GovCERT.HK

Weekly IT Security News Bulletin, 2022-W16

18 April – 24 April 2022

Headlines

Beware of BlackByte ransomware

- A security vendor detailed the analysis of the BlackByte ransomware, which first emerged as Ransomware as a Service (RaaS) in 2021 and was since then used to target multiple organisations including those in critical infrastructure sectors.

- BlackByte mainly targets Microsoft Exchange servers with known vulnerabilities and in particular exploits the ProxyShell vulnerabilities for initial access. Once gaining a foothold, a malicious web shell allowing remote code execution will be dropped onto the compromised Exchange Server before the encryption process begins. While no exfiltration capability is observed, the analysis found that BlackByte took advantage of WinRAR to compress local data, potentially in preparation for future exfiltration. The ransomware will leaves a ransom note in all directories where encryption occurs.

- To create pressure on victims to pay the ransom, the threat actors leverages double extortion as part of the attack by shaming the victims through listing their information on the cybercrime marketplace.

Advice

- Apply latest security patches on your Windows systems as soon as updates/patches are released.
- Stay aware of the latest trends and imminent threats of ransomware and adopt security measures to mitigate the risks.
- Implement regular air gapped backups of all data to minimise impact caused by the ransomware attack.

Sources

- Palo Alto Networks

Malware targets Docker for cryptomining operations

- Security researchers observed a botnet cryptomining campaign targeting poorly secured or misconfigured Docker services. With Docker gaining popularity to run application workloads on cloud platforms, the campaign leveraged exposed Docker APIs in an attempt to mine cryptocurrency on their Linux system hosts.

- Docker provides a set of APIs for developers to build, deploy and manage their containers on local servers or cloud platforms using simple commands. However, these APIs may be exposed to the Internet if not configured correctly. In a case reported by the security researcher, the threat actor scanned for exposed Docker APIs as an initial access vector to systems and ran a malicious container to fetch a malicious image file that contained a malicious script from an attacker-controlled remote server.

- Once the script was deployed, it would subsequently terminate daemon processes, disable cloud monitoring services and dropped the cryptocurrency miners together with backdoor malware on the infected systems. To spread laterally, threat actors would also leverage SSH keys found on the infected systems and repeat the infection process.

Advice

- Avoid exposing cloud resources to the Internet and consider adopting a Zero-Trust policy for any incoming network traffic.
- Secure containers from potential risks by applying the latest security updates in a timely manner.
- Establish monitoring for Docker workloads and stay vigilant against any suspicious system resource utilisation.

Sources

- CrowdStrike
- BleepingComputer

Product Vulnerability Notes & Security Updates

1. **Automated Logic WebCTRL**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-109-02

2. **Debian**

   https://www.debian.org/security/2022/dsa-5115
   https://www.debian.org/security/2022/dsa-5116
   https://www.debian.org/security/2022/dsa-5117
   https://www.debian.org/security/2022/dsa-5120
   https://www.debian.org/security/2022/dsa-5121
   https://www.debian.org/security/2022/dsa-5122
   https://www.debian.org/security/2022/dsa-5123

3. **Delta Electronics Products**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-104-01
   https://us-cert.cisa.gov/ics/advisories/icsa-22-111-01

4. **Drupal**

   https://https://www.drupal.org/sa-core-2022-008
   https://https://www.drupal.org/sa-core-2022-009

5. **Elcomplus Products**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-109-04
   https://us-cert.cisa.gov/ics/advisories/icsa-22-109-05

6. **F5 Products**

   https://support.f5.com/csp/article/K21054458

7. **FANUC ROBOGUIDE Simulation Platform**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-109-03

8. **Hitachi Energy MicroSCADA Pro/X SYS600**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-111-03

9. **IBM Products**

   https://www.ibm.com/support/pages/node/6573293

10. **Interlogix Hills ComNav**

    https://us-cert.cisa.gov/ics/advisories/icsa-22-109-01

11. Johnson Controls Metasys Products

https://us-cert.cisa.gov/ics/advisories/icsa-22-104-02
https://us-cert.cisa.gov/ics/advisories/icsa-22-111-02

