

Are Virtual Machines the New Gold for Cyber Criminals?

 mcafee.com/blogs/other-blogs/mcafee-labs/are-virtual-machines-the-new-gold-for-cyber-criminals/

June 10, 2021



Introduction

Virtualization technology has been an IT cornerstone for organization for years now. It revolutionized the way organizations can scale up IT systems in a heartbeat, allowing them to be more agile as opposed to investing into dedicated “bare-metal” hardware. To the outside untrained eye, it might seem that there are different machines on the network, while in fact all the “separate” machines are controlled by a hypervisor server. Virtualization plays such a big role nowadays that it isn’t only used to spin up servers but also anything from virtual applications to virtual user desktops.

This is something cyber criminals have been noticing too and we have seen an increased interest in hypervisors. After all, why attack the single virtual machine when you can go after the hypervisor and control all the machines at once?

In recent months several high impact CVEs regarding virtualization software have been released which allowed for Remote Code Execution (RCE); initial access brokers are offering compromised VMware vCenter servers online, as well as ransomware groups developing specific ransomware binaries for encrypting ESXi servers.

VMware CVE-2021-21985 & CVE-2021-21986

On the 25th of May VMware disclosed a vulnerability impacting VMware vCenter servers allowing for Remote Code Execution on internet accessible vCenter servers, version 6.5,6.7 and 7.0. VMware vCenter is a management tool, used to manage virtual machines and ESXi servers.

CVE-2021-21985 is a remote code execution (RCE) vulnerability in the vSphere Client via the Virtual SAN (vSAN) Health Check plugin. This plugin is enabled by default. The combination of RCE and default enablement of the plugin resulted in this being scored as a critical flaw with a CVSSv3 score of 9.8.

An attacker needs to be able to access vCenter over TCP port 443 to exploit this vulnerability. It doesn't matter if the vCenter is remotely exposed or when the attacker has internal access.

The same exploit vector is applicable for CVE-2021-21986, which is an authentication mechanism issue in several vCenter Server Plug-ins. It would allow an attacker to run plugin functions without authentication. This leads to the CVE being scored as a 'moderate severity', with a CVSSv3 score of 6.5.

While writing this blog, a Proof-of-Concept was discovered that will test if the vulnerability exists; it will not execute the remote-code. The Nmap plugin can be downloaded from this location: https://github.com/alt3kx/CVE-2021-21985_PoC.

Searching with the Shodan search engine, narrowing it down to the TCP 443 port, we observe that close to 82,000 internet accessible ESXi servers are exposed. Zooming in further on the versions that are affected by these vulnerabilities, almost 55,000 publicly accessible ESXi servers are potentially vulnerable to CVE-2021-21985 and CVE-2021-21986, providing remote access to them and making them potential candidates for ransomware attacks, as we will read about in the next paragraphs.

Ransomware Actors Going After Virtual Environments

Ransomware groups are always trying to find ways to hit their victims where it hurts. So, it is only logical that they are adapting to attacking virtualization environments and the native Unix/Linux machines running the hypervisors. In the past, ransomware groups were quick to abuse earlier CVEs affecting VMware. But aside from the disclosed CVEs, ransomware groups have also adapted their binaries specifically to encrypt virtual machines and their management environment. Below are some of the ransomware groups we have observed.

DarkSide Ransomware

```
[CFG] Root Path...../vmfs/volumes/
[CFG] Key Size.....548 Bytes
[CFG] Public Key.....VALID
[CFG] Part Size.....500mb
[CFG] Space Size.....0mb
[CFG] Min Size.....1mb
[CFG] Search Extension.....vmdk,vmem,vswp,log,vmsn
[CFG] New Extension.....darkside
```

Demo of Darkside encrypting an ESXi server: <https://youtu.be/SMWlckvLMoE>

Babuk Ransomware

Babuk announced on an underground forum that it was developing a cross-platform binary aimed at Linux/UNIX and ESXi or VMware systems:

