COVID 19-related Targeted Attack Campaign by Hacker groups

Overview

It is learnt through credible channels that hacker groups are planning a large-scale targeted attack campaign against Indian individuals and businesses (small, medium, and large enterprises).

The hacking campaign is expected to use malicious emails under the pretext of local authorities in charge of dispensing government-funded Covid-19 support initiatives. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information.

The attack campaign is expected to start on 21st June 2020.
Any unusual activity or attack should be reported immediately at incident@certin.org.in. with the relevant logs, email headers for the analysis of the attacks and taking further appropriate actions

Description

Hackers claiming to have 2 million individual email IDs are planning to send emails with the subject: free COVID-19 testing for all residence of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad, inciting them to provide personal information. The email may look as follows:

Best Practices

Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization’s website directly through browser.

Enforce application whitelisting on all endpoint workstations. This will prevent droppers or unauthorized software from gaining execution on endpoints

Block/restrict connectivity to the malicious domains/IPs shared by CERT-In from time to time. If any of the machines are found contacting them, take volatile evidence, isolate the machine, start necessary mitigation and containment procedures. Take forensic image of the machine for root-cause analysis. It is recommended to restore the system from a known good back up or proceed to a fresh installation.

Keep up-to-date patches and fixes on the operating system and application software such as client side softwares, including Adobe Products (Reader, Flash player), Microsoft Office suite, browsers & JAVA applications.

Restrict execution of powershell/WSCRIPT in enterprise environment. Ensure installation and use of the latest version (currently v6.2.2) of PowerShell, with enhanced logging enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.

Control outbound DNS access. Permit internal enterprise systems to only initiate requests to, and receive responses from, approved enterprise DNS caching name servers. Monitor DNS activity for potential indications of tunnelling and data exfiltration, including reviewing DNS traffic for anomalies in query request frequency and domain length, and activity to suspicious DNS servers. The dnscat2 tool alternates between CNAME, TXT, and MX records when it is operating. Investigate abnormal amounts of these records going to the same second level domain, or a group of second level domains.

Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.

Consider deploying Microsoft's Enhanced mitigation Experienced Toolkit (EMET) which provides end node protection against zero-day vulnerabilities and blocks and prevents memory-based attack approaches. Reference: http://support.microsoft.com/kb/2458544

Enhance the Microsoft Office security by disabling ActiveX controls, Macros, Enabling Protect View, File Protection Settings.

Apply software Restriction policies appropriately. Disable running executable from unconventional paths.

Protect against drive-by-downloads through controls such as Browser JS Guard

Leverage Pretty Good Privacy in mail communications. Additionally, advise the users to encrypt / protect the sensitive documents stored in the internet facing machines to avoid potential leakage

Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.

Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header).

Block the attachments of file types,

"exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"

If using VPN services to access organizational networks, consider configuring mandatory 2 Factor authentication. It is recommended to consider an additional form of authentication, prior to granting access to internal network resources.

Consider limiting users' access using VPN services to a single IP address at a time. No multiple simultaneous remote access by the same user should be allowed.

Consider Geo-limiting users access to known geographical locations. Use Geo Location analysis to identify impossible connections, such as a user calling from 2 points geographically remote in a short period of time.

Check if the VPN software writes session data to the remote workstation's disk. If possible, use a connection method that keeps the data in memory only, preferably encrypted.

Maintain up-to-date antivirus signatures and engines.

Restrict users' ability (permissions) to install and run unwanted software applications.
Enforce a strong password policy and implement regular password changes.

Enable a personal firewall on workstations.

Disable unnecessary services on agency workstations and servers.
Exercise caution when using removable media (e.g. USB thumbdrives, external drives, CDs, etc.).

Scan all software downloaded from the Internet prior to executing.

Maintain situational awareness of the latest threats; implement appropriate

ACLs