ಡಾನ್ಸ್ ಆಫ್ ಹಿಲರಿ ಆತಂಕ

ಪಹಲ್ಗಾಮ್ ದಾಳಿಗೆ ಉತ್ತರವಾಗಿ ಭಾರತೀಯ ಸೇನೆ ನಡೆಸಿದ 'ಆಪರೇಷನ್ ಸಿಂಧೂರ್' ಕಾರ್ಯಾಚರಣೆ ಸಂದರ್ಭದಲ್ಲಿ ಪಾಕಿಸ್ತಾನ ಮೂಲದ ಹ್ಯಾಕರ್‌ಗಳು ಸೈಬರ್ ದಾಳಿ ನಡೆಸಿದ್ದರು.

■ ಶಶಿಕುಮಾರ್ ಸಿ.

ಭಾರತೀಯ ಸೇನೆ ನಡೆಸಿದ ಆಪರೇಷನ್ ಸಿಂಧೂರ್ ಕಾರ್ಯಾಚರಣೆ ಸಂದರ್ಭದಲ್ಲಿ ಪಂಜಾಬ್, ಹಿಮಾಚಲ ಪ್ರದೇಶ ಸೇರಿದಂತೆ ಉತ್ತರ ಭಾರತದ ಹಲವು ರಾಜ್ಯಗಳ ಮೇಲೆ ಪಾಕಿಸ್ತಾನದ ಹ್ಯಾಕರ್‌ಗಳು 'ಡಾನ್ಸ್ ಆಫ್ ಹಿಲರಿ' ಹೆಸರಿನ ಸೈಬರ್ ದಾಳಿ ನಡೆಸಿದ್ದಾರೆ. ಸದ್ಯ ಇದು ದೇಶದ ಇತರ ರಾಜ್ಯಗಳಿಗೂ ವ್ಯಾಪಿಸಿದೆ. ಸಾರ್ವಜನಿಕರು ಎಚ್ಚರದಿಂದಿರುವಂತೆ ಪೊಲೀಸರು ಸೂಚಿಸಿದ್ದಾರೆ.

'ಡಾನ್ಸ್ ಆಫ್ ಹಿಲರಿ' ಹೆಸರು ಎಷ್ಟು ಆಕರ್ಷಕವಾಗಿದೆಯೊ ಅದರೊಳಗೆ ಅಷ್ಟೇ ಖತರ್ನಾಕ್ ಸಂಚು ಅಡಗಿದೆ. ಒಂದೆಡೆ ಭಾರತ ಮತ್ತು ಪಾಕಿಸ್ತಾನ ನಡುವಿನ ಸಂಘರ್ಷ ನಡೆಯುತ್ತಿರುವಾಗಲೇ ಪಾಕಿಸ್ತಾನದ ಸೈಬರ್ ಅಪರಾಧಿಗಳು, ಹ್ಯಾಕರ್‌ಗಳು ಅಮಾಯಕ ಜನರನ್ನು ಉದ್ದೇಶವಾಗಿಟ್ಟುಕೊಂಡು ಸೈಬರ್ ದಾಳಿ ನಡೆಸುತ್ತಿದ್ದುದು, ಆ ದಾಳಿಗೆ ತುತ್ತಾಗಿ ಹಲವರು ವಂಚನೆಗೊಳಗಾದ ಪ್ರಕರಣಗಳು ಬೆಳಕಿಗೆ ಬಂದಿವೆ. ಡಿಜಿಟಲ್ ವಾರ್‌ನಂತೆ ನಡೆಯುತ್ತಿರುವ ಈ ಸೈಬರ್ ದಾಳಿಯ ಬಗ್ಗೆ ಜನರು ನಿಗಾವಹಿಸಬೇಕಿದೆ.

