KERALA POLICE INFORMATION CENTRE

Ph: 0471 2318188 Email: *info.pol@kerala.gov.in*

No.100/PR/PIC/PHQ/17 Date : 15.05.2017

കംപ്യൂട്ടർ സുരക്ഷ: ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

'വാനാക്രൈ' എന്ന കംപ്യൂട്ടർ റാൻസംവെയറിന്റെ ആക്രമണം കംപ്യൂട്ടറുകൾക്കും അവയിൽ ശേഖരിച്ചിരിക്കുന്ന വിവരങ്ങൾക്കും വലിയ തകരാർ വരുത്തുന്നത് നിരവധി രാജ്യങ്ങളെ ബാധിച്ചിരിക്കുകയാണ്. കേരളവും ഈ ഭീഷണിയിൽ നിന്ന് മുക്തമല്ല. ഈ സാഹചര്യത്തിൽ കംപ്യൂട്ടറുകളും അവയിൽ ശേഖരിച്ചിരിക്കുന്ന വിവരങ്ങളും ഓൺലൈൻ പ്രവർത്തനങ്ങളും സുരക്ഷിതമാക്കാൻ പരമാവധി ശ്രദ്ധിക്കണമെന്ന് കേരള പോലീസ് സൈബർ വിഭാഗം അഭ്യർത്ഥിച്ചു. ഉപയോക്താക്കൾ ഇതിനായി താഴെപ്പറയുന്ന കാര്യങ്ങൾ ശ്രദ്ധിക്കേണ്ടതാണ്.

കംപ്യൂട്ടറുകളിൽ ഉപയോഗിക്കുന്നത് പകർപ്പവകാശമുള്ള ഓപ്പറേറ്റിങ് സിസ്റ്റമാണെങ്കിൽ ഒറിജിനൽ മാത്രം ഉപയോഗിക്കുക. അല്ലെങ്കിൽ സ്വതന്ത്ര സോഫ്റ്റ്വെയർ അധിഷ്ഠിതമായ ഓപ്പറേറ്റിങ് സിസ്റ്റം ഉപയോഗിക്കുക.

റാൻസംവെയറുകൾ ബാധിച്ചാൽ ആവശ്യപ്പെടുന്ന പണം (Ransom amount) ഒരിക്കലും നൽകാൻ ശ്രമിക്കരുത്. അടിയന്തിരമായിCERT - Kerala/CERT.INDIA/ഐ.ടി.മിഷൻ/സൈബർ പോലീസ് എന്നിവിടങ്ങളിൽ ബന്ധപ്പെടുക.

സുപ്രധാന വിവരങ്ങളുടെ ബാക്ക് അപ്പ് പതിവായി എടുക്കുകയും അത് മറ്റൊരു സ്റ്റോറേജ് ഡിവൈസിൽ ഓഫ്ലൈനിൽ സൂക്ഷിക്കുകയും വേണം.

സ്പാം തടയുന്നതിനുള്ള ഒരു ഇ-മെയിൽ സാധൂകരണ സംവിധാനമായ ഡൊമെയ്ൻ പോളിസി ഫ്രെയിം വർക്ക് (എസ്.പി.എഫ്), Domain Message authentication reporting and conformance (DMARC), Domain Keys Identified mail (DKIM) എന്നിവ സ്ഥാപിക്കുക. റാൻസംവെയർ സാമ്പിളുകൾ ഭൂരിഭാഗവും ഇ-മെയിൽ ബോക്സുകളിൽ എത്തുന്നു.

ആവശ്യമില്ലാത്ത ഇ-മെയിൽ അറ്റാച്ച്മെന്റുകൾ തുറക്കാതിരിക്കുക. അത് നിങ്ങളുടെ കോൺടാക്ട് ലിസ്റ്റിൽ നിന്നുള്ള ആളുകളിൽ നിന്നും വന്നാൽപ്പോലും അതിൽ ഉൾപ്പെടുന്ന URL-ൽ ക്ലിക്ക് ചെയ്യരുത്, ബന്ധപ്പെട്ട URL വെബ്സൈറ്റുകളിലേക്ക് ബ്രൗസറുകളിലൂടെ നേരിട്ട് സന്ദർശിക്കുക.

