Mbinu Dijitali za Kuenda Kinyume na Vikwazo vya Umoja wa Mataifa

Uchunguzi wa Kifani wa Kikosi cha Mtandaoni cha Jamhuri ya Kidemokrasia ya Watu wa Kor ea

Imetayarishwa na Ashley Taylor

Utangulizi

Sekta ya mtandaoni ni safu mpya ya kutekeleza na kuenda kinyume na vikwazo vya Umoja wa Mataifa. Kwa sababu Intaneti inatoa nafasi pepe ya mawasiliano na miamala ya papo ha po, inatoa fursa zisizodhibitiwa na rahisi zaidi kwa wahusika wahalifu wanaokiuka mienend o inayokubalika kimataifa. Matumizi haramu ya teknolojia dijitali ni yanashinda nguvu maen deleo yanayofanywa na wanateknolojia halali, ambao kwa jumla huwa hawaupi kipaumbele usalama wa kimataifa kwenye biashara yao.

Jamhuri ya Kidemokrasia ya Watu wa Korea (DPRK) haswa imekuwa hodari zaidi kutumia vif aa dijitali ili kuenda kinyume na vikwazo. Wamebuni teknolojia dijitali ili kuzalisha mapato y a kufadhili juhudi zao haramu za usambazaji, kupata ufahamu na ujuzi wa kiufundi, kudhuru biashara na hadhi ya maadui wa nje, ikiwemo kuwasumbua wale wanaosimamia utekelezaji wa mfumo wa vikwazo vya Korea Kaskazini ulioidhinishwa na azimio la Umoja wa Mataifa la 1718 mnamo Oktoba 2006. Hivi karibuni Kim Jong-un alijivunia kuwa “uvamizi wa mtandao ni, pamoja na makombora na silaha za nyuklia, ni ‘upanga unaokata pande zote’ ambao unahakikisha kuwa jeshi letu lina uwezo wa kuvamia bila huruma."[1] Aliyekimbia jeshi la Kore a Kaskazini aliripoti kuwa kikosi cha mtandaoni kinachukuliwa kama silaha yenye nguvu zai

[1] kulingana na ripoti ya kituo cha utafiti kilichoko Washington kiitwacho Kituo cha Mafunzo ya Kimika kati na Kimataifa

di kwenye “Vita vya Siri” [2] na wanachama wake wanachukuliwa kama sehemu ya mabwen yenye, ikiwa mojawapo kati ya nyadhifa chache zinazolipa vizuri.

Je, watafanya nini zaidi ya haya? Ushahidi unadokeza kuwa wahusika wa serikali ya Korea K askazini na vibaraka wao wasio wa serikali wanazidi kutumia teknolojia za kuficha utambuli sho kama vile sarafusimbwa, mtandao wa giza, usimbaji, na uvamizi wa mtandaoni wa hali y a juu ambao ni taabu kugunduliwa. Ripoti ya Jopo la Wataalamu la Umoja wa Mataifa imekis ia kuwa Korea Kaskazini imepata milioni $571 USD kwa kuiba sarafusimbwa pekee.

Uchunguzi huu wa kifani kwanza utaangazia asili za kikosi cha mtandaoni cha Korea Kaskazi ni kwa kuangalia uvamizi uliorekodiwa uliotekelezwa kwa kutumia mbinu za jadi za kuvunja mifumo, kuorodhesha mikakati iliyotumiwa kwenye uvamizi na uingiliaji wa kitambo, na ku angalia ripoti zinazohusu Korea Kaskazini kuanza kutumia teknolojia za hali ya juu zaidi. Ma kala haya yatatamatishwa kwa mapendekezo ya hatua za miongozo ya udhibiti na usalama wa mtandaoni inayofaa kuidhinishwa.

Sekta ya Mtandaoni na Vikwazo vya Umoja wa Mataifa: Muktadha wa Udhibiti

Wajasiriamali wa teknolojia wanaotumia uwezo ukatizaji na ubadilishaji wenye kunufaisha s ana wa teknolojia dijitali kihistoria walishawishiwa na viwango hafifu vya udhibiti. Hata hivy o, utambuzi wa athari inayoweza kuwa na madhara ya teknolojia hizi mpya kwenye masuala ya siasa, usalama, na jamii sasa imewatia ari wadhibiti wa Marekani na Ulaya waingilie kati d hidi ya, na waadhibu, kampuni za teknolojia zinazokiuka viwango vya kitaifa na kimataifa.

Ingawa mipangilio ya kitaifa ya kudhibiti mtandao imeidhinishwa na nchi 138, nchi nyingi zi nadumisha makini kwenye kuzuia uhalifu nchini bila kujali kuhusu athari kwa usalama wa ki mataifa inayosababishwa na kujihami kwa sekta ya mtandao.[3] Baraza la Usalama la Umoja

[2] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

[3] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

wa Mataifa limeshughulikia vitisho hivi vya mtandaoni kwa mbinu isiyo na mpangilio na isiy odumu, licha ya kuwa na zaidi ya miaka 20 ya ripoti na ushahidi kuhusu jinsi teknolojia dijita li imekuwa ikizidisha viti na kuwanufaisha wahusika waliowekewa vikwazo. Hadi leo, Maafis a wa Kikazi wa Matendo ya Kifedha (FATF) inabadilisha polepole mapendekezo yake ya kuzu ia na kulinda dhidi ya mifumo dijitali ya kupinga ulanguzi wa pesa (AML), kupinga ufadhili w a ugaidi (CTF), na kupinga ufadhili wa usambazaji.

Kumekuwa na hatua huria kwenye mwelekeo wa vikwazo vya mtandaoni. Kwa mfano, Mare kani iliwekea vikwazo akaunti mbili za sarafusimbwa zilizokuwa zinamilikiwa na wananchi w a Irani, na EU imetoa mwongozo fulani, ikiwemo zana ya diplomasia ya mtandaoni. Licha ya haya, hatua hizi hazijafikia mbinu pana inayohitajika.

