Chris Lamb: Free software activities in July 2021

One of the original promises of open source software is that distributed peer review and transparency of process results in enhanced end-user security. However, whilst anyone may inspect the source code of free and open source software for malicious flaws, almost all software today is distributed as pre-compiled binaries. This allows nefarious third parties to compromise systems by injecting malicious code into ostensibly secure software during the various compilation and distribution processes. The motivation behind the Reproducible Builds effort is to ensure no flaws have been introduced during this compilation process by promising identical results are always generated from a given source, thus allowing multiple third-parties to come to a consensus on whether a build was compromised.

[...]

As part of my role of being the assistant Secretary of the Open Source Initiative and a board director of Software in the Public Interest I attended their respective monthly meetings. As outlined in last months posts, however, my term on the OSI board has been slightly extended due to the discovery of a vulnerability in OSI's recent election - as a result, the 2021 election is currently being re-run.

Aaron Portnoy - ?There?s no silver bullet for ransomware or supply chain attacks? [3] [Ed: When you receive packages from Microsoft/GitHub/NPM you're basically begging for malware. Not just PRISM; Microsoft literally brings people from the NSA to run GitHub/NPM.]

This Week In Security: Fail2RCE, TPM Sniffing, Fishy Leaks, And Decompiling | Hackaday [4]
Fail2ban is a great tool for dynamically blocking IP addresses that show bad behavior, like making repeated login attempts. It was just announced that a vulnerability could allow an attacker to take over a machine by being blocked by Fail2ban. The problem is in the mail-whois action, where an email is sent to the administrator containing the whois information. Whois information is potentially attacker controlled data, and Fail2ban doesn’t properly sterilize the input before piping it into the mail binary. Mailutils has a feature that uses the tilde key as an escape sequence, allowing commands to be run while composing a message. Fail2ban doesn’t sanitize those tilde commands, so malicious whois data can trivially run commands on the system. Whois is one of the old-school unix protocols that runs in the clear, so a MitM attack makes this particularly easy. If you use Fail2ban, make sure to update to 0.10.7 or 0.11.3, or purge any use of mail-whois from your active configs.

- **Ransomware Changes: DoppelPaymer Rebrands; Babuk Evolves**[5]

  One example is the DoppelPaymer - aka DopplePaymer - ransomware-as-a-service operation, which has gone relatively quiet since early May, posting no victims to its data leak site since May 6 and no leaked files since June 25. But one expert says the operation appears to have been rebranded by its operator, Evil Corp, in an attempt to avoid sanctions imposed on the crime group in December 2019 by the U.S. Treasury Department’s Office of Foreign Assets Control.

  The Babuk ransomware operation also recently appears to have altered its approach - if not splintered - following its late-April ransomware attack against the Metropolitan Police Department of Washington, D.C.

- **The Week in Ransomware - July 30th 2021 - €1 billion saved**[6]

  We also saw ransomware groups continue to innovate with LockBit 2.0 now using group policies to automate the deployment of their ransomware over a Windows domain.

  I shared what I know about the inner conflict of the Babuk ransomware gang...

- **Secure applications with Keycloak authentication tool**[7] [Ed: Is this journalism or "sales"?]

---

**Security**

**Source URL:** [http://www.tuxmachines.org/node/154019](http://www.tuxmachines.org/node/154019)

**Links:**

[1] [http://www.tuxmachines.org/taxonomy/term/59](http://www.tuxmachines.org/taxonomy/term/59)
[3] https://portswigger.net/daily-swig/aaron-portnoy-there-is-no-silver-bullet-for-ransomware-or-supply-chain-attacks