Ransomware

New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code

New findings showed that Cheerscrypt, a new Linux-based ransomware variant that compromises ESXi servers, was derived from the leaked Babuk source code. We discuss our analysis in this report.

By: Arianne Dela Cruz, Byron Gelera, McJustine De Guzman, Warren Sto.Tomas
May 25, 2022
Read time: 3 min (905 words)

We recently discovered that Cheerscrypt, the new Linux-based ransomware that we detected in multiple attacks targeting ESXi servers, was based on the leaked Babuk source code. Upon scrutiny, we found similarities between Cheerscrypt and the Linux version of the Babuk ransomware, specifically its ESXi version. The base code of [illegible] was lifted from the leaked Babuk source code, but modified and customized to suit the malicious [illegible] goals.

Brief background

Over the past few weeks, we observed several 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, during this period.

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.

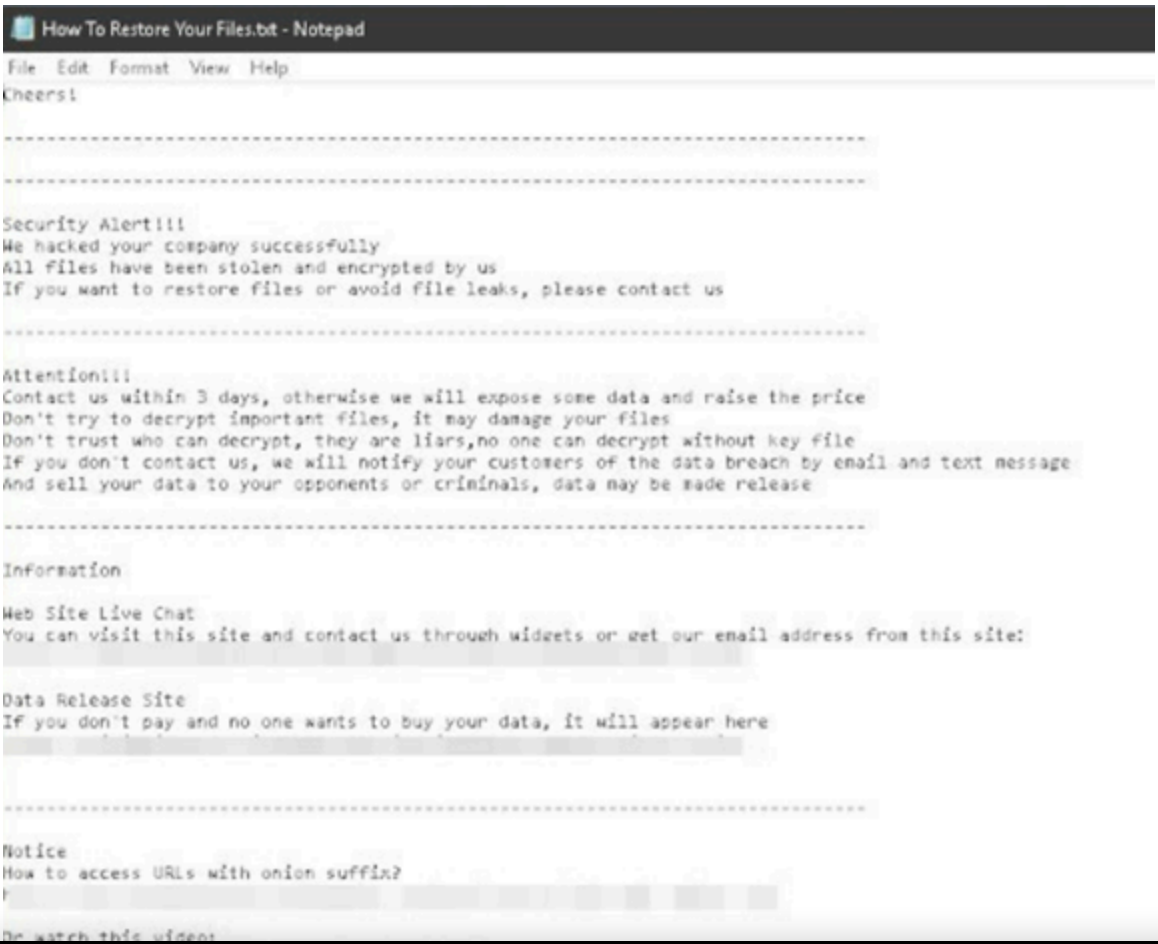
Infection routine

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

```
"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.



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
- .vmsn

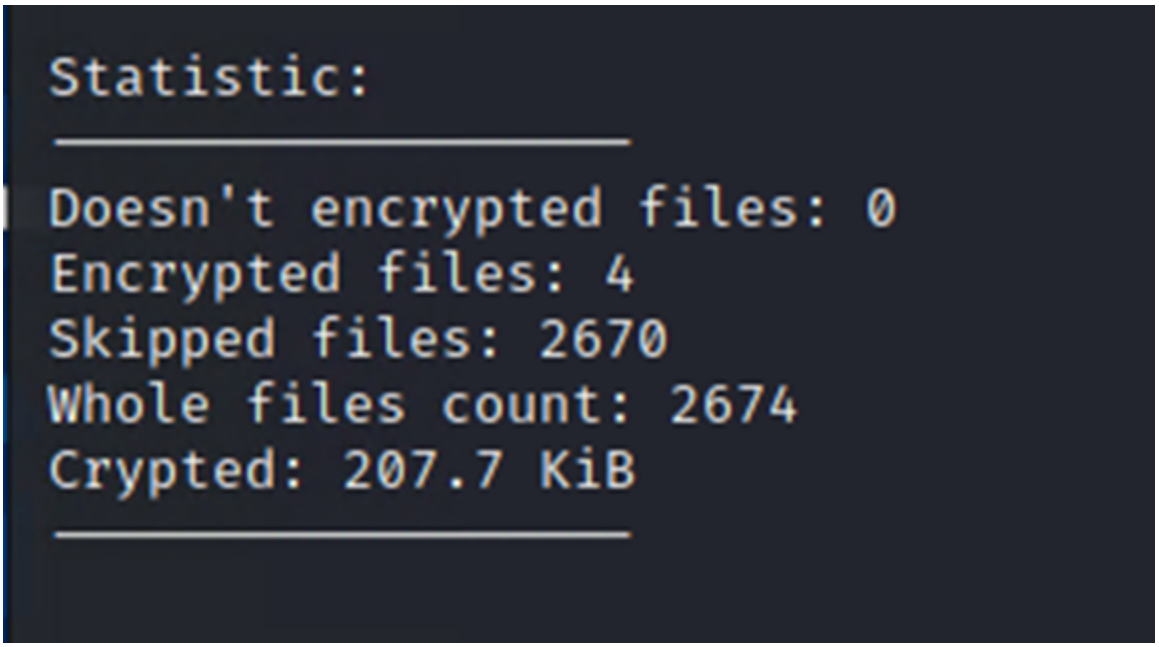


Figure 4. Console displayed after encryption

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.

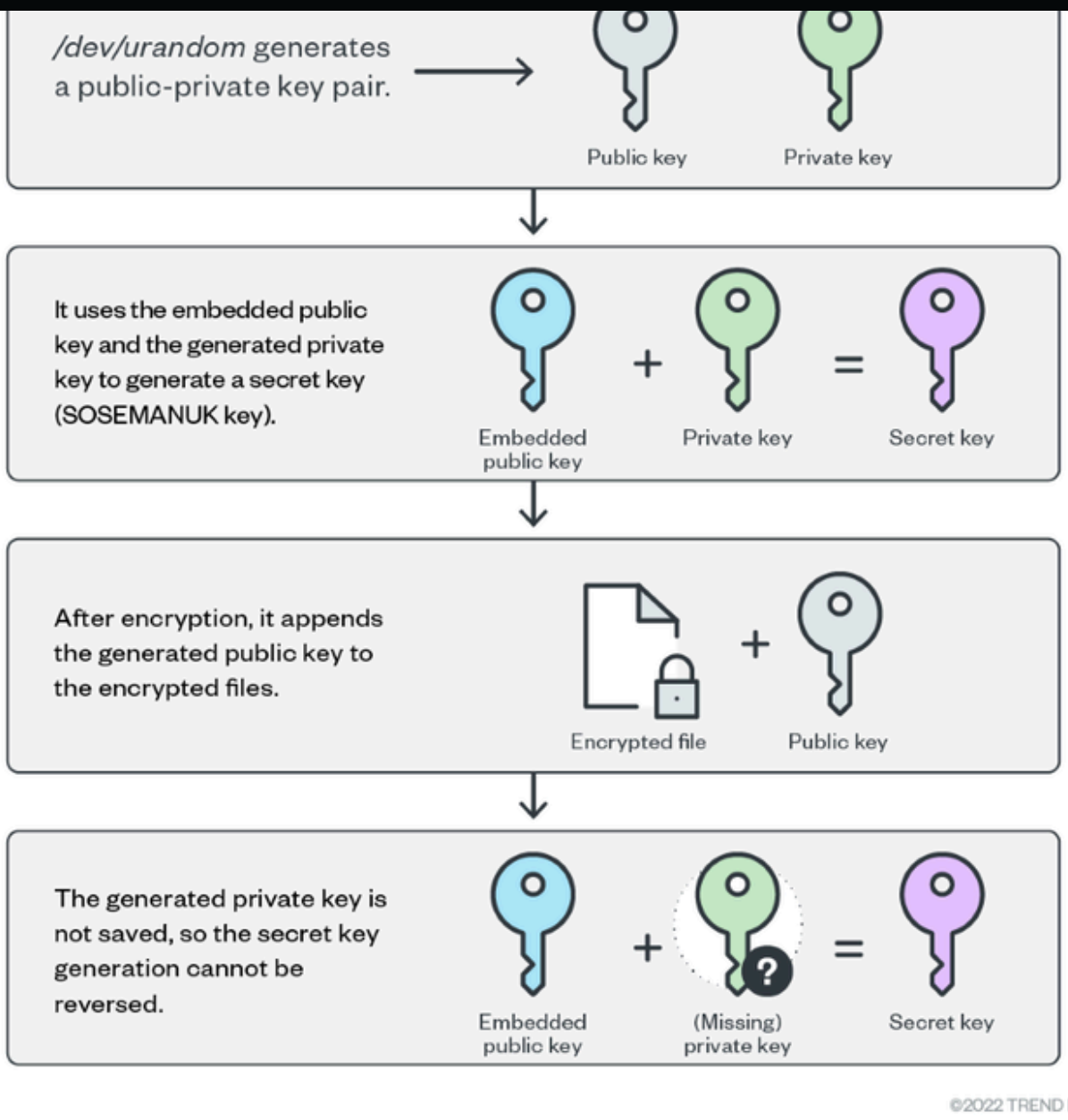


Figure 5. Cheerscrypt's encryption algorithm

New findings: Cheerscrypt linked to Babuk

Unlike Cheerscrypt, Babuk's malware version used to compromise ESXi servers ensured that the files were encrypted before it renamed the target files. This goes to show that

organizations when other malicious actors build upon the source code they leaked. We provide Babuk's source code for the malware variant specific to ESXi servers in Figure 6. In Figure 7, we can see that Cheerscrypt's source code was based on Babuk's source code that was leaked before.

