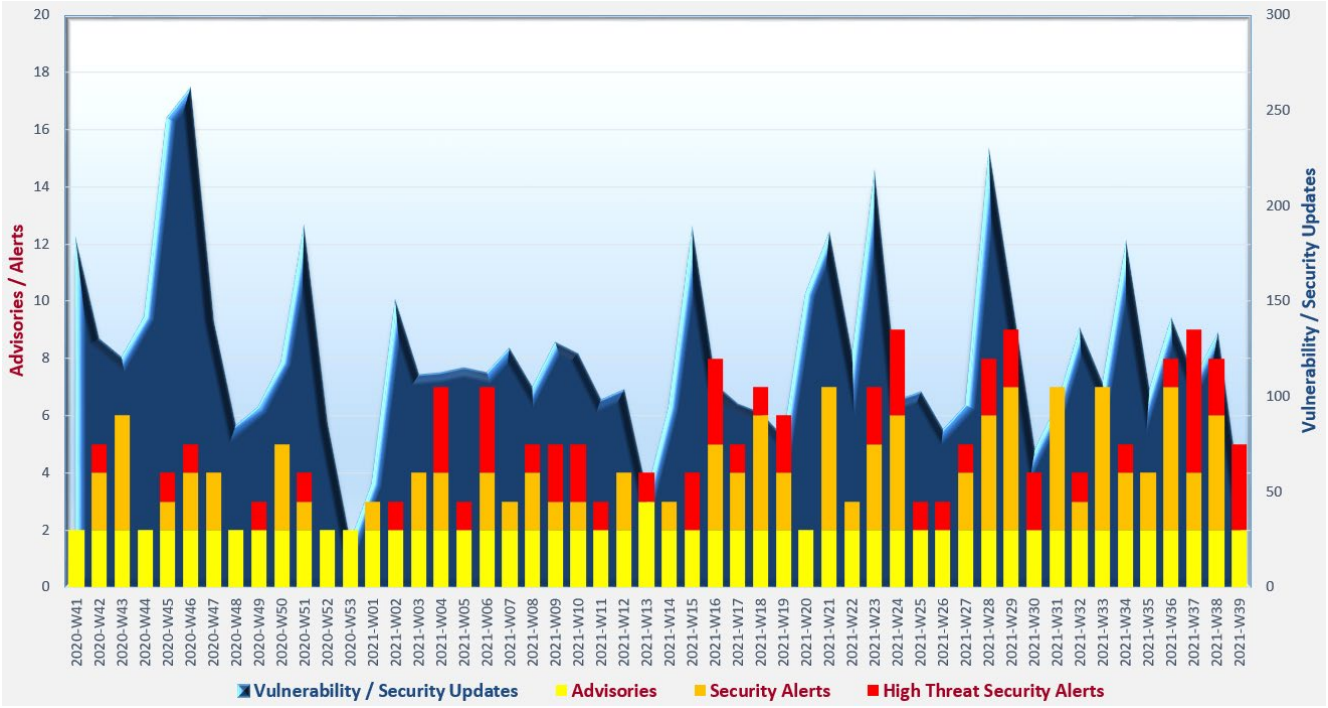
TLP:WHITE

Cyber Security Threat Trends 2021-M09

September 2021

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:WHITE information. Recipients may share with peers and partner organisations without restriction.

Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)



Trending:

- ✧ Malware activities, account takeover attacks and vulnerability exploitations are on the rise. Organisation should adopt risk-based vulnerability management, and apply security patches to their systems promptly. Layered approach in security defence should also be adopted, supported by implementation of up-to-date security protection solutions.

[1] https://www.first.org/tlp/

CERT Advisories

Active exploitation of vulnerabilities in various products

CERT bodies issued alerts regarding active exploitation against vulnerabilities in various products. Proof of Concept (PoC) codes for exploitation of some vulnerabilities were publicly available. System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.

- GovCERT.HK[2,3], HKCERT[4,5,6] JPCERT[7,8], and SingCERT[9], Australian Cyber Security Centre (ACSC)[10], Canadian Centre for Cyber Security[11], and Cybersecurity and Infrastructure Security Agency (CISA)[12] issued alerts regarding multiple vulnerabilities in Microsoft products. A remote code execution vulnerability (CVE-2021-40444) in MSHTML component affected all supported versions of Windows and Windows Server, including Windows 7 and Windows Server 2008, was being actively exploited.

