ENVELOPE

RATUZYUW RUEIFBS1607 2421828-UUUU--RUEDAEI.
ZNR UUUUU ZUI RUEOMCG0565 2421832

HEADER

R
291828Z AUG 12
FM OSC RESTON VA

TO RUZFNEL/547IS NELLIS AFB NV
RAYWAP/ATTORNEY GENERAL D BRANCH
RUZDADA/BUREAU OF ALCOHOL TOBACCO FIREARMS WASHI
RUOIAAA/CDR USPACOM HONOLULU HI
RUZFMXI/CDR USTRANSCOM INTEL CELL SCOTT AFB IL
RUEPNGA/CDRNGIC CHARLOTTESVILLE VA
RHMFISS/CDRUSASOIC WASHINGTON DC
RUEPWDC/DA AMHS WASHINGTON DC
RHEBAAA/DEPT OF ENERGY WASHINGTON DC//IN-1//
RUEPTRS/DEPT OF TREASURY WASHINGTON DC
RHEFDIA/DIA WASHINGTON DC
[redacted] (b)(3)
RUOIAAA/DIRNAVCRIMINVSERV QUANTICO VA
RHMFISS/DIRNAVCRIMINVSERV QUANTICO VA
RUEPMAX/GISA FT BRAGG NC
RAYAIK/HQJOC WASP
RUZDJWC/JWAC DAHLGREN VA
RUZDQAN/MARCORINTACT QUANTICO VA
RUZDNAI/NASIC WRIGHT PATTERSON AFB OH
RUGIZZZ/NGA DISSEM WASHINGTON DC
RUETIAA/NSACSS FT GEORGE G MEADE MD
RUCXONI/ONI WASHINGTON DC//2140//
RHMFIUU/PACAF IDHS HICKAM AFB HI
RHHJJPI/PACOM IDHS HONOLULU HI
RUEKJCS/SECDEF WASHINGTON DC
RUEHC/SECSTATE WASHINGTON DC//INR//
RUZEADH/UDITDUSAREUR HEIDELBERG GE
RUMICED/USAFCENT INTEL SHAW AFB SC//A2//
RHHJRAP/USARPAC INTEL FT SHAFTER HI//APIN//
RUMICEA/USCENTCOM INTEL CEN MACDILL AFB FL
RUCQSAB/USSOCOM INTEL MACDILL AFB FL

BT

CONTROLS

UNCLAS

FOR OFFICIAL USE ONLY

SECTION 1 OF 2
QQQQ
CITE OSC RESTON VA 221678

WARNING: TOPIC: FOUO, INTERNATIONAL POLITICAL

SERIAL:SAP20120829134001

BODY

COUNTRY: IRAN, ISRAEL, PAKISTAN, UNITED STATES

SUBJ: (U//FOUO) PKKH: CYBER WARFARE IS 'NEW THREAT TO PAKISTAN'S NATIONAL SECURITY'

SOURCE: KARACHI PKKH IN ENGLISH 29 AUG 12 (U//FOUO)

TEXT:

(U//FOUO) AN EXCLUSIVE REPORT BY PKKH CORRESPONDENT HASAN QURESHI: "CYBER WARS" TEXT DISSEMINATED AS RECEIVED WITHOUT OSC EDITORIAL INTERVENTION.

INTERNET

OSC TRANSCRIBED TEXT

CYBER WARS

SUBMITTED BY AURANGZEB ON AUGUST 28, 2012 - 7:24 PM

(ATTACHMENT NOT INCLUDED: SAP20120829134001001.JPG)

PKKH EXCLUSIVE (-VERTICAL-BAR-) HASAN QURESHI

THERE IS A NEW THREAT TO PAKISTAN'S NATIONAL SECURITY AND IT COMES IN THE FORM OF A COMPUTER CODE. LEAVE ASIDE MANNED CIA, MOSSAD AND RAW INTELLIGENCE, INFILTRATION AND SABOTAGE OPERATIONS WHICH HAVE BEEN COUNTERED BY THE ISI; THIS NEW THREAT IS SILENT AND FAR DEADLIER.

THE RISE OF CYBER WARFARE IS NOTHING NEW. IT HAS BEEN USED IN VARIOUS FORMS SINCE THE LATE 1980'S, PRIMITIVE THOUGH IT MAY HAVE BEEN. HOWEVER THE INCREASING SOPHISTICATION OF COMPUTER SYSTEMS HAS MEANT THAT IT IS NOW BEING EMPLOYED AS A FRONT LINE TOOL OF WAR. ONE CODE IN PARTICULAR -FIRST DISCOVERED IN 2010 LURKING IN IRANIAN NUCLEAR ENRICHMENT FACILITIES- IS STUXNET.

