Orangeworm (hackersgroep) bedreigt medische software o.a. van scanners

Sinds kort is de hackersgroep Orangeworm zeer actief om met het Kwampir-virus netwerken te besemetten. Men heeft het daarbij speciaal gemunt op de medische sector, omdat veertig procent van de besmettingen gevonden is in computersystemen van ziekenhuizen, medische apparatuur en toeleveringsbedrijven van zorginstellingen, maar ook farmaceutische bedrijven. Het Kwampir-virus, waarmee deze hackersgroep, waarvan eigenlijk nauwelijks iets bekend is, behoort tot de categorie van de Trojan-horse virussen en wordt meestal als Win32/Kwampir aangeduid. Het lijkt erop dat Organgeworm niet willekeurig te werk gaat, maar gericht zijn doelen uitzoekt om te besmetten.

Het virus is al in 2015 ontdekt. Symantec, één van de grote bedrijven die antivirus-software maakt, beschreef in 2016 al wat dit virus doet en hoe het verwijderd moet worden. Het virus creëert binnen de besmette hardware een zogenaamde “backdoor”, waardoor het toegang heeft tot een besmet systeem en ook bestanden kan downloaden.

Beeldvormende systemen

Binnen ziekenhuizen is het virus ook aangetroffen op beeldvormende systemen(Medical Imaging Devices), zoals Röntgenapparatuur en MRI-scanners. Het binnendringen van virussen in de besturingssystemen van beeldvormende systemen

is een groot probleem. Virussen kunnen de werking van die apparaten verstoren en schade berokkenen aan de patiënten en de apparatuur. Ik schreef er zeer kort geleden een artikel over. Het binnendringen van computervirussen in ziekenhuizen is sowieso een groot probleem, omdat hele systemen plat gelegd kunnen worden, maar ook gevoelige data de zorginstellingen onrechtmatig kunnen verlaten. Met het virus lijkt de hackersgroep ook gefocust te zijn op onderdelen van ziekenhuissoftware, waarin de patiënt toestemmingen vastlegt voor een noodzakelijke behandeling(en). Dat is ook een zeer zorgelijke ontwikkeling omdat op die wijze onterechte en onrechtmatige toestemmingen van patiënten in de ziekenhuissystemen terecht kunnen komen.

Werking

Het virus lijkt niet al te geheim zijn werk te doen en is op zich niet moeilijk te detecteren. De malware kopieert zich in onderdelen van een ICT-netwerk en verspreidt zich via een bepaalde lijst van “command and control” computerservers. Het cybersecurity-bedrijf Symantec denkt dat het de bedoeling is dat Orangeworm ten dele bedoeld is om de infrastructuur van aangetaste systemen vast te leggen, maar dat een aanval nog kan komen. Die aanval kan dan gebruik maken van de verzamelde data over de systemen. Symantec heeft ook een lijst van zogenaamde Indicators of Compromis(IOC). (bron Webwereld) Daarmee kunnen systeembeheerders aan de hand van zogenaamde “fingerprints” zoeken naar kenmerken van het virus binnen de instellingssoftware.

Daders

Op dit moment gist men noch wie er achter de doelgerichte aanvallen zit met een relatief “oud” virus, dat ook relatief makkelijk te detecteren is. Binnen de cybersecurity-wereld denk men eerder aan een individu of een kleine groep individuen dan aan een door een staat georganiseerde of daardoor gefaciliteerde groep.

Zorgelijk

Het is uitermate zorgelijk dat zorginstellingen zo onder vuur liggen door criminele activiteiten. Anders kan je dit niet noemen. Het eventueel plat kunnen leggen van de systemen met ransomnware (zie Wannacry-virus-aanval) op basis van de vergaarde kennis met het Kwampir-virus is mogelijk. Daarnaast kan de werking van apparatuur geblokkeerd en verstoord worden. Ook kan na weglekken van administratieve en medische gegevens daarmee grootscheepse financiële fraude worden gepleegd. Op basis van gemanipuleerde toestemmingen voor behandelingen kunnen medische activiteiten bij een patiënt gestart worden die helemaal niet de bedoeling zijn.

Wake-up-call

Het is duidelijke wake-up-call voor werkers in de zorg en voor ICT-specialisten van zorginstellingen om alert te zijn op handelingen die de introductie van het virus mogelijk maken. Daarmee doel ik bijvoorbeeld op het gebruik van mobiele gegevensdragers zoals USB-sticks en mobiele harde schijven. Maar ook dient men consequent besturingssystemen te updaten met de laatste “patches” en erop toe te zie dat er geen door Microsoft of andere bedrijven uit gefaseerde besturingssystemen meer gebruikt worden.

W.J. Jongejan, 25 april 2018