12. McAfee

https://kc.mcafee.com/corporate/index?page=content&id=SB10381

13. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/662Q4K3MTGYRNK4HPTROD3ZFI3H2D2QA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DGAUAZBEGR57YHBPABYELAXXVLEITVUZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/G5YYTVAL4HMIDBKVGBDTZND7UELHVRC2/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GCTOZ6PYY7RHFKQZCR36S4INP2QDEWSL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GY3FXWPGNBOFA2QZOFDFNU2AZJWYEW7A/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KADIHA2DVB75ZOBL67G3SBOUENCMPRZ5/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/LFRGVANZSHVPH347SJNAHULVC5ZG2ZTV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/N3NSKDPRHUENCNFIPJHSG7V326EE6EYD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OSRKZNBHTNPBXXEBPZVNKUWSIPPLZXJE/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/OW6NT6ZHAVSZIH2A3BFFR2EWWDYFK7FZ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/RT4PK6MXMUBIFIGD2YA7HAH4DD43QU3Z/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/RT7EBWFKU35SW2PM3ELHR2KWX4F4JS47/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/TBRPZKOZUNORV3ZNXLKMNUZ2AUMPJ4Y6/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YDVWQ5ZUMZUOMBBPVXPXX6XNCBNZ2BMJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YGGYMG7MOCEOKAIHSJGJHXRP2IQLVF47/

14. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-1440.html
https://linux.oracle.com/errata/ELSA-2022-1442.html
https://linux.oracle.com/errata/ELSA-2022-1445.html

15. Red Products

https://access.redhat.com/errata/RHSA-2022:1336
https://access.redhat.com/errata/RHSA-2022:1356
https://access.redhat.com/errata/RHSA-2022:1357
https://access.redhat.com/errata/RHSA-2022:1363
https://access.redhat.com/errata/RHSA-2022:1370
https://access.redhat.com/errata/RHSA-2022:1378
https://access.redhat.com/errata/RHSA-2022:1379
https://access.redhat.com/errata/RHSA-2022:1389
https://access.redhat.com/errata/RHSA-2022:1390
https://access.redhat.com/errata/RHSA-2022:1394
https://access.redhat.com/errata/RHSA-2022:1396
https://access.redhat.com/errata/RHSA-2022:1402
https://access.redhat.com/errata/RHSA-2022:1407
https://access.redhat.com/errata/RHSA-2022:1410
https://access.redhat.com/errata/RHSA-2022:1413
https://access.redhat.com/errata/RHSA-2022:1417
https://access.redhat.com/errata/RHSA-2022:1418
https://access.redhat.com/errata/RHSA-2022:1440
https://access.redhat.com/errata/RHSA-2022:1441
https://access.redhat.com/errata/RHSA-2022:1442
https://access.redhat.com/errata/RHSA-2022:1443
https://access.redhat.com/errata/RHSA-2022:1444
https://access.redhat.com/errata/RHSA-2022:1445
https://access.redhat.com/errata/RHSA-2022:1461
https://access.redhat.com/errata/RHSA-2022:1462
https://access.redhat.com/errata/RHSA-2022:1463
https://access.redhat.com/errata/RHSA-2022:1469
https://access.redhat.com/errata/RHSA-2022:1476
https://access.redhat.com/errata/RHSA-2022:1478
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-03

16. Siemens Products

https://us-cert.cisa.gov/ics/advisories/icsa-22-104-04
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-05
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-06
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-07
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-08
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-09
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-10
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-11
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-12
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-13
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-14
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-15
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-16
https://us-cert.cisa.gov/ics/advisories/icsa-22-104-17

17. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.452938
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.453099
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.456633

18. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220716-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220720-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220727-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220736-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220802-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220844-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220845-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220930-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220942-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20220943-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20221040-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20221194-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221196-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221197-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221212-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221215-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221217-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221218-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221223-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221224-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221230-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221242-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221246-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221248-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221250-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221252-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221254-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221255-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221256-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221257-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221258-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221259-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221260-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221261-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221265-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221266-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221267-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221268-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221269-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221270-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221271-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221272-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20221273-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221274-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221275-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221276-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221277-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221278-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221283-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221285-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221288-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221289-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221292-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221293-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221294-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221296-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221297-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214940-1/
https://www.suse.com/support/update/announcement/2022/suse-su-202214941-1/

19. Ubuntu

https://ubuntu.com/security/notices/USN-5379-1
https://ubuntu.com/security/notices/USN-5380-1
https://ubuntu.com/security/notices/USN-5381-1
https://ubuntu.com/security/notices/USN-5382-1
https://ubuntu.com/security/notices/USN-5383-1
https://ubuntu.com/security/notices/USN-5384-1
https://ubuntu.com/security/notices/USN-5385-1

Sources of product vulnerability information:

Debian
Drupal
F5 Products
IBM
McAfee
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk