On August 2, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability in Ivanti Endpoint Manager.
CIS Security Advisories

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN
04 August 2023

In The News This Week

Russia's Cozy Bear is back and hitting Microsoft Teams to phish top targets

An infamous Kremlin-backed gang has been using Microsoft Teams chats in attempts to phish marks in governments, NGOs, and IT businesses, according to the Windows giant. In its latest crime spree, a crew that Microsoft Threat Intelligence now tracks as Midnight Blizzard uses previously compromised Microsoft 365 tenants to create domains that masquerade as organizations offering tech support. The gang then uses these domains to send Teams chat messages to targets in hope they follow links to webpages that phish their credentials – trick victims into entering their login details, basically. Microsoft used to call this group Nobelium, while other security researchers track the Russian gang as APT29 or Cozy Bear...
Read the rest of the story by Jessica Lyons Hardcastle here: The Register

Malicious Apps Use Sneaky Versioning Technique to Bypass Google Play Store Scanners

Threat actors are leveraging a technique called versioning to evade Google Play Store's malware detections and target Android users. "Campaigns using versioning commonly target users' credentials, data, and finances," Google Cybersecurity Action Team (GCAT) said in its August 2023 Threat Horizons Report shared with The Hacker News. While versioning is not a new phenomenon, it's sneaky and hard to detect. In this method, a developer releases an initial version of an app on the Play Store that passes Google's pre-publication checks, but is later updated with a malware component. This is achieved by pushing an update from an attacker-controlled server to serve malicious code on the end user device using a method called dynamic code loading (DCL), effectively turning the app into a backdoor... Read the full article here: The Hacker News

Hackers Released New Black Hat AI Tools XXXGPT and Wolf GPT

A hacker forum user was found to be promoting a malicious ChatGPT variant, boasting several illicit features dubbed "XXXGPT." While on the other hand, security analysts also discovered another black hat AI tool dubbed "Wolf GPT." Wolf GPT is a Python-built alternative to ChatGPT that promises complete confidentiality with multitudes of malicious intentions. Apart from this, the developers of these black hat AI tools claim that these tools are completely sophisticated and advanced, equipped with several revolutionary features and services. Specifically, the XXXGPT developers claim that they have backed their tool with a team of five experts mainly tailored to your project... Read the rest of the article here: Cyber Security News

New Version of Rilide Data Theft Malware Adapts to Chrome Extension Manifest V3

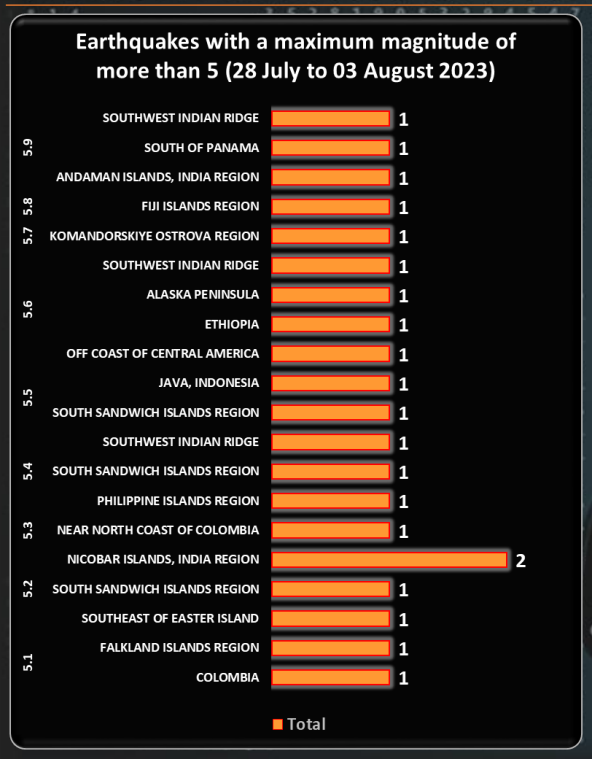
Cybersecurity researchers have discovered a new version of malware called Rilide that targets Chromium-based web browsers to steal sensitive data and steal cryptocurrency. "It exhibits a higher level of sophistication through modular design, code obfuscation, adoption to the Chrome Extension Manifest V3, and additional features such as the ability to exfiltrate stolen data to a Telegram channel or interval-based screenshot captures," Trustwave security researcher Pawel Knapczyk said in a report shared with The Hacker News. Rilide was first documented by the cybersecurity company in April 2023, uncovering two different attack chains that made use of Ekipa RAT and Aurora Stealer to deploy rogue browser extensions capable of data and crypto theft. It's sold on dark web forums by an actor named "friezer" for $5,000...
Read the full story by THN here: The Hacker News

Quarter of a million profiles hacked in British Columbia healthcare data breach

Hackers targeting organizations that employ healthcare workers in BC may have stolen the personal information of up to 240,000 individuals. The Health Employers Association of BC announced Tuesday it's dealing with the impacts of an illegal cyber-security attack on its servers that saw the information associated with nearly 240,000 email addresses be taken. The information accessed could include birthdates, social insurance numbers, passport information, driver's licences, education credentials, investigative reports, and other information about employees' dealings with affected programs. The breached servers belonged to Health Match BC, the BC Care Aide and Community Health Worker Registry, and the Locums for Rural BC program. The attack does not impact wider healthcare records for British Columbians who didn't use these programs...
Read the rest of the article by Megan Devlin here: DailyHive

Cyber attack forces Tempur Sealy to shut down its IT systems

LEXINGTON, Ky. – Tempur Sealy International had to shutter parts of its IT systems as a result of a "cybersecurity event" that hit July 23. The company said the shut down caused a "temporary interruption" of its operations. Legal counsel, a cybersecurity forensic firm and other incident response professionals have been hired to advise Tempur Sealy, and law enforcement agencies have been contacted. A number of Tempur Sealy retailers reached out to Furniture Today saying they had been unable to submit orders and had not received shipments. Read more here: Furniture Today



For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Web Browser Extensions, what information are you sharing?

All Internet browser software instances have some limitations in how the general user perceives and use it. This is where Browser Extensions come in. It is generally an interface provided by browsers like Google, Edge, Brave, Firefox, etc., for third-party software developers to create and implement their own browser enhancements or specific functionality for their software. This is in essence a good idea and there are tons of really good browser extensions available for whoever wants to use it. However, there is also the risk of unscrupulous developers that build in ways to siphon off various bits of data that can include usage data or even personally identifiable data with or without your consent. The question is, what are we sharing, and how can we manage it?

There has been a lot of media attention on the subject in the last few weeks and I thought it would be a good idea to share some insights this week. The content below is mostly covering Google Chrome as it is the most popular browser, but whatever browser you use, the principles will be the same.

How to Check If You're Using Malicious Chrome/Browser Extensions

Unfortunately, there's no single test you can run to check for malicious Chrome or other browser extensions. Instead, you have to keep an eye on all the extensions you've downloaded and look out for anything suspicious. Here's a quick review of the most important things to look out for:

- **Page redirects**: You're automatically redirected to a different website when you type in a URL.
- **Sudden increase in ads**: Especially a sudden increase in pop-up ads on websites you wouldn't normally expect.
- **Scareware**: Pop-ups that warn your device is infected and ask you to click through for removal.
- **Malvertising**: A seemingly legit extension asks you to download another extension outside of the Chrome Web Store.
- **Slow browser performance**: Your web browser takes significantly longer than usual to perform standard actions like loading web pages.
- **Malicious extension reports**: Keep tabs on reports of malicious Chrome extensions in the press, and uninstall anything dodgy.
- **Extension listing**: Chrome is pretty quick to remove dodgy extensions from its web store, once they're reported–so regularly check the listing pages for any extensions you use.
- **Extension reviews**: Also, keep an eye on reviews for all the extensions you use to look for any reports of malicious behavior.
- **Extension updates**: Monitor the date of the most recent updates to check developers are still supporting your extensions.

Although browser extensions can enhance your browsing experience, the bottom line is, try and use as little of them as possible.

How to Remove Extensions From Chrome

To remove browser extensions from Chrome, open up a new browser window on your computer and click the three dots ⋮ to the right of the address bar. On the following dropdown menu, click **Extensions > Manage Extensions** to access all the extensions stored in your browser.
Here, you can view all of your Chrome extensions in one place and check things like permissions by clicking on the **Details** button.
You can also activate or deactivate extensions by clicking the toggle switch at the bottom-right of each tab. This is helpful if you suspect one of your extensions is malicious, and you want to isolate them to identify the culprit.