Kama inavyoorodheshwa kwenye vifungu vifuatavyo, matumizi anuwai ya teknolojia dijitali yanayofanywa na Korea Kaskazini yanaashiria changamoto mseto inyokumba utekelezaji sh eria wa vikwazo kwenye sekta ya mtandaoni. Uwezo unaoonekana wa Korea Kaskazini kuwe za kutekeleza uvamizi madhubuti, usiogunduliwa kwa urahisi, na unaogharimu kidogo mtan daoni ili kupata data au mali ya kifedha yanayomilikiwa na serikali, kampuni, na watu binafs i ni kihamasishi kikuu cha kuidhinisha vifaa vya ushambulizi vya maelezo na dijitali. Pia kuna haja kwa viongozi wa sekta na watungaji kanuni kushughulikia kutumiwa kwa programu zisi zokuwa na madhara za raia kama vile sarafusimbwa au ngao za utambulisho kwenye uvami zi wa mifumo.

Kwenye daraja ya kimataifa, vikwazo viliopo dhidi ya Korea Kaskazini haviainishi matumizi mabaya ya miundombinu ya kimataifa ya mtandao kama matendo ya kuwekewa vikwazo. K wa ajili ya asili tata ya kushughulikia vitisho vya mtandaoni vinavyohusu Korea Kaskazini, vi ongozi legevu wa sekta na serikali wanajitia kwenye hatari ya:
(1) wananchi wa Korea Kaskazini kuvamia au kujitayarisha kuvamia mifumo yao ya kompyut a, ambao unasababisha upotezaji mapato, data muhimu, na uwezo wa kishughuli;
(2) kushindwa kwenye utiifu na upotezaji hadhi unaotokana na matendo ya Korea Kaskazini yanayosababisha ukiukaji wa vikwazo; na
(3) kuachwa nyuma kwenye juhudi na jitihada za kudhibiti sekta ya teknolojia, ambayo ina u wezekano wa kuwa na athari pana kwenye uchumi na usalama wao wa nchi.

Kwa ziada, kwenye maeneo ambapo sekta ya usalama mtandaoni na usimamizi wa serikali hauna njia zilizoimarishwa za ushirikiano na kushiriki elimu, kuna uwezekano mdogo zaidi w a kuitikia uvamizi wa mtandaoni kwa ufanisi na/au kwa kuwajibika.

Mitandao ya Wavuti ya Korea Kaskazini

Inakisiwa kuwa Korea Kaskazini ina hadi askari jeshi 6,000 wa mtandaoni, waliopangwa kwe nye vikundi tofauti vinavyojulikana kama Lazarus, Bureau 121, Hidden Cobra, Bluenoroff, Ap t 38, TEMP.Hermit, na Andariel. Mchango mkubwa wa silaha ya mtandaoni ya Korea Kaskazi ni unatokana na kuchuja mfumo wa elimu wa Korea Kaskazini, kuanzia utotoni, wa watoto wenye akili bora kabisa za kiufundi ili wapelekwe kwenye masomo ya uhandisi na sayansi za kompyuta, na mbeleni kwenye Chuo Kikuu cha Sayansi na Teknolojia cha Pyongyang (PUST), chuo kikuu pekee kinachofadhiliwa kutoka ng'ambo kilichoko nchini. PUST ilifunguliwa mn amo 2010 kwa mkataba baina ya serikali ya Korea Kaskazini na Taasisi ya Asia Kaskazini Mas hariki ya Elimu na Utamaduni (NAFEC). Baadhi ya wanaojitolea kutoka nje wanafanya kazi k wenye chuo kikuu, huku wengine wanakuja kwa wiki chache ili kufunza kozi.

Mnamo 2015, aliyekimbia Korea Kaskazini, Jang Se-yul, ambaye anasema kuwa alikuwa mm ojawapo kati ya viongozi wa kikosi cha mtandaoni, aliripoti kuwa mafunzo ya PUST yaliwata yarisha wanafunzi waweze kuvunja mifumo. PUST inakataa madai haya, ikidai kuwa hakuna ushahidi wa kutosha. Bila kujali haya, ni ukweli kuwa matokeo mbadala ya kufunzwa usala ma na uhandisi wa kompyuta ni kupata msingi wa jinsi ya kuvunja mifumo. Misingi ya sayan si ya kompyuta, kama vile jinsi ya kuandika programu za kompyuta, kuunda kanuni pepe (ta ratibu za kuchambua data) na kiolesura cha mfumo endeshi wa kompyuta pia ni muhimu sa na kwenye uvunjaji mifumo. Mwanafunzi yoyote halisi wa usalama mtandaoni mbeleni atate keleza majaribio ya uvunjaji mifumo wa ‘kofia nyeupe’, ambapo wanajaribu kuvunja kwe nye mitandao ya maelezo ili kufichua udhaifu wa mifumo hiyo.

Pindi wanapofunzwa vizuri, baadhi ya wanafunzi wanajiunga na kikosi cha mtandaoni huko Korea Kaskazini, huku wengine wanajiunga na timu za ng'ambo ili kutekeleza juhudi za kuvu nja mifumo, au wanaenda ng'ambo ili kuanzisha kampuni zifichazo ili kusaidia ukiukaji wa vi

kwazo.[4] Mashirika binafsi ya usalama yamechambua shughuli za intaneti za watumiaji weny e makao yao makuu nchini Korea Kaskazini ili kuelewa mtandao wa wafuasi walioko ng'amb o, na yalipata ithibati ya wafuasi walioko nchini Bangladeshi, Uchina, India, Indonesia, Keny a, Msumbiji, Nepali and Thailandi.[5]

Silaha kuu ya mtiririko huu wa uhodari ni matumizi ya teknolojia nyingi za hali ya juu, kama vile mbinu za kuficha utambulisho zinazowezesha uvamizi usiofichua utambulisho, na saraf usimbwa, ambazo zinawezesha njia mpya za kuzalisha fedha na kuhamisha kisiri mapato ya kuvunja mifumo. Ili kuonyesha uwezo wake wa kutumia mielekeo mipya ya mtandaoni, Kor ea Kaskazini iliandaa kongamano la blokicheni na sarafusimbwa huko PUST mnamo Aprili 2 019, lilioandaliwa kwa usaidizi wa mjasiriamali wa Uingereza.[6]

Teknolojia muhimu zaidi za kuficha utambulisho zinazotumiwa na Korea Kaskazini, na tekn olojia saidizi, zimefafanuliwa kwenye jedwali lifuatalo.

