CERT-PH Cybersecurity Threat Feeds

Issue Date	March 05, 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:

- Hacked SendGrid Accounts Used in Phishing Attacks to Steal Logins
- VMware Releases Fix for Severe View Planner RCE Vulnerability
- Experts Found A New Malware Likely Linked to SolarWinds Hackers
- Hackers Now Hiding ObliqueRAT Payload in Images to Evade Detection

- CRITICAL
- URGENT
- INFORMATION

Description

Hacked SendGrid Accounts Used in Phishing Attacks to Steal Logins

2021.03.04 | Source(s): Bleeping Computer

Analysis:

A phishing campaign targeting users of Outlook Web Access and Office 365 services collected thousands of credentials relying on trusted domains such as SendGrid. Dubbed as Compact, the threat actor behind this campaign has been operating since at least the beginning of 2020 and likely collected more than 400,000 credentials in multiple campaigns. According to cybersecurity researchers, the operators of the phishing campaign are using Zoom invites as a lure and an extensive list of email addresses to deliver messages from hacked accounts on the SendGrid cloud-based email delivery platform. The phishing website of the Compact campaign had distinct fingerprints in the code that permitted monitoring and detecting of a new site as soon as it became live.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hacked-sendgrid-accounts-used-in-phishing-attacks-to-steal-logins/]

VMware Releases Fix for Severe View Planner RCE Vulnerability

2021.03.03 | Source(s): Hacker News

Analysis:

Cybercriminals are observed to be deploying remote access Trojans under the guise of seemingly innocuous images hosted on infected websites. Dubbed as ObliqueRAT, the new malware campaign appears to be targeting organizations in South Asia that utilize malicious Microsoft Office documents forged with macros to spread a RAT. The malware has been linked with the threat actor tracked as Transparent Tribe. According to researchers, In addition to making use of a completely different macro code to download and deploy the RAT payload, the operators of the campaign have also updated the delivery mechanism by cloaking the malware in seemingly benign bitmap image files (.BMP files) on a network of adversary-controlled websites.

Read more:

[https://thehackernews[.]com/2021/03/hackers-now-hiding-obliquerat-payload.html]

Experts Found A New Malware Likely Linked to SolarWinds Hackers

2021.03.04 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered a new sophisticated second-stage backdoor on the servers of an organization compromised by the threat actors behind the SolarWinds supply-chain attack. Dubbed as Sunshuttle, is a GO-based malware featuring detection evasion capabilities. At the time of this writing, the infection vector used to install the backdoors is not yet known, but it is most likely dropped as a second-stage backdoor. According to experts, The new SUNSHUTTLE backdoor is a sophisticated second-stage backdoor that demonstrates straightforward but elegant detection evasion techniques via its blend-in traffic capabilities for C2 communications

Read more:

[https://www.bleepingcomputer[.]com/news/security/fireeye-finds-new-malware-likely-linked-to-solarwinds-hackers/]

Hackers Now Hiding ObliqueRAT Payload in Images to Evade Detection

2021.03.03 | Source(s): Hacker News

Analysis:

Cybercriminals are observed to be deploying remote access Trojans under the guise of seemingly innocuous images hosted on infected websites. Dubbed as ObliqueRAT, the new malware campaign appears to be targeting organizations in South Asia that utilize malicious Microsoft Office documents forged with macros to spread a RAT. The malware has been linked with the threat actor tracked as Transparent Tribe. According to researchers, In addition to making use of a completely different macro code to download and deploy the RAT payload, the operators of the campaign have also updated the delivery mechanism by cloaking the malware in seemingly benign bitmap image files (.BMP files) on a network of adversary-controlled websites.

Read more:
[https://thehackernews[.]com/2021/03/hackers-now-hiding-obliquerat-payload.html]

CERT-PH Recommendations:

- Users are advised to be cautious and always check the authenticity of the website before giving any private information or login credentials. Phishing attacks often use multiple redirects and unsecure connections before landing on the attacker's controlled website. If unsure of the website visited and causes to raise red flags, immediately put the website in your browser's list of locked webpages.
- Avoid installing unknown or unverified applications, especially from third-party distribution platforms.
- Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **VMware View Planner Security Patch** - version 4.6
- 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.*