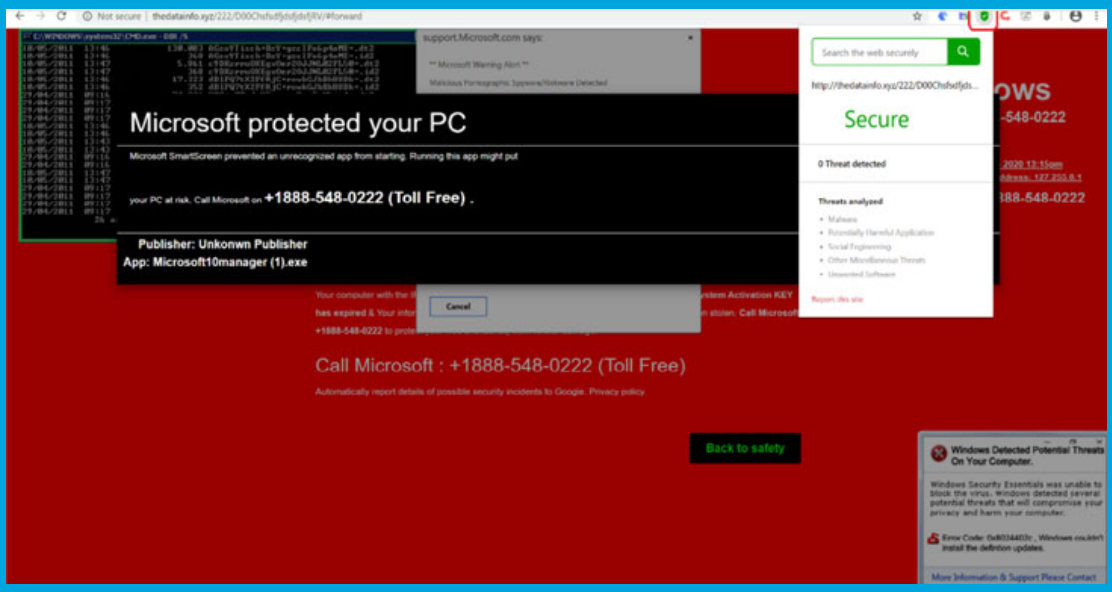
Security Newsletter

29 June 2020

Subscribe to this newsletter

Over 100 New Chrome Browser Extensions Caught Spying On Users



Google recently removed 106 more extensions from its Chrome Web Store after they were found illegally collecting sensitive user data as part of a "massive global surveillance campaign" targeting oil and gas, finance, and healthcare sectors. "This campaign and the Chrome extensions involved performed operations such as taking screenshots of the victim device, loading malware, reading the clipboard, and actively harvesting tokens and user input," Awake Security said.

The extensions in question posed as utilities offering capabilities to convert files from one format to the other, among other tools for secure browsing, while relying on thousands of fake reviews to trick unsuspecting users into installing them. In total, the extensions were downloaded nearly 33 million times over the course of three months before Awake Security reached out to Google in May.

Telemetry data has revealed that some of these extensions were active on the networks of "financial services, oil and gas, media and entertainment, healthcare and pharmaceuticals, retail, high-tech, higher education, and government organizations," although there's no evidence that they were actually used to collect sensitive data. It's recommended that users review extension permissions by visiting "chrome://extensions" on the Chrome browser, consider uninstalling those that are rarely used, or switch to other software alternatives that don't require invasive access to browser activity.

Read More on TheHackerNews

Turn on MFA Before Crooks Do It For You

Hundreds of popular websites now offer some form of multi-factor authentication (MFA), which can help users safeguard access to accounts when their password is breached or stolen. But people who don't take advantage of these added safeguards may find it far more difficult to regain access when their account gets hacked, because increasingly thieves will enable multi-factor options and tie the account to a device they control. Here's the story of one such incident.

Read More on KrebsOnSecurity

When Security Takes a Backseat to Productivity

[redacted]

Intelligence Brief

Intelligence Brief | 17 October 2017

[redacted] Memo To: Director, Central Intelligence Agency
Deputy Director, Central Intelligence Agency
Chief Operating Officer, Central Intelligence Agency

[redacted] From: WikiLeaks Task Force, [redacted]

[redacted] Subject: WikiLeaks Task Force Final Report

So ends a key section of a report the U.S. Central Intelligence Agency produced in the wake of a mammoth data breach in 2016 that led to Wikileaks publishing thousands of classified documents stolen from the agency's offensive cyber operations division. The analysis highlights a shocking series of security failures at one of the world's most secretive entities, but the underlying weaknesses that gave rise to the breach also unfortunately are all too common in many organizations today.

The CIA acknowledged its security processes were so "woefully lax" that the agency probably would never have known about the data theft had Wikileaks not published the stolen documents online. What kind of security failures created an environment that allegedly allowed a former CIA employee to exfiltrate so much sensitive data? Here are a few, in no particular order: Failing to rapidly detect security incidents; Moving too slowly to enact key security safeguards; No effective removable media controls. No single person empowered to ensure IT systems are built and maintained securely throughout their lifecycle ...

A key phrase in the CIA's report references deficiencies in "compartmentalizing" cybersecurity risk. At a high level (not necessarily specific to the CIA), compartmentalizing IT environments involves important concepts such as: Segmenting one's network so that malware infections or breaches in one part of the network can't spill over into other areas; Not allowing multiple users to share administrative-level passwords, etc.

Read More on KrebsOnSecurity

More #News

- How Apple Resolves the Problem of Apps Secretly Accessing Your Clipboard
- Maersk, me & notPetya

- DDoS botnet coder gets 13 months in prison
- Apple adds support for encrypted DNS (DoH and DoT)
- Chinese bank forced western companies to install malware-laced tax software
- New Lucifer DDoS malware creates a legion of Windows minions
- US Now Accuses Assange of Conspiring With Hacking Groups
- Docker Images Containing Cryptojacking Malware Distributed via Docker Hub
- Sony launches PlayStation bug bounty program with $50K+ rewards
- Microsoft releases first public preview of its Defender antivirus on Android
- 80,000 printers are exposing their IPP port online
- Office 365 now checks docs for known threats before editing
- BlueLeaks data dump exposes over 24 years of police records
- Visa Introduces Advanced Identity Score to Help Financial Institutions Prevent New Account Fraud
- Pwned Passwords, Version 6
- More than 75% of all vulnerabilities reside in indirect dependencies
- Dropbox adds password manager, vault, and other security features

#Patch Time!

- NVIDIA fixes kernel driver holes on Windows and Linux
- Adobe wants users to uninstall Flash Player by the end of the year
- AMD says it will fix new CPU bugs by the end of June 2020
- 79 Netgear router models risk full takeover due to unpatched bug
- Cisco Adds New Security Features to Webex, Patches Serious Vulnerabilities
- Drupal Patches Code Execution Flaw Most Likely to Impact Windows Servers
- Plex fixes Media Server bugs allowing full system takeover
- VLC Media Player 3.0.11 fixes severe remote code execution flaw
- Adobe Patches 18 Critical Code Execution Flaws Across Five Products

#Tech and #Tools

- astNetMon - A high performance DoS/DDoS load analyzer
- Behave!: monitoring browser extension for pages acting as bad boys.
- Detect PHP security vulnerabilities with Psalm
- Hardcoded secrets, unverified tokens, and other common JWT mistakes
- Red Team Techniques - June 2020
- Hashcat 6.0 released: 45% performance improvement on Bcrypt (among others)
- kubernetes-goat: learn and practice Kubernetes security.
- Evasor: A New Pen Test Tool for WindowAppLocker
- Sigma Importer: convert specific data sources into the Sigma generic and open signature format.
- Red Teaming Experiments
- AppLocker best practices
- Lessons learned from the Microsoft SOC—Part 3d: Zen and the art of threat hunting
- Sigma rules! The generic signature format for SIEM systems.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us