- GovCERT.HK[13,14,15,16], HKCERT[17],[18] and Canadian Centre for Cyber Security[19] issued alerts regarding multiple vulnerabilities in Google Chrome and Microsoft Edge (Chromium-based). Vulnerabilities (CVE-2021-30632, CVE-2021-30633 and CVE-2021-37973) were being actively exploited.

- JPCERT[20], ASCS[21] and CISA[22] issued alerts regarding a remote code execution vulnerability (CVE-2021-26084) in Atlassian Confluence Server and Data Center. PoC code for exploitation of the vulnerability was publicly available.

---

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=649
3 https://www.govcert.gov.hk/en/alerts_detail.php?id=641
4 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-september-2021
5 https://www.hkcert.org/security-bulletin/microsoft-windows-remote-code-execution-vulnerability_20210908
6 https://www.hkcert.org/blog/hkcert-urges-microsoft-windows-users-to-be-vigilant-against-malicious-exploit-of-critical-vulnerability
7 https://www.jpcert.or.jp/english/at/2021/at210041.html
8 https://www.jpcert.or.jp/english/at/2021/at210038.html
9 https://www.csa.gov.sg/en/singcert/Alerts/al-2021-052
10 https://www.cyber.gov.au/acsc/view-all-content/alerts/remote-code-execution-vulnerability-present-mshtml-component-microsoft-windows
11 https://www.cyber.gc.ca/en/alerts/active-exploitation-microsoft-mshtml-remote-code-execution-vulnerability
12 https://us-cert.cisa.gov/ncas/current-activity/2021/09/07/microsoft-releases-mitigations-and-workarounds-cve-2021-40444
13 https://www.govcert.gov.hk/en/alerts_detail.php?id=647
14 https://www.govcert.gov.hk/en/alerts_detail.php?id=648
15 https://www.govcert.gov.hk/en/alerts_detail.php?id=652
16 https://www.govcert.gov.hk/en/alerts_detail.php?id=659
17 https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20210914
18 https://www.hkcert.org/security-bulletin/google-chrome-remote-code-execution-vulnerabily_20210927
19 https://www.cyber.gc.ca/en/alerts/google-chrome-security-advisory-67
20 https://www.jpcert.or.jp/english/at/2021/at210037.html
21 https://www.cyber.gov.au/acsc/view-all-content/alerts/remote-code-execution-vulnerability-present-certain-versions-atlassian-confluence
22 https://us-cert.cisa.gov/ncas/current-activity/2021/09/03/atlassian-releases-security-updates-confluence-server-and-data

CERT Advisories

- GovCERT.HK[23,24], HKCERT[25,26], SingCERT[27], and CISA[28,29] issued alerts regarding actively exploited vulnerabilities (CVE-2021-30858, CVE-2021-30860, and CVE-2021-30869) in various Apple devices which upon exploitation could lead to arbitrary code execution on the affected devices.

- GovCET.HK[30], HKCERT[31], CERT NZ[32], MyCERT[33] and CISA[34] issued alerts regarding multiple vulnerabilities in VMware products. A file upload vulnerability (CVE-2021-22005) in VMware vCenter Server was being actively exploited.

- JPCERT[35] issued an alert regarding vulnerability in Ghostscript. Upon exploitation, an attacker can execute arbitrary commands on the affected system. PoC code for exploitation of vulnerability CVE-2021-3781 was publicly available.

Fortinet Fortigate VPN Credentials Leaked

MyCERT[36], SingCERT[37] and ACSC[38] issued alerts on a leakage of around 500,000 Fortinet Fortigate VPN credentials on a hacking forum. System administrators should patch their systems timely, review the logs of their systems for signs of unauthorised or unusual logins, monitor the network for any intrusion attempts, perform organisation-wide password reset, enforce strong passwords and enable multi-factor authentication where possible.

Cyber security self-assessment tools for SMEs

HKCERT[39] released the "Check Your Cyber Security Readiness" online self-assessment tools for SMEs to understand their cyber security postures. Assessment results with appropriate recommendations and actionable procedures from HKCERT or external resources would be provided.

