across multiple industries.
- INCONTROLLER is a collection of three separate Python-based frameworks, which we individually track as TAGRUN, CODECALL, and OMSHELL. They contain capabilities related to disruption, sabotage, and potentially physical destruction.
- We are also tracking two additional tools affecting Windows-based systems that may be related to this threat activity: ICECORE and an exploit for CVE-2020-15368.
- INCONTROLLER is very likely state sponsored. We are unable to link the activity to existing clusters of threat activity, but we note that the activity is consistent with Russia's historical interest in ICS.
- This malware poses a critical risk to organizations leveraging the targeted equipment. Organizations should take immediate action to determine if the targeted ICS devices are present in their environments and begin applying vendor-specific countermeasures, discovery methods, and hunting tools, which we describe in this report.

Overview of State-Sponsored Threat Activity Pertinent to OT Asset Owners

Critical Infrastructure (CI)

Fusion (FS)

August 17, 2021 05:58:12 PM, 21-00018084, Version: 1.4

Executive Summary

- Given the high-volume of state-sponsored threat activity pursuing a variety of objectives, it can be difficult to accurately distinguish and prioritize threats to operational technology (OT). We observe four broad types of cyber threat activity pertinent to OT asset owners: ambiguous threat activity, computer network attacks, OT-targeted espionage, and cyber physical attacks.
- While most state-sponsored threat activity against IT assets corresponds to cyber espionage, certain ambiguous, high-risk activity could indicate a willingness to conduct destructive attacks or pre-positioning for future OT activity. We are aware of a large amount of ambiguous threat activity and a moderate number of publicly documented state-sponsored computer network attacks.
- OT assets can be sabotaged via integrity-attacks and availability-attacks or targeted in confidentiality-attacks focused on OT assets or data. We are aware of a minor number of OT-targeted espionage operations and four publicly documented state-sponsored cyber physical attacks.
- State-sponsored threat actors will likely continue targeting the corporate infrastructure of OT-reliant organizations at a high frequency, which will provide many opportunities to pivot to OT assets if desired. While the risk of reprisal will likely limit cyber physical attacks to select targets, these attacks remain a high-risk to OT environments due to the potential for catastrophic impacts and physical harm.

Threat Detail

Given the high-volume of state-sponsored threat activity pursuing a variety of objectives, it can be difficult to accurately distinguish and prioritize threats to operational technology (OT). State-sponsored threat actors motivated to target cyber physical systems can reach their objectives in different ways. They can direct activity against IT assets to attempt to facilitate lateral movement to OT systems or attack IT assets and demonstrate a willingness for disruption. They can target OT assets to generate physical impacts or conduct espionage to gather intelligence for future attacks. Mandiant Threat Intelligence considers a variety of factors to help enumerate and prioritize threats to OT, such as sector targeting, aggression, capability, and actor motivation. We observe four types of non-mutually exclusive state-sponsored threat activity pertinent to OT asset owners, loosely ordered by ascending risk to OT:

- **Ambiguous Threat Activity:** Cyber activity with unclear objectives that poses a threat to OT-reliant organizations. This includes operations that overwhelmingly target public utilities or OT vendors and operations that pose a threat to such industries by leveraging aggressive initial access or lateral movement techniques (e.g., supply-chain attacks, worm-like malware, etc.). The ambiguity of intent leaves open the possibility that the activity will evolve into the higher-risk types listed as follows.
- **Computer Network Attacks:** Cyber attacks designed to disrupt data processes and workflows
- **OT-Targeted Espionage:** Cyber espionage in which the target is either OT or OT-related information
- **Cyber Physical Attacks:** Cyber attacks designed to sabotage physical processes

TTP: Targeting Air-Gapped Systems

Oct 31, 2019

19-00018652, Version: (1)



Executive Summary

- FireEye Threat Intelligence assesses with moderate confidence that malware-laden removable storage media, such as USB devices, remains the primary method threat actors use to gain access to air-gapped systems.
- We assess with low confidence that financially motivated exploitation of air-gapped systems is rare based on limited evidence of financially motivated interest in air-gapped systems, particularly "cold" cryptocurrency wallets.
- FireEye Threat Intelligence suggests that removable devices are introduced to air-gapped environments by insiders, both witting and unwitting, or individuals who obtain unauthorized physical access to a system, such as visitors.
- Although researchers have demonstrated novel methodologies to exfiltrate data from air-gapped systems, FireEye has not observed these means used in the wild.

North Korean campaign possibly targeting Israel IAI

====Wire Summary====

On the 06-07-2020 a Virus Total submitter related to the Israel

This document is a decoy and its content is only a picture relat

Once the document is open it will perform a remote template in

Cuteloop is a downloader that can collect system information a

This document is a part of a bigger North Korean campaign ta

This entire campaign is based on decoy documents that perfor

====Threat Detail====

- **Delivery Method:** Exploited decoy word document

Global Intelligence Programs / GIP-660

Andariel Actor Tracking

Edit Comment Assign Log work Agile Board More Start Timer Resolve Issue Request Info Rejected Start Process Watch Repro

Details

Type: Task Status: **OPEN**
Priority: Normal Resolution: Unresolved
Component/s: SIG-SAR
Labels: None

Additional Issue Stats

CAL Issue: No

Description

Collection of Andariel (soon to be Temp.Duriel) APT activity observed by FireEye:

April 2020:
xxxx

March 2020:
xxxx

UNC Groups Associated with Andariel

UNC1892 Indicator of activity attributed to an uncategorized threat group tracked by FireEye. Created by Emiel Haeghebaert on 2020-02-04 to track cluster of STEELDROP malware first observed in DTI.

UNC993 We suspect the threat group is based out of the Democratic People's Republic of Korea (DPRK) UNC993: Indicator of activity attributed to an uncategorized threat group tracked by FireEye. Created by Vengerik on 20180209, Suspected DPRK activity using specific VBA macro decryption routine and Office author name "Peiterpan". Overlaps with "Andariel" activity. **Basis of actor is RIFLE and ROGUEEYE to which this unc is tied to both**

*UNC1967 * We suspect the threat group is based out of the Democratic People's Republic of Korea (DPRK) **UNC1967**: Indicator of activity attributed to an uncategorized suspected North Korean-nexus threat group tracked by FireEye. Created by Fred Plan on 2020-03-12 to track LEADLIFT activity associated with **KKNPP (India nuclear plant)**

ware

19-00020630, Versio

CHEMICALS & MATERIALS ENERGY & UTILITIES

nuclear Power Plant (KKNPP) in India (19-00018852). In this

- The LEADLIFT sample is a host information-gathering utility that collects output from networking and process-related commands, browser history from Firefox and Google Chrome, and full filesystem listing of each drive on the machine.
- We recommend operational technology (OT) asset owners and defenders review the tactics, techniques, and procedures (TTPs) associated with the malware to hunt for similar tradecraft and identify similar malicious traffic patterns.

- The actor posted a 14-second cell-phone video of someone's computer displaying alleged schematics of an industrial control system (ICS) (Figures 2 and 3).
 - It is unclear if the video is related to OpRussia2. In the post the actor wrote [Arabic translation]: "SCADA CGR-GAS systems schematics." The video file had the name "ariftirtana-٢٠٢٠٠٨٢٢-0001." The middle section of the title contains Arabic numerals for "20200822." We could not identify anything related to "ariftirtana," although "Arif Tirtana" is associated with several Indonesian personas online.

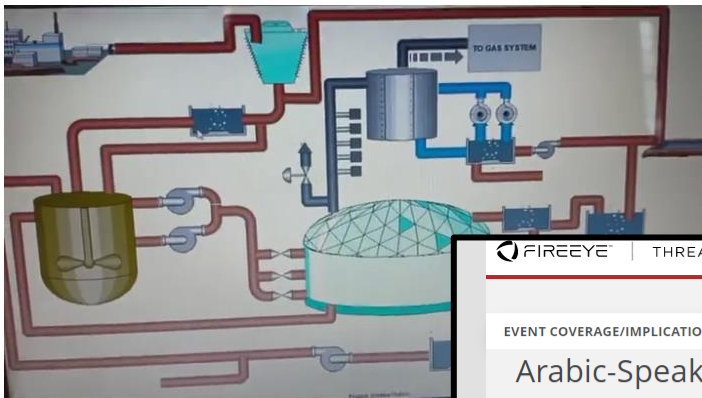


Figure 2: Alleged schematics of a

FIREEYE | THREAT INTELLIGENCE

Intelligence News Analysis Tools Alerts Support Admin

EVENT COVERAGE/IMPLICATION CP FS Analyst Access Pdf Download Indicators (none)

Arabic-Speaking 'Spider Team' Claims to Compromise Russian Nuclear Research Center and Posts Alleged ICS Schematics

Aug 26, 2020 20-00017147, Version: [1]

EUROPE UNITED STATES CYBER PHYSICAL CONSTRUCTION & ENGINEERING GOVERNMENTS ENERGY & UTILITIES

Executive Summary

- In August 2020, the Arabic-speaking actor "Spider Team" claimed to compromise a Russian nuclear research institute, allegedly obtaining documents they promised to publish soon.
- The actor posted industrial control system (ICS) schematics and test data allegedly obtained from the compromise. It is unclear if the leaked data is an immediate threat to any particular system.
- As hackers continue to bolster their reputation via this type of activity, there is an increasing risk that more valuable ICS-related information will be leaked or that ICS assets will be directly exposed or manipulated. We suggest organizations make an inventory of where critical process and production data reside on information technology (IT) networks, avoid storing ICS-related data in IT networks to the extent feasible, and collaborate with third-party vendors to determine third-party risk and information exposure.