എന്റർപ്രൈസസ് പരിതഃസ്ഥിതിയിൽ PowerShell -ന്റെ ഏറ്റവും പുതിയ വേർഷൻ ഇൻസ്റ്റാൾ ചെയ്തു എന്ന് ഉറപ്പാക്കുക. നിരീക്ഷണത്തിനും വിശകലനത്തിനുമായി ബന്ധപ്പെട്ട ലോഗുകൾ ഒരു കേന്ദ്രീകൃത ഡേറ്റാ ശേഖരത്തിലേക്ക് അയയ്ക്കുക.

നെറ്റ്വർക്കിൽ വെബ്, ഇ-മെയിൽ ഫിൽട്ടറുകൾ വിന്യസിക്കുക, മോശമായ ഡൊമെയ്നുകൾ, ഉറവിടങ്ങൾ, വിലാസങ്ങൾ എന്നിവയ്ക്കായി സ്കാൻ ചെയ്യാൻ ഈ ഉപകരണങ്ങൾ കോൺഫിഗർ ചെയ്യുക, സന്ദേശങ്ങൾ സ്വീകരിക്കുന്നതിനും ഡൗൺലോഡ് ചെയ്യുന്നതിനും മുമ്പായി ഇത് തടയുക. ഹോസ്റ്റിലും മെയിൽ ഗേറ്റ്വേയിലും വിശ്വസനീയമായ ആന്റിവൈറസ് ഉപയോഗിച്ച് എല്ലാ ഇ-മെയിലുകളും അറ്റാച്ചുമെന്റുകളും ഡൗൺലോഡുകളും സ്കാൻ ചെയ്യുക.

%APPDATA%, %PROGRAMDATA% & %TEMP% എന്നിവയിൽ നിന്നും ബൈനറികൾ തടയുന്നതിനുള്ള സോഫ്റ്റ്വെയർ വൈറ്റ്ലിസ്റ്റ് കർശനമായി നടപ്പിലാക്കൽ, ഈ ലൊക്കേഷനുകളിൽ നിന്ന് സാധാരണയായി റാൻസംവെയർ സാമ്പിൾ ഡ്രോപ്പുകളും പ്രവർത്തിപ്പിക്കും. എല്ലാ എൻഡ്പോയിന്റ് വർക്ക്സ്റ്റേഷനുകളിലും ആപ്ലിക്കേഷൻ വൈറ്റ്ലിസ്റ്റ് നടപ്പിലാക്കുക.

ഡാറ്റാബേസ്, ആധികാരികത, സെൻസിറ്റീവ് സിസ്റ്റങ്ങളിൽ ഉപയോഗിച്ചിരിക്കുന്ന കോഡുകളുടെ /സ്ക്രിപ്റ്റുകളുടെ സമഗ്രത ഉറപ്പുവരുത്തുക, ഡാറ്റാബേസുകളിൽ സംഭരിച്ചിരിക്കുന്ന വിവരങ്ങളുടെ സമഗ്രതയ്ക്കായി പതിവായി പരിശോധിക്കുക.

അനാവശ്യ സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിനും പ്രവർത്തിപ്പിക്കുന്നതിനും ഉപയോക്താക്കളെ നിയന്ത്രിക്കുക.

വർക്ക് സ്റ്റേഷനുകളിൽ വ്യക്തിഗത ഫയർവാളുകൾ ഇൻസ്റ്റാൾ ചെയ്യുക.

കർശനമായ ബാഹ്യ ഉപകരണ (USB, DVD drive etc.) ഉപയോഗ നയങ്ങൾ നടപ്പിലാക്കുക.

ഓപ്പറേറ്റിങ് സിസ്റ്റം തേർഡ് പാർട്ടി ആപ്ലിക്കേഷനുകളിൽ (എം.എസ്.ഓഫീസ്, ഏറ്റവും പുതിയ പാച്ചുകൾ ഉപയോഗിച്ച് ബ്രൗസറുകൾ, ബ്രൗസർ പ്ലഗിനുകൾ) നിലനിർത്തുക.

വെബ് ബ്രൗസ് ചെയ്യുമ്പോൾ സുരക്ഷിതമായ നടപടികൾ പിൻതുടരുക. ഉചിതമായ

ഉള്ളടക്ക നിയന്ത്രണങ്ങൾ ഉപയോഗിച്ച് വെബ്ബ്രൗസറുകൾ സുരക്ഷിതമാക്കിയതായി ഉറപ്പാക്കുക.

