

家 (<https://www.bleepingcomputer.com/>) > 新闻 (<https://www.bleepingcomputer.com/news/>)

> 安全 (<https://www.bleepingcomputer.com/news/security/>)

> 新的GwisinLocker勒索软件加密Windows和Linux ESXi服务器

新的GwisinLocker勒索软件加密Windows和Linux ESXi服务器

由
比尔·图拉斯
(<https://www.bleepingcomputer.com/author/bill-toulas/>)

八月 6, 2022

上午10: 05

0



一个名为“GwisinLocker”的新勒索软件系列针对韩国医疗保健，工业和制药公司，提供Windows和Linux加密器，包括支持加密VMware ESXi服务器和虚拟机。

新的恶意软件是一个鲜为人知的威胁行为者的产物，称为Gwisin，在韩语中意为“幽灵”。演员来历不明，但似乎对韩语有很好的了解。

此外，袭击恰逢韩国公共假日，发生在清晨，因此Gwisin很好地掌握了该国的文化和商业惯例。

上个月底 (<https://www.boannews.com/media/view.asp?idx=108704>)，有关Gwisin及其活动的报道首次出现在韩国媒体上，当时威胁行为者损害了该国的大型制药公司。

周三，Ahnlab (<https://asec.ahnlab.com/en/37483/>)的韩国网络安全专家发布了一份关于Windows加密器的报告，昨天，ReversingLabs (<https://blog.reversinglabs.com/blog/gwisinlocker-ransomware-targets->

south-korean-industrial-and-pharmaceutical-companies)的安全研究人员发布了他们对Linux版本的技术分析。

面向 Windows 和 Linux 服务器

当 GwisinLocker 加密 Windows 设备时，感染始于执行 MSI 安装程序文件，这需要特殊的命令行参数才能正确加载充当勒索软件加密程序的嵌入式 DLL。

要求命令行参数会使安全研究人员更难分析勒索软件。

当提供正确的命令行参数时，MSI 将解密其内部 DLL（勒索软件）并将其注入 Windows 进程，以逃避 AV 检测，这因公司而异。

该配置有时包括一个参数，该参数将勒索软件设置为在安全模式下运行。在这些情况下，它会将自身复制到 ProgramData 子文件夹，注册为服务，然后在安全模式下强制重新启动。

对于 ReversingLabs 分析的 Linux 版本，加密器非常注重加密 VMware ESXi 虚拟机，包括两个命令行参数，用于控制 Linux 加密器如何加密虚拟机。

下面列出了 GwisinLocker Linux 加密器的命令行参数：

```
Usage: Usage
-h, --help      show this help message and exit
Options
-p, --vp=       Comma-separated list of paths to encrypt
-m, --vm=       Kills VM processes if 1; Stops services and processes if 2
-s, --vs=       Seconds to sleep before execution
-z, --sf=       Skip encrypting ESXi-related files (those excluded in the configuration)
-d, --sd=       Self-delete after completion
-y, --pd=       Writes the specified text to a file of the same name
-t, --tb=       Enters loop if Unix time is
```

这些参数包括标志，该标志将执行以下命令以枚举 ESXi 虚拟机并关闭它们。--vm

```
esxcli --formatter=csv --format-param=fields=="DisplayName,WorldID" vm process list

esxcli vm process kill --type=force --world-id="[ESXi] Shutting down - %s"
```

为了避免使 Linux 服务器不可用，GwisinLocker 将从加密中排除以下目录。

```
"bin","boot","dev","etc","lib","lib64","proc","run","sbin","srv","sys","tmp","usr","var","bootbank","mbr","tardisks","tardisks.noauto","vmimages"
```

从加密中排除的进程 (ReversingLabs)

除非使用命令行参数，否则 Linux 勒索软件还将排除特定的 VMware ESXi 相关文件（state.tgz、useropts.gz、jumpstrt.gz等），以防止服务器无法启动。 --sf

最后，勒索软件在启动加密之前终止多个Linux守护程序，以使其数据可用于锁定过程。

```
"apache","httpd","nginx","oracle","mysql","mariadb","postgres","mongod",
,"elasticsearch","jenkins","gitlab","docker","svnserve","yona","zabbix",
,"graylog","java"
```

加密前终止的服务 (ReversingLabs)

