THREAT BULLETINS

Reversing Labs Discovers New Ransomware Family Targeting Healthcare Sector, GwisinLocker

TLP:WHITE

Aug 05, 2022

On August 4, 2022, malware researcher firm Reversing Labs released an in-depth blog post about the discovery of a new ransomware family, GwisinLocker ransomware, that has been observed targeting Linux-based systems in South Korean industrial and pharmaceutical companies. This malware has been newly developed by a little-known threat actor, dubbed Gwisin, which translates to ghost in Korean. The first known documentation of this group was seen in a report cataloged as new ransomware actors found in the third quarter of 2021. Finally, the analysis of GwisinLocker produced by Reversing Labs is the first public analysis of Gwisin-developed malware.

Health-ISAC members are encouraged to continue to implement hygienic cybersecurity practices and refresh employees on phishing techniques. Finally, due

to the targeting of VMware machines, Health-ISAC encourages shutting down virtual machines when they are not in immediate use.

For additional information including a ransom note sample and malware technical details, please see the comprehensive report from Reversing Labs here.

The malware developed by Gwisin, has been officially named GwisinLocker.Linux. However, there are also versions of the same malware that affect Windows systems. The prevalence of this group and the success they have experienced using ransomware shows that cybercriminal threats are still proving to be a legitimate concern despite evolving cybersecurity.

This group has been known to only target South Korean companies. At the time of writing, their motives appear purely financial through their non-political targeting of South Korean pharmaceutical and industrial companies. This group is familiar with South Korean culture and holidays. From a tactics standpoint, their attacks all seem to have been launched from a platform of in-depth knowledge of the system. This is evident in the files they encrypt, the directories that store the malware, and the directories left untouched to ensure the Linux machine continues to run. This has led some to believe that this group may be a North Korean APT actor, but this remains unconfirmed.

The group possesses sophisticated offensive cyber capabilities that offer them the opportunity to compromise systems and permit extensive dwell time in victim networks prior to deploying the GwinsinLocker.Linux ransomware. The combination of highly sophisticated offensive cyber capabilities, the implementation of double extortion practices, and a hyperfocus on the theft of sensitive data belonging to South Korean firms in sectors including industrial and pharmaceuticals is grounds for reviewing and refining existing policies and procedures to mitigate this threat. Due to VMware ESXi being a widely utilized enterprise tool and is ubiquitous across sectors, the risk posed by the threat group likely extends to South Korean firms in other sectors, as well.

Indicators of Compromise:

Indicators of Compromise have been entered into Health-ISACs automated sharing platform for those members ingesting automated threat indicators.

The following hashes and strings correspond to files associated with active GwisinLocker Linux variants and attacks:

- /tmp/.66486f04-bf24-4f5e-ae16-0af0fdb3d8fe - Mutex
- !!!_HOW_TO_UNLOCK_MCRGNX_FILES_!!!.TXT - Ransom Note
- ce6036db4fee35138709f14f5cc118abf53db112

– GwisinLocker Ransomware (32-bit ELF)

- e85b47fdb409d4b3f7097b946205523930e0c4ab

– GwisinLocker Ransomware (64-bit ELF)

Reference(s)	ReversingLabs, Mitre, VMware, CISA, Health-ISAC

Recommendations

Health-ISAC recommends shutting down virtual environments when they are not in direct use. Additionally, it is recommended to disable VMware shared folders with the host machine, disable virtual and host environment clipboard sharing, and disable remote SSH logins.

It is also recommended to have backups of sensitive information. To avoid total data loss if corporate networks are subjected to data exfiltration. Cloud architecture is a more secure alternative to local storage due to its decentralized structure.

Finally, internal threat hunting teams should scan corporate networks for IOCs contained within this report on scheduled intervals, ensuring no Gwisin actor is masking a presence within private networks.

Sources

Reversing Labs-GwisinLocker Ransomware Targets South Korean Industrial and Pharma Firms

Lazarus Group

Securing the ESXi Hypervisor

CISA RANSOMWARE GUIDE

HCIP - Health Industry Cybersecurity Practices

Alert ID 3f9ca962

View Alert

Tags GwinsinLocker, Pharmaceutical, Industrial, VMware ESXi, ReversingLabs

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**