Cybersecurity Threat

April 2023 Newsletter

National Cybersecurity Strategy in the United States and Healthcare

Increased involvement by governments in the cybersecurity landscape has ramped up in late February and early March, with the Biden administration launching its National Cybersecurity Strategy. The healthcare sector is implicitly discussed in the Strategy's increased defenses for critical infrastructure. Regulatory requirements will expand with added emphasis on third-party risk management and vendor accountability.

HHS & HSCC: Cybersecurity Framework Implementation Guide

The US Department of Health and Human Services (HSS) and the Health Sector Coordinating Council (HSCC) have released the Cybersecurity Framework Implementation Guide. It seeks to help healthcare organizations stay on top of threats, vulnerabilities, and controls. It does not replace other programs and is not a roadmap to compliance, but its controls being tightly aligned with the NIST Cybersecurity Framework mark more attention being given to healthcare.

TikTok is a Data Vacuum

TikTok uses aggressive and invasive data collecting techniques. The app makes a fortune (close to $9 billion dollars) in advertising revenue in the USA alone. Advertisers can choose their targets using psychographic microtargeting. The app collects network information, hourly location, unrecorded videos, keystroke cadence, and an inventory of your device's configuration and applications. Over 28,000 apps outside of TikTok contribute to their trove. TikTok gave itself these rights in its 2021 amendments to its privacy policy.

If you must use TikTok, be careful. Here's four immediate steps to take:

1. **Don't share your location.** Deny location sharing in your phone settings and in the app.
2. **Reduce your social network exposure.** Don't sync your contacts or Facebook friends.
3. **Reduce your exposure to advertising.** Turn off in-app ad targeting.
4. **Limit data sharing.** Don't use social login; set up your account with e-mail credentials.
5. **Use TikTok on the Web.** Uninstall the app.

Threat Landscape Shifts

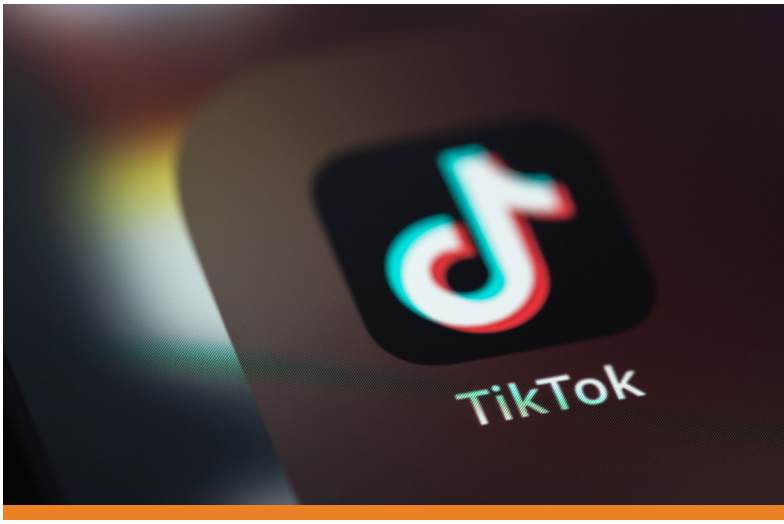
Since the new year, we have seen increased involvement by governments in the cybersecurity landscape. This has ramped up in late February and early March, with the Biden administration launching its National Cybersecurity Strategy. The strategy marks technology as critical infrastructure and clearly defines minimal cybersecurity requirements to be implemented by different industries. Particular attention is given to the defense of critical infrastructure, attached regulations are bound to increase in scope as cyber threats grow as national security issues.

Critical Infrastructure Targeted by Russia

On the anniversary of Russia's invasion of Ukraine, the Canadian Center for Cybersecurity (CCCS) published an alert on cyberattacks against Ukraine's allies. They echo CISA's warnings of increased cyberattacks on governmental agencies and critical infrastructure of nations supporting Ukraine. The CCCS lists defacement of websites and Distributed Denial of Service (DDoS) attacks are likely and contains proactive recommendations.