What to Do After Removing Malicious Chrome Extensions

Now that you've identified and removed any malicious Chrome extensions, you want to take some precautionary steps to protect your device.

(1) **Update Google Chrome** - Make sure you're running the latest version of Google Chrome. Most browser updates add security upgrades and fix minor bugs so it's a good idea to regularly update Chrome or turn on automatic updates. You can do this by opening up Chrome on your computer and selecting the three-dot icon to the right of the address bar. Then, click **Settings > About Chrome > Automatically update Chrome** for all users. This allows Chrome to automatically update your browser when you close and relaunch it. Keep in mind that, if you keep the Chrome app open for extended periods of time, you'll have to manually run updates. You'll know when an update is ready, though, as Chrome adds an Update button next to the three-dot icon.

(2) **Run a Safety Check in Chrome** - Now that you're running the latest version of Chrome, it's time to run a safety check. In Chrome, click the three-dot icon to the right of the address bar and select **Settings > Privacy and security**. On the next page, you'll see a section called Safety check, and you can start the scan by clicking the **Check now** button. The check only takes a few seconds and the results will pop up on-screen once the check is done. You'll see it scans for any harmful extensions and also check that you're running the latest version of Chrome, have safe browsing turned on, and whether you've got any password compromises.

(3) **Scan Your Device With Antivirus Software** - After removing a malicious Chrome extension, you want to make sure your device is clean. Choosing the best AV (antivirus) software for your needs can feel overwhelming. Keep in mind that the prevalence and severity of security threats are increasing all the time, and quality antivirus software is often the last line of defence against attacks. Although there are many free AV offerings out there, bear in mind that being free, it will only have basic scanning functionality.

(4) **Only Download Extensions From the Chrome Web Store** - Always download Chrome extensions from the official Chrome Web Store. Never download extensions from third-party websites, even if you're getting the extension directly from the developer. Trusted providers should always link to the extension page on the Chrome Web Store. For example, if you visit the Chrome extension page on NordVPN's website and click on Add to Chrome, it links to the extension page on the Chrome Web Store. If a website ever tries to install an extension to your browser directly (not via the Chrome Web Store), uninstall it immediately.

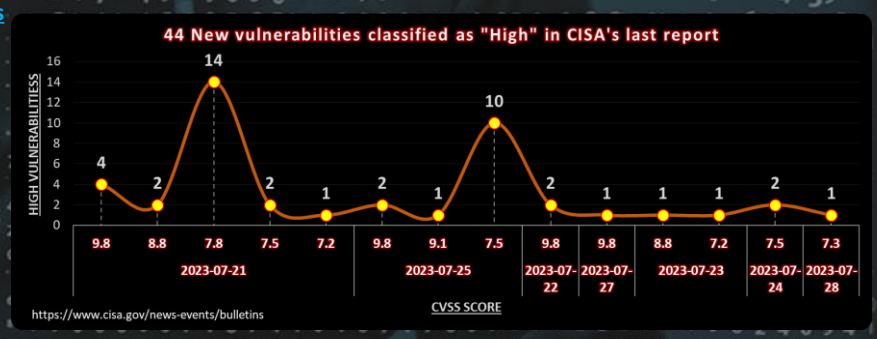
(5) **5. Manage Chrome Extension Permissions** - Even with legitimate extensions, you can review and manage permissions for Chrome extensions to make sure they're not doing anything you're uncomfortable with. When you download a new extension from the Chrome Web Store, you should see a pop-up explaining which permissions it needs to operate. Read these carefully and make sure the purpose of the extension justifies these permission requests–especially when it states: "Read and change all your data on all websites". You can also review these permissions for existing extensions by returning to the extension management page and clicking on Details. Scroll down to Permissions and you can review the permissions the extension requires to operate correctly.

That is all I have space for in this post, please check out the following resources to learn more: MUO, Cyber News, The Sun, eSecurity, HyperText

Other Interesting News and Cyber Security bits:

- What are Self-Driving Cars and How Do They Work?
- How Do Fuel Cell Electric Vehicles Work Using Hydrogen?
- Who's Hacked? Latest Data Breaches And Cyberattacks (Cybercrime Magazine)
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
IRIS Interactive Earthquake Map
Marine Traffic
SatelliteXplorer Track satellites in orbit



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com