GovCERT.HK

Weekly IT Security News Bulletin, 2017-W9

27 February – 5 March 2017

Headlines

RATANKBA: Delving into large-scale watering holes against enterprises

- In February 2017, malware infections from legitimate websites onto workstations of enterprises were found in North America, Europe, South America and Asia Pacific regions, notably Taiwan, Hong Kong, China, and Bahrain. The targeted industries also varied and included telecommunications, banking, data centre operations, management consulting, information technology, pharmaceutics, insurance, aviation and education.

- Legitimate and trusted websites frequently visited by potential targets were injected with malicious JavaScript code. Once the target users accessed the compromised websites, the code fingerprinted browser components and loaded corresponding vulnerability exploits, such as those for Adobe Flash, from the attackers' malware and exploit kit-hosting systems. That was a typical watering hole attack strategy.

- The attack performed multistage infection. RATANKBA, one of the initial malware downloaded to the victim, would survey the victim's system information. The final payload would be only delivered to those targets of interest. The infected computers were seen connecting to far-flung locations worldwide, possibly for data exfiltration.

Advice

- Secure websites from malicious injections by timely patching all software and regularly health-checking with vulnerability scanning and/or penetration testing.

- Secure workstations from malware infection by timely patching all software, especially the operating system, web browser and related software such as Adobe Flash.

- Deploy application control and limit user privileges especially when accessing the Internet, which could limit malware activities.

- Employ firewalls and intrusion detection systems on top of proactive network monitoring against data exfiltration.

Sources

- Trend Micro Blog
- PCWorld

Three years after Heartbleed, how vulnerable are you?

- In 2014, a vulnerability in the OpenSSL cryptographic library named "Heartbleed" drove many organisations all over the world into a panic. At the time, both software developers and customers had little knowledge about the open source components being used in their own products or systems. To prevent the same panic, they should understand where the components reside in their products, which of them are vulnerable and which customers are exposed.

- The software development model has changed from mostly homegrown software with a few commercial libraries 10 to 20 years ago to projects using at least 50% open source and all digitally delivered components mostly uneasy to locate in the source tree.

- A current listing of dependencies and bill of materials (BOM) are suggested for organisations to create a list of components used in their systems. By reviewing the BOM against published vulnerabilities of open source components, system administrators should be able to determine whether their systems are affected by the vulnerabilities and be well-prepared to assess the risks, set priorities and take mitigation measures.

Advice

- Understand and document what software components and versions are used in systems.

- Keep the component list updated and regularly check against published vulnerabilities of the component software.

Source

- DarkReading

Product Vulnerability Notes & Security Updates

1. **CentOS**
   https://lists.centos.org/pipermail/centos-announce/2017-February/022287.html
   https://lists.centos.org/pipermail/centos-announce/2017-February/022293.html
   https://lists.centos.org/pipermail/centos-announce/2017-March/022294.html

2. **Cisco Products**
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170301-cpi
   https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170301-nga

3. **Debian**
   https://www.debian.org/security/2017/dsa-3793
   https://www.debian.org/security/2017/dsa-3794
   https://www.debian.org/security/2017/dsa-3795
   https://www.debian.org/security/2017/dsa-3796
   https://www.debian.org/security/2017/dsa-3797
   https://www.debian.org/security/2017/dsa-3798
   https://www.debian.org/security/2017/dsa-3799
   https://www.debian.org/security/2017/dsa-3800

4. **Eaton xComfort Ethernet Communication Interface**
   https://ics-cert.us-cert.gov/advisories/ICSA-17-061-01

5. **F5 Products**
   https://support.f5.com/csp/article/K22216037

6. **IBM WebSphere Application Server**
   https://www.ibm.com/support/docview.wss?uid=swg21999311
   https://www.ibm.com/support/docview.wss?uid=swg21998379
   https://www.hkcert.org/my_url/en/alert/17030101

7. **Mageia**
   http://advisories.mageia.org/MGASA-2017-0063.html
   http://advisories.mageia.org/MGASA-2017-0064.html
   http://advisories.mageia.org/MGASA-2017-0065.html
   http://advisories.mageia.org/MGASA-2017-0066.html
   http://advisories.mageia.org/MGASA-2017-0067.html
   http://advisories.mageia.org/MGASA-2017-0068.html
   http://advisories.mageia.org/MGASA-2017-0069.html

8. **Microsoft Internet Explorer and Edge**
   https://www.hkcert.org/my_url/en/alert/17022701
   https://bugs.chromium.org/p/project-zero/issues/detail?id=1011

