CYBER SECURITY as a SERVICE

Managed Detection and Response

Come difendersi dalle nuove minacce informatiche e l'importanza dei servizi MDR.

Hafnium: pandemia di un attacco.
Cosa si nasconde dietro l'attacco divenuto pandemia.

Mercoledì 12 maggio alle 17.00 (durata: 1 ora)

Cynet

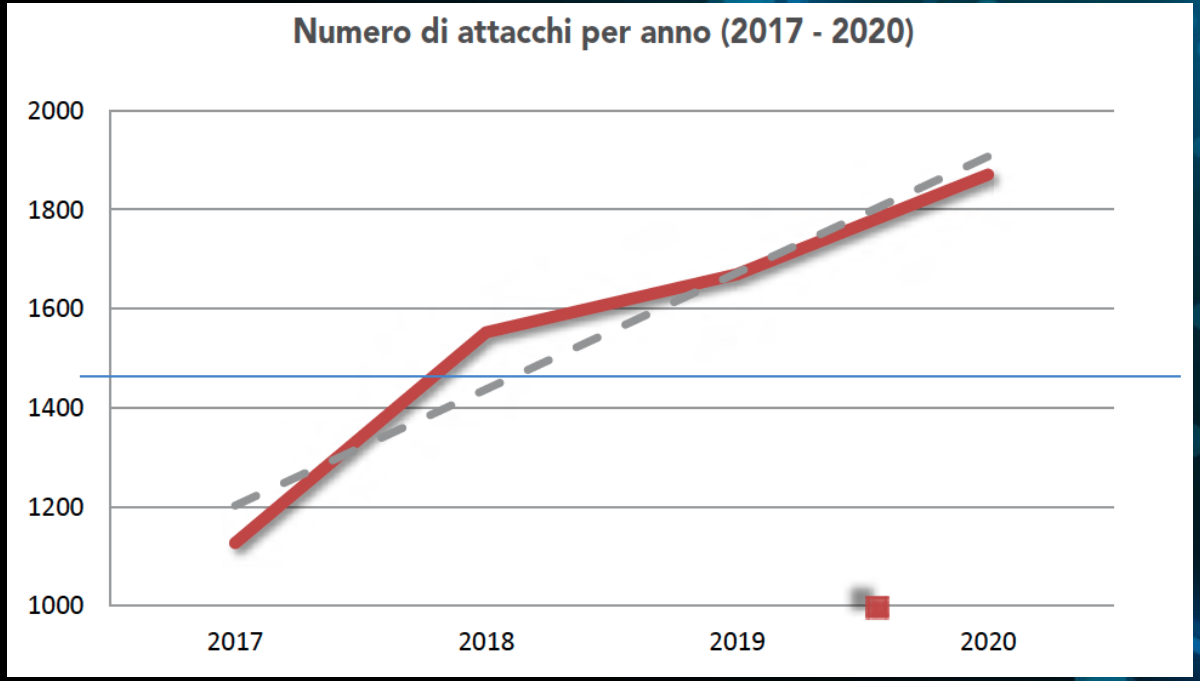
25° OTS

Agenda

- Partnership OTS – CYNET (Filippo Torrini - OTS)
- Servizio MDR as a Service OTS – CYNET (Massimo Montedoro - OTS)
- Soluzione MDR Cynet (Marco Lucchina - Cynet)
- Hafnium: l'attacco divenuto pandemia: (Raffaele Amodeo – Cynet
  - Come si sviluppa l'attacco, tattiche tecniche e procedure
  - Simulazione, della risposta all'attacco Hafnium
- Domande e risposte

Perché siamo qui?

Il numero di attacchi rilevati nel 2020 segna una differenza del **+29%** (**+12%** rispetto al 2019, **+ 20%** rispetto al 2017) rispetto alla media degli attacchi per anno del triennio precedente (1.449), visualizzata con una linea blu orizzontale nel grafico seguente.



