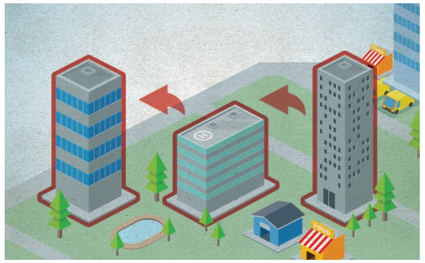
FASTWEB-7LAYERS BANCHE&SICUREZZA 2021

SOC (R)EVOLUTION

FASTWEB un passo avanti

7 LAYERS

NEWS DAL MONDO: LA SETTIMANA TIPO



DAL FURTO ALL'OSTAGGIO: IL 38% DELLE ISTITUZIONI FINANZIARIE HA SPERIMENTATO UN AUMENTO DEGLI ATTACCHI DI ISLAND HOPPING

UNA MISCONFIGURATION DI UN BUCKET S3 HA ESPOSTO DATI PERSONALI DI 7883 IMPIEGATI

L'ITALIA È TRA I PAESI PIÙ COLPITI DAL CYBERATTACCO A MICROSOFT EXCHANGE

NON SOLO SOLDI, MA INFORMAZIONI: IL CYBERCRIMINE ALL'ATTACCO DELLE BANCHE

L'ATTACCO SOLARWINDS, IN REALTÀ UN'OPERAZIONE DI SPIONAGGIO SU LARGA SCALA

DUE CRITICAL ZERO-DAY VULNERABILITIES TROVATE IN MIGLIAIA DI ATM

CyberCrime Revenue

https://www.blockchain.com/btc/address/19iqYbeATe4RxghQZJnYVFU4mjUUu76EA6?page=

Wallet Exchange Explorer Buy Bitcoin Trade

Sponsored Content

Explorer Bitcoin Explorer Address Search your transaction, an address or a block USD

Address

This address has transacted 22,862 times on the Bitcoin blockchain. It has received a total of 309,566,552.53862696 BTC ($17,434,336,271,808.76) and has sent a total of 309,554,854.00616188 BTC ($17,433,677,427,540.19). The current value of this adc 11,698.53246508 BTC ($658,844,268.58).

Address	19iqYbeATe4RxghQZJnYVFU4mjUUu76EA6
Format	BASE58 (P2PKH)
Transactions	22,862
Total Received	$17,434,336,271,808.76
Total Sent	$17,433,677,427,540.19
Final Balance	$658,844,268.58

Payment Request Donation Button

https://www.blockchain.com/btc/address/3DF62rvkkybk7EH3KJU7oRytLoSL4R1D1A

Wallet Exchange Explorer Buy Bitcoin Trade

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 4.69951976 BTC ($262,270.66) and has sent a total of 4.69951976 BTC ($262,270.66). The current value of this address is 0.00000000 BTC ($0.00).

Address	3DF62rvkkybk7EH3KJU7oRytLoSL4R1D1A
Format	BASE58 (P2SH)
Transactions	2
Total Received	4.69951976 BTC

https://www.blockchain.com/btc/address/1HsHZBVPA35ZashPCtGmarhUDetBP6auvW

Wallet Exchange Explorer Buy Bitcoin Tra

Sponsored Content

Explorer Bitcoin Explorer Address Search your transaction, an address or a block USD

Address

This address has transacted 14 times on the Bitcoin blockchain. It has received a total of 13.56000000 BTC ($756,053.94) and has sent a total of 13.56000000 BTC ($756,053.94). The current value of this address is 0.00000000 BTC ($0.00).

Address	1HsHZBVPA35ZashPCtGmarhUDetBP6auvW
Format	BASE58 (P2PKH)
Transactions	14
Total Received	$756,053.94
Total Sent	$756,053.94
Final Balance	$0.00

Payment Request Donation Button

2021-02-25 12:47

QZJnYV... 18032.32996552 BTC

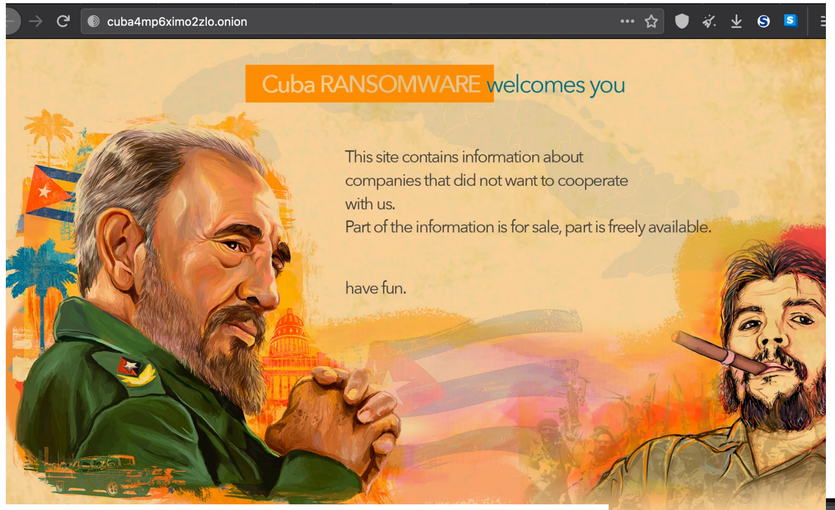
-4.69951976 BTC

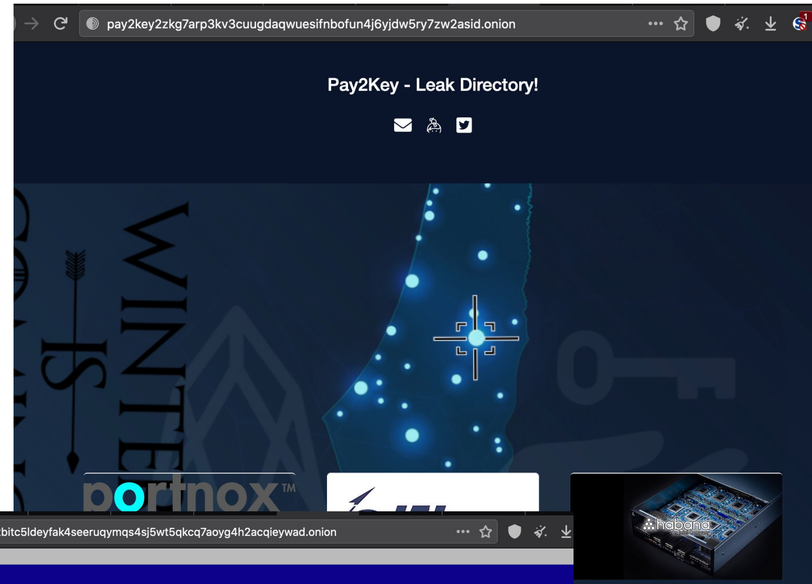
Ransomware groups Wiki

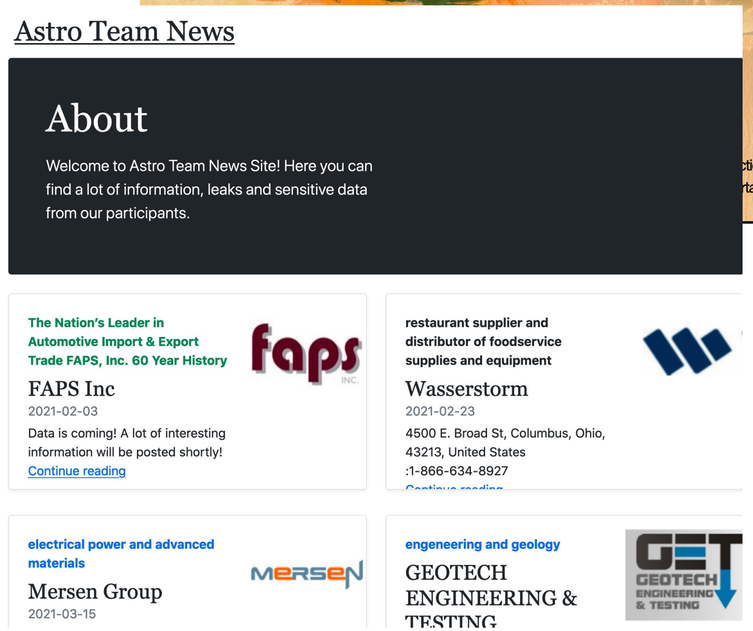
Ransomware groups Wiki

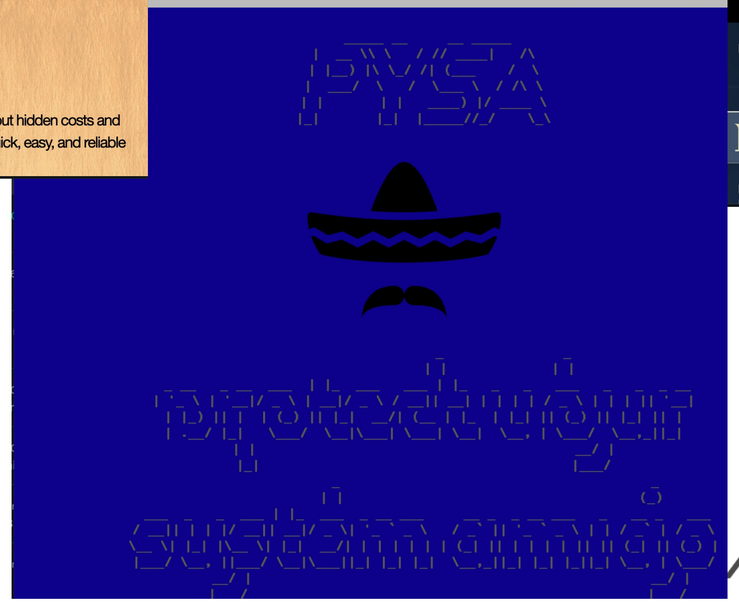
(Updated on March 23, 2021)

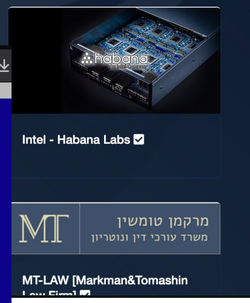
Id.	Name	No. of victims	Onion Site	Status
1	Conti	291	Link	Up
2	MAZE	266	No Link	-
3	Egregor	206	No Link	-
4	Sodinokibi (REvil)	178	Link	Up
5	DoppelPaymer	174	Link	Up
6	NetWalker	144	No Link	-
7	Pysa	103	Link	Down
8	Avaddon	61	Link	Up
9	DarkSide	58	Link	Up
10	CL0P	43	Link	Up
11	Nefilim	32	Link	Up
12	Everest	26	Link	Up
13	Suncrypt	22	Link	Up
14	Ragnar_Locker	22	Link	Up
15	Ragnarok	20	Link	Up
16	Mount Locker	17	Link	Up
17	BABUK LOCKER	15	Link	Up
18	RansomEXX	14	Link	Up
19	AKO	9	No Link	-
20	LockBit	9	No Link	-
21	Cuba	9	Link	Up
22	Sekhmet	6	No Link	-
23	Pay2Key	6	Link	Up
24	Team Snatch	6	No Link	-
25	Astro Team	5	Link	Up
26	Ranzy Locker	3	Link	Up
27	NEMTY	1	No Link	-