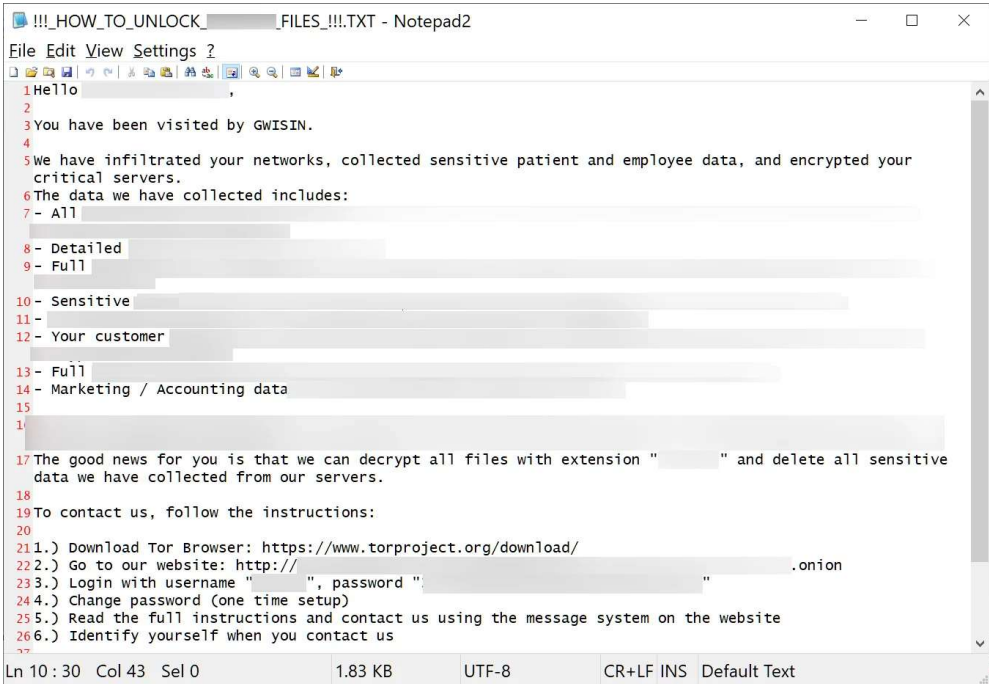
加密文件时，加密器使用带有 SHA256 哈希的 AES 对称密钥加密。

为每个受害者定制

无论攻击针对的操作系统如何，所有加密器都经过自定义，以在赎金记录中包含公司名称，并对加密文件名使用唯一的扩展名。

对于BleepingComputer已知的一个受害者，威胁行为者大量定制了赎金记录，以包括在攻击期间被盗的特定数据，我们在下面的注释中对其进行了编辑。

赎金票据被命名为“!!!_HOW_TO_UNLOCK_[company_name]_文件_!!!.TXT”和用英语写成，有些人警告受害者不要联系韩国执法机构或KISA（韩国互联网和安全局）。



GwisinLocker 赎金票据
示例来源: BleepingComptuer

相反，受害者被告知使用Tor浏览器访问洋葱地址，使用提供的凭据登录，并按照支付赎金和恢复文件的说明进行操作。

虽然AhnLab和VersingLabs指出，GwisinLocker主要针对韩国工业和制药公司，但BleepingComputer知道一家医疗保健诊所也成为目标。

相关文章:

新的 Luna 勒索软件加密 Windows、Linux 和 ESXi 系统

(<https://www.bleepingcomputer.com/news/security/new-luna-ransomware-encrypts-windows-linux-and-esxi-systems/>)

New RedAlert Ransomware 针对 Windows、Linux VMware ESXi 伺服器

(<https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/>)

Microsoft Azure 现在拥有具有临时存储的机密虚拟机

(<https://www.bleepingcomputer.com/news/microsoft/microsoft-azure-now-has-confidential-vms-with-ephemeral-storage/>)

Linux 版本的 Black Basta 勒索软件针对 VMware ESXi 服务器

(<https://www.bleepingcomputer.com/news/security/linux-version-of-black-basta-ransomware-targets-vmware-esxi-servers/>)

Microsoft Defender 现在更擅长在 Windows 11 上阻止勒索软件

(<https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-now-better-at-blocking-ransomware-on-windows-11/>)

格维辛洛克 ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/GWISINLOCKER/](https://www.bleepingcomputer.com/tag/gwisinlocker/))

LINUX ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/LINUX/](https://www.bleepingcomputer.com/tag/linux/))

勒索软件 ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/RANSOMWARE/](https://www.bleepingcomputer.com/tag/ransomware/))

韩国 ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SOUTH-KOREA/](https://www.bleepingcomputer.com/tag/south-korea/))

虚拟机 ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VIRTUAL-MACHINE/](https://www.bleepingcomputer.com/tag/virtual-machine/))

VMWARE ESXI ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VMWARE-ESXI/](https://www.bleepingcomputer.com/tag/vmware-esxi/))

窗户 ([HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/WINDOWS/](https://www.bleepingcomputer.com/tag/windows/))

(<https://www.bleepingcomputer.com/author/bill-toulas/>)

比尔·图拉斯

([HTTPS://WWW.BLEEPINGCOMPUTER.COM/AUTHOR/BILL-TOULAS/](https://www.bleepingcomputer.com/author/bill-toulas/))

✉ ([MAILTO:BILL.TOULAS@BLEEPINGCOMPUTER.COM](mailto:bill.toulas@bleepingcomputer.com))

🐦 ([HTTPS://TWITTER.COM/BILLTOULAS](https://twitter.com/billtoulas))

Bill Toulas 是一位技术作家和信息安全新闻记者，在各种在线出版物上拥有超过十年的经验。作为一名开源倡导者和 Linux 爱好者，他目前在关注黑客攻击，恶意软件活动和数据泄露事件以及探索技术迅速改变我们生活的复杂方式方面找到了乐趣。

[← 上一篇文章](#)

[下一篇 →](#)

发表评论

您需要登录才能发表评论

登录

还不是会员？立即注册

(<https://www.bleepingcomputer.com/posting-guidelines/>)

(<https://www.bleepingcomputer.com/forums/index.php?app=core&module=global§ion=register>)

您可能还喜欢：

热门故事



Twitter证实零日漏洞用于公开**540**万个账户的数据
(<https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/>)



DuckDuckGo浏览器现在大多数时候都会阻止所有微软跟踪器。
(<https://www.bleepingcomputer.com/news/security/duckduckgo-browser-now-blocks-all-microsoft-trackers-most-of-the-time/>)

订阅电子报

要接收来自BleepingComputer的(/)定期更新和新闻，请使用下面的表格。

电子邮件地址...

提交

NEWSLETTER SIGN UP

SUBMIT

Follow us:    

(<https://www.bleepingcomputer.com/>)

MAIN SECTIONS

News (<https://www.bleepingcomputer.com/>)

Downloads (<https://www.bleepingcomputer.com/download/>)

Virus Removal Guides (<https://www.bleepingcomputer.com/virus-removal/>)

Tutorials (<https://www.bleepingcomputer.com/tutorials/>)

Startup Database (<https://www.bleepingcomputer.com/startups/>)

Uninstall Database (<https://www.bleepingcomputer.com/uninstall/>)

File Database (<https://www.bleepingcomputer.com/filedb/>)

Glossary (<https://www.bleepingcomputer.com/glossary/>)

COMMUNITY

Forums (<https://www.bleepingcomputer.com/forums/>)

Forum Rules (<https://www.bleepingcomputer.com/forum-rules/>)

Chat (<https://www.bleepingcomputer.com/forums/t/730914/the-bleepingcomputer-official-discord-chat-server-come-join-the-fun/>)

USEFUL RESOURCES

Welcome Guide (<https://www.bleepingcomputer.com/welcome-guide/>)

Sitemap (<https://www.bleepingcomputer.com/sitemap/>)

COMPANY

About BleepingComputer (<https://www.bleepingcomputer.com/about/>)

Contact Us (<https://www.bleepingcomputer.com/contact/>)

Send us a Tip! (<https://www.bleepingcomputer.com/news-tip/>)

Advertising (<https://www.bleepingcomputer.com/advertise/>)

Write for BleepingComputer (<https://www.bleepingcomputer.com/write-for-bleepingcomputer/>)

Social & Feeds (<https://www.bleepingcomputer.com/rss-feeds/>)

Changelog (<https://www.bleepingcomputer.com/changelog/>)

Terms of Use (<https://www.bleepingcomputer.com/terms-of-use/>) - Privacy Policy (<https://www.bleepingcomputer.com/privacy/>) - Ethics Statement (<https://www.bleepingcomputer.com/ethics-statement/>)

Copyright @ 2003 - 2022 **Bleeping Computer LLC**® (<https://www.bleepingcomputer.com/>) - All Rights Reserved