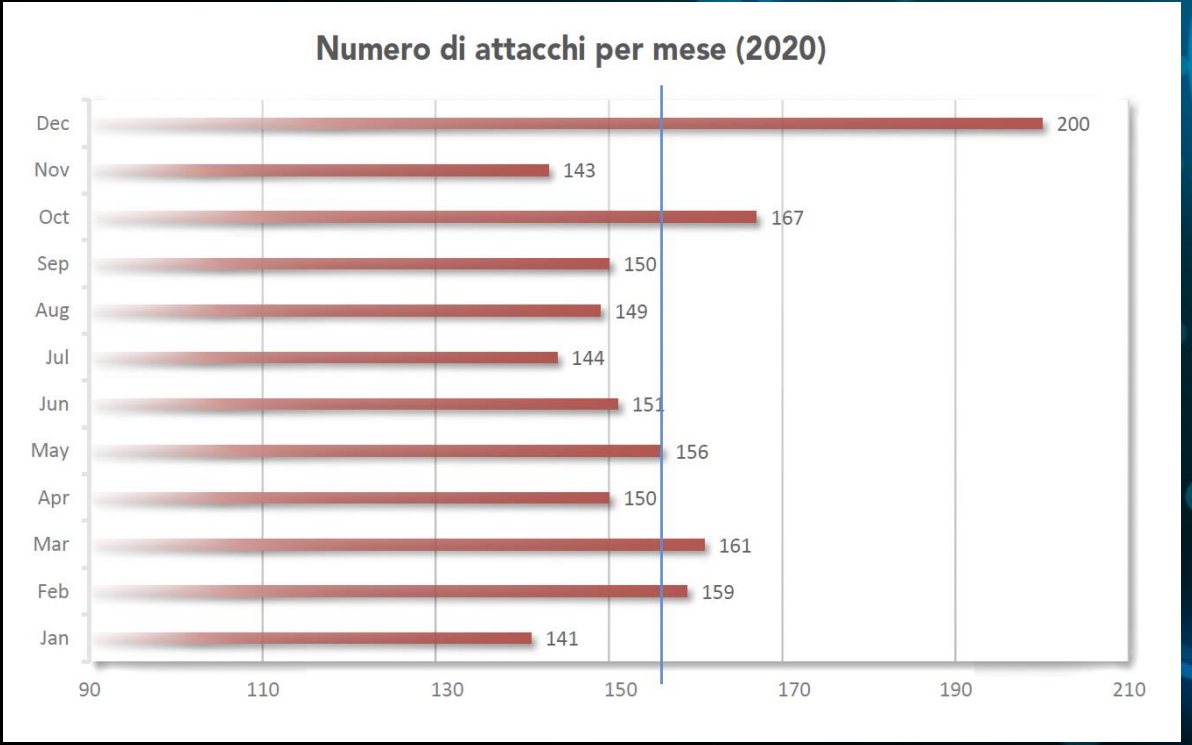
Fonte ultimo rapporto clusit 2021

Perché siamo qui?

Nel 2020 sono stati registrati in media **156 attacchi gravi al mese** a livello globale (rispetto ad una media di 94 al mese nel 2017, e di 120 al mese nel triennio 17-19).

Il picco massimo mensile di sempre si è avuto nel dicembre 2020 (200 attacchi).

Oltre a dicembre, i mesi peggiori nel 2020 sono stati febbraio, marzo ed ottobre.



Fonte ultimo rapporto clusit 2021

Perché siamo qui?

Nel 2020 le categorie più colpite sono state **Multiple Targets (attacchi verso bersagli multipli in parallelo)** (374 attacchi).

Interessante sottolineare l'aumento di attacchi singoli verso la categoria "Others" **(+164,2%),** nuove tipologie non ancora classificate.

VITTIME PER TIPOLOGIA	2017	2018	2019	2020	2020 su 2019	Trend 2020
Institutions: Gov - Mil - LEAs - Intelligence	179	252	247	258	4.5%	↗
Multiple targets	222	304	395	374	-5.3%	↗
Health	80	159	203	215	5.9%	↗
Banking / Finance	117	157	100	97	-3.0%	↗
Online Services / Cloud	95	129	186	177	-4.8%	↗
Research - Education	71	109	141	207	46.8%	↑
Software / Hardware Vendor	68	109	70	113	61.4%	↑
Entertainment / News	115	102	83	69	-16.9%	↓
Critical Infrastructures	40	57	50	70	40.0%	↑
Hospitability	34	45	27	22	-18.5%	↓
GDO / Retail	24	39	37	35	-5.4%	↗
Others	40	30	53	140	164.2%	↑
Org / ONG	8	18	17	26	52.9%	↑

HAFNIUM - Un attacco senza precedenti

Who is HAFNIUM?