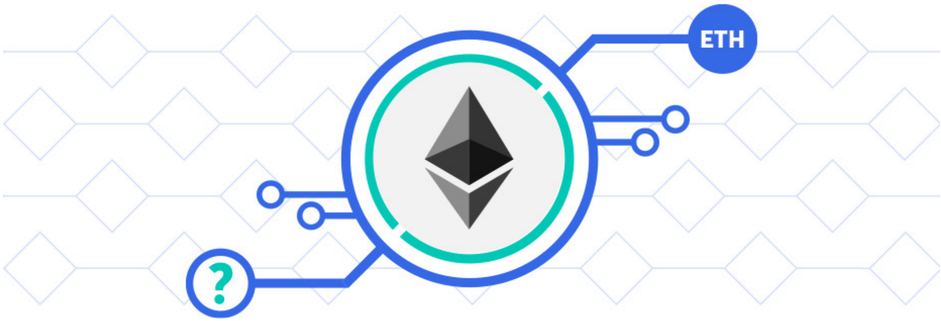






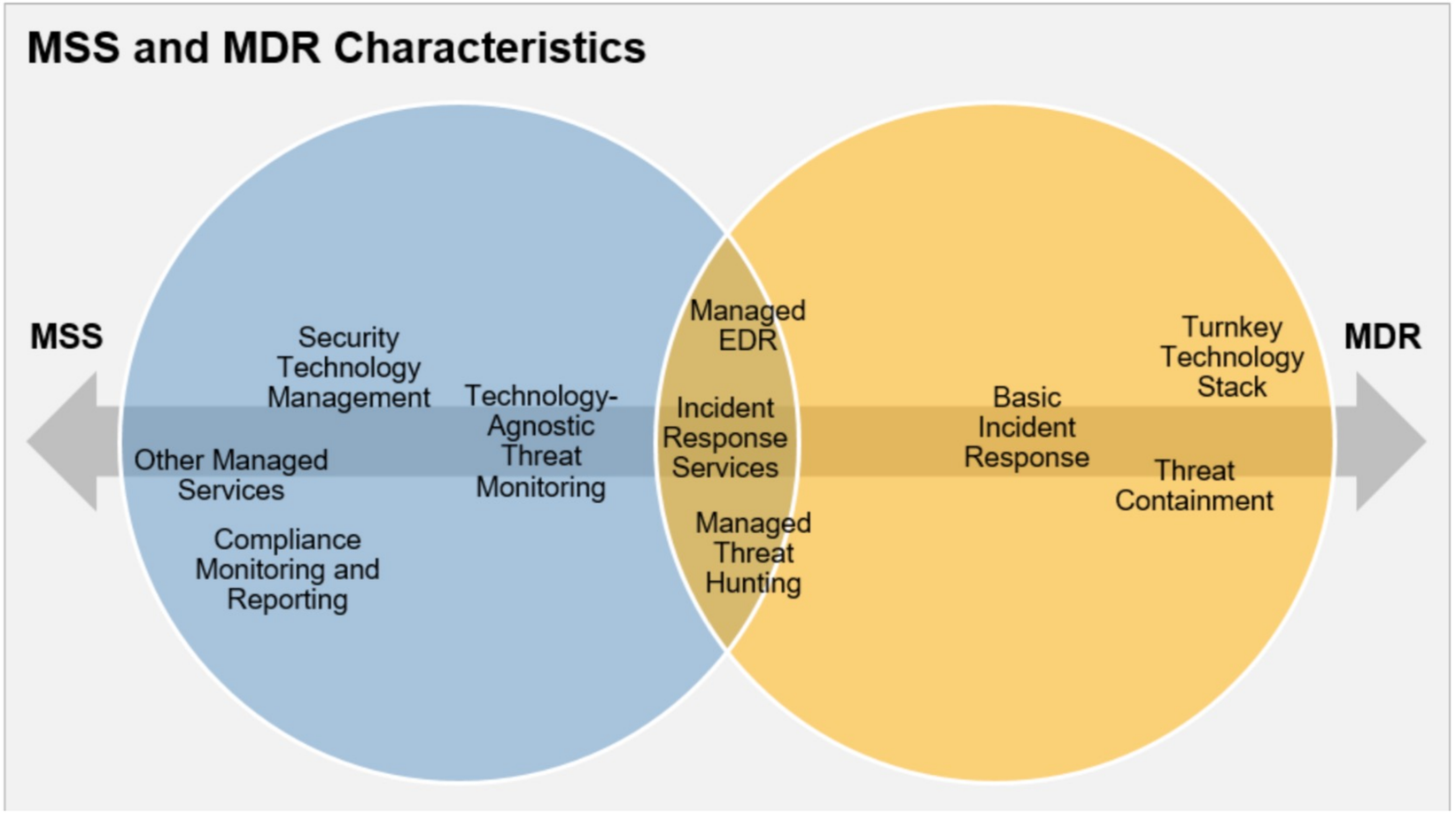
VICTIM VALUE

- Ransomware
- CyberEspionage
- Cyberwarfare
- Extortion
- Phising &Scam
- Fraud
- DDoS ransom
- Leak DB reselling
- Leak Pwd reselling
- Botnet Rent



SOC vs MDR

MSSP SOC vs MDR



Modello LEGACY SOC

Proposizione standard

SIEM + monitoring service o sonda network con funzioni AI/UEBA
Lista dei data source compatibili + EPS
System Engineers – NO CyberAnalyst
24x7 NOC – NO CyberAnalyst skills
No RED e PURPLE team skill