Threat Detail

RELATED REPORTS

- Cyber Physical Threat Actor Spotlight: Jerusalem Electronic Army (JEA) [See the report >](#)
- Recent OT Incidents Highlight an Increased Threat Posed by Low-Skilled Threat Actor [See the report >](#)
- Update: OT Systems in Israeli Water & Wastewater Sector Targeted Possibly by Jerusalem Electronic Army [See the report >](#)
- Red Lion N-Tron 702-W 2.0.26 Hidden Functionality Vulnerability [See the report >](#)
- Red Lion N-Tron 702-W 2.0.26 Cross-Site Request Forgery Vulnerability [See the report >](#)

כיצד הארגון יכול להשתמש במודיעין סייבר?



- מה הם ה-IOCs הספציפיים?
- אילו צעדי מנע ניתן לממש על מנת
להגן פרואקטיבית כנגד איומים אלו?



- באילו TTPs השחקנים הללו
משתמשים?
- מה תהיה ההשפעה הפוטנציאלית
על הארגון?



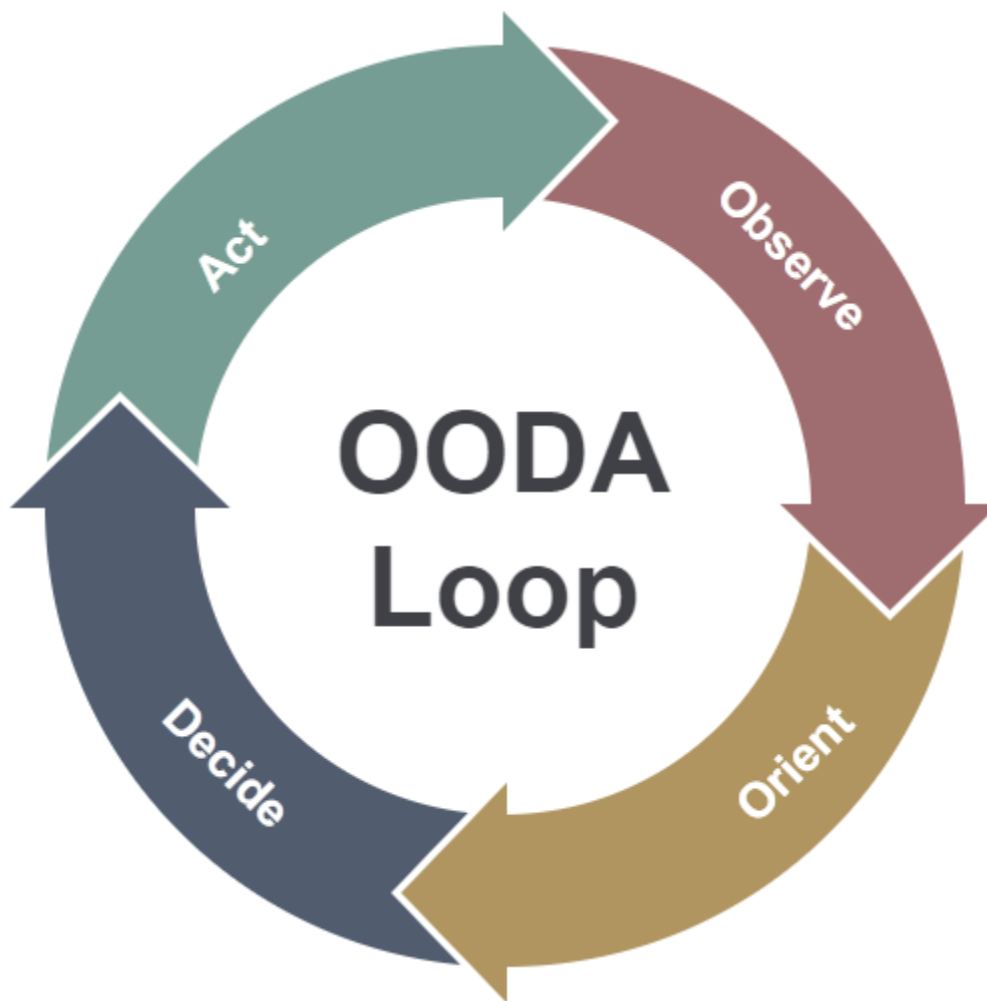
- מה הם האיומים על הארגון,
בהתבסס על התעשייה והגיאוגרפיה?
- אילו שחקנים ינסו לתקוף את
הארגון, ומדוע?



Models

OODA Loop

מתודולוגיה לקבלת החלטה
הגדרת תוכנית עבודה

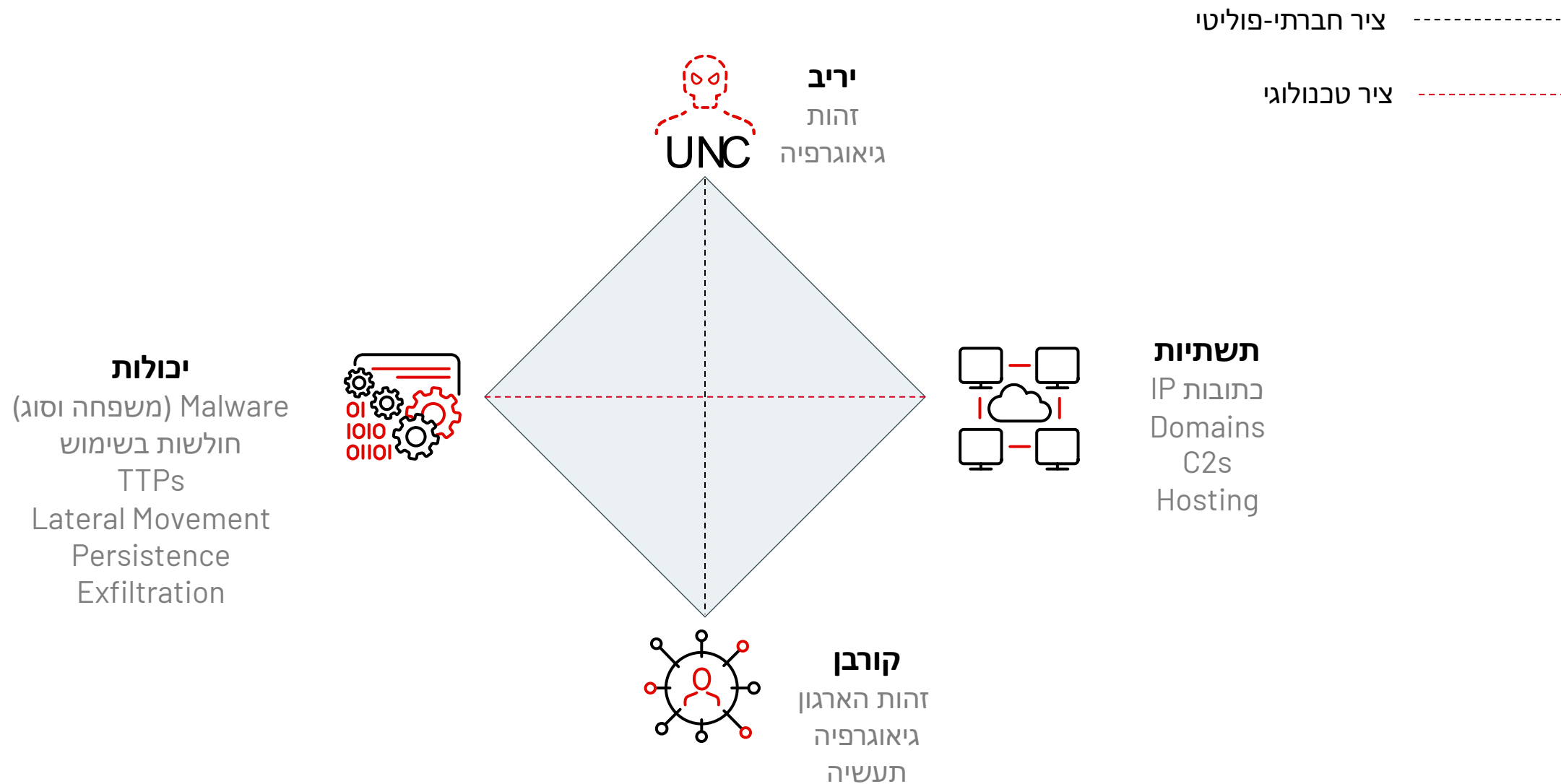


מהו המצב העדכני של הארגון?
מדוע יש צורך בשינוי?
כמה חשוב לבצע את השינוי?

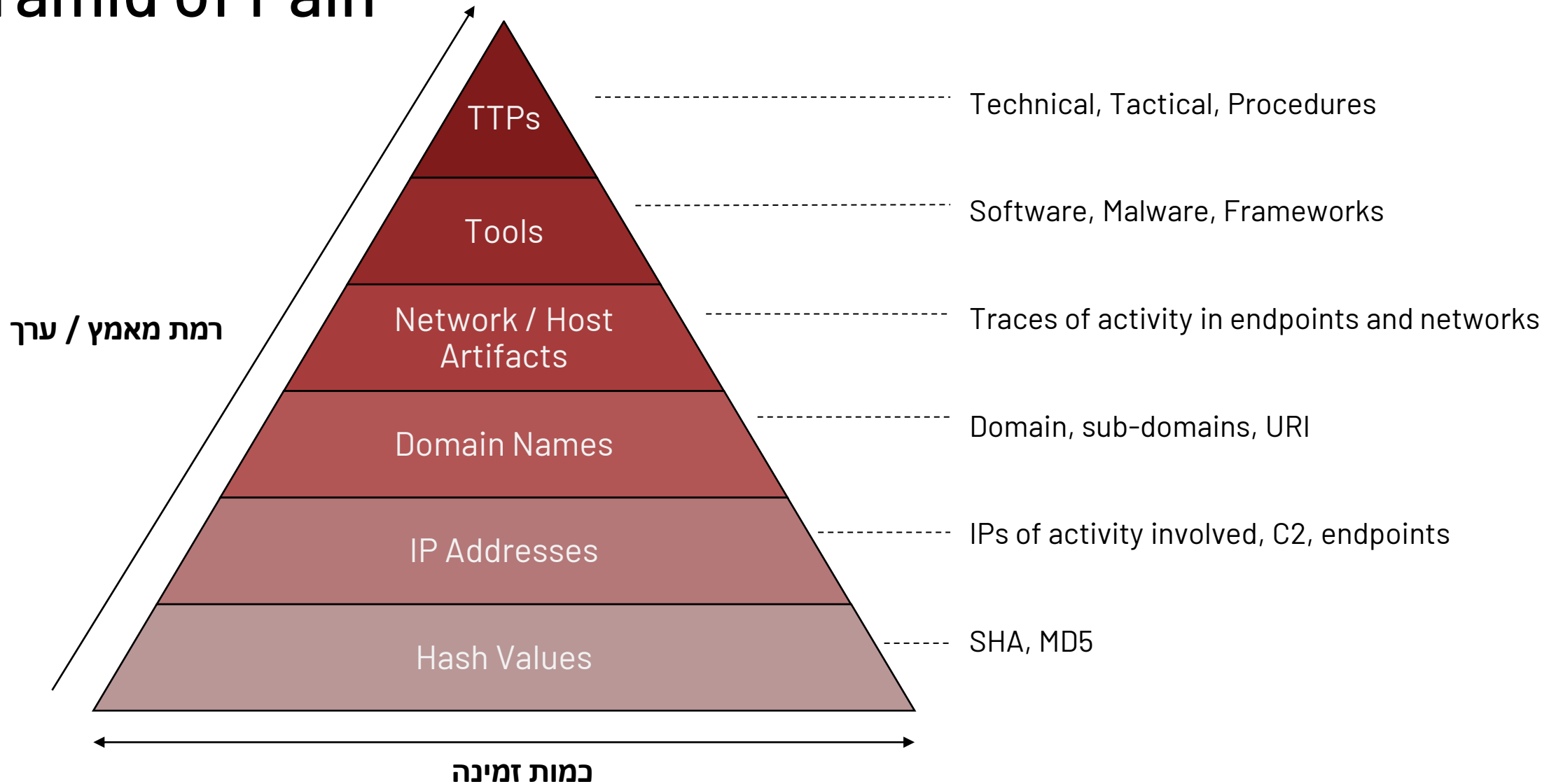
מהי הדרך המדויקת למטרה?
כיצד הארגון יתמודד עם מכשולים
ועיכובים?

היכן נמצא עכשיו הארגון ביחס
למטרה?
מה המרחק למטרה?

Diamon Model of Intrusion Analysis



Pyramid of Pain



The Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control (C2)
- Actions on Objectives

CYBER KILL CHAIN®

Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.