HAFNIUM primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

HAFNIUM has previously compromised victims by exploiting vulnerabilities in internet-facing servers, and has used legitimate open-source frameworks, like Covenant, for command and control. Once they've gained access to a victim network, HAFNIUM typically exfiltrates data to file sharing sites like MEGA.

In campaigns unrelated to these vulnerabilities, Microsoft has observed HAFNIUM interacting with victim Office 365 tenants. While they are often unsuccessful in compromising customer accounts, this reconnaissance activity helps the adversary identify more details about their targets' environments.

HAFNIUM operates primarily from leased virtual private servers (VPS) in the United States.

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

HAFNIUM - Un attacco senza precedenti

microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

OLD Personal Work Utili Logicmonitor Host... Portal Gmail Translate Treccani - La cult... News Notizie Nutar

Microsoft | Security Solutions Products Operations Partners Resources Trust Center All Microsc

March 2, 2021

HAFNIUM targeting Exchange Servers with 0-day exploits

Microsoft Threat Intelligence Center (MSTIC)
Microsoft 365 Defender Threat Intelligence Team
Microsoft 365 Security

Scan Exchange log files for indicators of compromise

The Exchange Server team has created a script to run a check for HAFNIUM IOCs to address performance and memory concerns. That script is available here: https://github.com/microsoft/CSS-Exchange/tree/main/Security.

The FBI is remotely hacking hundreds of computers to protect them from Hafnium

They went inside unprotected computers to remove the threat

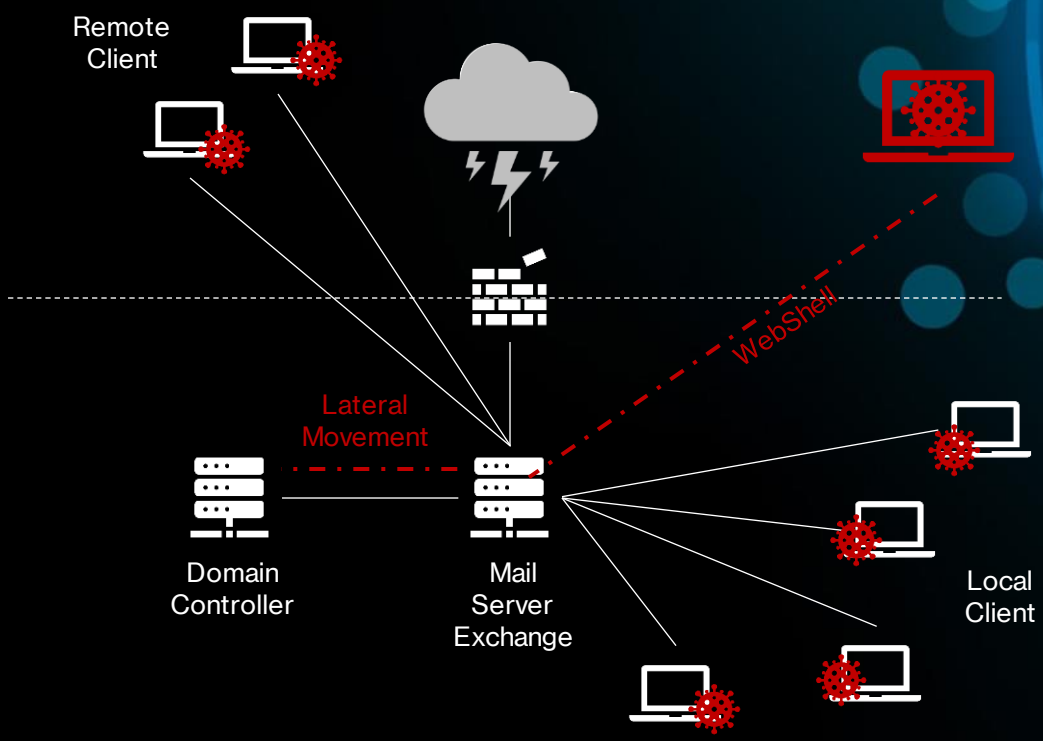
By Sean Hollister | @StarFire2258 | Apr 13, 2021, 8:25pm EDT

SHARE

Illustration by Alex Castro / The Verge

Email (required)

HAFNIUM - Un attacco senza precedenti



OTS + CYNET = MDR SaaS

MDR – Cyber Security as a Service

H24 SOC
DETECTION

FULLY
CLOUD

H24
RESPONSE

MDR – Cyber Security as a Service