New Linux-Based Ransomware Cheerscrypt Targets ESXi Devices

Trend Micro Research detected "Cheerscrypt", a new Linux-based ransomware variant that compromises ESXi servers. We discuss our initial findings on in this report.

By: Arianne Dela Cruz, Byron Gelera, McJustine De Guzman, Warren Sto.Tomas May 25, 2022 Read time: 2 min (673 words)

Save to Folio

[Subscribe](#)

We recently observed multiple Linux-based [ransomware](#) detections that malicious actors launched to target [VMware ESXi](#) servers, a bare-metal hypervisor for creating and running several virtual machines (VMs) that share the same hard drive storage. We encountered [Cheerscrypt](#), a new ransomware family, that has been targeting a customer's EXSi server used to manage VMware files.

In the past, ESXi servers were also attacked by other known ransomware families such as [LockBit](#), [Hive](#), and [RansomEXX](#) as an efficient way to infect many computers with ransomware.

This blog entry provides an overview of Cheerscrypt's infection routine based on the information we have gathered so far.

Infection routine

The ransomware requires an input parameter specifying the path to encrypt so that it can proceed to its Infection routine.

Figure 1. Ransomware command line

Upon execution, it implements the following command to terminate VM processes using [ESXCLI](#):

"esxcli vm process kill —type=force —world-id=$(esxcli vm process list|grep 'World ID'|awk '{print $3}')"

The termination of the VM processes ensures that the ransomware can successfully encrypt VMware-related files. Similar to other infamous ransomware families, Cheerscrypt employs the [double extortion](#) scheme to coerce its victim to pay the ransom, as shown on their ransom note in Figure 2.
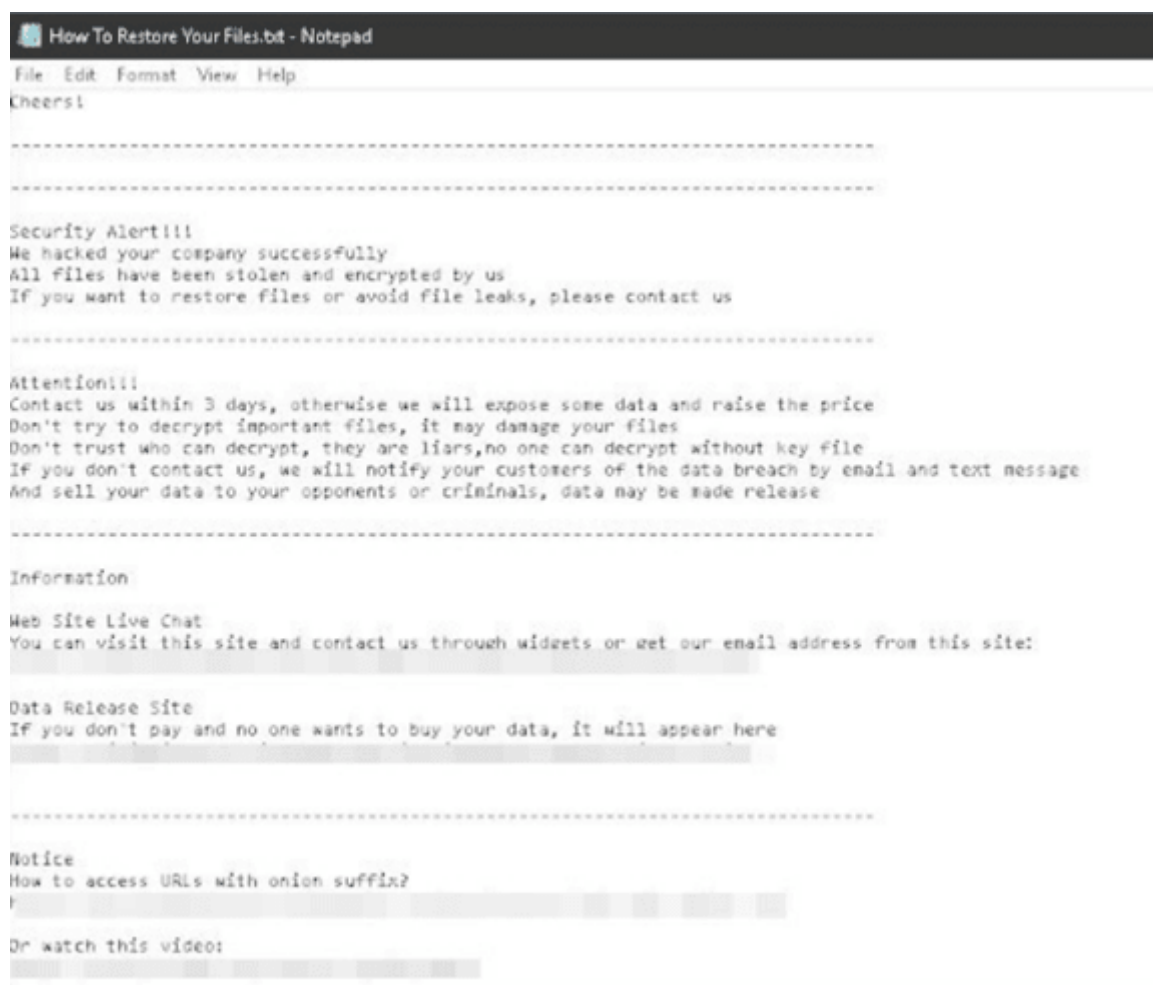
Figure 2. Cheerscrypt's ransom note