സെക്യൂരിറ്റി സോണുകളിലെ നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ, സെഗ്രിജേഷൻ എന്നിവ സെൻസിറ്റീവ് വിവരവും നിർണായക സേവനങ്ങളും പരിരക്ഷിക്കാൻ സഹായിക്കുന്നു. ഫിസിക്കൽ നിയന്ത്രണങ്ങൾ, വെർച്വൽ ലോക്കൽ ഏരിയ നെറ്റ്വർക്കുകൾ എന്നിവ ഉപയോഗിച്ച് ബിസിനസ് പ്രോസസ്സുകളിൽ നിന്ന് അഡ്മിനിസ്ട്രേറ്റീവ് നെറ്റ്വർക്ക് വേർതിരിക്കുക.

exe/pif/tmp/url/vb/vbe/scr/reg/cer/pst/cmd/com/ ബാറ്റ്/dll/Dat/hlp/hta/js/wsf എന്നീ എക്സ്റ്റൻഷനുള്ള ഫയൽ അറ്റാച്ചുമെന്റുകൾ ബ്ലോക്ക് ചെയ്യുക.

ഡാറ്റ റെക്കോർഡ് അല്ലെങ്കിൽ ബാഹ്യ ഘടകങ്ങളുടെ അംഗീകൃതമല്ലാത്ത എൻക്രിപ്റ്റ് ചെയ്ത ഉള്ളടക്കങ്ങൾക്കായി ഡാറ്റാ ബേസുകളുടെ ബാക്കപ്പ് ഫയലുകളുടെ ഉള്ളടക്കം പരിശോധിക്കുക (backdoors/malicious scripts)

മൈക്രോസോഫ്റ്റ് ഉൽപ്പന്നങ്ങളിൽ മാക്രോകൾ അപ്രാപ്തമാക്കുക. വിൻഡോസിനുവേണ്ടി, നിർദ്ദിഷ്ട ക്രമീകരണങ്ങൾ പ്രവർത്തിപ്പിക്കുന്നതിൽ നിന്നും ഇന്റർനെറ്റിൽ നിന്നും ആരംഭിക്കുന്ന മൈക്രോകൾ തടയാവുന്നതാണ്.

കുറഞ്ഞത് പ്രത്യേക പരിഗണനയുള്ള ഫയൽ, ഡയറക്ടറി, നെറ്റ്വർക്ക് പങ്കിടൽ അനുമതികൾ ഉൾപ്പെടെയുള്ള ആക്സസ് നിയന്ത്രണങ്ങൾ കോൺഫിഗർ ചെയ്യുക. ഒരു ഉപയോക്താവിന് നിർദ്ദിഷ്ട ഫയലുകൾ മാത്രം വായിക്കണമെങ്കിൽ ആ ഫയലുകൾ, ഡയറക്ടറികൾ, അല്ലെങ്കിൽ ഷെയറുകൾക്ക് അവർക്ക് റൈറ്റ് ആക്സസ് പാടില്ല.

എല്ലാ സിസ്റ്റങ്ങളിലും അപ്ഡേറ്റ് ആന്റിവൈറസ് സോഫ്റ്റ്വെയറുകൾ ഉപയോഗിക്കുക.

ഇൻസ്റ്റലേഷനുവേണ്ടി പരമാവധി Enhanced Mitigation Experience Tool kit അല്ലെങ്കിൽ host-level anti-exploitation tool ഉപയോഗിക്കുക.

റിമോട്ട് ഡസ്ക്ടോപ്പ് സംവിധാനം ഡിസേബിൾ ചെയ്യുക.

അനധികൃതമായി access ചെയ്യാത്ത വിധത്തിൽ ഉദ്യോഗസ്ഥരുടെ ഡേറ്റാ സ്റ്റോർ ചെയ്യണം.

നിർണായക വിലയിരുത്തൽ, പെനട്രേഷൻ ടെസ്റ്റിംഗ് (വി.എ.പി.ടി), സുപ്രധാന നെറ്റ്വർക്കുകൾ/സിസ്റ്റങ്ങളുടെ വിവരങ്ങൾ സെക്യൂരിറ്റി ഓഡിറ്റ്, പ്രത്യേകിച്ചും ഡേറ്റാബേസ് സെർവറുകളിൽ, CERTIN empaneled auditors-ൽ നിന്നും നടത്തുക. പതിവായ ഇടവേളകളിൽ ഓഡിറ്റുകൾ ആവർത്തിക്കുക.

****