Teknolojia za Uvamizi Unaoficha Utambulisho na Kuenda Kinyume na Vikwazo

Teknolojia	Ufafanuzi na matumizi ya Korea Kaskazini
Intraneti	mtandao uliojitenga ambao haujaunganishwa na mtandao huria n a wazi ulimwenguni; muunganisho wa ndani wa seva na kompyuta zilizooanishwa ambazo zinaruhusu tu ufikiaji wa kurasa na faili fula ni (k.v. miundombinu ya Intaneti ya Korea Kaskazini ni intraneti ina yoitwa Kwangmyong ambayo inaweza kufikiwa ndani ya mipaka ya Korea Kaskazini tu)
Mtandao wa Giza	sehemu ya Intaneti ambayo haijumuishwi na injini maarufu za utaf utaji kama vile Google au Yahoo, ambayo inamaanisha kuwa kuras

[4] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

[5] https://www.recordedfuture.com/north-korea-internet-usage/

[6] https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-cryptocurrency-blockchain-conference-pyongyang-a8643391.html

Teknolojia	Ufafanuzi na matumizi ya Korea Kaskazini
	a hizi si rahisi kugunduliwa isipokuwa ikiwa mtumiaji anajua pale p a kutafuta; ambapo shughuli haramu zinaweza kutokea bila kugun duliwa, kama vile makongamano na sehemu za soko za kupata sila ha, mali ya kiakili yaliyoibwa na kadhalika.
Tor	kivinjari kinachoruhusu ufikiaji wa mtandao wa giza. Inaweza kupa kuliwa bure na mtu yoyote ambaye ana ufikiaji wa Intaneti
Usimbaji	kusimba data kwa misimbo ya sisi inayomilikiwa na washiriki wana onuiwa tu. Inatumiwa ili kutuma ujumbe uliosimbwa, ili maelezo ya weze kupitishwa kwenye itifaki za Intaneti bila kugunduliwa, na pia inatumiwa kama kijenzi cha usanifu wa kimsingi ili kuunda sarafusi mbwa. Wananchi wa Korea Kaskazini walitumia programu ya kutu ma ujumbe uliosimbwa, WeChat ili kuratibu uhamishaji baina ya m eli
Sarafusimbwa	aina ya pesa dijitali, ambapo kila toleo kina sheria maalum za jinsi k oini zinazalishwa na jinsi zinavyoweza kutumiwa. Inatumia usimbaj i ili kuzifanya koini zisiweze kufuatiliwa na kuficha utambulisho wa watumiaji, ambayo inamaanisha kuwa utambulisho halisi hauhitaji ki ili kuzipata au kuzibadilisha. Kila sarafusimbwa, miongoni mwa maelfu, zina sheria zao zenyewe na matakwa ya soko ya kupata koi ni. Miamala inarekodiwa kwenye ratiba ya pamoja, inayoitwa bloki cheni
Blokicheni	hifadhidata inayojumuisha ratiba maalum ya miamala ya sarafusim bwa. Pindi maingizo yanapofanywa, huwa ni taabu au inagharimu s ana kuyabadilisha, kwa hivyo, ni njia muhimu ya kufuatilia data ‘i nayoaminiwa’ kila muda unapopita. Kila muamala huwa unaonek ana milele na mtandao mzima. Sarafu ya kienyeji ya blokicheni kwa jumla huwa inahitajika ili kuingiliana kwenye mtandao. Mitandao hi i ya blokicheni na sarafu zao inaweza kuwepo hadharani, kama vile Bitikoini, au kwa faragha, ambapo inaweza kutumiwa na kikundi te ule

Teknolojia	Ufafanuzi na matumizi ya Korea Kaskazini
Mtandao Pepe wa F aragha (VPN)	huduma inayomruhusu mtumiaji aunde lango la faragha ili kufikia i ntaneti ya hadharani bila utambulisho kujulikana, ili data, maelezo na ufikiaji wao wa mtandao usiweze kufuatiliwa na/au yaliyomo ya o hayawezi kutazamwa wala kupigwa marufuku
Seva Pepe ya Farag ha (VPS)	huduma ya kuweka programu za mtandao ambayo haihitaji matu mizi ya seva ya mtu mwingine kama vile Google, Microsoft, au Amaz on
Usalama wa Daraja ya Usafiri (TLS)	Daraja ya ziada ya usimbaji inayoongezwa kwenye mitandao ya ma elezo ili kuhakikisha kuwa data yote inayohamishwa kupitia mtand ao haipatikani wala haitazamwi kwa urahisi
Mitandao ya Kijamii	mitaa ya mtandaoni, au sehemu kwenye ulimwengu dijitali ambap o watu wanaingiliana. Kwenye mfano wa Korea Kaskazini, mitanda o ya kijamii ni muhimu ili kusambaza propaganda yao kwa wafuasi wao walioko ng'ambo, na pia kuunda akaunti bandia ili kuzisaidia bishara zifichazo na kutekeleza mikakati mingine ya uvamizi wa mif umo bila kufichua utambulisho wao halisi

Kuanzia Aprili 2018, watafiti wa usalama walipata ongezeko la 1,200% kwenye matumizi ya huduma binafsi za Intaneti, ambazo zinasaidia wananchi wa Korea Kaskazini kwenye utafiti na uvamizi wao. Vifaa hivi, pamoja na Intraneti ya Korea Kaskazini iliyokwamizwa sana, Kwa ngmyong, zinapunguza uwezo wa ujasusi wa mtandaoni na mawakala ya usalama wa kuele wa kikamilifu kikosi cha mtandaoni cha Korea Kaskazini.[7]

Wananchi wa Korea Kaskazini bado wanatumia mtandao wa umma, haswa mitandao ya kija mii, ili kuratibu kuenda kinyume na vikwazo. Wamekuwa wakijitenga na mitandao ya kijamii ya Kimagharibi tangu mwisho wa 2017 na wamekuwa wakitumia matoleo ya Kichina, amba po wanaweza kujiingiza kwa urahisi bila kutambuliwa. Ambayo hayawiani na haya ni kuend elea kutumia LinkedIn, ambayo bado inaendelea kuwa muhimu ili kuunda lakabu bandia (y

[7] https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/#more-29249
ripoti ya matumizi ya intaneti

aani, lakabu isiyokuwa na uhusiano na Korea Kaskazini) ili kuimarisha kampuni zifichazo, ku unda uhusiano na wale wenye uwezekano wa kuwa waathiriwa wa uvamizi wa mtandaoni n a kuelewa vizuri jinsi ya kuvunja mifumo yao, na kukuza fursa za kibiashara kama vile sarafu mpya za dijitali. Matukio haya yanaendelea kuorodheshwa kwenye vifungu vifuatavyo.