Successfully encrypted files are renamed with the .Cheers extension. However, the ransomware first renames the files it will encrypt before encrypting the files. Thus, if the access permission for the file was not granted, it cannot proceed with the actual encryption.

```
printf("file:%s\n", a1);
v18 = 0;
n = 0LL;
if ( file_status_401BB2(a1, &v3) == 0 )
{
  memset(&s, 0, 0x1001uLL);
  strcpy(&s, src);
  strcat(&s, ".Cheers");
  rename(src, &s);
  stream = fopen(&s, "r+b");
  if ( stream )
  {
    ptr = malloc(0xA00000uLL);
    if ( ptr )
    {
      sub_40155A(&v12, 32);
      v12 &= 0xF8u;
      HIBYTE(v15) &= 0x7Fu;
      HIBYTE(v15) |= 0x40u;
      sub_4054F4(&v16, &v12, &unk_60F3C0);
      sub_4054F4(&v11, &v12, &unk_40E260);
```

Figure 3. Cheerscrypt renames the sample before encryption.

For each directory it encrypts, it will drop the ransom note named, "How to Restore Your Files.txt". It seeks out log files and VMware-related files with the following extensions:

- · .log
- · .vmdk
- · .vmem
- · .vswp
- · .vmsn

After successful encryption, it displays the following console that contains the data statistics of its routine:

