certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CURRENT ACTIVITIES

"CORONAVIRUS PANDEMIC [COVID-19] BASED CYBER ATTACKS"

Original Issue Date:March 23, 2020

Novel Coronavirus, originated in December 2019 is a viral disease spread worldwide.

It has been reported that Threat Actors are using the COVID-19 pandemic as a cyberattack vector for their own notorious gains.

Cyber criminals are taking advantage of victims increased craving for information about the Novel Coronavirus due to fear and uncertainity associated with it as the outbreak of the disease is progressing worldwide.

ATTACK STAGES-

PRIMARY SET OF ATTACKS:

The Threat actors employed references related to COVID-19 in phishing attacks to steal information and drop additional malware.

TACTICS AND ATTACK PROCEDURES INVOLVED POST INITIAL PHASE OF ATTACKS:

Threat actors devise following new strategies to target victims with scams or malware campaigns:

- Use of Legitimate corporate branding in the name of COVID-19 to send malware to victims
- Using names of trusted organizations in phishing attacks in order to attain credibility and to lure victims to further open attachment
- Using promotional code
- Coronavirus Maps
- "COVID19" as discount codes used by different hacking groups to promote their goods (malicious malware or exploit tools) for financial gain sold over dark net
- Trojan being delivered via Android app that lures victims offering Coronavirus safety mask upon installation.
- Coronavirus tracker App that takes away access of android microphone and camera once installed.

MALWARE FAMILIES RELATED TO COVID-19:

- AGENT TESLA
- TRICKBOT
- LOKIBOT
- EMOTET
- TRICKYMOUSE
- VICIOUS PANDA CAMPAIGN
- AZORULT
- CRIMSON RAT
- COVIDLOCK

Best Practice and Recommendations

1. The majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense.
2. Allow remote access to the organization's network strictly with two-factor authentication.
3. Systems having antivirus and a malware protection program on it and making sure they are always up to date with latest signatures.
4. Administrators applying strict application whitelisting, blocking unused ports, turning off unused services, and monitoring outgoing traffic to prevent infections from occurring.
5. Checking all services and devices for remote access for updates of firmware and security patches. Internet-facing open ports of remote-control services are a key target for attacks.
6. Disable use of Macros in Microsoft office. COVID-19 used VBA Macros as an initial step for targeting victims.

Contact Information

Email:info@cert-in.org.in

Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India