Ransomware targeting VMware ESXi

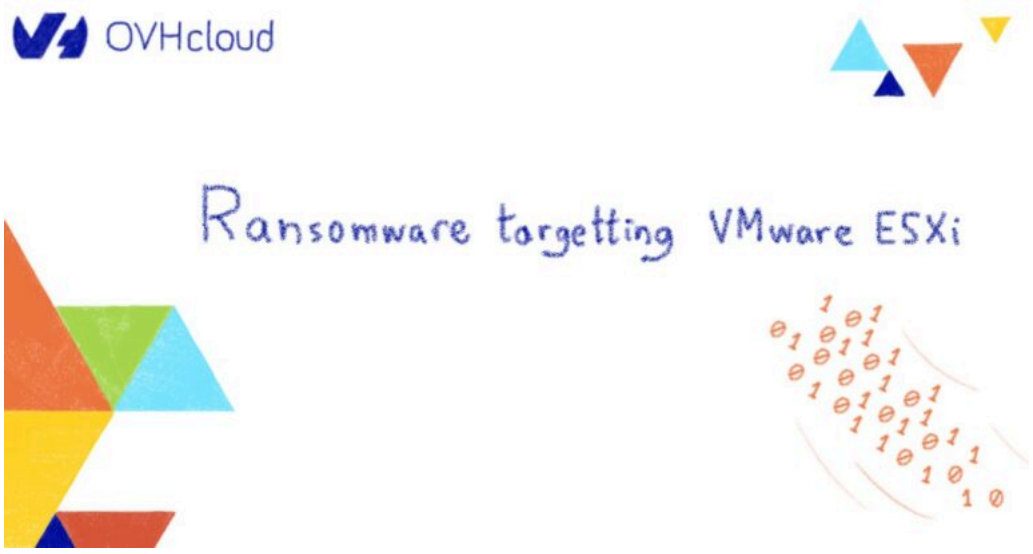
By Julien Levrard

Published: 2023-02-03 · Archived: 2026-04-05 22:44:12 UTC

A wave of attacks is currently targetting ESXi servers. No OVHcloud managed service are impacted by this attack however, since a lot of customers are using this operating system on their own servers, we provide this post as a reference in support to help them in their remediation.

These attacks are detected globally. According to experts from the ecosystem as well as authorities, the malware is probably using CVE-2021-21974 as compromission vector. Investigation are still ongoing to confirm those assumptions.

Our technical teams are working to identify the detailed characteristics of the attack all the while coordinating with our peers from other CERTs and security teams.



Update 07/02/2023

We continue our investigations and to provide support to our customers.
We prioritize our efforts:

- to identify our impacted customers on our networks to provide the most accurate and appropriate information to help them to recover from the attack.
- to identify potentially vulnerable customers to ensure they mitigate the risks appropriately as soon as possible in the case of on an other wave of similar attack.

Several security researchers may have found a link between the Babuk Ransomware source code leaked in September 2021. The encryption cipher (Sosemanuk) is used in the both cases but the code structure seems to be slightly different.

```
4014e3: 48 8b b5 58 ff ff ff          movq    -168(%rbp), %rsi
4014ea: 8b bd 8c fd ff ff             movl    -628(%rbp), %edi
4014f0: ba 00 00 10 00                movl    $1048576, %edx
4014f5: e8 de f4 ff ff                callq   0x4009d8 <read@plt>
4014fa: 48 89 85 20 ff ff ff          movq    %rax, -224(%rbp)
401501: 48 83 bd 20 ff ff ff ff       cmpq    $-1, -224(%rbp)
401509: 75 1e                         jne     0x401529 <encrypt_simple+0x1e3>
40150b: be 01 00 00 00                movl    $1, %esi
401510: bf a2 84 40 00                movl    $4228258, %edi
401515: e8 e0 f8 ff ff                callq   0x400dfa <print_error>
40151a: c7 85 3c fd ff ff 03 00 00 00 movl    $3, -708(%rbp)
401524: e9 1d 03 00 00                jmp     0x401846 <encrypt_simple+0x500>
401529: 48 8b 8d 20 ff ff ff          movq    -224(%rbp), %rcx
401530: 48 8b 95 58 ff ff ff          movq    -168(%rbp), %rdx
401537: 48 8b b5 58 ff ff ff          movq    -168(%rbp), %rsi
40153e: 48 8d bd 60 ff ff ff          leaq    -160(%rbp), %rdi
401545: e8 19 6b 00 00                callq   0x408063 <sosemanuk_encrypt>
40154a: 48 8b 85 20 ff ff ff          movq    -224(%rbp), %rax
401551: 48 f7 d8                      negq    %rax
401554: 48 89 c6                      movq    %rax, %rsi
401557: 8b bd 8c fd ff ff             movl    -628(%rbp), %edi
40155d: ba 01 00 00 00                movl    $1, %edx
401562: e8 c1 f4 ff ff                callq   0x400a28 <lseek@plt>
401567: 48 83 f8 ff                   cmpq    $-1, %rax
40156b: 75 1e                         jne     0x40158b <encrypt_simple+0x245>
40156d: be 01 00 00 00                movl    $1, %esi
401572: bf bd 84 40 00                movl    $4228285, %edi
401577: e8 7e f8 ff ff                callq   0x400dfa <print_error>
```

In addition to the recovery procedure described earlier, we noted that the encryption process is only impacting a small amount of data within the file. Depending of your VM OS and file system type, you might be able to recover data with data revery tools, at least partially. Be carefull, this tools might have irreversible action on the file so, We recommend to copy the VM files on an other location to protect the data before trying any recovery operation.

We are referencing a list of companies that can assist you to recover your data and reconstruct your systems. The list of companies will be available at OVHcloud support.

We also remind to our customers acting as Data Controller that they might have legal requirements to notify autorities in case of security incident. Ensure you declared the incident to the appropriate autorities within the right timeframe.
You will find below the Data Protection Autorities procedures for databreach violation for mainly impacted countries and CERT websites as well. Check with your legal department or counsel to ensure you notify the right organisation according to your status.

For PII data controllers:

- France: https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- Italy: https://servizi.gpdp.it/databreach/s/
- Belgium: https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles
- Spain: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion
- Poland : https://uodo.gov.pl/pl/501/2278

- UK: https://ico.org.uk/for-organisations/report-a-breach/
- Germany: https://formulare.bfdi.bund.de/lip/form/display.do?%24context=E72B6A6366642AE42118
- Portugal: https://www.cnpd.pt/databreach/
- Quebec: https://www.cai.gouv.qc.ca/incident-de-confidentialite-impliquant-des-renseignements-personnels/aviser-commission-et-personnes/

CERT:

- France: https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/
- Italy: https://cert-agid.gov.it/contatti/
- Belgium : https://www.cert.be/fr/signaler-un-incident
- Spain: https://www.ccn-cert.cni.es/gestion-de-incidentes/notificacion-de-incidentes.html
- Poland: https://incydent.cert.pl/#!/lang=en
- UK: https://report.ncsc.gov.uk/
- Canada: https://www.cyber.gc.ca/en/incident-management
- Germany: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/Kontakt/kontakt_node.html
- Portugal: https://www.cncs.gov.pt/pt/certpt/

Additionnal references:
https://www.bleepingcomputer.com/news/security/
https://www.bleepingcomputer.com/forums/t/782193/esxi-ransomware-help-and-support-topic-esxiargs-args-extension/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
https://blogs.vmware.com/security/2023/02/83330.html
https://members.loria.fr/MMinier/static/papers/sosemanuk_08.pdf

Update on 05/02/2023

We continue to work on the technical analysis in coordination with authorities and security community to determine IOCs and understand how the malware is behaving after the initial compromission.

So far we identified the following behavior:

- The compromission vector is confirmed to use a OpenSLP vulnerability that might be CVE-2021-21974 (still to be confirmed). The logs actually show the user *dcui* as involved in the compromission process.
- Encryption is using a public key deployed by the malware in /tmp/public.pem
- The encryption process is specifically targeting virtual machines files (“*.vmdk*”, “.vmx”, “*.vmxf*”, “.vmsd”, “*.vmsn*”, “.vswp”, “*.vmss*”, “.nvram”,”*.vmem”)
- The malware tries to shutdown virtual machines by killing the VMX process to unlock the files. This function is not systematically working as expected resulting in files remaining locked.
- The malware creates argsfile to store arguments passed to the encrypt binary (number of MB to skip, number of MB in encryption block, file size)
- No data exfiltration occurred.

In some cases, encryption of files may partially fail, allowing to recover data. Enes Sönmez (@enes_dev), a turkish security researcher has documented the procedure for recovery of VMDK files. The procedure is described on his blog (https://enes.dev/). We tested this procedure as well as many security experts with success on several impacted servers. The success rate is about 2/3. Be aware that following this procedure requires strong skills on ESXi environnements. Use it at your own risk and seek the help of experts to assist.

In the previous version of the post, we made the assumption the attack was linked to the Nevada Ransomware which was a mistake. No material can lead us to attribute this attack to any group. Attribution is never easy and we leave security researchers to make their own conclusions.