Figure 4. Console displayed after encryption

Encryption algorithm

Cheerscrypt's executable file contains the public key of a matching key pair with the private key being held by the malicious actor. The ransomware uses SOSEMANUK stream cipher to encrypt files and ECDH to generate the SOSEMANUK key. For each file to encrypt, it generates an ECDH public-private key pair on the machine through Linux's /dev/urandom. It then uses its embedded public key and the generated private key to create a secret key that will be used as a SOSEMANUK key. After encrypting the file, it will append the generated public key to it. Since the generated private key is not saved, one cannot use the embedded public key with the generated private key to produce the secret key. Therefore, decryption is only possible if the malicious actor's private key is known. The infection chain is shown on Figure 5.
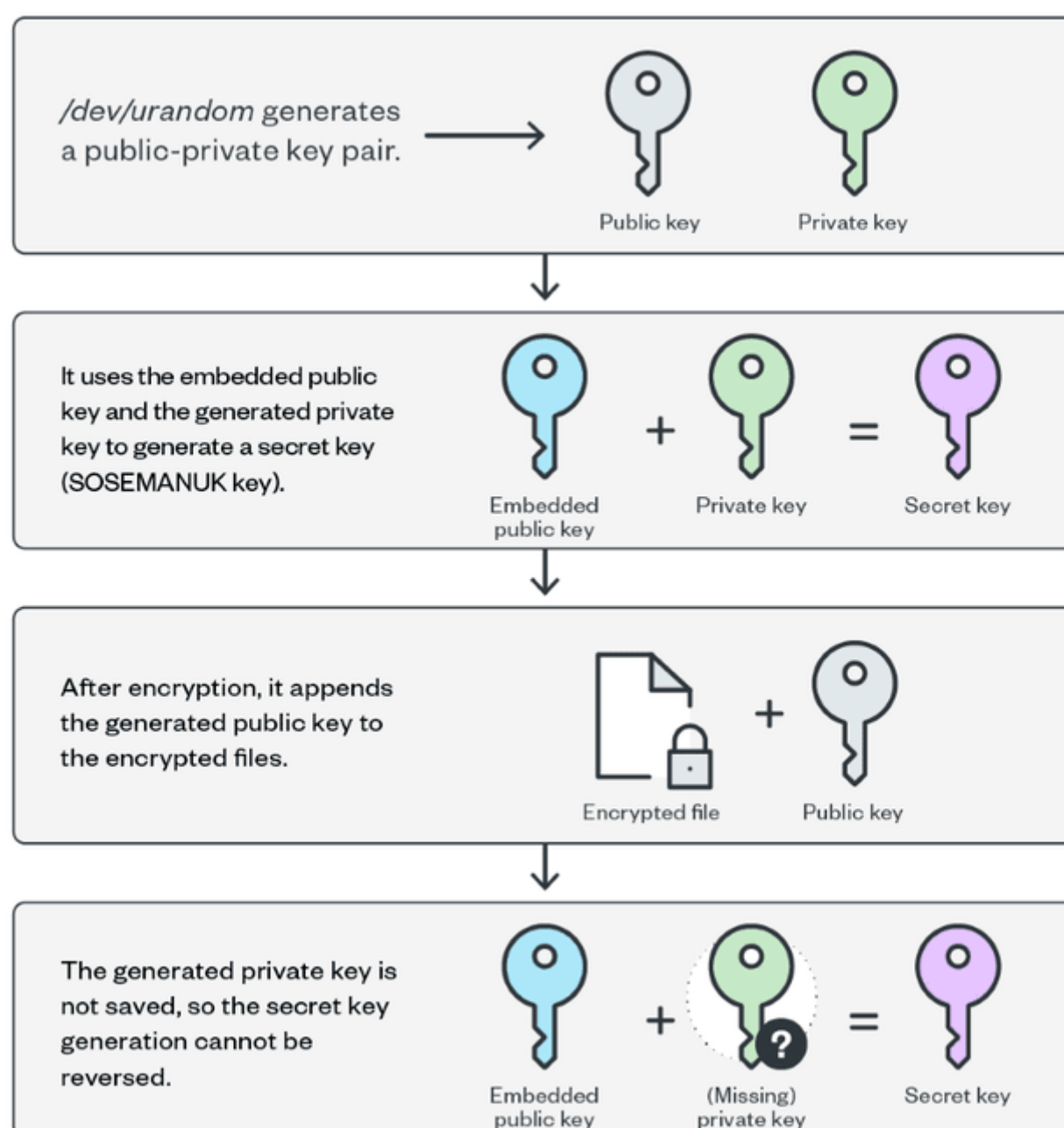
Figure 5. Cheerscrypt's encryption algorithm

Conclusion

ESXi is widely used in enterprise settings for server virtualization. It is therefore a popular target for ransomware attacks. As mentioned, compromising EXSi servers has been a scheme used by some notorious cybercriminal groups because it is a means to swiftly spread the ransomware to many devices.

Organizations should thus expect malicious actors to upgrade their malware arsenal and breach as many systems and platforms as they can for monetary gain.

Recommendations

A proactive stance that ensures solid cybersecurity defenses against modern ransomware threats is crucial for organizations to thrive in an ever-changing threat landscape. To protect systems against similar attacks, organizations can establish security frameworks that systematically allocate resources based on an enterprise's needs.

Organizations can benefit from following the security frameworks established by the [Center of Internet Security](#) and the [National Institute of Standards and Technology](#) when developing their own cybersecurity strategies. The frameworks they created help security teams to mitigate risks and minimize exposure to threats. Adopting the best practices discussed in their respective frameworks can save organizations the time and effort when they customize their own. Their frameworks guide organizations through the entire process of planning while providing suggestions on measures that need to be established first.

Tags [Endpoints](#) | [Ransomware](#) | [Research](#) | [Articles, News, Reports](#)

Authors

- Arianne Dela Cruz

  Threats Analyst

- Byron Gelera

  Threats Analyst

- McJustine De Guzman

  Threats Analyst

- Warren Sto.Tomas

  Sr. Threat Research Engineer

[Contact Us Subscribe](#)

Related Articles

- [Celebrating 15 Years of Pwn2Own](#)
- [New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware](#)
- [The Fault in Our kubelets: Analyzing the Security of Publicly Exposed Kubernetes Clusters](#)

[See all articles](#)