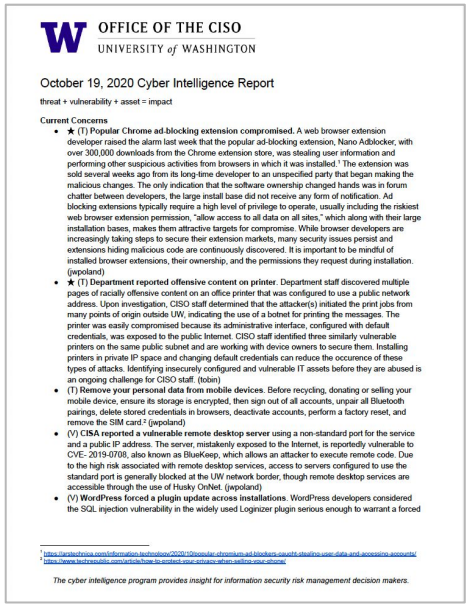
Web Security Shorts

News Bytes for November 2020

UNIVERSITY *of* WASHINGTON

News bytes?



OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

October 19, 2020 Cyber Intelligence Report

threat + vulnerability + asset = impact

Current Concerns

- ★ (T) **Popular Chrome ad-blocking extension compromised.** A web browser extension developer raised the alarm last week that the popular ad-blocking extension, Nano Adblocker, with over 300,000 downloads from the Chrome extension store, was stealing user information and performing other suspicious activities from browsers in which it was installed.[1] The extension was sold several weeks ago from its long-time developer to an unspecified party that began making the malicious changes. The only indication that the software ownership changed hands was in forum chatter between developers, the large install base did not receive any form of notification. Ad blocking extensions typically require a high level of privilege to operate, usually including the riskiest web browser extension permission, "allow access to all data on all sites," which along with their large installation bases, makes them attractive targets for compromise. While browser developers are increasingly taking steps to secure their extension markets, many security issues persist and extensions hiding malicious code are continuously discovered. It is important to be mindful of installed browser extensions, their ownership, and the permissions they request during installation. (jwpoland)
- ★ (T) **Department reported offensive content on printer**. Department staff discovered multiple pages of racially offensive content on an office printer that was configured to use a public network address. Upon investigation, CISO staff determined that the attacker(s) initiated the print jobs from many points of origin outside UW, indicating the use of a botnet for printing the messages. The printer was easily compromised because its administrative interface, configured with default credentials, was exposed to the public Internet. CISO staff identified three similarly vulnerable printers on the same public subnet and are working with device owners to secure them. Installing printers in private IP space and changing default credentials can reduce the occurence of these types of attacks. Identifying insecurely configured and vulnerable IT assets before they are abused is an ongoing challenge for CISO staff. (tobin)
- (T) **Remove your personal data from mobile devices**. Before recycling, donating or selling your mobile device, ensure its storage is encrypted, then sign out of all accounts, unpair all Bluetooth pairings, delete stored credentials in browsers, deactivate accounts, perform a factory reset, and remove the SIM card.[2] (jwpoland)
- (V) **CISA reported a vulnerable remote desktop server** using a non-standard port for the service and a public IP address. The server, mistakenly exposed to the Internet, is reportedly vulnerable to CVE- 2019-0708, also known as BlueKeep, which allows an attacker to execute remote code. Due to the high risk associated with remote desktop services, access to servers configured to use the standard port is generally blocked at the UW network border, though remote desktop services are accessible through the use of Husky OnNet. (jwpoland)
- (V) **WordPress forced a plugin update across installations**. WordPress developers considered the SQL injection vulnerability in the widely used Loginizer plugin serious enough to warrant a forced

[1] https://arstechnica.com/information-technology/2020/10/popular-chromium-ad-blockers-caught-stealing-user-data-and-accessing-accounts/
[2] https://www.techrepublic.com/article/how-to-protect-your-privacy-when-selling-your-phone/

The cyber intelligence program provides insight for information security risk management decision makers.

Taken from CISO's weekly Cyber Intelligence Report

- ✓ Curated to be relevant - issues likely to affect UW
- ✓ Helpful in improving our *situational awareness*
- ✓ Guaranteed to make you more interesting at your next Zoom happy hour

Blocking Ads, But Suddenly Bad

Popular Chrome ad-blocking extension compromised

UNIVERSITY of WASHINGTON

What happened?