Mbinu zinazotumiwa na Korea Kaskazini ili Kuenda Kinyume na Vikwazo

Jedwali lifuatalo ni ufafanuzi wa mbinu zinazotumiwa na wananchi wa Korea Kaskazini kwe nye uvamizi anuwai.

Mbinu	Ufafanuzi
Virusi vya Kudhuru	Wavunjaji mifumo wanasakinisha programu ya kompyuta yenye madhara kwenye kompyuta ya mwathiriwa inayoweza kutimiza malengo anuwai, k ama vile kumpatia mvunjaji mifumo ufikiaji wa kompyuta ya mwathiriwa
Vibotipepe	Wavunjaji mifumo wanapoteka nyara kompyuta nyingi na kujenga miund ombinu ya kuratibu uvamizi ambayo inahitaji kiasi kikubwa cha nguvu ya usindikaji kama vile DDOS (ijayo)
Unyimaji Hud uma Uliosam bazwa (DDO S)	Kutumia kompyuta nyingi (mara nyingi viboti pepe) ili kujaribu kufikia uku rasa fulani wa mtandao ili ipatiwe uzito kupita kiasi na iache kufanya kazi. Uvamizi huu huwa mara nyingi unalenga kuharibu bishara (k.v. biashara y a kawaida kutoweza kuendelea)
Utapeli Data	Kutuma mawasiliano bandia kama vile baruapepe bandia zinazowahadaa watumiaji waingize manenosiri yao kwenye ukurasa wa mtandao unaomil ikiwa na wavunjaji mifumo, na/au kupakia faili bandia inayojumuisha viru si vya utekaji nyara
Utapeli Data wenye Shaba ha	Inafanana na utapeli data isipokuwa waathiriwa huwa wanalengwa kwa makini zaidi, baada ya utafiti wa usuli kufanywa na wavamizi, ili kung'amu a yale ambayo mwathiriwa anaweza kuhadaiwa nayo kwa urahisi, kama vi le kwa kuunda akaunti bandia na kufanya urafiki naye kwenye mitandao y

Mbinu	Ufafanuzi
	a kijamii
Kufyonza Udhaifu wa Mfumo	Kutafuta upungufu kwenye miundombinu/mifumo endeshi kama vile Microsoft Windows ambao utawawezesha wavunjaji mifumo waifikie kompyuta. Upungufu huu ni muhimu kwa wavunjaji mifumo ili waweze kuratibu uvamizi uliosambaa unaoathiri waathiriwa wengi kwa wakati mmoja; waathiriwa ambao wote wanatumia programu sawia yenye upungufu huo
Virusi	Programu ya kompyuta iliyobuniwa ili kuambukiza kompyuta na kusababisha matokeo maalum (k.v. kuangamiza faili, kuiba maelezo) ambayo inajisambaza yenyewe, yaani inatafuta njia ya kuambukiza kompyuta nyingi iwezekanavyo kupitia kompyuta iliyoambukizwa, na kwa haya, kusababisha uharibifu wa kiasi kikubwa kwa kipindi kifupi cha muda
Ubadilishanaji/Biashara ya Sarafusimbwa	Sekta iliyonawiri ya huduma inayoruhusu watumiaji wabadilishe sarafusimbwa ziwe sarafusimbwa zingine na sarafu rasmi (sarafu zinazoidhinishwa na serikali). Kuhusiana na Korea Kaskazini, ubadilishanaji huu unaweza kubadilisha koini zilizoibiwa ziwe pesa taslimu, na/au kuficha kwa urahisi umiliki halisi wa koini zilizoibiwa kwa kubadilisha sarafusimbwa moja ili kupata nyingine. Kuna vituo vingi vya ubadilishaji wa sarafusimbwa vinavyowezesha ubadilishanaji bila udhibiti wowote.
Uchimbaji Sarafusimbwa	Kila sarafusimbwa ina sheria zilizobainishwa za jinsi koini mpya zinaweza kupatikana, ambayo mara nyingi inahitaji kutumia kompyuta maalum zenye GPU zenye nguvu za kusindika data mara kwa mara zinapokuwa zinashindana ili zijishindie koini mpya zinazotolewa kwenye kiasi fulani cha muda
Toleo la Awali la Koini (ICO)	Uzalishaji wa sarafusimbwa mpya wenye kufanya mchango wa fedha ili kuuza mapema sehemu ya koini hizo, pamoja na ahadi za jinsi watumiaji watakavyoweza kuzitumia koini, mara nyingi kwa matarajio ya mapato ya fedha
Uvamizi wa Kishawishi	Mvamizi anaathiri tovuti inayomvutia mtu/watu wanaolengwa na anaongeza msimbo ili kumhadaa mtumiaji aende kwenye ukurasa mpya wa tovuti utakaomhadaa asakinishe virusi vya kudhuru

Mbinu	Ufafanuzi
Virusi vya Utekaji Nyara (ai na ya virusi)	Virusi vya utekaji nyara vitakavyosimba hifadhi kuu ya mwathiriwa na kuitisha fidia kwenye kipindi fulani cha muda ikiwa mwathiriwa anataka data yake irudishwe, lau sivyo ipotee milele

Mbinu Maalum zinazotumiwa ili Kuenda Kinyume na Vikwazo

Ingawa mbinu zilizozungumziwa hapo juu zinaweza kuwa vijenzi pweke vya uvamizi au upataji, mara nyingi zinachanganywa pamoja kwenye mbinu zifuatazo na kurudiwa kwenye mat ukio kadhaa.

Mbinu za Kudhuru Maadui, Kuiba Maelezo, na Mara Nyingine Kudai Fidia

Wananchi wa Korea Kaskazini wana historia ya kutekeleza uvamizi wa mtandaoni ili kudhuru maadui wao. Wameweza kusababisha uharibifu mwingi, kama vile kwenye mfano wa uvamizi wa Sony Pictures. Kwa ajili ya kukaribia kutolewa filamu inyoonyesha kuuawa kwa Kim Jong-un, wavamizi wa Korea Kaskazini waliharibu faili, walitoa maelezo nyeti, kama vile maelezo ya mishahara ya waajiriwa, ambayo ilisababisha janga la kutokuwepo kwa usawa wa kijinsia kwenye kampuni hiyo, na kusababisha hasara ya milioni $100 USD ya uharibifu unaohusu mtandao kwa kampuni hiyo.

Kama inavyoonyeshwa kwenye jedwali lifuatalo, uvamizi wa mifumo unaotekelezwa na Korea Kaskazini unabadilika na kujumuisha njia za kuzalisha mapato mbali na kusababisha madhara. Virusi vya Wannacry vya 2017 vilisambaa kote ulimwenguni, na kuambukiza kompyuta na kusimba data yao yote. Wannacry kisha iliamilisha dai linalotegemea wakati la malipo ya fidia kupitia bitikoini, ikiwa watumiaji wanataka kurudishiwa data yao. Kwa sababu ni vigumu kuhusisha bitikoini na wamiliki halisi, ni vigumu sana kujua ni kiasi gani cha pesa kilichopewa Korea Kaskazini kutokana na uvamizi huu. Angalau $140,000 USD ilifuatiliwa, ingawa kuna uwezekano mkubwa kuwa kiasi halisi ni kikubwa zaidi. Hata hivyo, uharibifu uliofanywa kwenye biashara zilizoambukizwa ulisababisha gharama ya mamilioni ya pesa na mara nyingi ulisababisha matokeo mabaya sana, kama vile kuzimwa kompyuta muhimu sana kwenye hospitali za Uingereza.

Matukio (mpangilio wa wakati)	Mbinu Zilizotumiwa	Uharibifu Ujulikanao Kufanyika
DDOS (2009)	kibotipepe, ddos	Milioni $31 hadi milioni $46 USD za uharibifu
DDOS (2011)	kibotipepe, ddos	tovuti 40, diski kuu 820 ziliambukizwa
320 Dark Seoul (2013)	utapeli data wenye shabaha, virusi vya kudhuru	data iliyoangamizwa, milioni $75 USD za ukarabati
Sony Pictures (2014)	utapeli data wenye shabaha, virusi vya kudhuru	jaribio la utekaji nyara ambalo halikufaulu la maelezo nyeti yaliyoibiwa, kisha ikayavuja maelezo na kusababisha uharibifu wa sifa, na gharama za kurekebisha mifumo ya kompyuta ~ milioni $100
Uvamizi wa Korea Hydro & Nuclear Power (2014)	utapeli data wenye shabaha, virusi vya utekaji nyara	ilishambulia mifumo ya waajiriwa 3,571 wa na kujaribu kuangamiza diski zao za kompyuta. Wavamizi mifumo walipata na kutoa ramani za ujenzi wa mitambo misita ya kuzalisha nishati ya nyuklia kwa nyakati sita tofauti kwenye Twitter na ikadai bilioni $10 USD
Interpark (2016)	virusi vya utekaji nyara	ilivuja maelezo binafsi ya watumiaji milioni 10.3. Ilijaribu kudai fidia ya milioni $2.7 kwa bitikoini
Kampuni zisizojulikana kwenye sekta za ulinzi (2016)	kufyonza udhaifu wa mfumo	ilipata na kuvuja data ya kisiri, kama vile ramani za ujenzi wa ndege
Mamlaka ya Usimamizi wa Fedha nchini Poland (2017) miongoni mwa shabaha zingine	uvamizi wa kishawishi, virusi vya kudhuru	ilielekeza benki zilizokuwa zinazuru tovuti hadi kwenye ukurasa mbadala ambapo waathiriwa wanashawishiwa wapakue virusi vya utekaji nyara. Labda ilitumiwa kwenye uvamizi wa SWIFT (kifungu kifuat

Matukio (mpangilio wa wakati)	Mbinu Zilizotumiwa	Uharibifu Ujulikanao Kufanyika
		acho)
Virusi vya Wannacry (2017)	matumizi ya udhaifu wa mfumo ili kuingiza virusi vya utekaji nyara ambavyo vilisimba faili za kompyuta zinazolengwa na kudai fidia ya bitikoini ili kuokoa faili	angalau $140,000 USD za sarafusimbwa zilipewa Korea Kaskazini, uharibifu madhubuti ulifanywa kwa biashara na taasisi kama vile hospitali za Uingereza
Jopo la Wataalamu la Umoja wa Mataifa Linaloangazia Korea Kaskazini	haijulikani	liliendea kinyume kamati kwa kuchelewesha utoaji wa ripoti yao kuhusu Korea Kaskazini

Mbinu za Kuzalisha Mapato Pekee

Kwenye miaka ya hivi karibuni wananchi wa Korea Kaskazini wameonyesha kuwa wanapendelea kuzalisha mapato kupitia uhodari wao mtandaoni. Mnamo Februari 2016, wavunjaji mifumo wa Korea Kaskazini walitapeli data kwa kulenga waajiriwa wa Benki Kuu ya Bangladeshi na wakasakinisha virusi vya utekaji nyara ili kupata vyeti vyao halali vya mfumo wa ulimwengu wa kutuma ujumbe baina ya benki wa SWIFT. Kisha wakaathiri akaunti ya Bangladeshi kwenye Hazina ya Taifa la Marekani na wakajaribu kuhamisha USD milioni $951 la fedha za benki hiyo hadi kwenye akaunti kote ulimwenguni, lakini wakaweza kupata USD milioni $81. Pesa hizo zikaenda kwenye akaunti nchini Ufilipino na ikalanguzwa kupitia akaunti kadhaa za benki, biashara ya kupokea pesa, na kasino.[8] Ushambulizi sawia wa mfumo ulijaribiwa mara kadhaa kwenye benki kote ulimwenguni, huku uvunjaji mwingine wa mifumo ukifaulu kupata USD milioni $10 hadi 15 kwa kila uvamizi.