---

23 https://www.govcert.gov.hk/en/alerts_detail.php?id=646
24 https://www.govcert.gov.hk/en/alerts_detail.php?id=658
25 https://www.hkcert.org/security-bulletin/apple-products-remote-code-execution-vulnerabilities_20210914
26 https://www.hkcert.org/security-bulletin/apple-products-multiple-vulnerabilities_20210924
27 https://www.csa.gov.sg/en/singcert/Alerts/al-2021-054
28 https://us-cert.cisa.gov/ncas/current-activity/2021/09/13/apple-releases-security-updates-address-cve-2021-30858-and-cve
29 https://us-cert.cisa.gov/ncas/current-activity/2021/09/23/apple-releases-security-updates
30 https://www.govcert.gov.hk/en/alerts_detail.php?id=656
31 https://www.hkcert.org/security-bulletin/vmware-products-multiple-vulnerabilities_20210927
32 https://www.cert.govt.nz/it-specialists/advisories/active-scanning-for-vmware-vcenter-vulnerability/
33 https://www.mycert.org.my/portal/advisory?id=MA-817.092021
34 https://us-cert.cisa.gov/ncas/current-activity/2021/09/24/vmware-vcenter-server-vulnerability-cve-2021-22005-under-active
35 https://www.jpcert.or.jp/english/at/2021/at210039.html
36 https://www.mycert.org.my/portal/advisory?id=MA-815.092021
37 https://www.csa.gov.sg/en/singcert/Alerts/al-2021-053
38 https://www.cyber.gov.au/acsc/view-all-content/alerts/suspected-user-credentials-stolen-fortinet-devices-leaked-online
39 https://www.hkcert.org/blog/introducing-check-your-cyber-security-readiness-online-self-assessment-tools

CERT Advisories

Hardening remote access and remote storage solutions

HKCERT[40] published an article that provided actionable security measures on securing remote access systems such as Virtual Private Network (VPN) and remote storage such as Network-attached Storage (NAS) devices.

Study results showed cyber defence readiness of organisations in Hong Kong improved

The Hong Kong Productivity Council (HKPC) released the study results on the readiness of Hong Kong organisations in tackling cyber threats in 2021[41]. The study was conducted by HKPC and supported by HKCERT, surveyed 380 organisations from 6 industry sectors. The results revealed that the overall index was 49.6, increased by 2.7 from a similar survey last year. Most industry sectors attained Basic level while Financial Services sector continued to remain at Managed level. The two cyber attacks most encountered by the survey respondents were phishing email and ransomware.

Security events in Hong Kong increased 43% in Q2 2021

HKCERT released its Hong Kong Security Watch Report (Q2 2021)[42]. The number of security events increased from 5,017 in Q1 2021 to 7,191 in Q2 2021, due to increase of security events in defacement, phishing, malware hosting and Botnet (Bots). There was no Botnet Command and Control Centre (C&C) security event for seven consecutive quarters. The most targeted web server type in defacement events was Nginx (309 events). Although Mirai remained the largest botnet family, its number continued to drop and decremented 24.3% in Q2 2021. Avalanche and Nymaim botnets skyrocketed 266.8% and 559.7%, and ranked the second and third largest botnet family, respectively.

[40] https://www.hkcert.org/blog/patch-vulnerabilities-in-remote-access-and-remote-storage-now
[41] https://www.hkcert.org/blog/hkt-hong-kong-enterprise-cyber-security-readiness-index-2021-blog
[42] https://www.hkcert.org/watch-report/hong-kong-security-watch-report-q2-2021

Industry Insight on Cyber Security Threat Trends

Malware activities increased but botnet events dropped in Q2 2021

Nuspire issued the "Quarterly Threat Landscape Report, Q2 2021"[43] based on study of 90 billion traffic logs gathered from thousands of devices. The key findings were:

- **An increase of more than 40% was observed in malware activity comparing with Q1 2021.** Visual Basic for Applications (VBA) agents remained the most active malware variants, with activities went up by nearly 2.7 times as compared to Q1 2021.
- **Botnet activity decreased by about 50% as compared to Q1 2021.** The cause of the decrease could be due to the shutdown of Emotet botnet. Andromeda was the most active botnet, accounted for almost 48% of detected botnet activity in Q2 2021. Activity of Torpig botnet skyrocketed near the end of Q2 2021.
- **Brute force attempts on Server Message Block (SMB) and Secure Shell (SSH) soared with peak activities increased by around 85 times and 35 times respectively as compared to the start of Q2 2021.** Attackers actively targeted exposed and vulnerable internet-facing devices for brute force attacks.
- **Spikes in ransomware activities were detected in the second and third weeks of Q2 2021.** Attackers exploited vulnerabilities of different products such as VPN solutions and operating systems to penetrate to organisations' networks to cause damage.
- Organisations should adopt a layered approach in security defence, deploy endpoint protection and next-generation anti-malware solution, apply network segregation, follow least privilege principle and conduct regular security awareness training to educate their staff with up-to-date defence knowledge against emerging cyber security threats. System administrators should deploy system patches in a timely manner, deploy firewalls and Intrusion Prevention Systems (IPS), and disable unused services and network ports.