A : ADVANCED

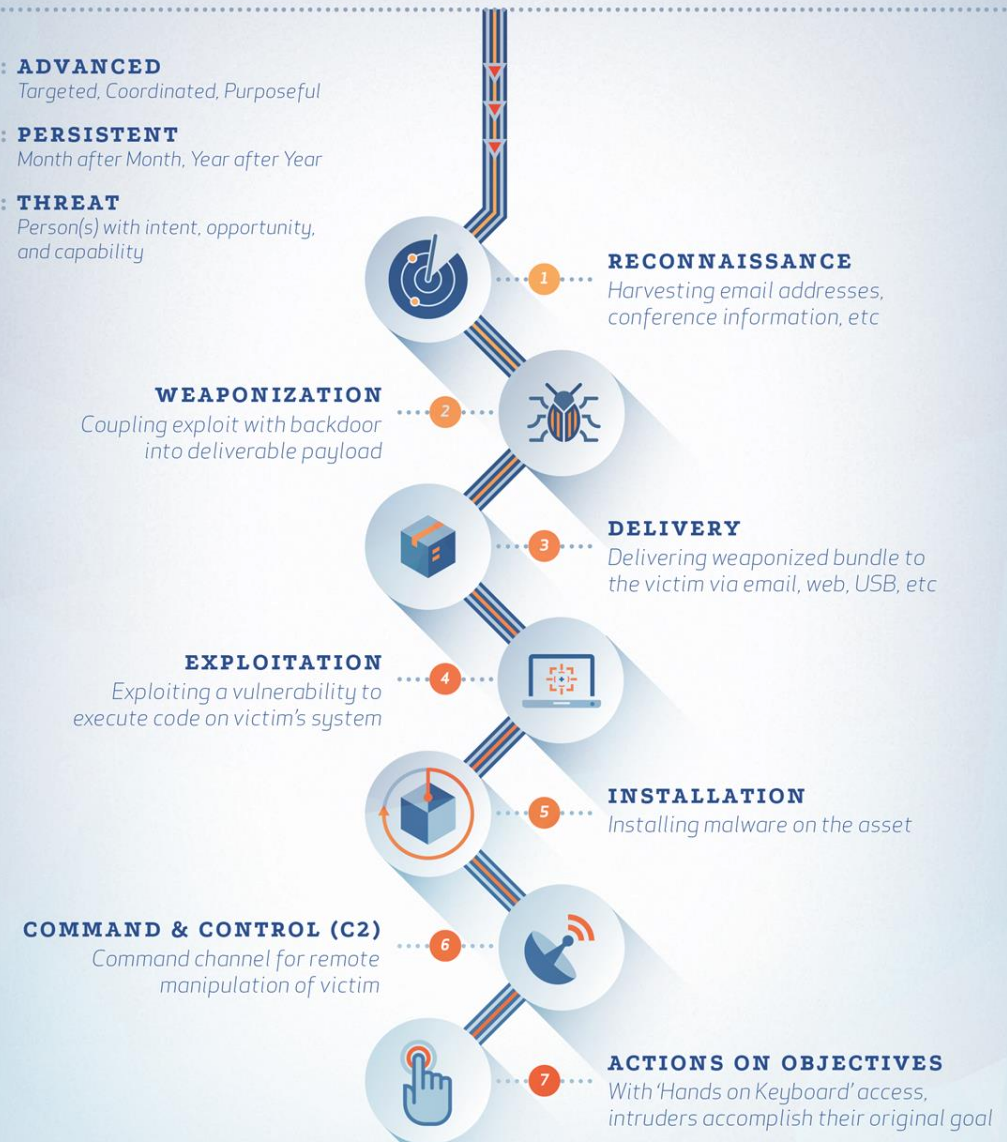
Targeted, Coordinated, Purposeful

P : PERSISTENT

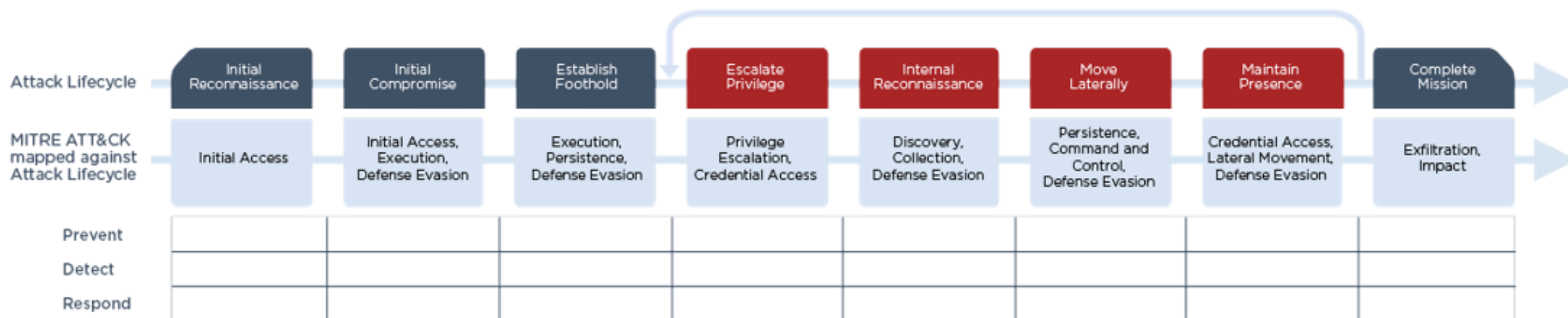
Month after Month, Year after Year

T : THREAT

Person(s) with intent, opportunity, and capability



The Mandiant Attack Lifecycle



MITRE ATT&CK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task		Binary Padding		Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl	Access Token Manipulation		Account Manipulation		Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling	Bypass User Account Control		Bash History		Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping			Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Other Network Medium
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking		Credentials in Files		Browser Bookmark Discovery	Logon Scripts		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel
	CMSTP	Image File Execution Options Injection		Credentials in Registry		Domain Trust Discovery		File and Directory Discovery			
Spearpishing Attachment	Command-Line Interface	Plist Modification		Exploitation for Credential Access		File and Directory Discovery	Logon Scripts	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearpishing Link	Compiled HTML File	Valid Accounts		Forced Authentication		Network Service Scanning	Pass the Hash	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Resource Hijacking
Spearpishing via Service	Control Panel Items	Accessibility Features		BITS Jobs		Network Share Discovery	Pass the Ticket	Email Collection	Domain Fronting		Scheduled Transfer
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History		Hooking	Remote Desktop Protocol	Man in the Browser	Domain Generation Algorithms	Scheduled Transfer	Service Stop
Trusted Relationship	Execution through API	Applnit DLLs		CMSTP		Input Capture	Remote File Copy	Man in the Browser	Domain Generation Algorithms		Stored Data Manipulation
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing		Input Prompt	Permission Groups Discovery	Man in the Browser	Man in the Browser	Screen Capture	Video Capture
		Dylib Hijacking		Compiled HTML File		Kerberoasting	Process Discovery	Replication Through Removable Media	Fallback Channels		
Exploitation for Client Execution	File System Permissions Weakness		Component Firmware		Keychain		Query Discovery	Shared Webroot	Multiband Communication	Multi-hop Proxy	Multilayer Encryption
	Hooking		Component Object Model Hijacking		LLMNR/NBT-NS Poisoning and Relay		Remote System Discovery	SSH Hijacking	Multi-Stage Channels	Port Knocking	
Graphical User Interface	Launch Daemon		Control Panel Items		Password Filter DLL		System Information Discovery	Taint Shared Content	Remote Access Tools	Remote File Copy	Standard Application Layer Protocol
InstallUtil	New Service		DCShadow		Private Keys		System Network Configuration Discovery	Third-party Software	Remote Access Tools	Remote File Copy	
Mshst	Path Interception		Deobfuscate/Decode Files or Information		Securityd Memory		System Network Configuration Discovery	Windows Admin Shares	Remote File Copy	Standard Application Layer Protocol	Standard Cryptographic Protocol
PowerShell	Port Monitors		Service Registry Permissions Weakness		Two-Factor Authentication Interception		System Network Connections Discovery	Windows Remote Management	Standard Application Layer Protocol	Standard Cryptographic Protocol	
Regsvcs/Regasm	Setuid and Setgid		Disabling Security Tools		DLL Side-Loading		System Owner/User Discovery	System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port
Regsvr32	Startup Items		Execution Guardrails		Exploitation for Defense Evasion		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Rundll32	Web Shell		Exploitation for Privilege Escalation		File Deletion		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Scripting	.bash_profile and .bashrc		SID-History Injection		File Permissions Modification		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Service Execution	Account Manipulation		Sudo		File System Logical Offsets		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Signed Binary Proxy Execution	Authentication Package		Sudo Caching		Gatekeeper Bypass		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Signed Script Proxy Execution	BITS Jobs		Sudo Caching		Group Policy Modification		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Source	Browser Extensions		Sudo Caching		Hidden Files and Directories		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Space after Filename	Change Default File Association		Sudo Caching		Hidden Users		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Third-party Software	Component Firmware		Sudo Caching		Hidden Window		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Trusted Developer Utilities	Component Object Model Hijacking		Sudo Caching		HISTCONTROL		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
User Execution	Create Account		Sudo Caching		Indicator Blocking		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Windows Management Instrumentation	External Remote Services		Sudo Caching		Indicator Removal from Tools		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
Windows Remote Management	Hidden Files and Directories		Sudo Caching		Indicator Removal from Tools		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service
XSL Script Processing	Hypervisor		Sudo Caching		Indicator Removal from Tools		System Service Discovery	System Time Discovery	Virtualization/Sandbox Evasion	Uncommonly Used Port	Web Service

ATT&CK

Tactics (Technical Goals) > Techniques > Sub-Techniques

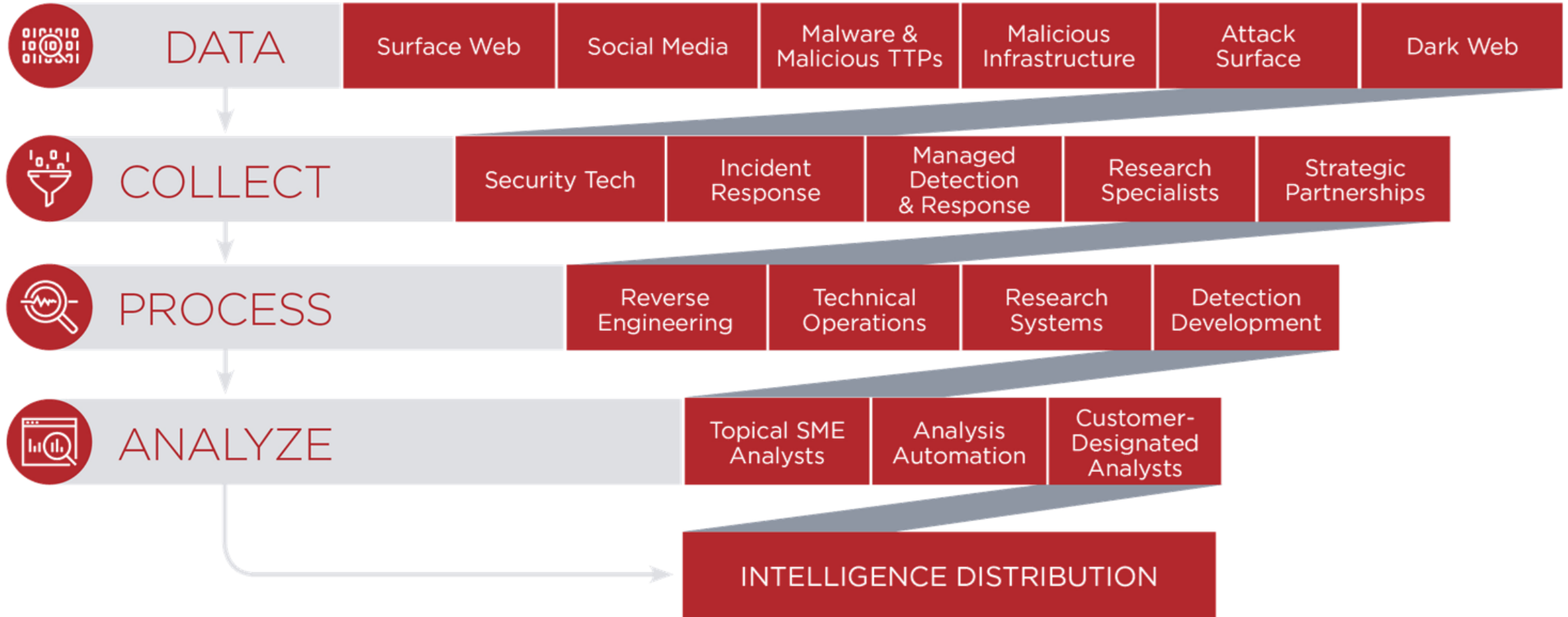
Key Takeaways

- מודל היהלום (The Diamond Model) חיוני להבנת יכולות היריב והמטרות שלו
- בפירמידת הכאב יש להתמקד בטיפוס אל החוד, כלומר זיהוי ה-TTPs של היריב
- ניתן לזהות את השלבים השונים של מבצע הסייבר של היריב באמצעות ה-Kill Chain ו-Attack Lifecycle
- מסגרת ה-ATT&CK חיונית לעבודה עם CTI, לטובת זיהוי היריב ובמסגרת תרגול תקיפה