SOC ≠ SIEM
Cybersecurity ≠ Prodotti
Machine Learning ≠ Efficacia

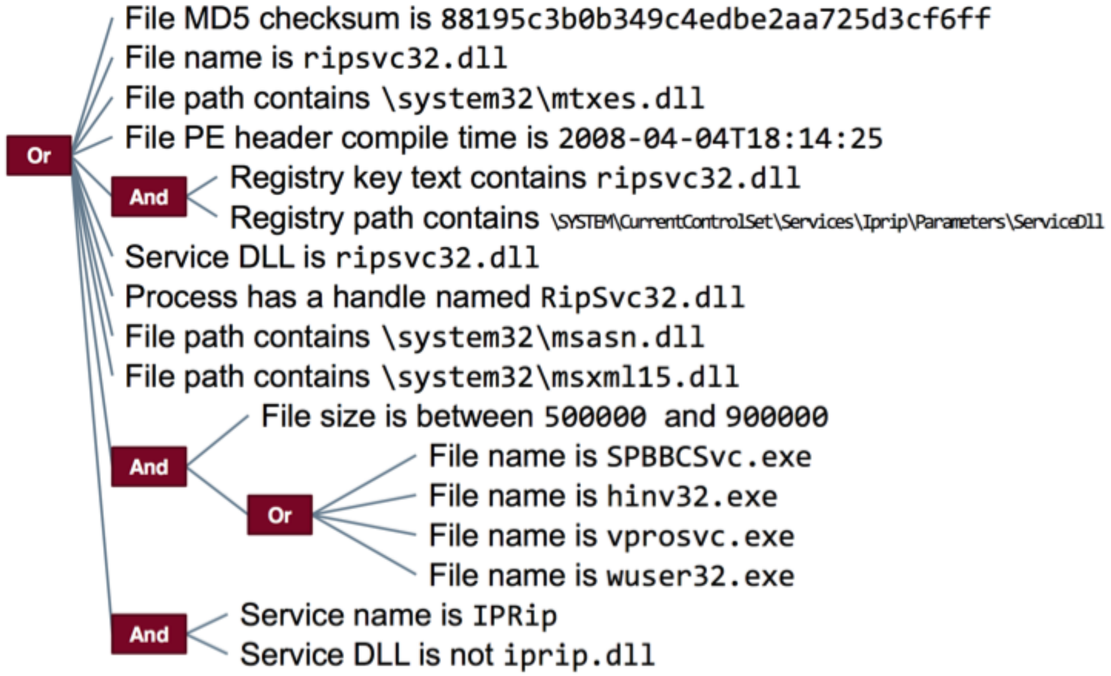
INDICATOR OF COMPROMISE

Indicator of Compromise: un artefatto individuato su reti o sistemi elaborativi che indica, con un elevato grado di confidenza, la presenza di un'intrusione informatica.

Deve essere:

- specifico
- deve rendere complesso per l'attaccante evadere l'IoC individuato
- facile da elaborare, modificare e condividere

What does an IoC look like?



TTPs: TATTICHE, TECNICHE E PROCEDURE

Per poter fronteggiare efficacemente attacchi di tipo ATP gli analisti devono disporre di una serie di informazioni tra cui:

- Chi mi sta attaccando? Perchè?
- Come mi stanno attaccando?
- Stanno attaccando i miei partner/fornitori/terze parti o i miei competitors?
- Che metodi stanno usando? Quali skill/tools?

Per una risposta efficace è fondamentale catalogare le tattiche, tecniche, e procedure (TTPs) utilizzate da ogni attaccante durante tutte le fasi di un attacco, nonché la condivisione delle informazioni raccolte.

Cyber Attack Life Cycle

Che problemi risolve l’MDR?

Troppi (falsi) allarmi
Troppi allarmi possono sovraccaricare un piccolo team di sicurezza. La stanchezza nella gestione degli avvisi porta a un monitoraggio inadeguato, fa sì che gli operatori trascurino altre attività e lascia una rete aperta ad un attacco.

Threat Analysis
È difficile identificare minacce gravi dal rumore degli alert. Un elemento dannoso può sembrare un avviso casuale, mentre gli errori comuni possono sollevare bandiere rosse in tutto il sistema. Per determinare la causa, l'ambito e lo stato di un problema, un team IT deve analizzare la situazione.
Investendo in MDR, un'azienda garantisce strumenti di analisi avanzati ed esperti di sicurezza in grado di interpretare gli eventi nella rete.

Attacchi avanzati e minacce
Un team IT scarsamente formato può avere difficoltà di fronte a una minaccia avanzata. I fornitori di MDR sono dotati di specialisti della sicurezza in grado di tenere il passo con gli attacchi informatici moderni. Investendo in MDR, ti assicuri che i migliori talenti del settore monitorino le tue reti e i tuoi dispositivi.

Time Expensive Deployment
La configurazione di un SOC legacy basato su SIEM richiede molto tempo.

THREAT INTELLIGENCE DATA SOURCES

1. Human intelligence

- Incident response
- Reverse engineers, TI analysts
- Joint investigations with law enforcement agencies
- Undercover agents on the dark web; in-depth analysis
- Hackers' communication channels on Jabber/IRC
- Exchange of information and networking within the community

2. Malware intelligence

- ISP-level sensors
- Proprietary fraud detection solution
- Proprietary anti-APT solution
- Honeypot network
- Spamtraps
- Sinkholing
- Malware emulators
- External Threat Hunting System (a solution for identifying malicious infrastructures and extracting threat-related data)
- External sandboxes and cooperation with AV vendors

3. Data intelligence

- Botnet and phishing C&C servers
- C&C servers of web skimmers (Java sniffers)
- Phishing log collection points
- Card shops
- ATS malware
- Compromised data checkers (crime-to-crime services)

4. Open-source intelligence

- Paste sites
- Code repositories (Git)
- Messaging apps
- Vulnerabilities and exploits
- Social media
- URL sharing services

Threats & actors
Cybercriminals
nation-state
Darkweb
Threat landscape
Analyst reports

Compromise and leaks
Compromised accounts
Compromised bank cards ·
IMEI
Mules
Public leaks
Git leaks

