NY SKADLIG KOD SOM KAN SLÅ UT ELNÄT UPPTÄCKT

Information om en ny skadlig kod som är direkt inriktad på angrepp mot ICS-miljöer, och närmare bestämt automation i elnät, har precis blivit publik. Det Slovakiska antivirusföretaget ESET har arbetat med att i detalj undersöka uppbyggnaden av den skadliga koden och har delat med sig av information till andra säkerhetsföretag som ockås arbetat med analys av skadlig kod. Enligt uppgift kommer så kommer ursprungskoden från angreppet mot Ukraina i december 2016. Utredare och säkerhetsspecialister från ESET kommer till cybersecuritykonferensen CS3STHLM i oktober och berättar om och diskuterar koden.

Robert Lipovski, en av utredarna på ESET, konstaterar i Washington Post: -" Den potentiella skada en sådan malware kan göra är enorm."

Namn som ESET satt på den skadliga koden är **Win32/Industroyer,** medan andra även kallar det **CRASHOVERRIDE,** vilket kommer från företaget Dragos utredning.

Robert Malmgren, en av Sveriges ledande experter inom området, och som arrangerar CS3STHLM, berättar: -"Attackprogrammet nyttjar inte några nya sårbarheter i IT-system, varför vissa personer kanske drar felaktiga slutsatser att det här programmet inte är så intressant. Denna slutsats är olycklig och felaktig. Det intressanta här är att programmet är specialskrivet för att kunna påverka många typer av utrustningar i elnätet, bland annat för att stänga av skydd i elanläggningar eller att direkt styra elsystemskomponenter. Det är därför Lipovski slutsats är så skrämmande."

Det som gör Industroyer unikt är dess moduluppbyggnad och mer specifikt de specifika moduler som upptäckts och som är för att styra utrustning via standardiserade SCADA/ICS-protokoll. Förutom att kunna kommunicera via dessa protokoll, så har ESET också identifierat att Industroyer också har kod för att slå ut så kallade reläskydd. De protokoll som finns i Industroyer är sådana som används som standard inom många europeiska och svenska elbolag för. Det skall särskilt noteras att Industroyer/CRASHOVERRIDE, till skillnad mot den tidigare skadliga koden Stuxnet, lätt kan användas/återanvändas i andra miljöer än den miljö i vilken den ursprungliga kopian hittade.

ESETs specialister kommer att hålla dragningen "Industroyer: biggest threat to industrial control systems since Stuxnet" på CS3Sthlm i oktober där fler detaljer om utredningen kommer att presenteras.

För information angående den skadliga koden kontakta:
Robert Malmgren
070-833 03 78

För information om CS3STHLM kontakta:
Maria Engström Østby
Press Officer CS3STHLM
070-512 42 93

www.cs3sthlm.se

FAKTA CS3STHLM
CS3STHLM arrangers av Omnisiens som ägs av svenska cyber security experterna Robert Malmgren; framröstad som Sveriges främsta IT säkerhetsspecialist i Computer Sweden, och Erik Johansson, PhD; säkerhetsforskare, rådgivare, och konsult i gränssnittet mellan IT, Informationsteknologi, och OT Operational Technology.