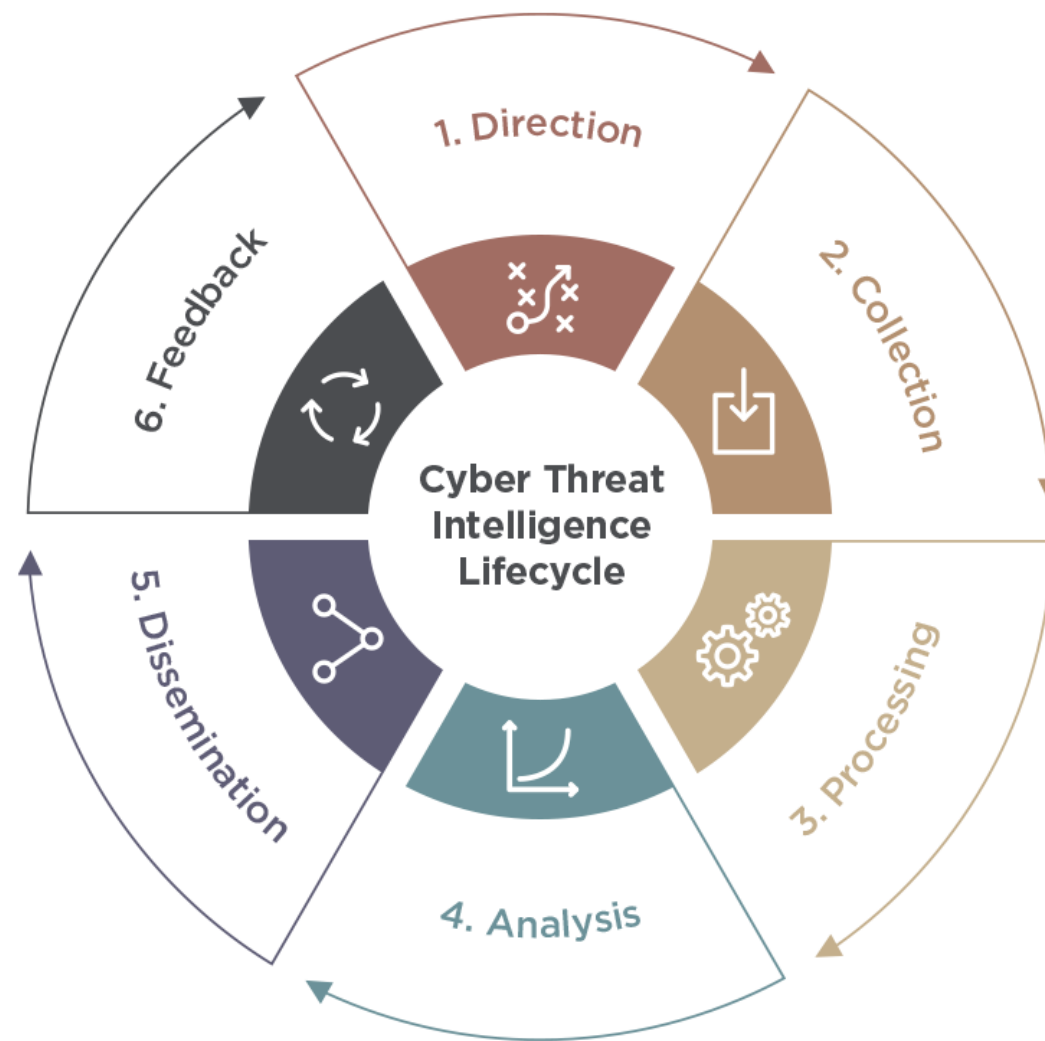


Intelligence Cycle

Intelligence Creation Process



מעגל המודיעין



איך אמור להיראות התוצר הסופי?
באיזה פורמט?
למי הוא מיועד?
אילו מסקנות ולקחים ניתן להפיק?



מה המיקוד שלנו?
מה מעניין אותנו?
למה זה מעניין אותנו?

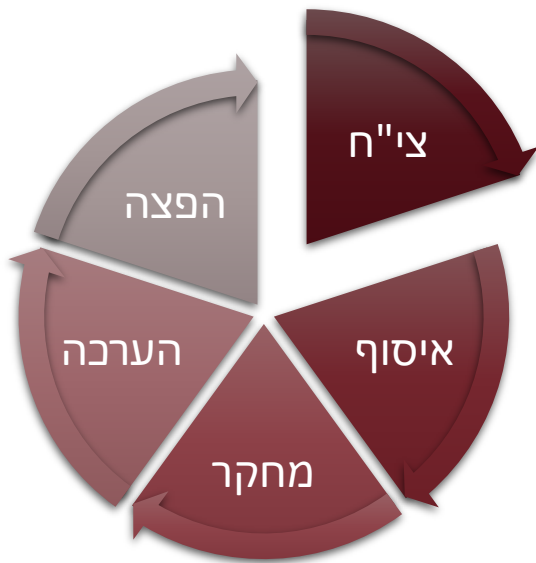
איזה סוג מידע ייתן לי מענה?
איך נשיג את המידע?
באילו שיטות נשתמש?

אילו תובנות ומסקנות אנו מצופים לתת?
איך אמנע מהסקת מסקנות שגויות או לא מבוססות?
איך נימנע מכשל בהערכה?

איך אעבד את המידע?
איך אגזור ממנו תובנות ומסקנות?
מתי עוצרים?

צי"ח (ציון ידיעות חיונית)

- נקבע לפי צרכי הלקוח בשקלול המודיעין שבידנו
- נקבע בשיתוף עם הלקוח
- הרזולוציה של השאלות שאנו שואלים משתנה – שאלות אסטרטגיות ושאלות טקטיות
- שאלות אסטרטגיות – דוגמאות:
 - אילו שחקנים מטרגטים את מגזר הלקוח בארץ / בעולם?
 - איך אותם שחקנים פועלים?
 - איך ניתן להתמגן מפניהם?
- שאלות טקטיות – דוגמאות:
 - מה פשר ההתרעה שקפצה ב-SOC?
 - מי השחקן שעומד מאחורי אתר שמתחזה לאתר הלקוח?
 - מה מטרת השחקן שסורק פגיעות ל-Log4j? האם פועל באופן ממוקד למגזר הלקוח?



איסוף (Collection)

• מקורות Mandiant:

– חקירות IR

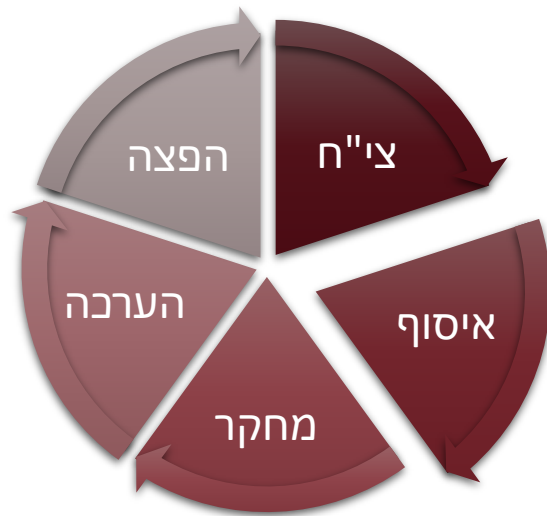
– Managed SOC

– מידע ממוצרי FireEye (Cloud, Email, Network, Endpoint)

– מחקר שוטף

– חיפוש פרואקטיבי ב-Darknet, בפורומי Hacking וברשתות חברתיות

– מקורות צד ג'



Black Shadow
3.4K subscribers

Pinned Message
They did not contact us ...So first data is here...

If you do not contact us , it will be more 😊

<https://blackshadow.cc>
<https://t.me/blackshadowsleaks3>
3.4K edited 11:25

Black Shadow pinned a photo

Unread Messages

Black Shadow
We have more data now !

9k users of :
<https://dan.co.il> 🔥

120k users of :
<https://pegasusisrael.co.il> 🔥

17k users of :
<https://doctorticket.com> 🔥

and ...
just 1% (1000) of database of :
<https://www.atarf.co.il/> 🔥

download all from here :
[@blackshadowdata](#) 🔥 222 21:12

MUTE

SELLING Bar Ilan university of Israel Data For sale
by DarKrypt - 4 hours ago

DarKrypt
New User
MEMBER
Posts 1
Threads 1
Joined Aug 2021
Reputation 0

4 hours ago · This post was last modified: 4 hours ago by DarKrypt.

Hi
Mass Data of Bar Ilan University of Israel (largest public research universities in Israel) is for sale
Data includes :

Personal information and documents ,
Scientific article ,
Factors ,
Laboratories documents ,
PHD proposals and articles ,
Classification research ,
Covid-19 Researches ,
Medical Sciences articles ,
Students and professors Names and Emails
etc

Data size : 20 TB 😊

DragonForce Malaysia

#OPSBEDIL3.0
ATTENTION!

30/8/2021
12:00 AM - TARGET LIST -

IP : 192.118.30.136	PORT :	HTTPS://CELLCOM.CO.IL/
IP : 157.90.16.11	443	HTTPS://FOOD.CO.IL/
IP : 31.154.7.247		HTTPS://WWW.MIZRAHI-TEFAHOT.CO.IL/

GREETINGS THE GOVERNMENT OF ISRAEL. WE ARE DRAGONFORCEMALAYSIA

Thread '#OPSBEDIL 3.0 DDOS ATTACK LAUNCH !'
<https://dragonforce.io/threads/opsbedil-3-0-ddos-attack-launch.6272/>
9667 11:42 PM

INDONESIA SECURITY DOWN
Stop the war or we'll takedown all your Government sites?

7 SITE GOVERNMENT ISRAEL TAKEDOWN OLEH ISD TEAM

<http://.gov.il/>
<http://.gov.il/> <http://w.gov.il/>
<http://il/>
<http://.gov.il/>
<http://.gov.il/>
<http://i.org.il/>

37 Muhammad Arif, 17:10



• מקורות צד ג'

- Passive DNS –
- Dancing Penguin- ו VirusTotal –
- מנועי סריקה ו-Reputation –
- מקורות נוספים –

נראה שמדובר בפעילות ממוקדת מול תשתית של שהתקיימה ב-8 בספטמבר לאורך כמעט כל

– **שנים של עשרות מגה בייט ב-8 בספטמבר**

.75.184	- [.]gov[.]il
205.180	- [.]gov[.]il
205.113	- [.]gov[.]il
205.91	- [.]gov[.]il
205.209	- [.]gov[.]il
205.90	- [.]gov[.]il
205.85	- [.]gov[.]il
205.195	- gov[.]il

ממליץ לבדוק איזו תעבורה עברה בין ה-IP הראשון ברשימה (מודגש) לבין השרת החשוד. לגבי השאר זה נראה יותר כמו ניסיונות תקיפה/סריקה, אבל ממליץ לוודא שגם שם לא הצליחו להזליג שום דבר

זיהינו ב-VT קבצים שעולים מאותו submitter, שלהרבה מהם שיוך רפואי, בפרט נראה שהקבצים כוללים מידע של מטופלים ושרטוטים/תכנונים של מבנים בבית החולים.

מצרף קובץ המכיל פירוט של כלל הקבצים שה-submitter העלה. בסך הכול מדובר ב-52 קבצים שהוא העלה מאוגוסט 2015 עד היום (חלקם היו קיימים ב-VT כבר קודם ולא מכילים מידע רגיש כפי שניתן לראות באקסל המצורף). מספר דוגמאות שעלו בשבועות האחרונים (נראה שההעלאות נהיו תכופות יותר החל מסוף דצמבר 2021):

1. pdf1-50 - 0e4aa71b1c53746007c8ba82eb254bb9 - LAB-P1- אשפוז יום המטולוגי - עלה ב-13 בינואר
2. ace3e897a60b5330b86e15afe69d3035 - ניתוח מחסן ליבה.doc - עלה ב-6 בינואר
3. e77b41e1ddd03c41ffd7b5c5c056d54a - דיון מקרים_סרטן_וושט_קיבה_לימודי_המשך_ינואר_2022.pptx_4.inna.cleaned_ - עלה ב-4 בינואר
4. dffe6189f7ecac5e764d74c181718cae - PATIENT_DATA.rar - עלה ב-2 בינואר
5. e510d5044d219d6d28e67b50f7d391f7 - COVIDSeq_384 samples_Lib 80_with_demo.xlsx - עלה ב-26 בדצמבר
6. 64a57c63ba6dc60093746a6b6e8a132f - חזקה.zip - עלה ב-26 בדצמבר
7. 13ce4079b85c0b5f04d0e4ccfff867a2 - חדר צילום 02072021 העמדת ציוד.pdf - עלה ב-22 בדצמבר
8. 93afb702fe8a1d73e0006a732a819207 - חדר צילום 2072021.dwg - עלה ב-22 בדצמבר

> Malicious
ISP

77.137.180.134

ORGANIZATION
Hot-Net Internet Services Ltd.

ACTOR
Unknown

Not Spoofable [?]

FIRST SEEN
2021-06-03

LAST SEEN
2022-01-23

COUNTRY
Israel

REGION
Tel Aviv

CITY
Tel Aviv

ASN
AS12849

OS
Windows 7/8

RDNS
dynamic-77-137-180-134.hotnet.net.il

Observed Activity

Shows the ports & protocols that this IP scanned, along with the paths that this IP requested. In addition, fingerprints of the SSH & TLS negotiation between this IP and the GreyNoise sensor are shown.

Ports Scanned [?]

PORT	PROTOCOL
445	TCP

Tags [?]

✕
⌵

- Eternalblue
- CVE-2017-0144
- SMBv1 Crawler

מחקר והערכה

מקרה בוחן: Lead שהגיע ממוצר FireEye ← פענוח שרשרת התקיפה ← שיוך לתוקף איראני

hi

we have prepared a list of email addresses and passwords you need in the form of a document.

please check them, then, in coordination with the it department, change their password.

also, strictly refrain from publishing this document with unrelated units.

noted: to display the content of the document, select the enable content option

download this list via the onedrive address below:

<https://1drv.ms/u/s!arbk8mlwrx7bbqtksf468tmi4ew>

password for extract: gov2021

thanks

regards

היי, מעדכן שלפני מספר דקות זיהינו מייל phishing זדוני שנשלח אליכם אתמול בערב בשעה 20:00. להערכתנו מדובר בניסיון תקיפה של קבוצה איראנית שאנו מכנים TEMP.Zagros (מוכרת גם כ-MuddyWater).

המייל נשלח מכתובת המייל israel[.]profit-fs[.]com - מדובר בדומיין לגיטימי של חברת פרופיט שירותים פיננסיים. המייל מנוסח באנגלית, ומבקש מהמשתמש ללחוץ על קישור ל-OneDrive שממנו יורד קובץ אקסל זדוני עם מאקרו. המאקרו מתקין סקריפט זדוני ומייצר לו פרסיסטנטיות. הסקריפט מתקשר עם שרת C2 (אשלח עוד רגע את ה-IP שלו).

אנו מעמיקים כרגע בפרטי המקרה ונעדכן כשהיה לנו ממצאים נוספים.

עוד רגע אשלח מזהים וצילום מסך של המייל כדי שתוכלו לחפש אצלכם.

✓ 17:30



THREAT RESEARCH

UNC215: Spotlight on a Chinese Espionage Campaign in Israel

S. THREAT INTEL TEAM

PRIZED GROUPS (UNC GROUPS)

Impromise tradecraft and operational tactics, techniques, and espionage group we track as UNC215. While UNC215's targets East, Europe, Asia, and North America, this report focuses on operations at Israeli entities.

On the July 19, 2021, [announcements](#) by governments in North America and European governmental organizations, such as the North Atlantic Treaty Organization and the European Union, condemning widespread cyber espionage by the Chinese Government. These coordinated statements attributing the attacks to the Chinese Government corroborate our long-standing findings of targeting of private companies, governments, and various other entities. This blog post shows yet another region where Chinese

Exploiting Trust Relationships

UNC215 leveraged trusted third parties in a 2019 operation targeting an Israeli government network. As illustrated in Figure 2, the operators were able to access their primary target via RDP connections from a trusted third party using stolen credentials and used this access to deploy and remotely execute FOCUSFJORD on their primary target.

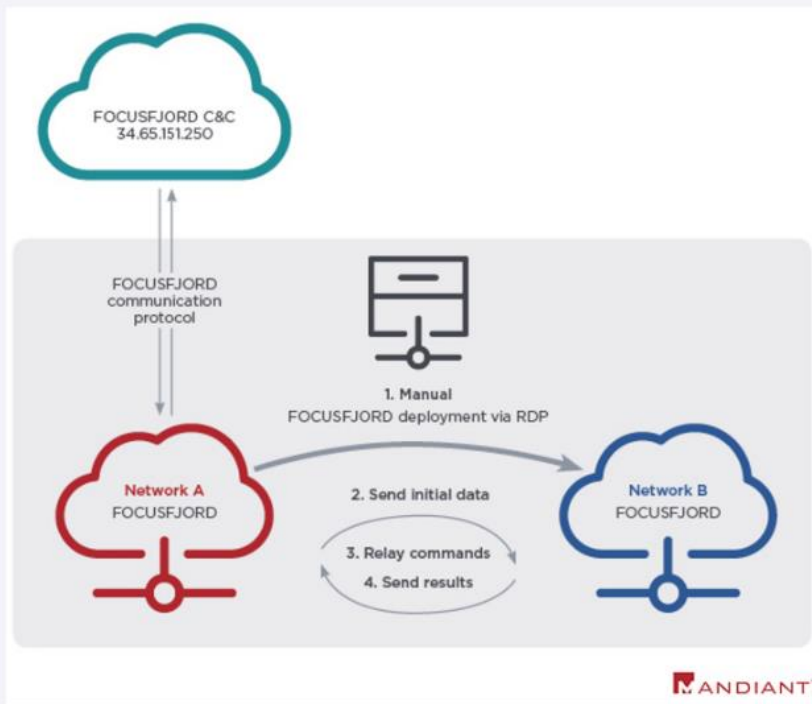


Figure 2: Two FOCUSFJORD samples configured to proxy C2 traffic



AIA Analyst Role



How We Look at a CTI Framework

ESSENTIAL ELEMENTS



CYBER THREAT PROFILE

- Geography, Industry, Sector, High-value Targets
- Environmental, Business and Operational Knowledge
- Threats, Vulnerabilities and Exposure



STAKEHOLDER ANALYSIS

- Business Area, Key People, Data and Assets
- Desired Intelligence
- Consumption Needs
- CTI Use Cases Mapped to Service Catalog



INTELLIGENCE REQUIREMENTS

- Criteria, Categorization and Prioritization
- Sources and Methods
- Intent and Expected Actions
- Alignment and Intel Gap Analysis

CORE PRACTICES



CTI LIFECYCLE MANAGEMENT

- Collections and Processing
- Analyst Tradecraft/Expertise
- Analytic Framework
- Production Standards



TECHNOLOGY INTEGRATION

- Threat Intelligence Platform (TIP)
- API and SIEM Integration
- Source Management
- Supporting Analytic Toolsets

