Cutting Through the Cybersecurity Noise

Here's what's important this week: September 10th, 2021

Take Action

- This is your friendly reminder to sign up for this month's Cyber Threat Brief! We have a new, revamped format, so we hope to see you on the 4th Thursday of this month! Sign-Up link: https://register.gotowebinar.com/register/1562816556709846030
- People implement security in various ways. For programmers, security is through coding practices. The Hacker News created a cute article with fun descriptions about hardening the code of imbedded systems, such as your smart toaster. The article talks about why people may worry about their IoT, why coding practices for IoT is specialized, and how people can learn about finding code vulnerabilities on a practice/game platform called secure code warrior.
  Note: This analyst has not tried the game, but it looks nice.
  Reference: https://thehackernews.com/2021/09/fighting-rogue-toaster-army-why-secure.html
- The Open Web App Security Project (OWASP) released a peer review draft for 2021's top 10 most exploited web application security vulnerabilities! For anyone who has interest in supporting the research, you may want to have a look.
  Reference: https://owasp.org/Top10/

Be Aware

- The REvil's "Happy Blog", the ransomware operator's blog, was taken down after they hacked Kaseya. The group and its websites have since gone dark, until recently. The Happy Blog is available again, as of September 7th, and likely means compromises involving REvil's ransomware will start happening, again.
  Reference:
  - https://www.flashpoint-intel.com/blog/revil-is-back-on-exploit-and-trying-to-restore-its-reputation/
  - https://thehackernews.com/2021/09/russian-ransomware-group-revil-back.html
  - https://www.bleepingcomputer.com/news/security/revil-ransomwares-servers-mysteriously-come-back-online/

Arizona Cyber Trends

This Week's Trends

The AZSOC, a member of AZ-ISAC, received alerts of an executable called the "wavebrowser.exe". The wavebrowser process starts another executable called "SWUpdaterSetup.exe", which reaches out to "swupdate[.]com". These sets of files are likely to get blocked when run, but they have been found on a surprising quantity of machines.

IOCS for the event at this time:

SWUpdaterSetup.exe

adae512e5a87c04e2c7e7c8c953c2a802b38b8510cc9bd42620f7afc92c93eef

wavebrowser.exe
a781d948a8f5153fb2104d839f40cf92879ad36160bbeb74b48b3ce4a3657fff

Domain:
swupdater[.]com

IPs:
52.200.14.37
23.20.8.233

At this time AZSOC has requested a global block for the IPs observed. If you find these files on your system, one possible solution may also be to simply delete the files.
AZSOC found an article on WebNavgatorBrowser by Crowdstrike and it looks like WaveBrowser could be a "rebranded" name.

If you would like to receive IOCs like this, as they come in, please ask us about becoming a partner with AZ-ISAC to receive these IOCs through the Malware Information Sharing Platform (MISP)!

Reference: https://www.crowdstrike.com/blog/webnavigationbrowser-adware-analysis-and-recommendations/

Reminders

Report potential, suspected, and/or confirmed cyber threats to the ACTIC via:

- https://www.azactic.gov/Tips/
- ACTIC@AZDPS.GOV
- ACIP@AZDPS.GOV
- (602) 644-5805 or (877) 2 S A V E A Z (272- 8329)

* If links don't come through, cut and paste all referenced URLs into your browser to access the sites.