ಪಂಜಾಬ್ ಹಾಗೂ ಹಿಮಾಚಲ ಪ್ರದೇಶದ ಹಲವೆಡೆ ಇಂಥ ಪ್ರಕರಣಗಳು ಬೆಳಕಿಗೆ ಬಂದಿವೆ. ಪಂಜಾಬ್ ಪೊಲೀಸರು ಹಾಗೂ ಹಿಮಾಚಲ ಪ್ರದೇಶದ ಶಿಮ್ಲಾ ಸೈಬರ್ ಸೆಲ್ ಎಕ್ಸ್ ಮೂಲಕ ಈ ಬಗ್ಗೆ ಪೋಸ್ಟ್ ಮಾಡಿವೆ. ಪಾಕಿಸ್ತಾನದ ಸೈಬರ್ ಹ್ಯಾಕರ್‌ಗಳು ಈ ಕೃತ್ಯದ ಹಿಂದಿದ್ದು, ಭಾರತೀಯ ನಾಗರಿಕರು ಮತ್ತು ಸಂಸ್ಥೆಗಳನ್ನು ಗುರಿಯಾಗಿಸಿಕೊಂಡು ಡ್ಯಾನ್ಸ್ ಆಫ್ ದಿ ಹಿಲರಿ ಮಾಲ್‌ವೇರ್ ಹರಿಬಿಟ್ಟಿದ್ದಾರೆ.

ಹಿಲರಿ ಆಫ್ ಡಾನ್ಸ್ - ಏನಿದು?

ಹಿಲರಿ ಆಫ್ ಡಾನ್ಸ್ ಎನ್ನುವುದು ಕುತಂತ್ರಾಂಶದ ಮಾಲ್‌ವೇರ್. ಲಿಂಕ್, ಮೆಸೇಜ್ ಅಥವಾ ಡಾಕ್ಯುಮೆಂಟ್ ಮಾದರಿಯ ಈ ಕುತಂತ್ರಾಂಶವು ಹೆಸರಿನಲ್ಲಿ ಉಲ್ಲೇಖಿಸಿದಂತೆ ನೃತ್ಯದ ವಿಡಿಯೊಗೆ ಸಂಬಂಧಿಸಿದ್ದಲ್ಲ. ಆಕರ್ಷಕ ಹೆಸರು ಮತ್ತು ಫೈಲ್ ಸ್ವರೂಪದೊಂದಿಗೆ ಇದು ರೂಪುಗೊಂಡಿರುತ್ತದೆ.

ವಾಟ್ಸ್‌ಆ್ಯಪ್, ಫೇಸ್‌ಬುಕ್, ಟೆಲಿಗ್ರಾಂ ಸೇರಿದಂತೆ ಇನ್ನಿತರ ಸೋಷಿಯಲ್ ಮೀಡಿಯಾ ಪ್ಲಾಟ್‌ಫಾರ್ಮ್‌ಗಳ ಮೂಲಕ ಅಮಾಯಕ ಜನರೇ ಹಿಲರಿ ಆಫ್ ಡಾನ್ಸ್‌ನ ಟಾರ್ಗೆಟ್. ದೊಡ್ಡ ದೊಡ್ಡ ಅಕ್ಷರಗಳಲ್ಲಿ ಕಾಣುವಂತೆ ಇದನ್ನು ಲಿಂಕ್, ಮೆಸೇಜ್ ಅಥವಾ ಡಾಕ್ಯುಮೆಂಟ್ ಮಾದರಿಯಲ್ಲಿ ರವಿಸಿ ಸೋಷಿಯಲ್ ಮೀಡಿಯಾಗಳಲ್ಲಿ ಹಂಚಿಕೊಳ್ಳಲಾಗುತ್ತಿದ್ದು, ಇದನ್ನು ಕ್ಲಿಕ್ಕಿಸಿದಾಗ ಇದರಲ್ಲಿ ಅಡಗಿರುವ ಮಾಲ್‌ವೇರ್ ಜನರಿಗೆ ಗೊತ್ತಾಗದಂತೆ ಅವರ ಸ್ಮಾರ್ಟ್‌ಫೋನ್‌ಗಳಲ್ಲಿ ರಹಸ್ಯವಾಗಿ ಇನ್‌ಸ್ಟಾಲ್ ಆಗುತ್ತದೆ. ಅಲ್ಲದೆ, ಬ್ಯಾಕ್‌ಗ್ರೌಂಡ್‌ನಲ್ಲಿ ಇದು ಚಾಲ್ತಿಯಲ್ಲೇ ಇರುತ್ತದೆ.