[8] https://www.thecipherbrief.com/kim-digs-cybercrime-coin-sanctions-cant-snatch

Baada ya uvamizi huu, wavunjaji mifumo wa Korea Kaskazini walianza kudumisha makini k wenye juhudi zao kwenye vituo vya ubadilishanaji wa sarafusimbwa, huduma zinazofanya k azi kama benki za mtandaoni za kubadilishana sarafusimbwa anuwai. Wahalifu walilenga vi pochi dijitali ambapo vituo vya ubadilishanaji wa sarafusimbwa vinahifadhi fedha zinazowe kwa baina ya miamala ya wateja. Vipochi hivi vinavutia sana kwa sababu vina kiasi kubwa ch a fedha za wateja. Kuiba saini dijitali (manenosiri) yanayodhibiti vipochi hivi na kuzielekeza upya fedha kunazalisha mapato mengi sana.

Korea Kaskazini ilihusika kwenye 75% ya uvamizi wa mifumo ya vituo vya ubadilishanaji sar afusimbwa ulioripotiwa (jumla ya USD milioni ~$882) kuanzia mwisho wa 2016 hadi Majira y a Kupuputika ya 2018. Kipato hiki cha dijitali ni taabu kufuatiliwa na kwa hivyo kinaweza kut umiwa kuenda kinyume na kukiuka ukwamishaji mali na vikwazo vya Umoja wa Mataifa.

Matukio Yajulikan ayo (mpangilio wa wakati)	**Mbinu Zilizotumiwa**	**Madhara Yaliyofanyika / Athari zinazokisiwa**
Wizi wa mtandaoni wa Benki ya Bangla deshi (2016)	utapeli data wenye shabaha, virusi vya utekaji nyara, uhamishaji pesa kitapeli k upitia SWIFT	iliiba USD milioni $81
Ilivunja mifumo ya kasino za mtandao ni (2016, 2017)	virusi vya utekaji nyara, viliingiza kilagh ai kwenye mchezo wa kamari	haijulikani
Benki ya Kimataifa ya Far Eastern (201 7)	utapeli data wenye shabaha, virusi vya utekaji nyara, uhamishaji pesa kitapeli k upitia SWIFT	USD milioni $60 ilihamishw a, lakini nyingi kati ya hizi zi lirejeshwa
Standard Chartere d Plc - Bancomext (2018)	utapeli data wenye shabaha, virusi vya utekaji nyara, uhamishaji pesa kitapeli k upitia SWIFT	jaribio lililoshindikana la k uvamia mifumo ili kupata USD milioni $110, ingawa U SD milioni $15 iliibiwa kuto ka kwenye uvamizi mwingi

Matukio Yajulikanayo (mpangilio wa wakati)	Mbinu Zilizotumiwa	Madhara Yaliyofanyika / Athari zinazokisiwa
		ne uliofanywa kwenye ben ki za Meksiko
Banco de Chile (2018)	utapeli data wenye shabaha, virusi vya utekaji nyara, uhamishaji pesa kitapeli kupitia SWIFT	USD milioni $10 ilipatikana, nyingi zilihamishwa hadi kwenye akaunti huko Hong Kong
Duka la Open Bazaar la bidhaa za Korea Kaskazini -(tangu 2016)	iliunda duka la kuuza vipengee maalum vya Korea Kaskazini kama vile sigara, pesa, na stempu	haijulikani
Kituo cha ubadilishanaji cha Yazipon (2017)	utapeli data wenye shabaha ili kupata nenosiri la akaunti ya ubadilishanaji, kituo cha ubadilishanaji wa sarafusimbwa	USD milioni $5.3 ziliibiwa
Virusi vya utekaji nyara vya Andariel (2017)	ilisakinisha virusi vya utekaji nyara vilivyochimba sarafusimbwa kwenye kompyuta iliyolengwa	koini 70 za onero coins, USD $26,000 zilipatikana
Kituo cha ubadilishanaji cha Coinis (2017)	utapeli data wenye shabaha ili kupata nenosiri la akaunti ya ubadilishanaji, kituo cha ubadilishanaji wa sarafusimbwa	USD milioni $7 ziliibiwa
Kituo cha ubadilishanaji cha Youbit (2017)	utapeli data wenye shabaha ili kupata nenosiri la akaunti ya ubadilishanaji, kituo cha ubadilishanaji wa sarafusimbwa	USD milioni $5,6 ziliibiwa
Kituo cha ubadilishanaji cha Coincheck (2018)	utapeli data wenye shabaha ili kupata nenosiri la akaunti ya ubadilishanaji yenye sarafusimbwa mpya iitwayo Koini ya NEM, kituo cha ubadilishanaji wa sarafusimbwa	USD milioni $534 ziliibiwa

Matukio Yajulikanayo (mpangilio wa wakati)	Mbinu Zilizotumiwa	Madhara Yaliyofanyika / Athari zinazokisiwa
Kituo cha ubadilishanaji cha Bitthumb (2018)	utapeli data wenye shabaha ili kupata nenosiri la akaunti ya ubadilishanaji, kituo cha ubadilishanaji wa sarafusimbwa	USD milioni $32 ziliibiwa
Interstellar, Stellar, HOLD, au HUZU (2018)	toleo la Awali la Koini (ICO) la sarafusimbwa mpya; jina lilibadilishwa mara nyingi ili kujaribu kuficha asili	haijulikani
MarineChain (2018)	ICO ya sarafusimbwa mpya iliyodai kuwa inauza umiliki wa meli kubwa ili kutapeli watu.	fedha zilizopatikana hazijulikani kwa ajili mradi ulififia ulipofichuliwa. Hata hivyo, inaashiria mbinu mpya ya kukwepa vikwazo vilivyowekewa usafirishaji bidhaa kwa kuunda njia mpya ya kuficha umiliki wa chombo cha usafiri
Kuchimba/kubadilishana sarafusimbwa (2015 - sasa)	kutumia kompyuta nchini Korea Kaskazini ili kuchimba sarafusimbwa anuwai kisha kuzibadilisha ziwe sarafu inayotumika, au kuzitumia kununua bidhaa zinginе	inakadiriwa kuwa laki $1.50/$2.00 USD zilipatikana kwa mwaka

