GovCERT.HK

Weekly IT Security News Bulletin, 2022-W02

10 January – 16 January 2022

Headlines

DDoS attacks that come combined with extortion demands are on the rise

- A security vendor's statistics for distributed denial-of-service (DDoS) attacks reflected a rise in ransom DDoS attacks by 175% in Q4 2021 compared to the previous quarter. According to the survey conducted, one in five DDoS attacks was accompanied by a ransom note from the attacker during 2021. The trend raised in December 2021 where one in three of the organisations surveyed said they received a ransom letter relating to a DDoS attack.

- Targets of DDoS attacks commonly include online retailers, cloud-based business applications, streaming services and online games. The statistics was based on traffic from botnets detected and analysed by the vendor. In Q4 2021, the Manufacturing industry was the most frequently attacked, recording a significant 641% increase in the number of attacks as compared with Q3 2021, followed by the Business Services and Gaming/Gambling industries.

- Regarding the attack vectors, the percentage of SYN flood attacks significantly decreased in Q4 2021. A massive spike in Simple Network Management Protocol (SNMP), Microsoft SQL (MSSQL), and generic UDP-based DDoS attacks was observed.

Advice

- Design and build a resilient network architecture that avoids single points of failure and enables flexible resource deployment, such as redundant Internet connections and cloud-based platforms.
- Engage network or service providers for anti-DDoS services, such as content delivery networks or clean pipe services for necessary protection against DDoS attacks.
- Monitor network traffic by automated tools or managed network services to identify attacks early for a timely response.
- Stay vigilant of the threat of DDoS attacks and prepare contingency plan(s) for scenarios when under attack.

Sources

- Cloudflare
- ZDNet

A new cross-platform backdoor malware

- Security researchers revealed a cross-platform malware known as SysJoker targeting Windows, Mac, and Linux operating systems. According the researchers, SysJoker is a backdoor program designed for establishing an initial access on a target machine. SysJoker was found masquerading as a system update to avoid suspicion but each sample observed was tailored for a specific target.

- The malware analysis result suggested that SysJoker could exfiltrate information about infected machine such as MAC address, IP address and user name to a command-and control (C2) server. To connect and communicate with the C2 server, SysJoker first retrieved a file hosted at Google Drive and then decoded the link inside the file. The researchers discovered that the link of the C2 server was changed several times during the time of the analysis and thus suggested that the attacker was actively involved in the campaign.

- Besides exfiltration of machine information, SysJoker could relay various instructions from the C2 server to the compromised machine for subsequent attacks or pivot to move further into the network. SysJoker could also maintain persistence on targeted machines by adding an entry to the registry "Run" key.

Advice

- Perform regular security scanning with memory scanners to detect fileless malware that resides in memory.
- Deploy endpoint detection and response (EDR) or security information and event management (SIEM) solutions for effective detection of malicious scripts or processes running across systems and networks.
- Monitor network traffic system and application logs to identify abnormal activities.

Sources

- Intezer
- Threatpost

Product Vulnerability Notes & Security Updates

1. Citrix

https://support.citrix.com/article/CTX335432
https://support.citrix.com/article/CTX338435

2. Debian

https://www.debian.org/security/2022/dsa-5037
https://www.debian.org/security/2022/dsa-5038
https://www.debian.org/security/2022/dsa-5039
https://www.debian.org/security/2022/dsa-5040
https://www.debian.org/security/2022/dsa-5041
https://www.debian.org/security/2022/dsa-5042
https://www.debian.org/security/2022/dsa-5043

3. FreeBSD

https://www.freebsd.org/security/advisories/FreeBSD-SA-22:01.vt.asc

4. Huawei Products

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160330-01-openssl-en

5. Johnson Controls VideoEdge

https://us-cert.cisa.gov/ics/advisories/icsa-22-011-01

6. Juniper Products

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11260
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11261
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11262
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11263
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11264
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11265
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11267
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11268
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11269
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11270
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11271
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11272
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11274
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11275
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11276
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11277
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11278
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11279
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11280
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11281
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11282

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11283
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11284
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11285
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11286
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11287
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11288
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11289
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11290
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11291
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11292
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11293
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11294
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11296

7. Mitsubishi Products

https://us-cert.cisa.gov/ics/advisories/icsa-22-013-01
https://us-cert.cisa.gov/ics/advisories/icsa-22-013-07

8. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2OQK3YBZP7LLGFOZF2RYGZC5GDDRHRI6/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/6QFPACQDVZMSNEBMXPO5WA2LCCPKDKR2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/BMN5QRPEKDGOKDHBMC6SXHPA733I43MV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/D2476MS7B5R3KZZUCZGHTC6PPIJ5FNFI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DAZJOOODJLFD53X2AQIEWTT3MS53WDSD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DKIXTCVYQEKZ2ANWGLWL5Q77ZMIOTQJ2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/IRYD4Y2CDUYSBVQUIDXTTBL6H6XYW54G/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LN5Z3Y5OA2VGDDD23VAZE2P4IULBASWF/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PH3Q2TLVW235XFTNU2563GON62BFYPLP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QYJBECOXKL6LM6PP3ZL5EKF4GRPTFTD5/

9. Oracle Linux

https://linux.oracle.com/errata/ELSA-2021-4913.html
https://linux.oracle.com/errata/ELSA-2021-4916.html
https://linux.oracle.com/errata/ELSA-2021-9575.html
https://linux.oracle.com/errata/ELSA-2021-9577.html
https://linux.oracle.com/errata/ELSA-2021-9591.html
https://linux.oracle.com/errata/ELSA-2022-0059.html
https://linux.oracle.com/errata/ELSA-2022-0063.html
https://linux.oracle.com/errata/ELSA-2022-0064.html
https://linux.oracle.com/errata/ELSA-2022-0124.html

https://linux.oracle.com/errata/ELSA-2022-0130.html
https://linux.oracle.com/errata/ELSA-2022-9010.html
https://linux.oracle.com/errata/ELSA-2022-9011.html
https://linux.oracle.com/errata/ELSA-2022-9012.html
https://linux.oracle.com/errata/ELSA-2022-9013.html
https://linux.oracle.com/errata/ELSA-2022-9014.html
https://linux.oracle.com/errata/ELSA-2022-9017.html
https://linux.oracle.com/errata/ELSA-2022-9023.html

10. Red Hat

https://access.redhat.com/errata/RHSA-2022:0024
https://access.redhat.com/errata/RHSA-2022:0026
https://access.redhat.com/errata/RHSA-2022:0042
https://access.redhat.com/errata/RHSA-2022:0043
https://access.redhat.com/errata/RHSA-2022:0044
https://access.redhat.com/errata/RHSA-2022:0047
https://access.redhat.com/errata/RHSA-2022:0059
https://access.redhat.com/errata/RHSA-2022:0063
https://access.redhat.com/errata/RHSA-2022:0064
https://access.redhat.com/errata/RHSA-2022:0065
https://access.redhat.com/errata/RHSA-2022:0072
https://access.redhat.com/errata/RHSA-2022:0073
https://access.redhat.com/errata/RHSA-2022:0074
https://access.redhat.com/errata/RHSA-2022:0075
https://access.redhat.com/errata/RHSA-2022:0076
https://access.redhat.com/errata/RHSA-2022:0078
https://access.redhat.com/errata/RHSA-2022:0081
https://access.redhat.com/errata/RHSA-2022:0082
https://access.redhat.com/errata/RHSA-2022:0108
https://access.redhat.com/errata/RHSA-2022:0124
https://access.redhat.com/errata/RHSA-2022:0125
https://access.redhat.com/errata/RHSA-2022:0126
https://access.redhat.com/errata/RHSA-2022:0130
https://access.redhat.com/errata/RHSA-2022:0132
https://access.redhat.com/errata/RHSA-2022:0133
https://access.redhat.com/errata/RHSA-2022:0138

11. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-22-013-02
https://us-cert.cisa.gov/ics/advisories/icsa-22-013-03
https://us-cert.cisa.gov/ics/advisories/icsa-22-013-04
https://us-cert.cisa.gov/ics/advisories/icsa-22-013-05
https://us-cert.cisa.gov/ics/advisories/icsa-22-013-06

12. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220040-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220041-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220042-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220043-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220045-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20220050-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220052-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220056-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220060-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220061-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220062-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220064-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220065-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220068-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20220069-1/

13. Ubuntu

https://ubuntu.com/security/notices/USN-5043-2
https://ubuntu.com/security/notices/USN-5210-2
https://ubuntu.com/security/notices/USN-5212-2
https://ubuntu.com/security/notices/USN-5217-1
https://ubuntu.com/security/notices/USN-5218-1
https://ubuntu.com/security/notices/USN-5219-1
https://ubuntu.com/security/notices/USN-5222-1
https://ubuntu.com/security/notices/USN-5223-1
https://ubuntu.com/security/notices/USN-5224-1
https://ubuntu.com/security/notices/USN-5224-2
https://ubuntu.com/security/notices/USN-5225-1
https://ubuntu.com/security/notices/USN-5226-1
https://ubuntu.com/security/notices/USN-5227-1
https://ubuntu.com/security/notices/USN-5229-1

Sources of product vulnerability information:

Citrix
Debian
FreeBSD
Huawei
Juniper
openSUSE
Oracle Linux
Red Hat
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk