CERT-PH Cybersecurity Threat Feeds

Issue Date	February 08, 2021
TLP: GREEN	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

• Microsoft Warns of Increasing OAuth Office 365 Phishing Attacks • Malicious Extension Abuses Chrome Sync to Steal Users' Data • Fortinet Fixes Critical Vulnerabilities in SSL VPN And Web Firewall • Mozilla fixes Windows 10 NTFS Corruption Bug in Firefox	• CRITICAL • URGENT • INFORMATION

Description

Microsoft Warns of Increasing OAuth Office 365 Phishing Attacks

2021.02.05 | Source(s): Bleeping Computer

Analysis:

Microsoft has warned of an increasing number of consent phishing, also known as OAuth phishing, attacks targeting remote workers during recent months. OAuth phishing is an application-based attack variant where the attackers attempt to trick targets into providing malicious Office 365 OAuth apps (web apps registered by the attackers with an OAuth 2.0 provider) with access to their Office 365 accounts. Once access is granted, threat actors take over the targets' Microsoft accounts and make API calls through the attacker-controlled malicious Office 365 OAuth app. The compromised Office 365 accounts provide the attackers with access to victims' emails, files, contacts, as well as sensitive information and resources stored on corporate SharePoint document management/storage systems and/or OneDrive for Business cloud storage spaces.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-warns-of-increasing-oauth-office-365-phishing-attacks/]

Malicious Extension Abuses Chrome Sync to Steal Users' Data

2021.02.05 | Source(s): Bleeping Computer, ZDNet

Analysis:

The Google Chrome Sync feature can be abused by threat actors to harvest information from compromised computers using maliciously-crafted Chrome browser extensions. Camouflaged as Forcepoint Endpoint Chrome Extension for Windows, is a malicious addon that can be installed directly from Chrome, bypassing the Chrome Web Store installation channel, after enabling Developer mode. Once installed, the extension drops a background script designed to check for oatuh_token keys in Chrome's storage which would then get automatically synced to the user's Google cloud storage. From there, the threat actors would only need to log into the same Google account on another system running the Chrome browser to get access to the synced sensitive data.

Read more:

[https://www.bleepingcomputer[.]com/news/security/malicious-extension-abuses-chrome-sync-to-steal-users-data/]
[https://www.zdnet[.]com/article/google-chrome-syncing-features-can-be-abused-for-c-c-and-data-exfiltration/]

Fortinet Fixes Critical Vulnerabilities in SSL VPN And Web Firewall

2021.02.07 | Source(s): Bleeping Computer

Analysis:

Fortinet has fixed multiple severe vulnerabilities ranging from Remote Code Execution (RCE) to SQL Injection, to Denial of Service (DoS) that impacts its products such as the FortiProxy SSL VPN and FortiWeb Web Application Firewall (WAF) products. One of which exists in FortiProxy SSL VPN, tracked as CVE-2018-13381, that can be triggered by a remote unauthenticated actor through a crafted POST request. Due to a buffer overflow in the SSL VPN portal of FortiProxy, a specially crafted POST request of large size, when received by the product is capable of crashing it, leading to a Denial of Service (DoS) condition.

Read more:
[https://www.bleepingcomputer[.]com/news/security/fortinet-fixes-critical-vulnerabilities-in-ssl-vpn-and-web-firewall/]

Mozilla fixes Windows 10 NTFS Corruption Bug in Firefox

2021.02.06 | Source(s): Bleeping Computer

Analysis:

Mozilla fixes a Windows 10 NTFS corruption bug that allows non-privileged users to mark an NTFS volume as dirty from being triggered from the browser. Once the volume was marked dirty, Windows 10 would display an error dialog that states the drive was corrupted and prompt the user to reboot to fix the problem. In Firefox 85 and earlier, the NTFS corruption bug could be triggered simply by trying to access the NTFS bug path in the browser's address bar. With the release of Firefox 85.0.1, instead of trying to access the path, Firefox will simply ignore the path and not attempt to access it.

Read more:

Read more:
[https://www.bleepingcomputer[.]com/news/software/mozilla-fixes-windows-10-ntfs-corruption-bug-in-firefox/]

CERT-PH Recommendations:

o Organizations may protect their remote workforce from OAuth phishing attacks by using publisher verified apps and only allowing access to OAuth apps trusted by the organization or provided by verified publishers.

o For administrators, manage and evaluate consent request, audit apps and consented permissions in your organization to ensure applications being used are accessing only the data they need and adhering to the principles of least privilege.

o Update any vulnerable system/applications/devices to their latest and patched versions:

- **Fortinet Products**
- **FortiProxy SSL VPN**
- **FortiWeb**
- **FortiDeceptor**
- **Mozilla Firefox** - version 85.0.1

o To block attackers abusing Google Chrome’s Sync API for harvesting and exfiltrating data from corporate environments, group policies are urged to create a list of approved CHrome extensions and block all others who haven’t been checked for red flags.**o** Agencies must protect their assets and perimeter by minimizing the point of entry that an unwanted attacker might take. Thus, actions must be taken such as:

- Closing misconfigured and/or unused ports that are accessible in the public internet.
- Regularly monitoring and patching of systems, software application, and devices.
- Educating employees regarding cyber hygiene and cybersecurity best practices.

Critical	*The information stated is deemed to be crucial to organizations and can significantly shift security concerns and issues based on following events.*
Urgent	*The information stated needs to be addressed timely, which may require immediate attention and/or prompt action.*
Information	*The information stated is good to know knowledge that provides awareness and understanding to the topic.*