ESXi OS can only be installed on bare metal servers. We launched several initiatives to identify vulnerable servers, based on our automation logs to detect ESXI installation by our customers.
We have limited means of action since we have no logical access to our customer servers. For identified bare metal hosts:

- We sent emails on Friday's afternoon to warn customer of the risk and provide them information on to mitigate the risk
- We blocked the OpenSLP port (427) between internet and the servers with ESXI installed. Customer can deactivate the filtering rule in their management interface if the use of port 427 is required for whatever reason.

We launched scan to identify compromised hosts, by testing the presence of the web page and/or the ssh banner specifying the host has been compromised to notify impacted customers.

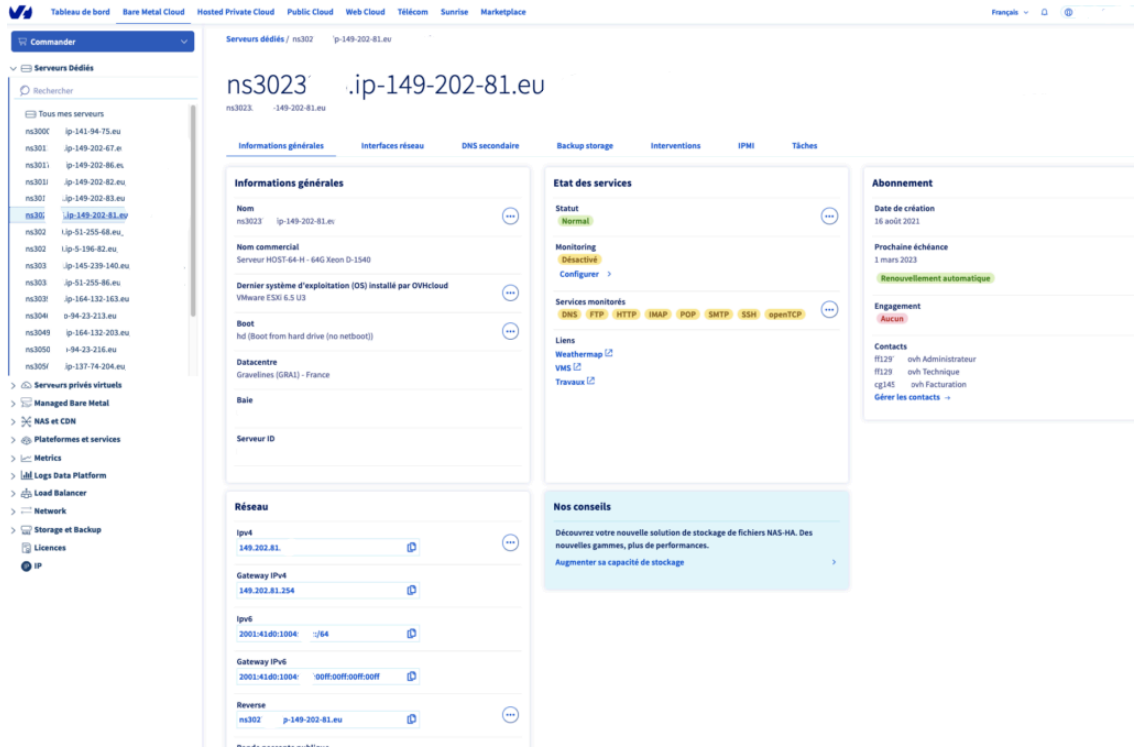
Our support team is fully mobilized to help our customers to protect their systems and to help them to recover if they are impacted by the attack.

Additionnal references:
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
https://enes.dev/
https://straightblast.medium.com/my-poc-walkthrough-for-cve-2021-21974-a266bcad14b9

First response action items on 03/02/2023

The attack is primarily targetting ESXi servers in version before 7.0 U3i, apparently through the OpenSLP port (427).

To check your version of ESXi, please refer to your server page in your customer interface to identify wich version has been deployed on the server or to the ESXi interface on the system itself.



So far, we can identify the following recommendations regarding our services:

For Bare Metal customer using ESX-i we strongly recommend in emergency :

- to deactivate the OpenSLP service on the server or to restrict access to only trusted IP addresses (https://kb.vmware.com/s/article/76372)
- to upgrade you ESXi on the latest security patch

In a second time, ensure:

- your data are backed up (on immutable storage?)
- only necessary services are active and filtered with ACL to only trusted IP adresse
- monitor your system for any abnormal behaviour.

Our clients using VMware Private Cloud are not impacted. By design, the SSL gateway prevent this typology of attack by blocking the external access to this port (OpenSLP 427).

For our Public Cloud customers, there is no dependency to ESXi so no risk are identified.

No other product among OVHcloud's portfolio is threatened by this ransomware campaign.

We will update this blog post with any information that could help to reduce the risk associated with this threat.

Additionnal references:

- https://kb.vmware.com/s/article/76372
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21974

Source: https://blog.ovhcloud.com/ransomware-targeting-vmware-esxi/