Ni wazi kuwa, kila muda unapoendelea, wavunjaji mifumo wa Korea Kaskazini wanaelekea kwenye uvamizi wa kuzalisha mapato, haswa ule unaotumia viwango dhaifu vya udhibiti unaozunguka sarafusimbwa. Inaonyesha wazi kuwa wananchi wa Korea Kaskazini wako kwenye nafasi murwa ya kufaidika na mielekeo ya kiteknolojia. Uvamizi wao wa vituo vya ubadilishanaji wa sarafusimbwa na ICO unawiana vizuri na bashasha ya dhana iliyotokea mwisho wa mwaka wa 2017 hadi mwanzo wa mwaka wa 2018 wakati thamani ya soko ya sarafu dijitali il

ifikia kilele. Soko zima la koini hizi lilibadilika baina ya dola bilioni $128.9 na bilioni $818.1 za Marekani.[9]

Hatua za Mapendekezo za Usalama Mtandaoni

Ili kushughulikia vitisho hivi, hatua za usalama mtandaoni zinaweza kuidhinishwa na, amba po inafaa, zinaweza kuhitajika na kanuni. Nyanja mbili muhimu zaidi za kuzuia uvamizi mtan daoni ni:

(1) Kumuelimisha mwajiriwa jinsi ya kutambua majaribio ya kuvunja mifumo kama vile utap eli data wenye shabaha na viambatisho vinavyoshukiwa

Bila kujali daraja ya usalama ya teknolojia mpya kama vile blokicheni, mbinu kama vile utap eli data wenye shabaha zitapendelewa kama mbinu za kuathiri mifumo. Uhalalishaji wa vige zo viwili unaweza kupunguza athari ya ukiukaji, lakini hauchukui nafasi ya kuhitaji kuelimish wa.[10] Mradi bora kabisa wa elimu unajumuisha mtaala unaoonyesha mifano ya kitambo yen ye mitihani ambapo waajiriwa wanaweza kutambua faili / baruapepe inazoonekana kuwa ni za kitapeli. Mwishowe, waajiriwa wa IT wanafaa kujihusisha mara kwa mara kwenye uvamizi wa ‘kofia nyeupe’, ambapo wanajaribu kuwahadaa waajiriwa kwa jaribio la kuvunja mifu mo linaloigizwa.

(2) Kudumisha itifaki za mfumo wa IT ziwiane na viwango vya sekta ya usalama mtandaoni, i kiwemo kuwa na ufahamu wa uvamizi wa hivi karibuni wa mtandao.

[9] https://coinmarketcap.com/charts/

[10] uhalalishaji wa vigezo viwili ni taratibu ya usalama inayomhitaji mtumiaji athibitishe utambulisho w ake mbali na kuingiza msimbo uliopokewa kwenye kifaa cha simu. Ni bora kutumia programu ili kute keleza uhalalishaji kuliko kutumia nambari ya simu ya mkononi kwa sababu nambari za simu zinawez a kudhibitiwa kwa urahisi zaidi na wavunjaji mifumo.

Kama ilivyotajwa kwenye ripoti hii, uvamizi mwingi wa Korea Kaskazini unalenga udhaifu kw enye itifaki za mfumo wa uendeshaji. Timu za usalama/IT zinafaa kudumisha ufahamu wao kwa:

- Kuunda manenosiri madhubuti[11] na kutekeleza mfumo unaohitaji kubadilisha manen osiri mara kwa mara na, ikiwezekana, kutumia mfumo wa kudhibiti manenosiri;
- Kushughulikia matoleo yote ya viraka na kuyahusisha kwa upesi;
- Kusombeza mifumo endeshi ya kitambo iwe mifumo ya hivi karibuni;
- Kudumisha programu ya hivi karibuni ya kulinda dhidi ya virusi, inapohusika, na kuch anganua programu zote zinazopakuliwa kutoka Intaneti kabla ya kuzisakinisha;
- Kuzuia uwezo (vibali) vya watumiaji vya kusakinisha na kuendesha programu zisizota kikana na kuhusisha kanuni ya uhuru kidogo zaidi kwa mifumo na huduma zote;
- Kuchanganua na kuondoa viambatisho vya baruapepe vinavyoshukiwa. Kampuni na mashirika yanaweza kuzuia ujumbe wa baruapepe zinazotoka kwenye vyanzo vinavy oshukiwa ambazo zinajumuisha viambatisho;[12] na
- Kuwezesha kilinzi binafsi kwenye kompyuta za shirika na kukisanidi kikate maombi y a miunganisho yasiyoitishwa.

Kushughulikia Virusi vya Utekaji Nyara

- Cheleza mifumo mara kwa mara, na idumishe nakala iiliyosimbwa ya hifadhi rudufu z a hivi karibuni iwe nje ya kituo na nje ya mtandao
- Kuna programu zinazodai kuwa zinakomesha virusi vya utekaji nyara kwa kuzuia usi mbaji usioruhusiwa wa faili. Maafisa wa usalama wanafaa kukagua vifa hivi.

Udhibiti na Mamlaka

[11] Tazama https://www.us-cert.gov/ncas/tips/ST04-002 ili kupata maelezo zaidi kuhusu kuu nda manenosiri madhubuti.

