GovCERT.HK

Weekly IT Security News Bulletin, 2021-W13

29 March – 4 April 2021

Headlines

Evolving threats from malware

- As revealed in the findings from an analysis conducted by a network security vendor on malware attacks observed in 2020, malware is becoming more advanced by adopting various tactics to evade detection by endpoint protection tools.

- It highlights that a nine-fold increase in fileless malware from previous year was observed in 2020. Unlike the traditional malware which requires malicious payloads to be saved in the victims' local storage, fileless malware only needs a dropper like word document with embedded macro to initiate exploit kits like PowerSploit and CobaltStrike for injecting malicious code into running processes. As the malicious code resides in the system memory, the malware can hardly be detected and stopped. The malware can persist even if the malicious script has been removed from the infected systems.

- Another common way to circumvent detection is to deliver the malware through encrypted channels or through phishing emails from legitimate domains. About half of the attacks observed at the network perimeter in Q4 of 2020 were encrypted. The number of malware sent through HTTPS has increased by 41% and encrypted zero-day variants also increased 22% in Q3. Attackers can host malware in public cloud services or storage with HTTPS connections enabled. Without effective inspection on encrypted traffic and the email content, it can be difficult to block traffic or emails containing malware solely based on domains which can be used for legitimate purposes.

Advice

- Do not open files from untrusted sources and block the execution of macro or scripts embedded in the files.
- Disable PowerShell script execution or only allow trusted scripts which have been digitally signed to execute on your systems.
- Deploy endpoint security protection solutions to detect any malicious scripts or processes running on the system.

Sources

- WatchGuard
- InfoSecurity

Mitigate risks in adopting public cloud

- The Cloud Security Alliance (CSA) published the findings of their recent survey on security concerns and challenges in public cloud usage.

- While over half of the respondent organisations were running over 40% of their workloads in public cloud, many respondents also had concerns over adoption of public cloud, including network security (58%) and staff lack of cloud expertise (47%). To get relief from the shortage of staff expertise and knowledge, many organisations chose to adopt security management tools for better detection of network risks and misconfigurations. They also aimed to obtain higher visibility and automate the change management over security controls in their cloud environment.

- Over 70% respondents adopted the native and additional security controls offered by public cloud service providers and almost 50% used virtual editions of traditional firewalls deployed in the cloud. For the security management tools, about half of the respondents were using cloud native tools and 35% adopted their self-developed scripts leveraging the APIs provided by the public cloud vendors. About 30% chose to manage cloud security by manual processes.

- Among the 11% respondents who have encountered security incidents over the past 12 months, those reported incidents were mainly caused by cloud provider issues (26%), security misconfiguration (22%), security attacks (20%) and network bandwidth issues (16%). The top two causes can be attributed to human error and misconfiguration, echoing the findings of lack of staffing and expertise in respondent organisations.

Advice

- Regularly review the security of public cloud services and ensure proper security controls are in place.
- Establish proper security policies and templates, automate the configuration, and perform regular checks to reduce the risk of misconfiguration.

Sources

- CSA

Massive social media account information exposed online

- Account information including IDs, full names, phone numbers, email addresses, birth dates, location and other sensitive personal data of 553 million Facebook users from over 100 countries was made available online for free. About three million Hong Kong users were believed to be impacted.

- As confirmed by Facebook, the data was leaked in 2019 due to a security bug which was then fixed by Facebook in the same year. Some researchers speculated that malicious actors abused the Facebook's developer API to extract the data before restriction on API access to phone numbers and other data was exerted.

- The leaked data can be used to impersonate the victims and be exploited for carrying out various malicious acts like phishing, social engineering scams, cyberbullying, doxxing and marketing on those victim users. Affected users are reminded to stay alert of any suspicious phone calls, emails or messages. Users may also consider removing the leaked phone numbers from other registered services and change their phone numbers if possible.

- In response to the incident, the Office of the Privacy Commissioner for Personal Data has issued the "Guidance on Protecting Personal Data Privacy in the Use of Social Media ad Instant Messaging Apps", aiming to provide the public with practical advices on how to mitigate the risks associated with social media and instant messaging apps.

Advice

- Developer should monitor and restrict API access to avoid data scrapping by malicious actors.
- Review permission and privacy settings of social media accounts and examine privacy policy and any privacy risks to your personal data.
- Avoid sharing sensitive information on social media or restrict such information to be visible to people on a need basis.

Sources

- Bleeping Computer
- Business Insider
- PCPD

Product Vulnerability Notes & Security Updates

1. **CentOS**

   https://lists.centos.org/pipermail/centos-announce/2021-March/048296.html

2. **Citrix Hypervisor**

   https://support.citrix.com/article/CTX306565

3. **Debian**

   https://www.debian.org/security/2021/dsa-4879
   https://www.debian.org/security/2021/dsa-4880
   https://www.debian.org/security/2021/dsa-4881

4. **F5 F5OS**

   https://support.f5.com/csp/article/K98221124

5. **Gentoo Linux**

   https://security.gentoo.org/glsa/202103-01
   https://security.gentoo.org/glsa/202103-02
   https://security.gentoo.org/glsa/202103-03
   https://security.gentoo.org/glsa/202103-04

6. **Google Chrome**

   https://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_30.html

7. **Oracle Linux**

   https://linux.oracle.com/errata/ELSA-2021-0990.html
   https://linux.oracle.com/errata/ELSA-2021-1002.html
   https://linux.oracle.com/errata/ELSA-2021-1024.html
   https://linux.oracle.com/errata/ELSA-2021-9137.html
   https://linux.oracle.com/errata/ELSA-2021-9140.html
   https://linux.oracle.com/errata/ELSA-2021-9141.html

8. **Red Hat**

   https://access.redhat.com/errata/RHSA-2021:0943
   https://access.redhat.com/errata/RHSA-2021:0956
   https://access.redhat.com/errata/RHSA-2021:0957
   https://access.redhat.com/errata/RHSA-2021:0958
   https://access.redhat.com/errata/RHSA-2021:1002
   https://access.redhat.com/errata/RHSA-2021:1004
   https://access.redhat.com/errata/RHSA-2021:1024
   https://access.redhat.com/errata/RHSA-2021:1028
   https://access.redhat.com/errata/RHSA-2021:1032
   https://access.redhat.com/errata/RHSA-2021:1039

https://access.redhat.com/errata/RHSA-2021:1044
https://access.redhat.com/errata/RHSA-2021:1050
https://access.redhat.com/errata/RHSA-2021:1051

9. Slackware

https://www.slackware.com/security/viewer.php?l=slackware-security&y=2021&m=slackware-security.425248

10. SUSE

https://www.suse.com/support/update/announcement/2021/suse-su-20210966-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210972-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210974-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210975-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210987-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210988-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210989-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210990-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210998-1/
https://www.suse.com/support/update/announcement/2021/suse-su-20210999-1/

11. Trend Micro

https://success.trendmicro.com/solution/000286019
https://success.trendmicro.com/solution/000286157

12. Ubuntu

https://ubuntu.com/security/notices/USN-4896-1
https://ubuntu.com/security/notices/USN-4897-1
https://ubuntu.com/security/notices/USN-4898-1

13. VMware Products

https://www.vmware.com/security/advisories/VMSA-2021-0004.html

14. Xen

https://xenbits.xen.org/xsa/advisory-371.html

Sources of product vulnerability information:

CentOS
Citrix
Debian
F5
Gentoo Linux
Google Chrome
Oracle Linux
Red Hat
Slackware
SUSE

Trend Micro
Ubuntu
VMware
Xen

Contact:

cert@govcert.gov.hk