Malware
Malware detonation
Targeted Trojans
Phishing kits
Vulnerabilities

IoC, TTP & TA

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search

- NEODYMIUM
- Night Dragon
- OilRig
- Orangeworm
- Patchwork
- PittyTiger
- PLATINUM
- Poseidon Group
- PROMETHIUM
- Putter Panda
- Rancor
- Rocke
- RTM
- Sandworm Team

		name Lazarus Group.
APT39	Chafer	APT39 is an Iranian cyber espionage group that has been active since at least 2014. They have targeted t telecommunication and travel industries to collect personal information that aligns with Iran's national pr
APT41		APT41 is a group that carries out Chinese state-sponsored espionage activity in addition to financially m activity. APT41 has been active since as early as 2012. The group has been observed targeting healthcar technology, and video game industries in 14 countries.
Axiom	Group 72	Axiom is a cyber espionage group suspected to be associated with the Chinese government. It is respon Operation SMN campaign. Though both this group and Winnti Group use the malware Winnti for Window groups appear to be distinct based on differences in reporting on the groups' TTPs and targeting.
BlackOasis		BlackOasis is a Middle Eastern threat group that is believed to be a customer of Gamma Group. The grou shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regio correspondents, and think tanks. A group known by Microsoft as NEODYMIUM is reportedly associated c BlackOasis operations, but evidence that the group names are aliases has not been identified.
BlackTech		BlackTech is a cyber espionage group operating against targets in Eas Japan and Hong Kong.

				maintain persistence on victim systems.[1]
Enterprise	T1055		Process Injection	APT41 malware TIDYELF loaded the main WINTERLOVE component by injecting it into the iexplore.exe process.[1]
Enterprise	T1090		Proxy	APT41 used a tool called CLASSFON to covertly proxy network communications.[1]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	APT41 used RDP for lateral movement.[1]
Enterprise	T1496		Resource Hijacking	APT41 deployed a Monero cryptocurrency mining tool in a victim's environment.[1]
Enterprise	T1014		Rootkit	APT41 deployed rootkits on Linux systems.[1]
Enterprise	T1053	.005	Scheduled Task/Job:	APT41 used a compromised account to create a scheduled task on a system.[1]

Software

ID	Name	References	Techniques
S0073	ASPXSpy	[1]	Server Software Component: Web Shell
S0190	BITSAdmin	[2]	BITS Jobs, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol, Ingress Tool Transfer, Lateral Tool Transfer
S0069	BLACKCOFFEE	[1]	Command and Scripting Interpreter: Windows Command Shell, File and Directory Discovery, Indicator Removal on Host: File Deletion, Multi-Stage Channels, Process Discovery, Web Service: Dead Drop Resolver, Web Service: Bidirectional Communication
S0160	certutil	[2]	Deobfuscate/Decode Files or Information, Ingress Tool Transfer, Subvert Trust Controls: Install Root Certificate
S0020	China Chopper	[1]	Application Layer Protocol: Web Protocols, Brute Force: Password Guessing, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, File and Directory Discovery, Indicator Removal on Host: Timestomp, Ingress Tool Transfer, Network Service Scanning, Obfuscated Files or Information: Software Packing, Server Software Component: Web Shell
S0154	Cobalt Strike	[2]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Token Impersonation/Theft, Access Token Manipulation: Parent PID Spoofing, Access Token Manipulation: Make and Impersonate Token, Account Discovery: Domain Account, Application Layer Protocol, Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, BITS Jobs, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Visual Basic,