ಈ ವೈರಸ್ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಮಾತ್ರವಲ್ಲದೆ ಬ್ಯಾಂಕಿಂಗ್ ಮಾಹಿತಿಯನ್ನೂ ಕದಿಯುತ್ತದೆ. ಇದನ್ನು ಬಳಸಿಕೊಂಡು ಸೈಬರ್ ಅಪರಾಧಿಗಳು ಜನರ ಬ್ಯಾಂಕ್ ಖಾತೆಯಲ್ಲಿನ ಹಣ ಎಗರಿಸುವುದರ ಜೊತೆಗೆ ಅವರ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿಯನ್ನು ಕದ್ದು ದುರುಪಯೋಗ ಮಾಡಿಕೊಳ್ಳುತ್ತಾರೆ.

ಏನೆಲ್ಲಾ ಅಪಾಯ?

ವೈರಸ್ ವೈಯಕ್ತಿಕ ಮಾಹಿತಿ, ಬ್ಯಾಂಕ್ ಖಾತೆ ವಿವರಗಳು, ಪಾಸ್‌ವರ್ಡ್‌ಗಳು ಮತ್ತು ಇತರ ಸೂಕ್ಷ್ಮ ಡೇಟಾವನ್ನು ಕದಿಯಲಾಗುತ್ತದೆ. ನಿಮ್ಮ ಸಾಧನದ ಮೇಲೆ ನಿಯಂತ್ರಣ ಸಾಧಿಸುವುದರ ಜೊತೆಗೆ ಹ್ಯಾಕರ್‌ಗಳು ನಿಮ್ಮ ಫೋನ್ ಅಥವಾ ಕಂಪ್ಯೂಟರ್ ಮೇಲೆ ರಿಮೋಟ್ ಕಂಟ್ರೋಲ್ ಪಡೆದುಕೊಂಡು ನಿಮಗೆ ಗೊತ್ತಿಲ್ಲದೆ ನಿಮ್ಮ ಡಿವೈಸ್ ಅನ್ನು ಅವರು ನಿರ್ವಹಿಸುತ್ತಾರೆ. ಈ ಕುತಂತ್ರಾಂಶವು ಡಿವೈಸ್ ಕಾರ್ಯನಿರ್ವಹಣೆಯನ್ನು ನಿಧಾನಗೊಳಿಸುತ್ತದೆ. ಇದು ಪ್ರಮುಖ ಡೇಟಾವನ್ನು ನಾಶಪಡಿಸಿ, ಸಂಪೂರ್ಣ ಕ್ರ್ಯಾಶ್ ಮಾಡುವ ಸಾಧ್ಯತೆ ಇದೆ.

ಈ ವೈರಸ್ ಹಿಮಾಚಲ ಪ್ರದೇಶ ಸೇರಿದಂತೆ ದೇಶದ ಹಲವು ಭಾಗಗಳಲ್ಲಿ ಬಳಕೆದಾರರಿಗೆ ಅಪಾರ ತೊಂದರೆ ಉಂಟುಮಾಡಿದೆ. ಅಪರಿಚಿತ ಮೂಲಗಳಿಂದ ಫೈಲ್‌ಗಳನ್ನು ತೆರೆಯುವ ತಪ್ಪಿನಿಂದಾಗಿ ಅನೇಕ ಜನರಿಗೆ ಆರ್ಥಿಕ ಮತ್ತು ವೈಯಕ್ತಿಕ ಹಾನಿಯಾಗಿದೆ. ಈ ವೈರಸ್ ಜನರಿಗೆ ಮಾತ್ರವಲ್ಲದೆ ಸರ್ಕಾರಿ ಮತ್ತು ಖಾಸಗಿ ಸಂಸ್ಥೆಗಳಿಗೂ ಬೆದರಿಕೆಯಾಗುತ್ತಿದೆ.