Source: Nuspire

[43] https://www.nuspire.com/resources/q2-2021-threat-report/

Industry Insight on Cyber Security Threat Trends

Vulnerabilities continue to grow in 2021

Skybox Security released the "Vulnerability and Threat Trends Mid-Year Report 2021"[44], which summarised their findings on the latest common vulnerabilities and threat trends in the first six months of 2021. The key findings were:

- **9,444 vulnerabilities were published in the National Vulnerability Database (NVD) in H1 2021.** The upward trend on the number of vulnerabilities in recent years was expected to continue. Products with the most new vulnerabilities found in H1 2021 spread across different types of solutions and devices, including operating systems, web browsers and network devices.

- **The number of new vulnerabilities actively exploited in H1 2021 grew 30% compared to H1 2020.** Attackers targeted low or medium severity vulnerabilities, which might be more likely neglected by organisations, for gaining initial access to organisations' network for subsequent lateral movement or privilege escalation. Organisations should also consider a vulnerability's accessibility and exposure in their vulnerability management and patching prioritisation.

- **New vulnerabilities in Operational Technology (OT) were up 46% compared to H1 2020. The number of vulnerabilities in network devices such as routers, switches, firewalls and their operating systems also rose by nearly 20% from H1 2020.** Attackers were increasingly targeted these devices to cause impact to critical infrastructure, as these devices were difficult to patch and generic default credentials were found being used in many of these devices.

- **Cryptominers and ransomware were the two most fast-growing malware categories exploiting new vulnerabilities in H1 2021, accounted for 52% of new malware found**. The growing trend was expected to continue.

Source: Skybox Security

[44] https://www.skyboxsecurity.com/resource/vulnerability-threat-trends-midyear-report-2021/

Industry Insight on Cyber Security Threat Trends

In the first half of 2021, nearly 40% of Internet traffic were from bad bots

Barracuda Networks published the "Bot attacks: Top Threats and Trends"[45] report, which summarised the analysis on traffic patterns of first half of 2021. The key findings were:

- **Bad bots accounted for 39% of Internet traffic in H1 2021.** Activities performed by these bad bots included basic web scraping, price scraping, inventory hoarding, account takeover attacks, distributed denial of service (DDoS) attacks, etc. Some of them were advanced persistent bots which mimic human Internet browsing behaviour to evade detection and more targeted on e-commerce applications and login portals.
- **North America accounted for 67% of bad bot traffic.** Most of the bad bot traffic came from IP ranges of data centers, even though bad bot traffic from Virtual Private Server (VPS) hosting providers or residential IPs was more common in Europe than in North America.
- **Bad bot traffic followed standard workday traffic distribution, as attackers intended to blend within normal human traffic stream to avoid detection.** On the contrary, good bots had a relatively constant traffic rate throughout the day. Tactics used by bad bots included masquerading as legitimate vulnerability scanner to perform reconnaissance and scan for vulnerabilities, brute-forcing or overloading the login page of web sites by fabricating access from common web browsers, and so on.
- Organisations should consider adopting web application firewall (WAF), WAF-as-a-Service solution or anti-bot protection solutions. System administrators should configure their systems properly to protect their web and API applications.

Source: Barracuda Networks

[45] https://www.barracuda.com/bot-threat-report

Highlight of Microsoft September 2021 Security Updates

Product Family	Impact[46]	Severity	Associated KB and / or Support Webpages
Windows 10	Remote Code Execution	Critical ★★★★	KB5005565, KB5005566, KB5005568, KB5005569, KB5005573
Windows 8.1	Remote Code Execution	Critical ★★★★	KB5005563, KB5005613, KB5005627
Windows Server	Remote Code Execution	Critical ★★★★	KB5005563, KB5005565, KB5005568, KB5005573, KB5005575, KB5005607, KB5005613, KB5005623, KB5005627
Microsoft Office-related software	Remote Code Execution	Important ★★★	KB4484103, KB4484108, KB5001958, KB5001997, KB5001999, KB5002003, KB5002005, KB5002007, KB5002009, KB5002014

Note: Only widely-used Microsoft products are listed and it does not mean to be inclusive. For details, please refer to https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Sep.

Learn more:

High Threat Security Alert (A21-09-12): Multiple Vulnerabilities in Microsoft Products (September 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=649)

[46] The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.