GovCERT.HK

Weekly IT Security News Bulletin, 2022-W18

2 May – 8 May 2022

Headlines

Emotet is testing a new attack chain

- Security researchers have revealed that the threat actors behind Emotet are testing a new attack technique through a small scale malspam campaign. Emotet is a prolific botnet and trojan that targets Windows platforms to distribute follow-on malware payloads. Previous campaigns associated with Emotet have targeted thousands of customers with a large volume of messages in multiple geographic regions. The message volume could reach over one million in some cases.

- Typically, Emotet relies on Microsoft Excel or Word documents containing Visual Basic for Application (VBA) macros as an infection vector. Since Microsoft announced to block VBA macros obtained from the Internet by default in April 2022, threat actors start changing its tactics to leverage Excel Add-in (XLL) files in ZIP archives for dropping and execution of the Emotet payload.

- One of the Emotet campaign recently observed by the security researchers was that the email subjects were simple and the email bodies contained only an OneDrive URL with no other content. The OneDrive URL hosted zip files containing malicious Microsoft Excel Add-in (XLL) files. When executed, the XLL files will then drop and run the Emotet payloads. According to the researchers, the campaign is probably an attempt to evade detection and stay hidden without relying on macro-enabled documents.

Advice

- Stay vigilant of any suspicious attachments and hyperlinks on online communication platforms and verify the authenticity before opening attachments or clicking embedded links.
- Use robust endpoint security solutions and scan emails and web content for malicious payloads.
- Retain and closely monitor system logs to identify any anomalous or suspicious activity.

Sources

- Proofpoint
- Cyware

Be aware of browser-based malware

- A recent study on the prevalence of malware variants in the second half of 2021 revealed that cyber adversaries are maximising the remote work and learning attack vectors in their attacks. With the significant increase in remote work and learning, the study found that various forms of browser-based malware were prevalent. This often takes the form of phishing lures or scripts that inject code or redirect users to malicious sites.

- According to the study, attackers were often found using trending topics such as latest news about COVID-19, politics, sports or any current headline to attract users to visit their websites embedded with malicious scripts. Work from home users are likely more vulnerable to phishing attack due to fewer protections against malicious web content, for example the lack of web content filtering solutions.

- In addition, researchers also highlighted that the use of exploit kits (EKs) has helped attackers in their efforts to run malicious code. EKs are automated programs to identify and exploit known vulnerabilities on the victim's device, allowing attackers to download and execute malware. The whole process was transparent to the victim as EKs would fetch hidden code to exploit vulnerability in the victim's browser.

Advice

- Deploy endpoint detection and response (EDR) solutions with advanced features such as behavioural analysis and memory scanning.
- Enforce application whitelisting to avoid malicious programs or processes from running on the machine.
- Stay aware of the latest trends and imminent threats of malware variants and adopt security measures to mitigate the risks.

Sources

- ThreatPost

Product Vulnerability Notes & Security Updates

1. Debian

https://www.debian.org/security/2022/dsa-5126
https://www.debian.org/security/2022/dsa-5127
https://www.debian.org/security/2022/dsa-5128
https://www.debian.org/security/2022/dsa-5129
https://www.debian.org/security/2022/dsa-5130
https://www.debian.org/security/2022/dsa-5131

2. F5 Products

https://support.f5.com/csp/article/K03442392
https://support.f5.com/csp/article/K03755971
https://support.f5.com/csp/article/K06323049
https://support.f5.com/csp/article/K08510472
https://support.f5.com/csp/article/K14229426
https://support.f5.com/csp/article/K16187341
https://support.f5.com/csp/article/K17341495
https://support.f5.com/csp/article/K19473898
https://support.f5.com/csp/article/K21317311
https://support.f5.com/csp/article/K23231802
https://support.f5.com/csp/article/K23421535
https://support.f5.com/csp/article/K23454411
https://support.f5.com/csp/article/K24248011
https://support.f5.com/csp/article/K25451853
https://support.f5.com/csp/article/K31856317
https://support.f5.com/csp/article/K33552735
https://support.f5.com/csp/article/K37155600
https://support.f5.com/csp/article/K38271531
https://support.f5.com/csp/article/K39002226
https://support.f5.com/csp/article/K40019131
https://support.f5.com/csp/article/K41440465
https://support.f5.com/csp/article/K41877405
https://support.f5.com/csp/article/K44233515
https://support.f5.com/csp/article/K47662005
https://support.f5.com/csp/article/K49905324
https://support.f5.com/csp/article/K50899356
https://support.f5.com/csp/article/K51539421
https://support.f5.com/csp/article/K52322100
https://support.f5.com/csp/article/K52340447
https://support.f5.com/csp/article/K52379673
https://support.f5.com/csp/article/K53197140
https://support.f5.com/csp/article/K53593534
https://support.f5.com/csp/article/K54082580
https://support.f5.com/csp/article/K54460845
https://support.f5.com/csp/article/K55879220
https://support.f5.com/csp/article/K57110035
https://support.f5.com/csp/article/K57555833
https://support.f5.com/csp/article/K59904248
https://support.f5.com/csp/article/K64124988

https://support.f5.com/csp/article/K67397230
https://support.f5.com/csp/article/K68647001
https://support.f5.com/csp/article/K68816502
https://support.f5.com/csp/article/K70134152
https://support.f5.com/csp/article/K70300233
https://support.f5.com/csp/article/K71103363
https://support.f5.com/csp/article/K74302282
https://support.f5.com/csp/article/K80945213
https://support.f5.com/csp/article/K81952114
https://support.f5.com/csp/article/K82034427
https://support.f5.com/csp/article/K85021277
https://support.f5.com/csp/article/K85054496
https://support.f5.com/csp/article/K91589041
https://support.f5.com/csp/article/K92306170
https://support.f5.com/csp/article/K92807525
https://support.f5.com/csp/article/K93543114
https://support.f5.com/csp/article/K94093538
https://support.f5.com/csp/article/K94142349
https://support.f5.com/csp/article/K99123750

3. Fortinet

https://www.fortiguard.com/psirt/FG-IR-21-040
https://www.fortiguard.com/psirt/FG-IR-21-147
https://www.fortiguard.com/psirt/FG-IR-21-154
https://www.fortiguard.com/psirt/FG-IR-21-230
https://www.fortiguard.com/psirt/FG-IR-21-231
https://www.fortiguard.com/psirt/FG-IR-21-239
https://www.fortiguard.com/psirt/FG-IR-22-007
https://www.fortiguard.com/psirt/FG-IR-22-041
https://www.fortiguard.com/psirt/FG-IR-22-062

4. Johnson Controls Metasys

https://us-cert.cisa.gov/ics/advisories/icsa-22-125-01

5. OpenSSL

https://www.openssl.org/news/secadv/20220503.txt

6. openSUSE

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/2JCMDMJPGWUHHQLFLSCXHN4YC4SQA6AL/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/3HDAKTMAXX2QBKCCM4SN6LA2G7YJ2JXI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4FVSP2SFD2BB42ZDWXSP7S7353LK4HVU/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/4OWUGWIAVPNW5Z3FTCRLTTQ4LHHR4QUP/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/CJBZPGJMIRYGYR36ENBCVEGGRBWLR7JC/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/D37SKVKHRP37B5V42A6N2KQV52RKEYTM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/DIQNWTFOKNMW2T6CUMCM3JBIS5B4BVKI/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/FCSITPAR7Z2O2KAZU2BY6AIHLSVER5WD/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/HJFVJUKPT7GYOWBWGQSIVM3OEHKOEVVJ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/INEJ3DHWSEUMTE45WNDFF4RSSFHBATKT/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/JSL3A3EFXELNQREOPMKA3CGCYH5WGQXK/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/K2PVX53ZDWGIBQ7QQADMQXD57DGMFCPQ/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/KQIZDBENBA7SYCDEBOVU4TMJLSK3IIRM/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/PUXQNAUH2W6TRXYZGBDFHQTMXINVMOJB/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/QOMIJFSJP2YQC52MEBB2NBM3G6L7P4E3/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/T3J3HHAVYMMOAGIZ7DYMCAOKYZPJOLUN/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/WLEU7S6R4KPLD2NTWJBPTT2YBOELCAW3/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/YGJODFFWOOAPS5L5J374HGXSM7RJDUVX/
https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/thread/ZUZSBBYZKYVD4HONZ32ZACQYHB5SER7R/

7. Oracle Linux

https://linux.oracle.com/errata/ELSA-2022-1541.html
https://linux.oracle.com/errata/ELSA-2022-1552.html
https://linux.oracle.com/errata/ELSA-2022-1643.html
https://linux.oracle.com/errata/ELSA-2022-1703.html
https://linux.oracle.com/errata/ELSA-2022-1705.html
https://linux.oracle.com/errata/ELSA-2022-9344.html
https://linux.oracle.com/errata/ELSA-2022-9348.html

8. Red Hat

https://access.redhat.com/errata/RHSA-2022:1519
https://access.redhat.com/errata/RHSA-2022:1520
https://access.redhat.com/errata/RHSA-2022:1600
https://access.redhat.com/errata/RHSA-2022:1620
https://access.redhat.com/errata/RHSA-2022:1622
https://access.redhat.com/errata/RHSA-2022:1660
https://access.redhat.com/errata/RHSA-2022:1661
https://access.redhat.com/errata/RHSA-2022:1662
https://access.redhat.com/errata/RHSA-2022:1663
https://access.redhat.com/errata/RHSA-2022:1664
https://access.redhat.com/errata/RHSA-2022:1665
https://access.redhat.com/errata/RHSA-2022:1676

https://access.redhat.com/errata/RHSA-2022:1681
https://access.redhat.com/errata/RHSA-2022:1701
https://access.redhat.com/errata/RHSA-2022:1702
https://access.redhat.com/errata/RHSA-2022:1703
https://access.redhat.com/errata/RHSA-2022:1704
https://access.redhat.com/errata/RHSA-2022:1705
https://access.redhat.com/errata/RHSA-2022:1708
https://access.redhat.com/errata/RHSA-2022:1709
https://access.redhat.com/errata/RHSA-2022:1711
https://access.redhat.com/errata/RHSA-2022:1712
https://access.redhat.com/errata/RHSA-2022:1713
https://access.redhat.com/errata/RHSA-2022:1715
https://access.redhat.com/errata/RHSA-2022:1716
https://access.redhat.com/errata/RHSA-2022:1734
https://access.redhat.com/errata/RHSA-2022:1739

9. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.343175
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.356627
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.468558
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.482760
https://www.slackware.com/security/viewer.php?l=slackware-security&y=2022&m=slackware-security.490188

10. SUSE

https://www.suse.com/support/update/announcement/2022/suse-su-20220731-2/
https://www.suse.com/support/update/announcement/2022/suse-su-20221465-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221466-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221474-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221475-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221476-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221477-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221478-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221479-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221483-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221484-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221485-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221486-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221505-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221506-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221507-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221508-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221509-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221510-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221511-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221512-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221513-1/

https://www.suse.com/support/update/announcement/2022/suse-su-20221514-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221515-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221516-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221524-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221527-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221528-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221529-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221531-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221533-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221534-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221536-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221537-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221538-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221540-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221541-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221545-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221546-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221548-1/
https://www.suse.com/support/update/announcement/2022/suse-su-20221549-1/

11. Ubuntu

https://ubuntu.com/security/notices/USN-5354-2
https://ubuntu.com/security/notices/USN-5382-2
https://ubuntu.com/security/notices/USN-5390-2
https://ubuntu.com/security/notices/USN-5395-2
https://ubuntu.com/security/notices/USN-5399-1
https://ubuntu.com/security/notices/USN-5400-1
https://ubuntu.com/security/notices/USN-5400-2
https://ubuntu.com/security/notices/USN-5400-3
https://ubuntu.com/security/notices/USN-5401-1
https://ubuntu.com/security/notices/USN-5402-1
https://ubuntu.com/security/notices/USN-5403-1
https://ubuntu.com/security/notices/USN-5405-1

12. Yokogawa CENTUM and ProSafe-RS

https://us-cert.cisa.gov/ics/advisories/icsa-22-123-01

Sources of product vulnerability information:

Debian
F5 Products
Fortinet
OpenSSL
openSUSE
Oracle Linux
Red Hat
Slackware
SUSE
Ubuntu
US-CERT

Contact:

cert@govcert.gov.hk