- **Nano Adblocker**, with *over 300,000 downloads,* began stealing user info and exhibiting other suspicious behavior.
  "...end users noticed that infected browsers were automatically issuing likes for large numbers of Instagram posts, with no input from users"
- Extension was sold recently to an undisclosed party
- Aside from a developer forum, sale was largely unknown

https://arstechnica.com/information-technology/2020/10/popular-chromium-ad-blockers-caught-stealing-user-data-and-accessing-accounts/

Key bits

- Ad blocking extensions typically require a high degree of privilege to operate
- Browser extensions can be used to house malicious code
- Ownership of an extension (and the extension's overall intent) can change with little or no notice

What's to be done?

- Be judicious when choosing to use a browser extension.
  - ✓ Do you really need it?
  - ✓ Has the ownership changed?
  - ✓ Has there been a sudden change in reviews?
- Be aware of the permissions an extension initially requests.
  - ✓ Are they reasonable for the task(s) the extension is expected to perform?
  - ✓ Are they within your privacy and security comfort zone?
- Regularly audit your extensions and delete those you no longer use

Trust in The Force(d update)

WordPress forces plugin update across installations

UNIVERSITY *of* WASHINGTON

What happened?

- Wordpress developers discovered an SQL injection vulnerability in the **Loginizer** security plugin
- Deemed serious enough to forcibly (and somewhat controversially) push a security update
- According to a WP developer, the “lesser-known internal capability” to force an update has only been used five times since 2013.

https://www.zdnet.com/article/wordpress-deploys-forced-security-update-for-dangerous-bug-in-popular-plugin/

Key bits

- Wordpress plugins (like browser extensions) can be security threats (even the *security* plugins!)
- Plugins can change ownership, and can also be abandoned, unmaintained, and increasingly vulnerable.
- Not sure what an “SQL Injection” vulnerability or “unsanitized user input” is? We (CISO) have a remedy for that.

What's to be done?

- Be judicious when choosing to use a plugin on your site
  - ✓ Do you really need it?
  - ✓ Has the ownership changed?
  - ✓ Are there known security issues? Have previous issues been resolved, and if so, how quickly?
- Regularly audit your plugins and delete those you no longer use
- The same considerations can be applied to code libraries
- If you're a developer, learn secure coding practices (again, CISO can help)

Hi, it’s your boss, send money now!

Email fraud attempts continue

UNIVERSITY of WASHINGTON

What happened?

- Fraudster posing as academic association president contacted the group's treasurer, a UW faculty member, requesting a financial transfer.
- During a brief email exchange, the treasurer noticed the sender's email address was not correct.
- The attacker likely used publicly available information on the association's "About" page.

Key bits

- Humans are still the easiest path to committing cybercrime
- Email remains a highly effective tool for cybercriminals
- Public info is often used for fraud attempts
- Anyone who appears to work with money is more likely to see such attempts

What's to be done?

- Be a perpetually skeptical email user. Watch for:
  - ✓ Requests, especially *anything* related to money
  - ✓ Conveyed urgency
  - ✓ Misspellings, grammatical mistakes, strange email addresses
  - ✓ Links and attachments!
- When in doubt, verify (*not* by email please)
- Be intentional about what info you and/or your team posts online
- Be a conscientious email creator
  - ✓ Avoid links when possible, especially shortened links
- Use CISO's phishing resources

More things you can do right now

Check out CISO training resources

The Office of the CISO has produced and accumulated materials to educate you on cybersecurity. They're both awesome and free!

- Online training: https://ciso.uw.edu/education/online-training/
- Risk Advisories and Best Practices: https://ciso.uw.edu/education/risk-advisories/
- Infographics: https://ciso.uw.edu/education/infographics/

And much, much more.

Become a security advocate

A Community of Practice for people with an interest in learning about and promoting a culture of cybersecurity throughout the UW

- Work with the Office of the CISO to develop and promote best practices and awareness
- Build relationships, exchange information, collaborate, share expertise, and help us all reduce risk

Email **ciso@uw.edu** with "**Advocates**" in the subject line.

