GovCERT.HK

Weekly IT Security News Bulletin, 2022-W03

17 January – 23 January 2022

Headlines

Destructive malware discovered targeting multiple organisations

- Microsoft has discovered a destructive malware in attacks targeting multiple public and private sector organisations. The malware disguised as ransomware named WhisperGate is designed to permanently destroy files on a targeted device through two different components.

- The first component could overwrite the Master Boot Record (MBR) on the targeted system with a ransom note, causing the operating system and its data inaccessible. The second component would download a file corrupter malware that could overwrite the content of files carrying specific file extensions with a fixed number of 0xCC bytes, which correspond to an assembly language instruction for generating software interrupts.

- Microsoft found that the ransom note generated by the malware does not include a custom ID for threat actors to map the victim-specific decryption key, thus believing the ransom note is fake and the malware is intended for data destruction only. To protect endpoints against malware, Microsoft has provided relevant malware signatures for its anti-malware solutions.

Advice

- Install malware detection measures with the latest signatures.
- Keep an offline backup to avoid any case of corruption of data backup.
- Prepare contingency plan for scenarios when under attacks and ensure staff familiar with information security incident response procedures.

Sources

- Microsoft
- SecurityWeek
- US-CERT

Protecting NAS devices against evolving threats

- A recent report published by Trend Micro indicated an increase in malware families targeting network-attached storage (NAS) devices. The report suggested the main reasons why NAS devices continue to be a popular attack target and introduced some recommendations on how to secure NAS devices.

- NAS devices often contain plenty of valuable data of users. Exposing the devices to the Internet without sufficient security measures in place makes them as attractive exploitation target to the attackers, as said in the research report. Untimely patching and mitigation of security vulnerabilities in NAS devices also provides threat actors with a simple and direct way for intrusion.

- In addition to the lack of proper security measures, the advancement of processing power in modern NAS devices eases the effort of threat actors to launch attacks that is resource intensive like crytomining attacks. What makes the situation even worst is that the underlying operating system for NAS devices come with a diverse pool of libraries and tools, enabling malware developed in different programming languages to run.

Advice

- Avoid exposing NAS devices to the Internet whenever possible.
- Do not use the default administrator accounts and passwords and change all vendor-supplied default passwords before use.
- Enable two-factor authentication if the NAS device is supported.
- Observe and follow security guides provided by NAS manufacturers to harden and secure the NAS device.

Sources

- Trend Micro - News
- Trend Micro - Research Report

Product Vulnerability Notes & Security Updates

1. CentOS

https://lists.centos.org/pipermail/centos-announce/2022-January/073536.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073537.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073546.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073548.html
https://lists.centos.org/pipermail/centos-announce/2022-January/073549.html

2. Debian

https://www.debian.org/security/2022/dsa-5044
https://www.debian.org/security/2022/dsa-5046
https://www.debian.org/security/2022/dsa-5047
https://www.debian.org/security/2022/dsa-5048

3. F5 Products

https://support.f5.com/csp/article/K08402414
https://support.f5.com/csp/article/K08476614
https://support.f5.com/csp/article/K11742742
https://support.f5.com/csp/article/K16101409
https://support.f5.com/csp/article/K17514331
https://support.f5.com/csp/article/K24358905
https://support.f5.com/csp/article/K26310765
https://support.f5.com/csp/article/K28042514
https://support.f5.com/csp/article/K29500533
https://support.f5.com/csp/article/K30525503
https://support.f5.com/csp/article/K30573026
https://support.f5.com/csp/article/K30911244
https://support.f5.com/csp/article/K34360320
https://support.f5.com/csp/article/K40084114
https://support.f5.com/csp/article/K41415626
https://support.f5.com/csp/article/K44110411
https://support.f5.com/csp/article/K50343028
https://support.f5.com/csp/article/K53442005
https://support.f5.com/csp/article/K54892865
https://support.f5.com/csp/article/K57111075
https://support.f5.com/csp/article/K61112120
https://support.f5.com/csp/article/K68755210
https://support.f5.com/csp/article/K82793463
https://support.f5.com/csp/article/K91013510
https://support.f5.com/csp/article/K93526903
https://support.f5.com/csp/article/K96924184

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220112-01-infodis-en
https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220112-01-invalid-en

5. ICONICS and Mitsubishi Electric HMI SCADA

https://us-cert.cisa.gov/ics/advisories/icsa-22-020-01

6. McAfee

https://kc.mcafee.com/corporate/index?page=content&id=SB10378

7. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2IPUTP7LOLL5OLSQNM5GFCXGYDJHU7FP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4UJWNOWSKPBGYUCFFUB7ANJL7A2J2AML/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/5GEO4VASAXOQQYTQGGNCUBC3ZY3RFQT4/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/C3FMQXDJQJ2FMNZQPTMFMJPRBWP3GY2L/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DLYT44LA5ZMWEXSKKLL4QK25G4FZSHQA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GCAJV7QU7NXYUTY7OMBOV6LAES2X326R/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ILTMKWZNQBSX2H2MPF3XKXVDEDPDYAIB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JZDQSQYHYML6BZRVAEZ7TDW2LFGCJEZO/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KNMY24O54KQLQYLHBRWLMCEO42RIRELW/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LNFLD35UGUIRPTGF3HA3JP2MXLLHWPIX/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LO2K2OYJXIHKCXT4ZI6S7RGIOS27RIOY/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LQS3J3J4254A7C3LD55D7A432FZ2RFFI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LQX4BVMFKUTV6DOPDTL26H5DQJJFUPXZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OBUO7H3LKGBHC4SODDIXNRMKJH3PIZ7M/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/T4AYNB4WRJM6UGUGE4MCR3AAVYPLM2PP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/XW7HD7EA7DNOWMGKDOA6BCE6FBFET4WB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YB6DIPEMLRTDD3RU77DD7UYYKBEEKYDY/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZUS4G6GRHNJN7AR53SGJABSHRZM3XMOY/

8. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-5013.html
https://linux.oracle.com/errata/ELSA-2021-5014.html
https://linux.oracle.com/errata/ELSA-2021-5082.html
https://linux.oracle.com/errata/ELSA-2021-5142.html
https://linux.oracle.com/errata/ELSA-2021-5160.html
https://linux.oracle.com/errata/ELSA-2021-5171.html
https://linux.oracle.com/errata/ELSA-2021-9619.html
https://linux.oracle.com/errata/ELSA-2022-0143.html
https://linux.oracle.com/errata/ELSA-2022-0161.html
https://linux.oracle.com/errata/ELSA-2022-0162.html
https://linux.oracle.com/errata/ELSA-2022-0177.html
https://linux.oracle.com/errata/ELSA-2022-0199.html
https://linux.oracle.com/errata/ELSA-2022-9028.html
https://linux.oracle.com/errata/ELSA-2022-9029.html

9. Red Hat

https://access.redhat.com/errata/RHSA-2022:0083
https://access.redhat.com/errata/RHSA-2022:0114
https://access.redhat.com/errata/RHSA-2022:0143
https://access.redhat.com/errata/RHSA-2022:0146
https://access.redhat.com/errata/RHSA-2022:0151
https://access.redhat.com/errata/RHSA-2022:0152
https://access.redhat.com/errata/RHSA-2022:0155
https://access.redhat.com/errata/RHSA-2022:0157
https://access.redhat.com/errata/RHSA-2022:0158
https://access.redhat.com/errata/RHSA-2022:0161
https://access.redhat.com/errata/RHSA-2022:0162
https://access.redhat.com/errata/RHSA-2022:0163
https://access.redhat.com/errata/RHSA-2022:0164
https://access.redhat.com/errata/RHSA-2022:0176
https://access.redhat.com/errata/RHSA-2022:0177
https://access.redhat.com/errata/RHSA-2022:0178
https://access.redhat.com/errata/RHSA-2022:0184
https://access.redhat.com/errata/RHSA-2022:0186
https://access.redhat.com/errata/RHSA-2022:0187
https://access.redhat.com/errata/RHSA-2022:0188
https://access.redhat.com/errata/RHSA-2022:0190
https://access.redhat.com/errata/RHSA-2022:0191
https://access.redhat.com/errata/RHSA-2022:0199
https://access.redhat.com/errata/RHSA-2022:0202
https://access.redhat.com/errata/RHSA-2022:0203
https://access.redhat.com/errata/RHSA-2022:0205
https://access.redhat.com/errata/RHSA-2022:0216
https://access.redhat.com/errata/RHSA-2022:0219
https://access.redhat.com/errata/RHSA-2022:0222
https://access.redhat.com/errata/RHSA-2022:0223
https://access.redhat.com/errata/RHSA-2022:0225
https://access.redhat.com/errata/RHSA-2022:0226
https://access.redhat.com/errata/RHSA-2022:0227

10. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.456483
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.476837

11. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220079-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220080-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220081-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220088-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220090-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220091-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220091-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220101-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220102-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220103-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220104-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220107-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220108-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220110-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220111-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220112-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220113-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220114-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220115-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220118-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220119-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220126-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220128-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220130-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220131-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220133-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220134-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220135-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220136-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220137-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220138-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220139-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220141-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220142-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220144-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220145-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214875-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214876-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214877-1/

12. Trend Micro

https://success.trendmicro.com/solution/000290104

13. Ubuntu

https://ubuntu.com/security/notices/LSN-0084-1
https://ubuntu.com/security/notices/USN-5021-2
https://ubuntu.com/security/notices/USN-5227-2
https://ubuntu.com/security/notices/USN-5233-1
https://ubuntu.com/security/notices/USN-5233-2
https://ubuntu.com/security/notices/USN-5234-1
https://ubuntu.com/security/notices/USN-5235-1
https://ubuntu.com/security/notices/USN-5240-1
https://ubuntu.com/security/notices/USN-5241-1
https://ubuntu.com/security/notices/USN-5242-1
https://ubuntu.com/security/notices/USN-5243-1
https://ubuntu.com/security/notices/USN-5243-2
https://ubuntu.com/security/notices/USN-5244-1

14. VMware

https://www.vmware.com/security/advisories/VMSA-2022-0002.html

Sources of product vulnerability information:

CentOS
Debian
F5 Products
Huawei
McAfee
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT
VMware

Contact:

cert@govcert.gov.hk