and non-

MDR³

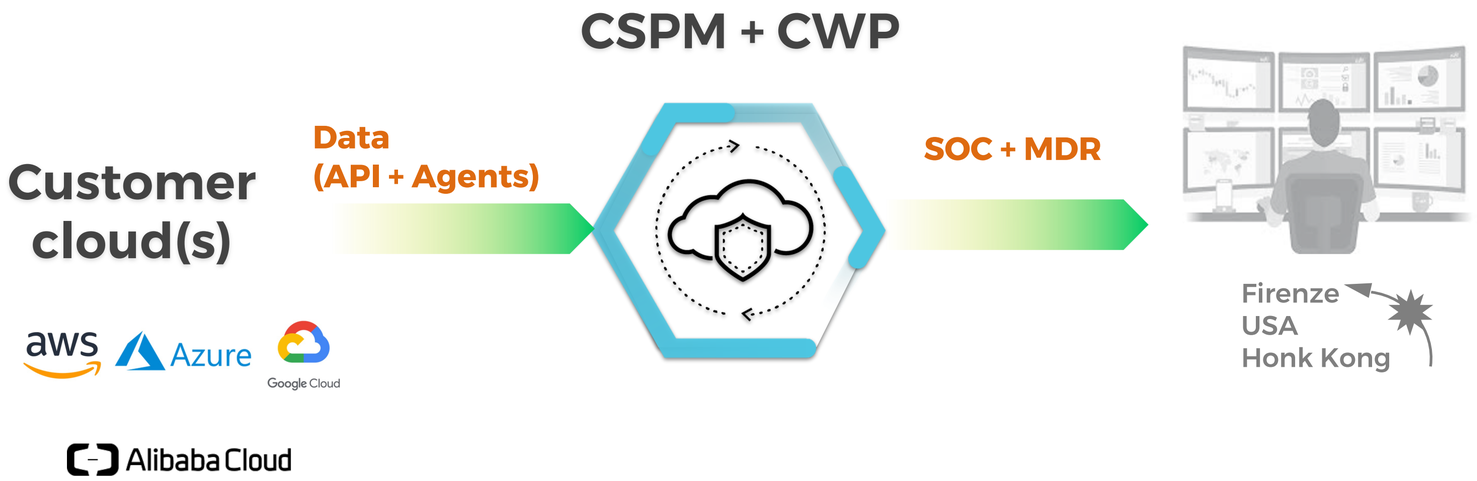
MDR Enterprise

MDR Service Platform:

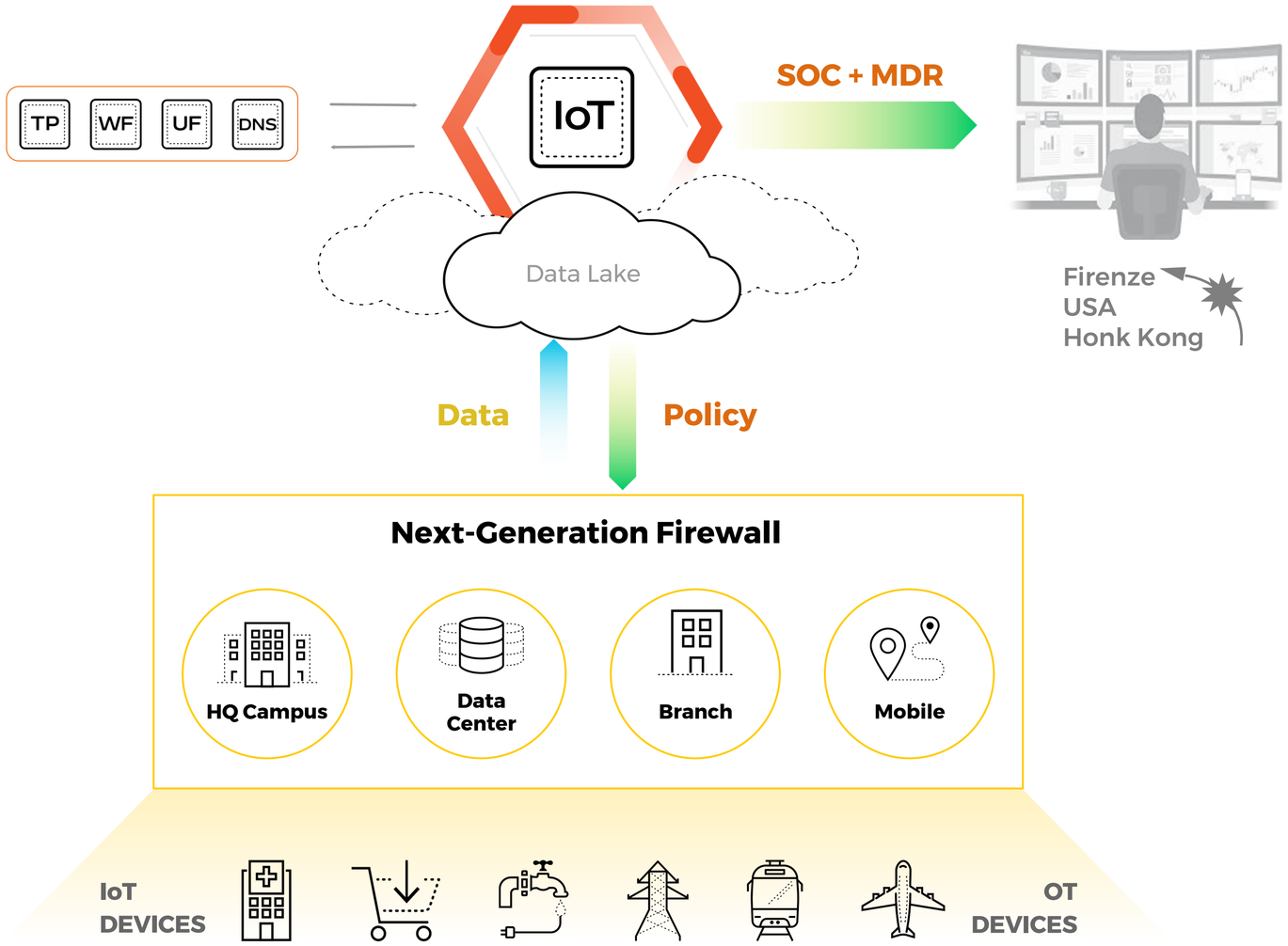
1. **EDR** o **XDR** per la protezione degli endpoint (client/server)
2. **Log Collector** o **SIEM** che riceve i log dagli apparati di sicurezza di terze parti e li invia alla piattaforma cloud di **Threat Intelligence** per effettuare una correlazione in real time con gli IoCs rilevati
3. **Threat Intelligence Platform** che riceve i log generati dall'ambiente ICT del cliente ed effettua una correlazione in real time dei dati ricevuti con gli IOC generati dinamicamente
4. **MITRE ATT&CK TTP mapping** consentire un'indagine approfondita e aiutare a bloccare le minacce prima che abbiano l'opportunità di causare danni.
5. **NGFW** IPS/IDS per l'analisi real time del traffico di rete
6. Servizio di **Managed Detection & Response** composto da analisti di sicurezza con competenze di ethical hacking