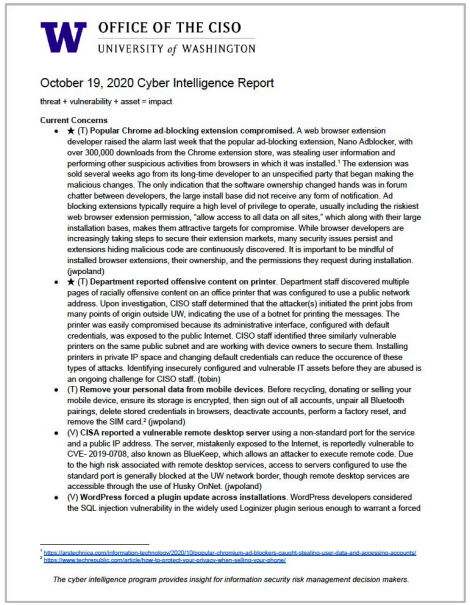
Take a secure coding class

Web App Security 101: Thinking Like an Attacker

- Get hands-on experience hacking a vulnerable web application
- Explore common vulnerabilities such as XSS, SQL injection, and web parameter tampering
- 3 hours
- Now, for a limited time, all online!
- Next session: **Weds, 12/9, 9 a.m. to noon** (limited seats)

Contact Pete Graff (UW-IT Slack or pgraff@uw.edu)

Subscribe to CISO's weekly cyber intelligence report



OFFICE OF THE CISO
UNIVERSITY of WASHINGTON

October 19, 2020 Cyber Intelligence Report

threat + vulnerability + asset = impact

Current Concerns

- ★ (T) **Popular Chrome ad blocking extension compromised.** A web browser extension developer raised the alarm last week that the popular ad-blocking extension, Nano Adblocker, with over 300,000 downloads from the Chrome extension store, was stealing user information and performing other suspicious activities from browsers in which it was installed.[1] The extension was sold several weeks ago from its long-time developer to an unspecified party that began making the malicious changes. The only indication that the software ownership changed hands was in forum chatter between developers, the large install base did not receive any form of notification. Ad blocking extensions typically require a high level of privilege to operate, usually including the riskiest web browser extension permission, "allow access to all data on all sites," which along with their large installation bases, makes them attractive targets for compromise. While browser developers are increasingly taking steps to secure their extension markets, many security issues persist and extensions hiding malicious code are continuously discovered. It is important to be mindful of installed browser extensions, their ownership, and the permissions they request during installation. (jwpoland)
- ★ (T) **Department reported offensive content on printer**. Department staff discovered multiple pages of racially offensive content on an office printer that was configured to use a public network address. Upon investigation, CISO staff determined that the attacker(s) initiated the print jobs from many points of origin outside UW, indicating the use of a botnet for printing the messages. The printer was easily compromised because its administrative interface, configured with default credentials, was exposed to the public Internet. CISO staff identified three similarly vulnerable printers on the same public subnet and are working with device owners to secure them. Installing printers in private IP space and changing default credentials can reduce the occurence of these types of attacks. Identifying insecurely configured and vulnerable IT assets before they are abused is an ongoing challenge for CISO staff. (tobin)
- (T) **Remove your personal data from mobile devices**. Before recycling, donating or selling your mobile device, ensure its storage is encrypted, then sign out of all accounts, unpair all Bluetooth pairings, delete stored credentials in browsers, deactivate accounts, perform a factory reset, and remove the SIM card.[2] (jwpoland)
- (V) **CISA reported a vulnerable remote desktop server** using a non-standard port for the service and a public IP address. The server, mistakenly exposed to the Internet, is reportedly vulnerable to CVE- 2019-0708, also known as BlueKeep, which allows an attacker to execute remote code. Due to the high risk associated with remote desktop services, access to servers configured to use the standard port is generally blocked at the UW network border, though remote desktop services are accessible through the use of Husky OnNet. (jwpoland)
- (V) **WordPress forced a plugin update across installations**. WordPress developers considered the SQL injection vulnerability in the widely used Loginizer plugin serious enough to warrant a forced

[1] https://arstechnica.com/information-technology/2020/10/popular-chromium-ad-blockers-caught-stealing-user-data-and-accessing-accounts/
[2] https://www.techrepublic.com/article/how-to-protect-your-privacy-when-selling-your-phone/

The cyber intelligence program provides insight for information security risk management decision makers.

Provides UW risk management decision makers with *curated and distilled* intelligence related to UW information security assets, threats, and vulnerabilities.

Email **ciso@uw.edu** with "**Cyber Intelligence Report**" in the subject line.

Thank you! Questions?

Peter Giles
gilesp@uw.edu

Pete Graff
pgraff@uw.edu

Jeane Marty
jeanem@uw.edu