Healthcare Against North Korean Hackers

CISA has published an alert on increased ransomware attacks on the healthcare infrastructure of Western countries by North Korea-backed hackers. The Maui and H0lyGh0st ransomware campaigns were previously leveraged by Pyongyang to attack US and South Korean hospitals. The alert includes common attacker tactics and techniques as well as preventive and remediation controls.



©2023 Flycast Partners, Inc. All Rights Reserved.

Identified Vulnerabilities and Patches

- A new Microsoft Outlook privilege escalation flaw is being exploited. It is triggered when attackers send a message with extended MAPI properties with UNC path to an SMB on a threat actor-controlled server.

  Our Thoughts: This is serious, but the impact is limited if your firewall doesn't pass internal network traffic (port 445, SMB).

- Fortinet has patched two critical vulnerabilities. The first vulnerability is serious, with a CVSS score of 9.8, and may let an unauthenticated attacker write on the system. The other, scored at 9.3, allows for arbitrary code execution with specialized HTTP requests.

  Our Thoughts: Keeping up with Fortinet's vulnerabilities is tiring – and crucial. Patch and do a hardening exercise on the firewall configuration as well.

- Users of SolarWinds IT services are told to immediately patch five high-severity flaws fixed in late February. The vulnerabilities, rated up to 8.8 on CVSS require admin privileges to execute.

  Our Thoughts: This isn't the SolarWinds supply chain-style breach we saw in 2021 – but remains an issue for organizations using this valuable tool. Remember to patch.

- CISA's Known Exploited Vulnerabilities Catalog was expanded to include flaws in Office, IOS, Windows, and the Cacti framework. CVE-2023-21715 overrides the Microsoft Office Publisher security feature bypass vulnerability. CVE-2022-46169 fixes a command injection vulnerability in Cacti. CVE-2023-21823 and CVE-2023-23376 are respectively a Windows Graphics Component remote code execution flaw and a common log file system driver privilege escalation vulnerability.

  Our Thoughts: These were announced in CISA's Patch Tuesday February updates, and immediate patching was enforced for governmental agencies. Do the same for all exploitable vulnerabilities.

- In February, the GoAnywhere vulnerability, a managed file transfer product licensed by Fortra to large organizations, was used to steal health information for over a million patients. Used at over 3,000 organizations, GoAnywhere exploits cause major damage as it is an unauthenticated remote code exploit. This was used by hackers earlier this month to steal the Social Security numbers from 140,000 customers of HatchBank as well.

  Our Thoughts: Look for alternative products, and patch what you have.

Active Exploits and Threat Actor Updates

- Ads targeted at Chinese-speaking individuals in Southeast and East Asia have been harboring malware. Using the FatalRAT malware, hackers are falsely offering Chinese language software not available in China. Spoofed services include Chrome, Firefox, and Telegram, with the intent being to gain control of the hacked computer.

  Our Thoughts: This is part of a continuing trend of abusing advertising. We will see more. Explore ad-blocking at your DNS, Firewall, and endpoint.

- OneNote Documents are increasingly used to spread, even bypass, the 'disable macros' setting to execute code. Attackers can run scripts and files through the OneNote attachments.

  Our Thoughts: This can be in a Phishing e-mail targeting your employees. Don't open OneNote attachments through e-mails.

- CCCS has issued an alert on a rise in Qakbot malware incidents. This malware, used by cyber criminals like the Russian group Black Basta, targets North American corporations. The alert describes tactics and techniques. Infections lead to ransomware or credential theft – attackers can deploy other tools like Cobalt Strike and Brute Ratel for further compromise.

  The Emotet malware also has returned after a three-month hiatus. Look for fake bills and invoices often sent as .zip files. Threat actors pad the files with data to hide Emotet and bypass modern antivirus software.

  Our Thoughts: It is commonly delivered by phishing emails sent from known or unknown email addresses. Use awareness training to inform at-risk privileged users, and ensure you have top-grade email filtering in place.

- The BlackLotus UEFI bootkit has been upgraded by threat actors to bypass Secure Boot. BlackLotus is exploiting a flaw from 2022, tracked as CVE-2022-21894, to set up persistence in the bootkit. Microsoft had patched the flaw, but its exploitation is still possible and done in the wild.

  Our Thoughts: This new technique is concerning but can be addressed by patching.

©2023 Flycast Partners, Inc. All Rights Reserved.