```
if ( a1 == 2 )
{
  v3 = sysconf(84);
  qword_610C50 = sub_40C320((2 * v3));
  putchar(10);
  sub_4017ED(a2[1]);
  sub_40C564(qword_610C50);
  sub_40C5C8(qword_610C50);
  putchar(10);
  puts("Statistic:");
  puts("------------------");
  printf("Doesn't encrypted files: %d\n", (dword_610C38 - dword_610C3C - dword_610C40), a2);
  printf("Encrypted files: %d\n", dword_610C3C);
  printf("Skipped files: %d\n", dword_610C40);
  printf("Whole files count: %d\n", dword_610C38);
  v4 = sub_401316(qword_610C48);
  printf("Crypted: %s\n", v4);
  puts("------------------");
  putchar(10);
}
else
{
  printf("Usage: %s /path/to/be/encrypted\n", *a2, a3, a2);
}
return 0LL;
```

Figure 6. Babuk's source code for the malware variant used to target ESXi servers

```
  newthread = 0LL;
  pthread_create(&newthread, 0LL, start_routine, 0LL);
  sub_4011D0(a2[1]);
  sub_40D0EA(qword_60FC50);
  sub_40D142(qword_60FC50);
  putchar(10);
  puts("Statistic:");
  puts("------------------");
  printf("Doesn't encrypted files: %d\n", (dword_60FC38 - dword_60FC3C - dword_60FC40), a2);
  printf("Encrypted files: %d\n", dword_60FC3C);
  printf("Skipped files: %d\n", dword_60FC40);
  printf("Whole files count: %d\n", dword_60FC38);
  v3 = sub_4018DA(qword_60FC48);
  printf("Crypted: %s\n", v3);
  puts("------------------");
  putchar(10);
}
else
{
  printf("Usage: %s /path/to/be/encrypted\n", *a2, a3, a2);
}
return 0LL;
```

Figure 7. Cheerscrypt's source code with similarities to Babuk's source code

Conclusion

ESXi is widely used in enterprise settings for server virtualization. It is therefore a popular target for ransomware attacks. As mentioned, compromising ESXi 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 can mitigate attacks and can be customized on an enterprise's needs.

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

Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis

Attacker Abuses Victim Resources to Reap Rewards from Titan Network

A Cybersecurity Risk Assessment Guide for Leaders

See all articles ›

Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900