MDR Cloud

- SOC + MDR Service
  24x7 Follow-the-Sun
- Compliance &
  Vulnerability Assessment
- Security Alerting
- Incident Report



MDR SCADA/OT/IoT

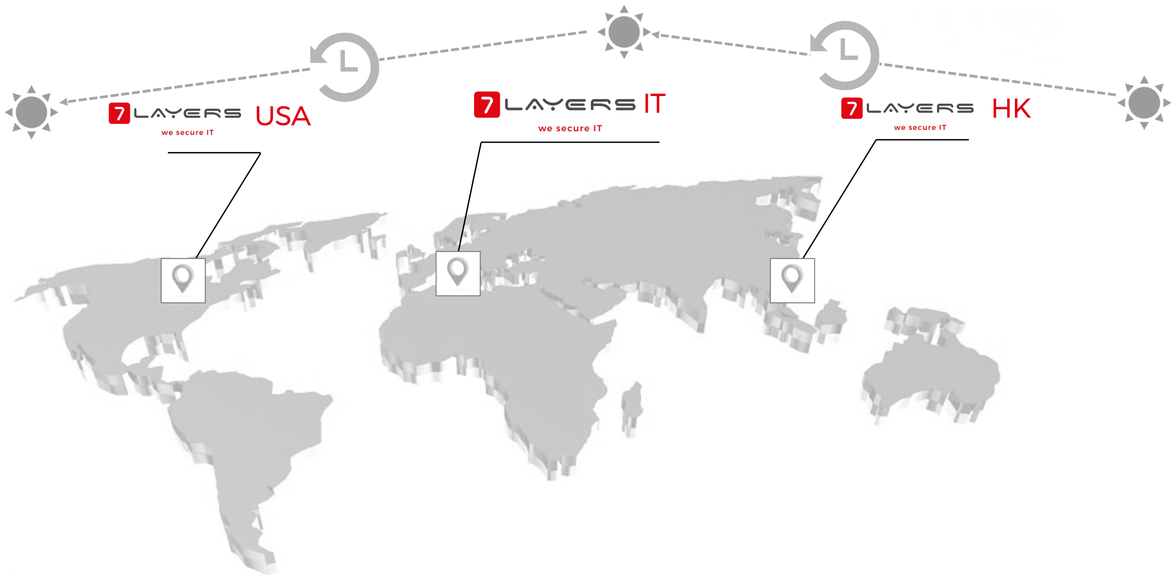


- SOC + MDR Service 24x7 Follow-the-Sun
- Cyber Threat Analysis
- Risk Compliance Analysis
- Passive Vulnerability Assessment

7Layers at a glance

Advanced Security Services

- SOC/CERT specializzato in servizi MDR
- Security-only company
- Global Customer Base
- 24x7 follow the sun
- 80+ Techical Certification



TEAM

- Security Analyst
- Senior Security Analyst
- Threat Hunter
- Threat Intel Researcher
- Red Team Specialists
- Incident Responder – CSIRT Analyst
- Malware Analyst

GRAZIE PER L'ATTENZIONE!

7 LAYERS
we secure IT

FASTWEB
un passo avanti