ಎಚ್ಚರಿಕೆಯ ಕ್ರಮಗಳೇನು?

- ಅಪರಿಚಿತ ಮೂಲದಿಂದ ಸ್ವೀಕರಿಸಲಾದ ವಿಡಿಯೊಗಳು, ದಾಖಲೆಗಳು ಸೇರಿದಂತೆ ಅನುಮಾನಾಸ್ಪದ ಫೈಲ್‌ಗಳನ್ನು ತೆರೆಯಬೇಡಿ.
- ಆಟೊ–ಡೌನ್‌ಲೋಡ್ ಆಫ್ ಮಾಡಿ. ಜೊತೆಗೆ ವಾಟ್ಸ್‌ಆ್ಯಪ್ ಮತ್ತು ಇತರ ಅಪ್ಲಿಕೇಷನ್‌ಗಳ ಆಟೊ–ಡೌನ್‌ಲೋಡ್ ಸೆಟ್ಟಿಂಗ್‌ಗಳನ್ನು ಸ್ಥಗಿತಗೊಳಿಸಿ.
- ಸಾಧನಗಳು, ಇಮೇಲ್ ಮತ್ತು ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮ ಖಾತೆಗಳಿಗೆ ಹೆಚ್ಚು ದಕ್ಷತೆಯ ಪಾಸ್‌ವರ್ಡ್‌ಗಳನ್ನು ಸೆಟ್ ಮಾಡಿ.
- ಸಾಮಾಜಿಕ ಮಾಧ್ಯಮಗಳಲ್ಲಿ ಬರುವ ಅಥವಾ ಕಾಣಿಸಿಕೊಳ್ಳುವ ಲಿಂಕ್‌ಗಳನ್ನು ಕ್ಲಿಕ್ಕಿಸದಿರಿ. ಪರಿಚಯವಿಲ್ಲದ ಲಿಂಕ್‌ಗಳು, ಪ್ರೊಫೈಲ್‌ಗಳು ಅಥವಾ ಸಂದೇಶಗಳ ತಂಟೆಗೆ ಹೋಗದೆ ಇರುವುದು ಒಳಿತು.
- ವಿಶ್ವಾಸಾರ್ಹ ಎನಿಸುವ ಆ್ಯಂಟಿವೈರಸ್ ಸಾಫ್ಟ್‌ವೇರ್ ಅನ್ನು ನಿಮ್ಮ ಡಿವೈಸ್‌ಗಳಿಗೆ ಅಳವಡಿಸಿಕೊಂಡು, ಫೈಲ್‌ಗಳನ್ನು ಸ್ಕ್ಯಾನ್ ಮಾಡಿಯೇ ತೆರೆಯಿರಿ.
- ಅಸಾಮಾನ್ಯ ಹೆಸರುಗಳು ಅಥವಾ ವಿಸ್ತರಣೆಗಳನ್ನು ಹೊಂದಿರುವ ಫೈಲ್‌ಗಳನ್ನು ತೆರೆಯುವ ಮೊದಲು ಅವುಗಳ ದೃಢೀಕರಣವನ್ನು ಪರಿಶೀಲಿಸಿ.
- ನಿಮ್ಮ ಸಾಧನ ಮತ್ತು ಅಪ್ಲಿಕೇಷನ್‌ಗಳನ್ನು ಇತ್ತೀಚಿನ ಆವೃತ್ತಿಗಳಿಗೆ ಅಪ್‌ಡೇಟ್ ಮಾಡಿಕೊಳ್ಳುವುದು ಒಳಿತು.
- ನಿಮ್ಮ ಫೋನ್‌ನಲ್ಲಿ ವೈರಸ್ ಬಂದಿದ್ದರೆ ತಕ್ಷಣವೇ ಇಂಟರ್ನೆಟ್ ಕಡಿತಗೊಳಿಸಿ. ■