9. **openSUSE**
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00042.html
   https://lists.opensuse.org/opensuse-security-announce/2017-02/msg00043.html
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00000.html
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00001.html
   https://lists.opensuse.org/opensuse-security-announce/2017-03/msg00002.html

10. **Oracle Linux**

https://linux.oracle.com/errata/ELSA-2017-0294-1.html
https://linux.oracle.com/errata/ELSA-2017-0307.html
https://linux.oracle.com/errata/ELSA-2017-0309.html
https://linux.oracle.com/errata/ELSA-2017-0323.html
https://linux.oracle.com/errata/ELSA-2017-0323-1.html
https://linux.oracle.com/errata/ELSA-2017-3520.html
https://linux.oracle.com/errata/ELSA-2017-3521.html
https://linux.oracle.com/errata/ELSA-2017-3522.html
https://linux.oracle.com/errata/ELSA-2017-0352.html
https://linux.oracle.com/errata/ELSA-2017-0388.html
https://linux.oracle.com/errata/ELSA-2017-0386.html
https://linux.oracle.com/errata/ELSA-2017-0396.html

11. **Red Hat**

https://access.redhat.com/errata/RHSA-2017:0323
https://access.redhat.com/errata/RHSA-2017:0324
https://access.redhat.com/errata/RHSA-2017:0328
https://access.redhat.com/errata/RHSA-2017:0329
https://access.redhat.com/errata/RHSA-2017:0330
https://access.redhat.com/errata/RHSA-2017:0331
https://access.redhat.com/errata/RHSA-2017:0332
https://access.redhat.com/errata/RHSA-2017:0333
https://access.redhat.com/errata/RHSA-2017:0334
https://access.redhat.com/errata/RHSA-2017:0336
https://access.redhat.com/errata/RHSA-2017:0337
https://access.redhat.com/errata/RHSA-2017:0338
https://access.redhat.com/errata/RHSA-2017:0344
https://access.redhat.com/errata/RHSA-2017:0345
https://access.redhat.com/errata/RHSA-2017:0346
https://access.redhat.com/errata/RHSA-2017:0347
https://access.redhat.com/errata/RHSA-2017:0359
https://access.redhat.com/errata/RHSA-2017:0361
https://access.redhat.com/errata/RHSA-2017:0365
https://access.redhat.com/errata/RHSA-2017:0366
https://access.redhat.com/errata/RHSA-2017:0372
https://access.redhat.com/errata/RHSA-2017:0386
https://access.redhat.com/errata/RHSA-2017:0387
https://access.redhat.com/errata/RHSA-2017:0388
https://access.redhat.com/errata/RHSA-2017:0396
https://access.redhat.com/errata/RHSA-2017:0402
https://access.redhat.com/errata/RHSA-2017:0403
https://access.redhat.com/errata/RHSA-2017:0435
https://access.redhat.com/errata/RHSA-2017:0444

12. **Sage XRT Treasury database**

http://www.kb.cert.org/vuls/id/742632

13. **Schneider Electric Conext ComBox**

https://ics-cert.us-cert.gov/advisories/ICSA-17-061-02

14. **Siemens SINUMERIK Integrate and SINUMERIK Operate**

https://ics-cert.us-cert.gov/advisories/ICSA-17-061-03

15. **Siemens RUGGEDCOM NMS**
    http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-363881.pdf
    https://ics-cert.us-cert.gov/advisories/ICSA-17-059-01

16. **SUSE**
    https://www.suse.com/support/update/announcement/2017/suse-su-20170568-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170569-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170570-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170571-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170575-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170582-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170585-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170586-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170594-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170595-1.html
    https://www.suse.com/support/update/announcement/2017/suse-su-20170596-1.html

17. **Ubuntu**
    https://www.ubuntu.com/usn/usn-3211-2/
    https://www.ubuntu.com/usn/usn-3212-1/
    https://www.ubuntu.com/usn/usn-3213-1/
    https://www.ubuntu.com/usn/usn-3214-1/
    https://www.ubuntu.com/usn/usn-3215-1/

Sources of product vulnerability information:

CentOS
CERT/CC
Cisco
Debian
F5
Google Project Zero
HKCERT
IBM
ICS-CERT
Mageia
openSUSE
Oracle Linux
Red Hat
Simens
SUSE
Ubuntu

Contacts:

cert@govcert.gov.hk