REALIZED CAPABILITIES



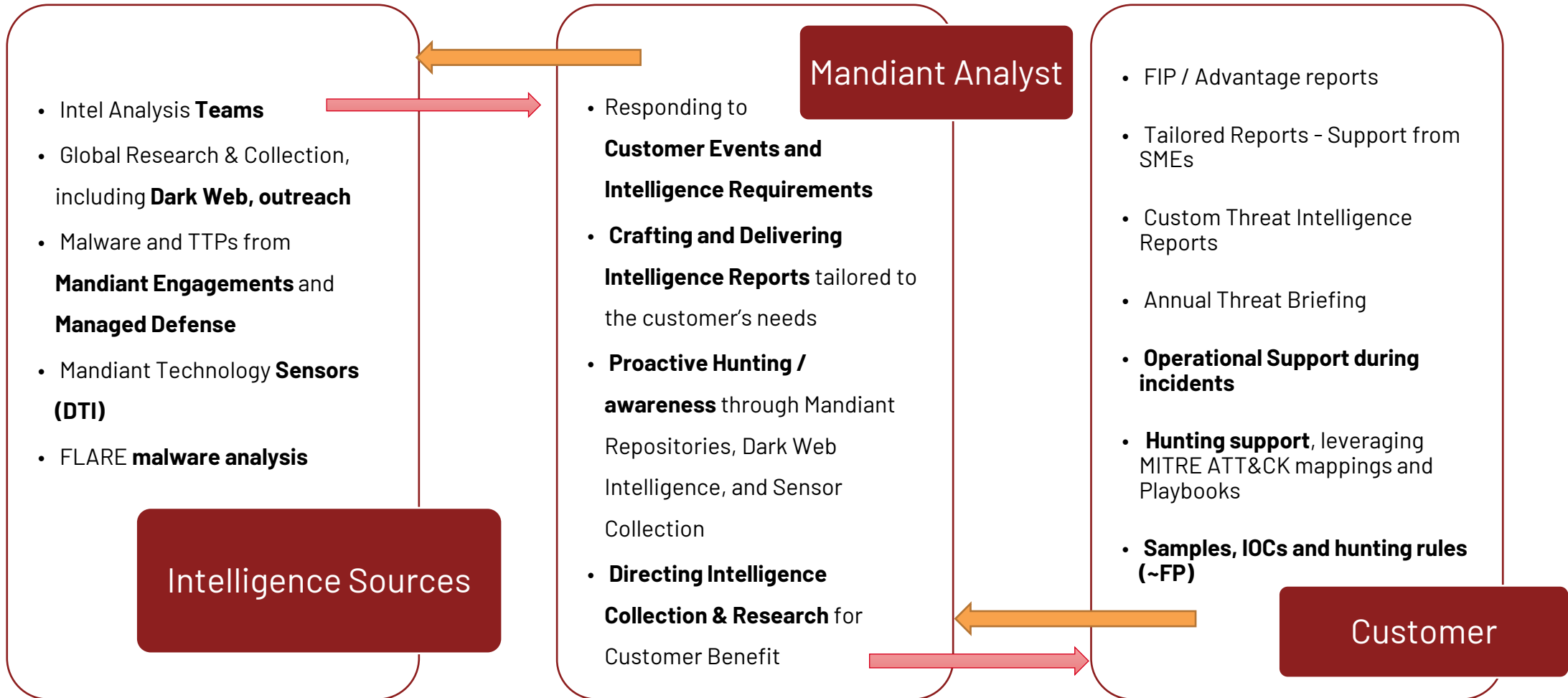
BUSINESS & CYBER OPERATIONS

- Cyber Strategy Support
- Cyber Risk Collaboration
- Analytic/Tactical Support to Cyber Defense Teams (SOC, IR, Hunt, Vuln Mgmt...)
- Community of Interest Sharing
- Threat Trending and Forecasting
- Proactive Threat Detection
- Repeatable and Effective Threat Communications

INTELLIGENCE-LED CAPABILITY EVOLUTION

Potential Workflows

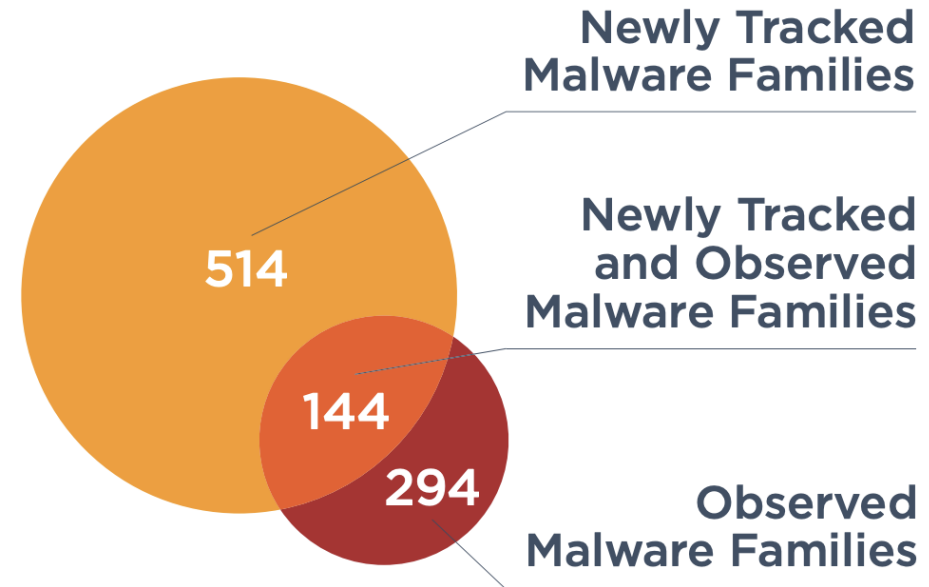
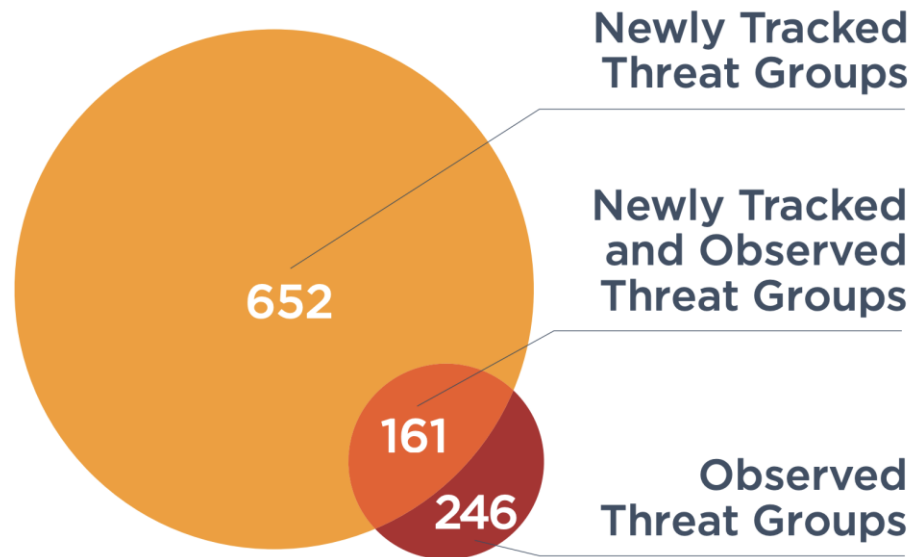
- Customized Intelligence
- Executive Briefings
- Intelligence Enrichment
- Raw Data
- Quick RFI Responses
- Custom Analyst Exchanges
- Rapid Delivery of New and Developing Threat Intelligence
- Operational Collaboration
- Intelligence Fusion
- Methodology Advisor
- Access to Subject Matter Experts
- Data Queries
- Operational Risk Advisor
- Access to Data from Beyond the Perimeter of the Customer Organization
- Ability to Task Global Team of Researchers
- Products can Remain in Secure Environment
- Malware Sample Sharing



Tracking Threats

A Dynamic Threat Landscape

Timely Intelligence More Important than Ever



Mandiant Threat Group Terminology



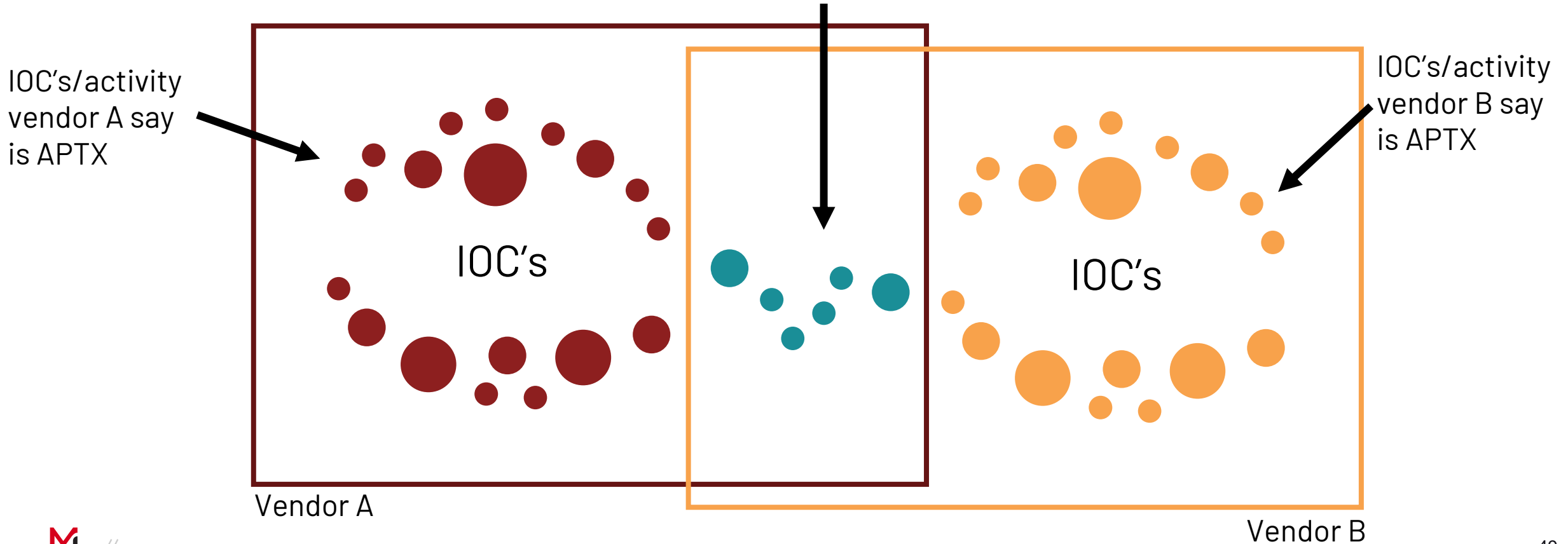
Activity

Cluster

Understanding Intel Vendor Naming

APT28 ≠ Tsar group ≠ Empire ≠ Fancy Bear

IOC's both vendors agree on being APTX

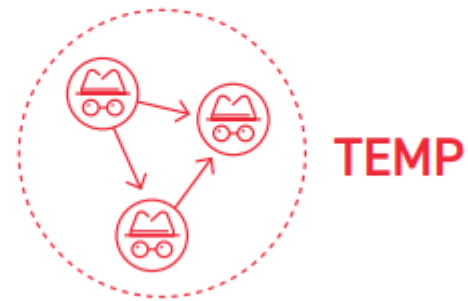


Mandiant's way of keeping track



Uncategorized

- Cluster of Threat Activity



Temporary

- Placeholder for Campaign or Group
- Promoted UNC's



Attributed

- Promoted UNC's
- Promoted TEMP/TEAM

Mandiant Threat Groups

APT1 China	APT14 China	APT25 China	APT36 Pakistan	338 China	FIN7 Financial Threat	Sandworm Team Russia	TEMP.Ace India	TEMP.Hyena Lebanon	TEMP.Shadow Financial Threat
APT2 China	APT15 China	APT26 China	APT37 North Korea	Conference Crew China	FIN8 Financial Threat	Termite Team China	TEMP.Armageddon Russia	TEMP.Isotope Russia	TEMP.Splinter Financial Threat
APT3 China	APT16 China	APT27 China	APT38 North Korea	Conimes Team China	FIN9 Financial Threat	Tonto Team China	TEMP.Avengers China	TEMP.Jafar Iran	TEMP.Tick China
APT4 China	APT17 China	APT28 Russia	APT39 Iran	CyberBerkut Russia	FIN10 Financial Threat	Turla Team Russia	TEMP.Barhopper China	TEMP.Katar India	TEMP.Toucan China
APT5 China	APT18 China	APT29 Russia	APT40 China	Fallout Team South Korea	FIN11 Financial Threat	The DarkOverlord Financial Threat	TEMP.Beanie Iran	TEMP.Lice Iran	TEMP.Traveler Financial Threat
APT6 China	APT19 China	APT30 China	APT41 China	FIN1 Financial Threat	FIN12 Financial Threat		TEMP.Beebus China	TEMP.MetaStrike Financial Threat	TEMP.Trident China
APT7 China	APT20 China	APT31 China		FIN2 Financial Threat	Hangover Team India		TEMP.Bengal India	TEMP.Omega Iran	UNC757 Iran
APT8 China	APT21 China	APT32 Vietnam		FIN3 Financial Threat	Havildar Team Pakistan		TEMP.Demon Financial Threat	TEMP.Overboard China	TEMP.Veles Russia
APT9 China	APT22 China	APT33 Iran		FIN4 Financial Threat	Koala Team Russia		TEMP.DragonOK China	TEMP.Peekaboo China	TEMP.Zagros Iran
APT10 China	APT23 China	APT34 Iran		FIN5 Financial Threat	Naikon Team China		TEMP.Hermit North Korea	TEMP.Scimitar Possible Egyptian Hamis Sympathizers	
APT12 China	APT24 China	APT35 Iran		FIN6 Financial Threat	Roaming Tiger China		TEMP.Hex China		

Iran – UNC788, UNC2428, UNC2448, UNC1530, UNC3371

China – UNC215

Russia – UNC2589

DPRK – Andariel(UNC614), UNC1130

Country Profile: Israel (2020)

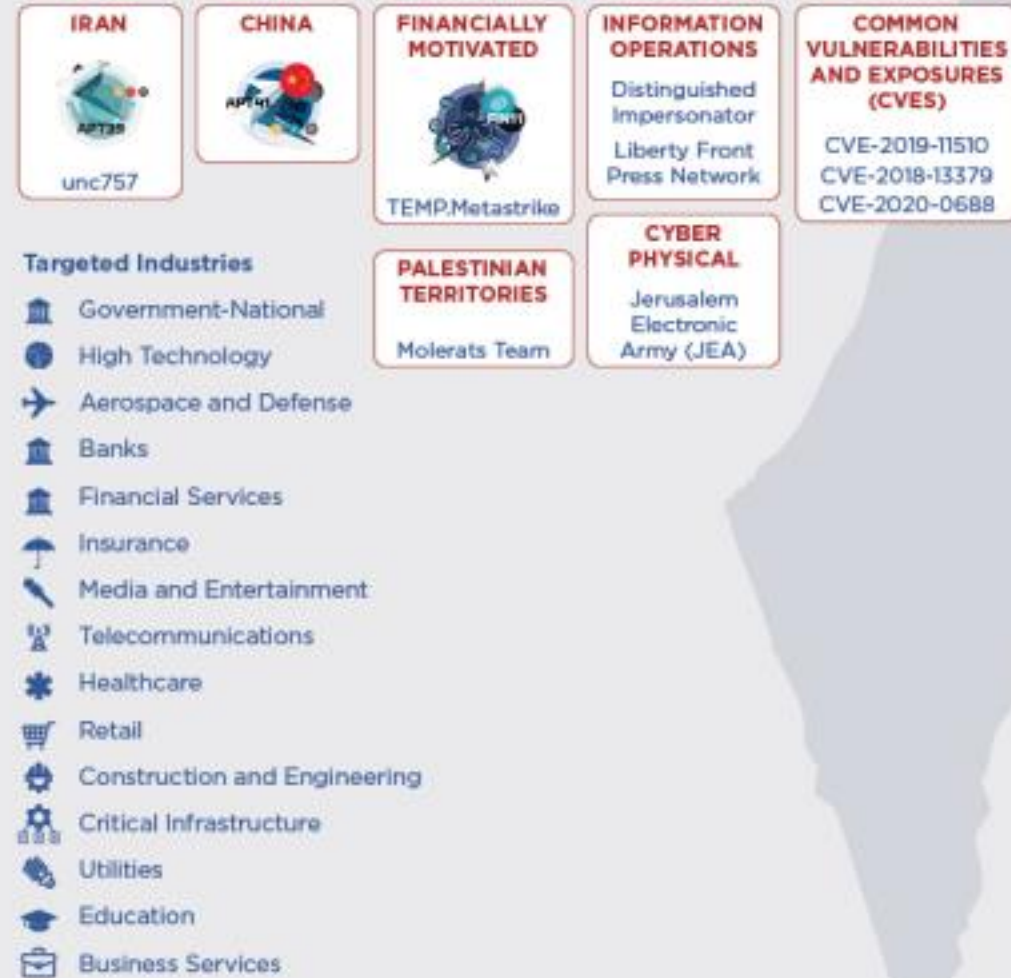
Strategic (ST)

October 08, 2020 02:24:00 PM, 20-00019709, Version: 1

Executive Summary

- Mandiant Threat Intelligence assesses with high confidence that cyber espionage operations pose a high-frequency and high-intensity threat to organizations and individuals in Israel, particularly those associated with government, high technology, and defense. Iranian, Palestinian, Chinese, and North Korean groups have targeted Israel.
- We assess with high confidence that financially motivated cyber crime represents a moderate-frequency and intensity threat to Israel and will continue to affect the nation for the foreseeable future.
- We assess with moderate confidence that foreign information operations represent a growing and high-frequency and intensity threat to Israel, both from campaigns attempting to manipulate domestic opinion and internationally targeted campaigns attempting to foster anti-Israel sentiments.
- Israel is a common target for hacktivist campaigns, particularly those with pro-Palestine, pro-Islam, and anti-Israel motivations, and such campaigns present a moderate-frequency but low-intensity threat. We expect hacktivist targeting of Israel to continue for the foreseeable future, particularly in response to triggering events, such as instances of conflict between Israeli forces and Palestinians.

POTENTIAL THREATS TO ISRAEL





Thank You

German Simkin
0547906908
german.simkin@mandiant.com

MANDIANT[®]

YOUR CYBERSECURITY ADVANTAGE