GovCERT.HK

Weekly IT Security News Bulletin, 2022-W23

6 June – 12 June 2022

Headlines

Be aware of QR code phishing attacks

- A recent security report highlighted phishing cases where attackers leveraged QR codes to bypass traditional security solutions that detect malicious URLs in emails. QR code is commonly used today for convenient access to a website or a merchant's information without inputting the actual information. However, it also enables threat actors to mask URLs so that an unsuspecting user scanning the code can get directed to a malicious site.

- In a credential phishing case, the attacker sent an email impersonating a bank for consent to data privacy changes or other relatively non-urgent actions and requested the victims to scan the QR code for instructions. The QR code was actually linked to a malicious site where unsuspecting users inputted their banking login credentials. This campaign cleverly diverged from the routine of attempting to create urgency such as issues in accounts to avoid being suspicious.

- While email is the main potential mode of delivery for QR code, threat actors may also strategically place malicious QR codes such as overlaying an existing QR code on a restaurant menu, advertisement or noticeboard in an effort to lure victims into accessing the malicious URLs.

Advice

- Check for any signs of tampering or fraud (e.g., spelling mistakes in emails) before scanning the QR code and only scan QR codes obtained from trusted sources.
- Verify the full URL embedded in QR codes before proceeding.
- Do not provide credentials or personal information if in doubt.

Sources

- Nuspire

Malware loaded using Word document properties

- Security researchers uncovered a phishing campaign using a new malware loader in Word documents to compromise devices. Named SVCReady, the malware loader uses Visual Basic for Applications (VBA) macro code to execute shellcode hidden in the properties of a Word document. Unlike other Office-related malware, the document does not use PowerShell or Microsoft HTML Applications program (MSHTA) to download further payloads from the web.

- According to the researchers, the malware has been under deployment since April 2022 and released serval updates in May 2022. Once the shellcode was executed, SVCReady gathered and exfiltrated system information to the command and control (C2) server using an encrypted channel. The malware loader was also capable of taking screenshots and running shell commands in addition to fetching additional payloads.

- To establish persistence, a scheduled task was created to run SVCReady when the system starts. During the investigation by the researchers, the scheduled task was not properly configured and does not start after the system was rebooted. The researchers believed that the malware loader was in the early stages of development.

Advice

- Stay extra vigilant against suspicious and unknown documents and do not open them unless their authenticity is verified.
- Deploy an Endpoint Detection and Response (EDR) solution to detect and respond to malicious behaviour on endpoints.
- Be aware of the latest trends and imminent malware threats and adopt security measures to mitigate the risks

Sources

- HP
- BleepingComputer

Product Vulnerability Notes & Security Updates

1. **Carrier LenelS2 HID Mercury access panels**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-153-01

2. **Debian**

   https://www.debian.org/security/2022/dsa-5156
   https://www.debian.org/security/2022/dsa-5157

3. **Dominion Voting Systems ImageCast X**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-154-01

4. **F5 Products**

   https://support.f5.com/csp/article/K13559191
   https://support.f5.com/csp/article/K29421535
   https://support.f5.com/csp/article/K95204515

5. **Fortinet**

   https://www.fortiguard.com/psirt/FG-IR-18-292
   https://www.fortiguard.com/psirt/FG-IR-21-024
   https://www.fortiguard.com/psirt/FG-IR-22-008
   https://www.fortiguard.com/psirt/FG-IR-22-021
   https://www.fortiguard.com/psirt/FG-IR-22-044
   https://www.fortiguard.com/psirt/FG-IR-22-071
   https://www.fortiguard.com/psirt/FG-IR-22-109

6. **GitLab**

   https://about.gitlab.com/releases/2022/06/01/critical-security-release-gitlab-15-0-1-released/

7. **Huawei Products**

   https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220601-01-6b47c6b6-en
   https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220608-01-1a91f8a4-en

8. **IBM Products**

   https://www.ibm.com/support/pages/node/6578665
   https://www.ibm.com/support/pages/node/6592573

9. **Illumina Local Run Manager**

   https://us-cert.cisa.gov/ics/advisories/icsa-22-153-02

10. Mitsubishi Electric Air Conditioning Systems

https://us-cert.cisa.gov/ics/advisories/icsa-22-160-01

11. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3IJTJMR6NXI4LZ6XNPTTPL53GRG5KSUG/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4VJQBTBCWDRPAVJ62BTMK5TJWKWFW6CK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/7YVS6P6QJPK5B4HQAT2XTPVX5KZ5WZ3B/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DLSQOI3SFC7MIFFPQQ4BFH3GPU3DQDMM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ECBLCJCXZ3FLNPQKVLDKMWDGHLACPF7G/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FCJIKKGQ72UAHX5RRZYYHVSHFNN2P7VV/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/GFMKINKNGWQOSEK7V5T7PPOCPWYUOGYM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/M6EOJDUBHXSFATXFVLSSBLO6MRB3LNKJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ROPFHAEWFSGDSF5CNARTGVY64E2BJE6P/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SL7GH2SRZRAUIJWXQSSMUW4BKBUFFNOD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/SSUXW5GXJ5EEVAOMVYHV4K76F7LQLIJA/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/T43T6NQGDIIJUPCGP2IPAWS5XMR2UCJG/

12. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-4855.html
https://linux.oracle.com/errata/ELSA-2022-4872.html
https://linux.oracle.com/errata/ELSA-2022-4930.html
https://linux.oracle.com/errata/ELSA-2022-4941.html
https://linux.oracle.com/errata/ELSA-2022-9460.html
https://linux.oracle.com/errata/ELSA-2022-9465.html
https://linux.oracle.com/errata/ELSA-2022-9466.html
https://linux.oracle.com/errata/ELSA-2022-9469.html
https://linux.oracle.com/errata/ELSA-2022-9471.html
https://linux.oracle.com/errata/ELSA-2022-14844.html
https://linux.oracle.com/errata/ELSA-2022-14857.html

13. PHP

https://www.php.net/archive/2022.php#2022-06-09-1
https://www.php.net/archive/2022.php#2022-06-09-2
https://www.php.net/archive/2022.php#2022-06-09-4

14. Red Hat

https://access.redhat.com/errata/RHSA-2022:4829
https://access.redhat.com/errata/RHSA-2022:4875
https://access.redhat.com/errata/RHSA-2022:4880
https://access.redhat.com/errata/RHSA-2022:4893
https://access.redhat.com/errata/RHSA-2022:4894
https://access.redhat.com/errata/RHSA-2022:4895
https://access.redhat.com/errata/RHSA-2022:4896
https://access.redhat.com/errata/RHSA-2022:4899
https://access.redhat.com/errata/RHSA-2022:4913
https://access.redhat.com/errata/RHSA-2022:4914
https://access.redhat.com/errata/RHSA-2022:4915
https://access.redhat.com/errata/RHSA-2022:4918
https://access.redhat.com/errata/RHSA-2022:4919
https://access.redhat.com/errata/RHSA-2022:4922
https://access.redhat.com/errata/RHSA-2022:4924
https://access.redhat.com/errata/RHSA-2022:4929
https://access.redhat.com/errata/RHSA-2022:4930
https://access.redhat.com/errata/RHSA-2022:4931
https://access.redhat.com/errata/RHSA-2022:4932
https://access.redhat.com/errata/RHSA-2022:4940
https://access.redhat.com/errata/RHSA-2022:4941
https://access.redhat.com/errata/RHSA-2022:4942
https://access.redhat.com/errata/RHSA-2022:4956
https://access.redhat.com/errata/RHSA-2022:4957
https://access.redhat.com/errata/RHSA-2022:4959
https://access.redhat.com/errata/RHSA-2022:4985

15. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.338048
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.409873
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.529253

16. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20221911-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221912-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221918-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221919-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221920-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221921-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221923-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221925-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221927-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221928-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221929-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221930-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221932-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20221933-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221934-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221939-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221940-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221942-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221945-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221947-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221948-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221949-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221955-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221974-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221988-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221989-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222000-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222003-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222004-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222005-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222006-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222010-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222015-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222029-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222030-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20222031-1/

17. Trend Micro

https://success.trendmicro.com/solution/000291095

18. Ubuntu

https://ubuntu.com/security/notices/USN-5396-2
https://ubuntu.com/security/notices/USN-5458-1
https://ubuntu.com/security/notices/USN-5459-1
https://ubuntu.com/security/notices/USN-5460-1
https://ubuntu.com/security/notices/USN-5461-1
https://ubuntu.com/security/notices/USN-5462-1
https://ubuntu.com/security/notices/USN-5462-2
https://ubuntu.com/security/notices/USN-5463-1
https://ubuntu.com/security/notices/USN-5464-1
https://ubuntu.com/security/notices/USN-5465-1
https://ubuntu.com/security/notices/USN-5466-1
https://ubuntu.com/security/notices/USN-5467-1
https://ubuntu.com/security/notices/USN-5468-1
https://ubuntu.com/security/notices/USN-5469-1
https://ubuntu.com/security/notices/USN-5470-1
https://ubuntu.com/security/notices/USN-5471-1
https://ubuntu.com/security/notices/USN-5472-1
https://ubuntu.com/security/notices/USN-5473-1
https://ubuntu.com/security/notices/USN-5474-1

19. Xen

https://xenbits.xen.org/xsa/advisory-401.html
https://xenbits.xen.org/xsa/advisory-402.html

Sources of product vulnerability information:

Debian
F5 Products
Fortinet
Huawei
IBM
openSUSE
Oracle Linux
PHP
Red Hat
Slackware
SUSE
Trend Micro
Ubuntu
US-CERT
Xen

Contact:

cert@govcert.gov.hk