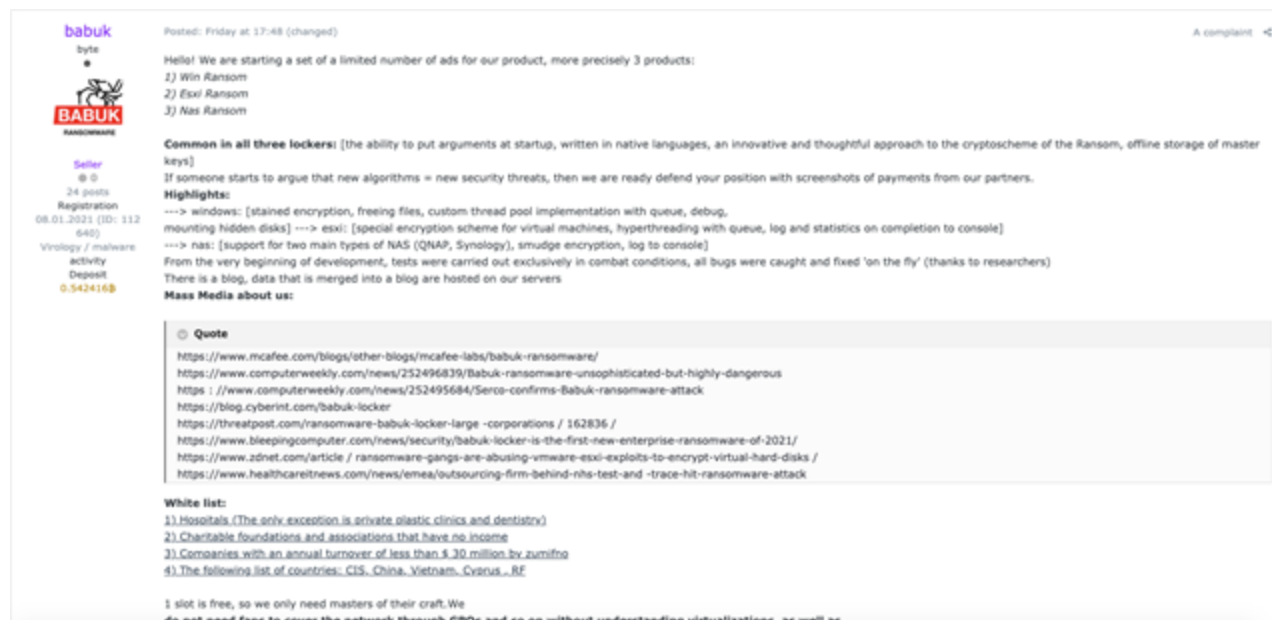


Figure 3. Babuk ransomware claiming to have built a Linux-based ransomware binary capable of mounting disks ESXi servers

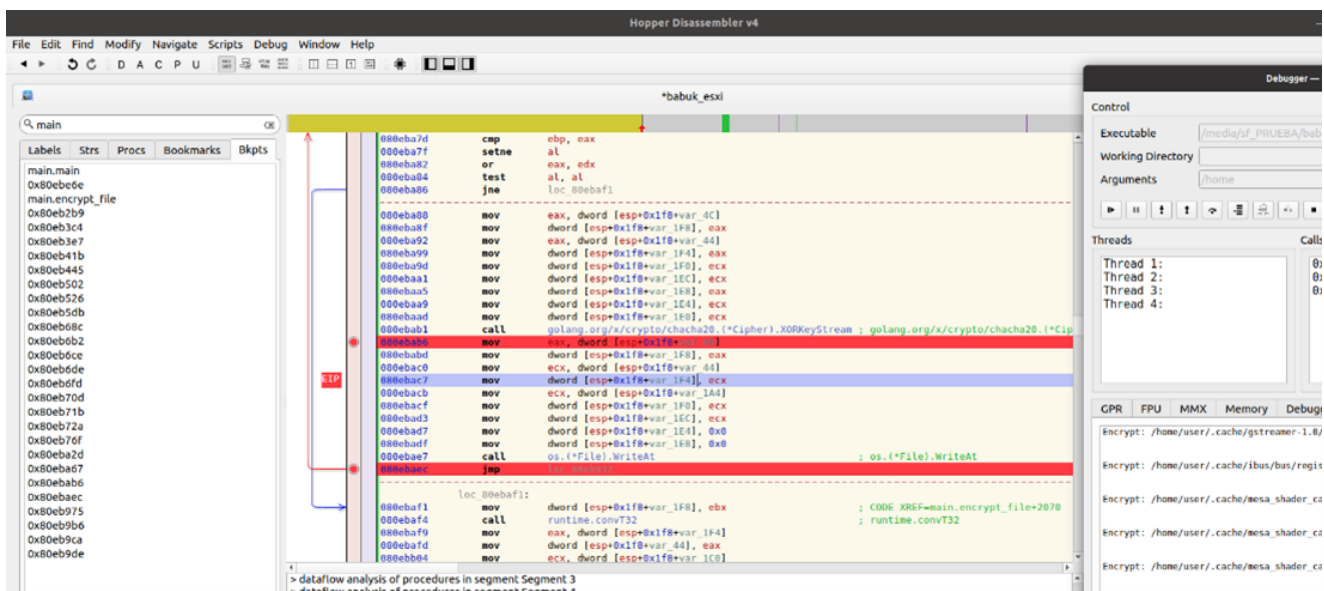
The malware is written in the open-source programming language Golang, most likely because it allows developers to have a single codebase to be compiled into all major operating systems. This means that, thanks to static linking, code written in Golang on a Linux system can run on a Windows or Mac system. That presents a large advantage to ransomware gangs looking to encrypt a whole infrastructure comprised of different systems architecture.

```

Package main: F:/AAA_PROD/BABUK_LOCK_curve25519/nas/enc
File: main.go
  encrypt_file Lines: 717 to 885 (88)
  main Lines: 885 to 825 (20)
  mainfunc1 Lines: 825 to 827 (2)
Package golang.org/x/crypto/curve25519: C:/Users/Krunker/go/src/golang.org/x/crypto/curve25519
File: curve25519.go
  fe18 Lines: 45 to 45 (8)
File: curve25519_generic.go
  feZero Lines: 18 to 29 (11)
  feAdd Lines: 29 to 35 (6)
  feSub Lines: 35 to 41 (6)
  feCopy Lines: 41 to 58 (9)
  feCswap Lines: 58 to 73 (23)
  feFromBytes Lines: 73 to 153 (88)
  feToBytes Lines: 153 to 269 (116)
  feMul Lines: 269 to 587 (238)
  feSquare Lines: 587 to 600 (133)
  feMul121668 Lines: 600 to 718 (58)
  feInvert Lines: 718 to 779 (61)
  scalarMultGeneric Lines: 779 to 795 (16)
Package golang.org/x/crypto/chacha20: C:/Users/Krunker/go/src/golang.org/x/crypto/chacha20
File: chacha_generic.go
  newUnauthenticatedCipher Lines: 88 to 128 (48)
  quarterRound Lines: 128 to 184 (56)
  (*Cipher).XORKeyStream Lines: 184 to 256 (72)
  (*Cipher).xorKeyStreamBlocksGeneric Lines: 256 to 352 (96)
  hChaCha20 Lines: 352 to 388 (36)

```

After being dropped on the ESXi server, the malware encrypts all the files on the system:



The malware was designed to target ESXi environments as we guessed, and it was confirmed when the Babuk team returned the decryptor named **d_esxi.out**. Unfortunately, the decryptor has been developed with some errors, which cause corruption in victim's files:

Overall, the decryptor is poor as it only checks for the extension ".babyk" which will miss any files the victim has renamed to recover them. Also, the decryptor checks if the file is more than 32 bytes in length as the last 32 bytes are the key that will be calculated later with other hardcoded values to get the final key. This is bad design as those 32 bytes could be trash, instead of the key, as the customer could make things, etc. It does not operate efficiently by checking the paths that are checked in the malware, instead it analyzes everything. Another error we noticed was that the decryptor tries to remove a ransom note name that is **NOT** the same that the malware creates in each folder. This does not make any sense unless, perhaps, the Babuk developers/operators are delivering a decryptor that works for a different version and/or sample.

The problems with the Babuk decryptor left victims in horrible situations with permanently damaged data. The probability of getting a faulty decryptor isn't persuading victims to pay up and this might be one of the main reasons that Babuk announced that it will stop encrypting data and only exfiltrate and extort from now on.

Initial-Access-Brokers Offering VMware vCenter Machines

It is not only ransomware groups that show an interest in virtual systems; several initial access brokers are also trading access to compromised vCenter/ESXi servers on underground cybercriminal forums. The date and time of the specific offering below overlaps with the disclosure of CVE-2021-21985, but McAfee ATR hasn't determined if this specific CVE was used to gain access to ESXi servers.

Вчера в 00:47

Selling vcenter/esxi access including login access like user/password in plaintext etc.

I have more than 1k vcenter/esxi host, some of them are school server, network sddc (software define data center), game company, hostinger server etc. The price is depend on company profile name and how many active vm inside (including storage size).

There's one common thing that i would like to mention. to be honest, i have a lot of these access but i can't gather some of them information about the company and domain, it's like these company use default domain like "photon-machine" ... but even tho they are not have specific domain name, most of them have like more of 100 active vm in there

called it **random access** for now, i will sell these random access that have no domain name \$150 for each 2 vcenter

for example these vcenter admin panel
<https://185>

you cannot determine which company that use these ip right, except you search it on whois or login inside and test a couple of vm and gather the config info after you logged in you find that these vcenter access have 2 active esxi with size more that 6TB storage (*image3.jpg*) but still, i cannot determine the company that use this vcenter cannot sell it \$100 for each of them (it's too expensive), so i sell it \$150 for each 2 vcenter that have default config

below is some context about the picture attachment :

image1.png
as you can see, i gain access to some of hostinger server with vsphere client(program to control esxi server) that located on vietnam. it is have windows and linux vm host inside with big size of hard drive. with this i can do remote console on the host and do whatever i want (upload shell on the hostinger, run miner/malware, etc).

image2.png
Malaysian Hosting Service, total more than 8TB storage

PS:
- If you know how to operate esxi/vcenter machine and interested with it hit me up and if you don't please skip this thread

Вложения

image2.png image1.png image3.jpg


Последнее редактирование: Вчера в 01:15


Жалоба Like + Цитата Ответ

Figure 4. Threat Actor selling access to thousands of vCenter/ESXi servers

VMware ESXi - User / Root accesses.

VoidZero · 03/13/2021



VoidZero 
RAID array
User

check in: 01.10.2020
Posts: 94
Reactions: fourteen

03/13/2021

Only Corporates servers!
Unlimited stock : *daily refreshed* .

User access: 10 \$ / each.
Minimum quantity: 5 servers.

Root access: 30 \$ / each.
Minimum quantity: 5 servers.

There is the possibility to choose your servers; between the current availability.

XMPP : " voidzero@thesecond.biz ".


 A complaint

Figure 5. Threat actor offering compromised VMware ESXi servers

Patching and Detection Advice

VMware urges users running VMware vCenter and VMware Cloud Foundation affected by CVE-2021-21985 and CVE-2021-21986 to apply its [patch](#) immediately. According to VMware, a malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. The disclosed vulnerabilities have a critical CVSS base score of 9.8.

However, we do understand that VMware infrastructure is often installed on business-critical systems, so any type of patching activity usually has a high degree of impact on IT operations. Hence, the gap between vulnerability disclosure and patching is typically high. With the operating systems on VMware being a closed system they lack the ability to natively install workload protection/detection solutions. Therefore, the defenses should be based on standard cyber hygiene/risk mitigation practices and should be applied in the following order where possible.

1. Ensure an accurate inventory of vCenter assets and their corresponding software versions.
2. Secure the management plane of the vCenter infrastructure by applying strict network access control policies to allow access only from special management networks.
3. Disable all internet access to vCenter/VMware Infrastructure.
4. Apply the released VMware patches.

5. McAfee Network Security Platform (NSP) offers signature sets for detection of CVE-2021-21985 and CVE-2021-21986.

Conclusion

Virtualization and its underlying technologies are key in today's infrastructures. With the release of recently discovered vulnerabilities and an understanding of their criticality, threat actors are shifting focus. Proof can be seen in underground forums where affiliates recruit pentesters with knowledge of specific virtual technologies to develop custom ransomware that is designed to cripple these technologies. Remote Desktop access is the number one access vector in many ransomware cases, followed by edge-devices lacking the latest security updates, making them vulnerable to exploitation. With the latest VMware CVEs mentioned in this blog, we urge you to take the right steps to secure not only internet exposed systems, but also internal systems, to minimize the risk of your organization losing its precious VMs, or gold, to cyber criminals.

Special thanks to Thibault Seret, Mo Cashman, Roy Arnab and Christiaan Beek for their contributions.

ATR Operational Intelligence Team

McAfee's Advanced Threat Research Operational Intelligence team operates globally around the clock, keeping watch of the latest cyber campaigns and actively tracking the most impactful cyber threats.