STUXNET IS A JOINT COOPERATION INITIATIVE BETWEEN AMERICA'S NATIONAL SECURITY AGENCY AND ISRAEL'S UNIT 8200, PART OF A LARGER PROGRAMME INITIATED BY GEORGE W. BUSH IN 2008 CALLED OPERATION OLYMPIC GAMES TO TARGET IRAN, PAKISTAN, AND MIDDLE EASTERN COUNTRIES ELECTRONICALLY. IT IS THE MOST COMPLICATED VIRUS CODE TO DATE; EXPLOITING GAPS IN SYSTEMS CALLED ZERO DAYS WHICH EVEN THE SYSTEM DESIGNERS ARE NOT AWARE OF. IT IS ALSO THE FIRST VIRUS CREATED FOR THE SPECIFIC PURPOSE OF CYBER WARFARE - A WEAPON MADE ENTIRELY OUT OF CODE.

THE VIRUS AND ITS VARIANTS CAN LIE DORMANT IN A SYSTEM FOR YEARS - BE THAT A POWER/COMMUNICATIONS GRID OR A NUCLEAR FACILITY- AND ONLY COME INTO ACTION WHEN A SPECIFIC 'TARGET' COMES INTO PLAY. FOR EXAMPLE IT CAN BE INSERTED INTO A COUNTRY'S MISSILE DEFENCE SHIELD OR MISSILE LAUNCH PROGRAM AND ONLY SPRING INTO ACTION WHEN THE CODES FOR THE MISSILES ARE INPUTTED AND THE LAUNCH BUTTON IS PRESSED, RENDERING A COUNTRY DEFENCELESS AT ITS HOUR OF NEED. THE SYSTEM NEED NOT BE CONNECTED TO THE INTERNET AS A DOUBLE AGENT WITH A USB DEVICE IS ALL THAT IS NEEDED.

IT WREAKED HAVOC AT IRAN'S NATANZ NUCLEAR ENRICHMENT PLANT, SETTING THEM BACK AT LEAST TWO YEARS. IT IS ALSO SUSPECTED OF BURROWING INTO THE SYSTEM AT THE BUSHEHR FACILITY, MEANING THAT WHEN THE PLANT FINALLY DOES COME ONLINE, IT COULD LEAD TO A NATIONAL ELECTRICITY BLACKOUT. THE US AND ISRAELIS PROGRAMMERS USED P-1 CENTRIFUGES ACQUIRED FROM LIBYA TO TEST THE RESULTS ON IRAN'S CENTRIFUGES AS THEY ALSO USE THE SAME. THE P-1 CENTRIFUGE DESIGN WAS GIVEN TO LIBYA AND IRAN BY PAKISTAN THROUGH DR. ABDUL QADEER KHAN, MEANING THAT PAKISTAN ALSO USES THOSE VERY SAME P-1'S IN SOME OF ITS OWN NUCLEAR FACILITIES.

STUXNET, THOUGH, IS OLD NEWS BY NOW. EVEN THE NEWLY DISCOVERED "FLAME" MALWARE FOUND RECENTLY IN SYSTEMS IN THE MIDDLE EAST WAS DEVELOPED SOME TIME AGO. WHILE DETAILS ABOUT THESE TWO TARGETED ATTACK PACKAGES ARE FINALLY EMERGING, THE NEXT GENERATION OF ATTACK TOOLS HAS NO DOUBT BEEN DEVELOPED AND LIKELY DEPLOYED.

A FURTHER ISSUE IS THAT STUXNET IS NOW AVAILABLE AS OPEN SOURCE SOFTWARE AND CAN BE REVERSE ENGINEERED BY ANYONE. A NON-STATE ACTOR, SUCH AS THE FOREIGN FUNDED OUTFITS TTP OR BLA ARE NOW FULLY CAPABLE OF ACQUIRING, REDESIGNING AND DEPLOYING THIS SOFTWARE AGAINST SENSITIVE TARGETS.

THE THREAT IS NOT LIMITED TO ATTACKS ON NATIONAL SECURITY INSTALLATIONS BECAUSE RECENTLY AN OFFSHOOT OF STUXNET DUBBED THE GAUSS VIRUS HAS BEEN FOUND LURKING ON SYSTEMS IN THE MIDDLE EAST. THIS CODE IS DIFFERENT TO THE ORIGINAL FROM WHICH IT WAS DEVELOPED AS ITS OBJECTIVE IS THE SURVEILLANCE OF THE FINANCIAL DATA OF SYSTEM USERS. THE MALWARE 'DUQU' USED FOR CYBER ESPIONAGE IS ALSO RELATED TO STUXNET. RUSSIA'S KASPERSKY LAB FIRST FLAGGED THE EXISTENCE OF THESE VIRUSES AND COMMENTED ON ITS WEBSITE, "AFTER LOOKING AT STUXNET, DUQU AND FLAME, WE CAN SAY WITH A HIGH DEGREE OF CERTAINTY THAT GAUSS COMES FROM THE SAME 'FACTORY' OR 'FACTORIES.' ALL THESE ATTACK TOOLKITS REPRESENT THE HIGH END OF NATION-STATE SPONSORED CYBER-ESPIONAGE AND CYBERWAR OPERATIONS." ACCORDING TO KASPERSKY LAB, GAUSS CAN ALSO STEAL PASSWORDS AND

ADMIN

BT
#1607
D16A

*** MISSING SECTION 2 OF SECTIONED MESSAGE ***

UNCLAS

NNNN

UNCLASSIFIED//FOUO

Approved for Release: 2017/02/15 C06586906