[12] Ili kupata maelezo zaidi kuhusu jinsi ya kushughulikia viambatisho vya baruapepe kwa usalama, taz ama Kutumia Tahadhari Unaposhughulikia Viambatisho vya Baruapepe. Fuata utendakazi sama unap ovinjari mtandao. Tazama Tabia Nzuri za Usalama na Kulinda Data Yako ili kupata maelezo zaidi. Kuz uia ruhusa hizi kunaweza kuzuia virusi vya utekaji nyara zisiendeshe au zipunguze uwezo wake wa ku sambaza kwenye mtandao

Kwenye usalama wa mtandaoni, vita vya maelezo, na utungaji kanuni husika, mkakati bora kabisa ni kulishughulikia tishio kabla halijatokea. Kwa nchi na viongozi wa sekta wanaosubir i mwongozo kuhusu kipengee cha mtandaoni cha vikwazo, ni bora kuchukua hatua ili kuhak ikisha kuwa kampuni za teknolojia dijitali zinafanya kazi ili kuhakikisha kuwa ukiukaji wa vik wazo hautokei kwenye sekta ya mtandaoni, na kihivi, kutoa fursa ili sekta isonge mbele kwa mujibu wa viwango vilivyofafanuliwa tayari vya amani na usalama wa binadamu. Pia kampu ni za teknolojia zinahitaji kuwasiliana kuhusu hatua zinazochukua ili kutii vikwazo vya Umoj a wa Mataifa.

Jina linalofaa kupewa kipaumbele zaidi ni utendakazi bora kwenye shughuli za mtandaoni k uchukuliwa jambo sawia kwenye ulimwengu halisi. Mwishowe, hakuna tofauti baina ya ulan guzi wa pesa na mali ya mtandaoni au ya kawaida. Kuwa teknolojia hizi ni mpya na zinaficha utambulisho kunakuza uwezo wa utendakazi wa kilaghai na matendo yenye hatari kufanyw a na mashirika ambayo tayari yamewekewa vikwazo na wahusika wapya wa vitisho. Kwa sa babu ya ongezeko la hatari, ni lazima utendakazi wa uangalifu unaoeleweka uwe madhubuti zaidi. Wahusika wanaopendelea kufanya shughuli kwenye mitandao ya maelezo iliyosimbw a sana au inayotegemea blokicheni wanajitenga na utendakazi wa sekta uliopo na mahitaji y aliyopo ya kuripoti. Kwa hivyo, umakini zaidi unahitajika kwa shirika lolote linalojihusisha k wenye miamala ya silaha au fedha, usafiri wa hewani au baharini, na maingiliano na wafany akazi au wanadiplomasia wa Korea Kaskazini, ambapo matumizi ya majukwaa haya yenye t eknolojia za hali ya juu yanapendekezwa.

Hatua zinazopendekezwa zinajumuisha:

- Kusisitiza ufichuzi kamili wa utambulisho unaoweza kuthibitishwa, lengo la miamala inayopendekezwa, na maelezo yoyote mengine husika yanayoweza kuchukuliwa ku wa ni muamala halisi;
- Kufafanua lengo la shughuli inayotaka kufanywa ili kuhakikisha kuwa hatua zote za k iuchumi zinatimiza malengo halali yanayoeleweka;
- Kuhalalisha wahusika wote waliohusika kwenye kuunda miradi mipya ya mtandaoni, kuhakikisha kuwa ufadhili na mali - bila kujali kama yanalipiwa kupitia sarafu dijitali au la – hayahusu ukiukaji wowote wa vikwazo wala hayatokani na mali yanayofaa ku zuiwa;

- Kulazimu mahitaji ya ufichuzi kwa kampuni yoyote inayotegemea teknolojia ya bloki cheni au mradi wowote wa kuhalalisha uhalali wa mali, yaliyomo kwenye vipochi dijit ali, au malengo ya mikataba maizi;
- Kushiriki maelezo kuhusu uvamizi wowote kwa jamii ya usalama wa mtandaoni na k uongeza ushirikiano kwa utafiti na kanuni;
- Kusisitiza vilinzi mahiri vya usalama wa mtandao kwa taasisi na kampuni za fedha, iki wemo ubadilishaji na watoaji wa sarafusimbwa, kwa kuanza na mafunzo ya virusi vya utekaji nyara/utapeli data/nenosiri na sera ya kulinda mfumo wa fedha wa taifa dhidi ya uingiliaji usioruhusiwa;
- Kuhakikisha kuwa kampuni za kuhifadhi data Mtandaoni zinathibitisha asili ya trafiki ya data kwenye tovuti zinazohifadhiwa nayo haichangii kwenye ukiukaji wa vikwazo;
- Kuhakikisha kuwa kampuni za mitandao ya kijamii au ya kidijitali zinafuatilia matang azo ili kuhakikisha kuwa hayachangii kwenye ukiukaji wa vikwazo; na
- Kulazimu majukumu ya uadilifu kwa wasimamizi wa vituo vya usindikaji wa wingu, ili kukuza ulinzi na kuhakikisha kuwa hawahifadhi shughuli zinazoweza kujumuishwa k wenye vikwazo k.v. virusi vya utekaji nyara.

Unaposhughulikia watu binafsi, kampuni au mashirika ambayo tayari yamewekewa vi kwazo vya Umoja wa Mataifa:

- Zuia biashara yote ya bidhaa, vijenzi au teknolojia zilizowekewa marufuku;
- Zuia akaunti za fedha na vipochi dijitali, na kuwekea onyo ripoti za miamala pale ina pohusika, na
- Zuia shughuli zote dijitali au ufikiaji wa akaunti kwenye majukwaa ya teknolojia dijita li, ikiwemo mitandao ya kijamii, sehemu pepe za soko, programu, usindikaji wa wing u na baruapepe, ikiwa kuna ishara kuwa shughuli zinaweza kuwa zinachangia ukiuka ji wa vikwazo.

Tamatisho

Kukubali uhodari wa kikosi cha mtandaoni cha Korea Kaskazini ni muhimu haswa kwa ajili j umuiya ya kimataifa inaendelea kujaribu kufanya makubaliano ya kupinga usambazaji wa n yuklia na Korea Kaskazini. Kuelewa njia ambazo Korea Kaskazini inatumia ili kupata teknoloj

ia na pesa itabidi kuangaziwe kwenye mazungumzo ya siku za usoni. Ili kung'amua hatua zij azo zitakazofanywa na Korea Kaskazini, itakuwa muhimu kudumisha makini kwenye mwele keo wa sekta ya teknolojia ya kuficha utambulisho, haswa sekta za sarafusimbwa na teknolo jia zilizosimbwa, na kupanua aina za manufaa ambazo mhusika pweke anaweza kupata kut okana na kutokuwepo kwa udhibiti kwenye nyanja hizi. Mawazo kuhusu jinsi Korea Kaskazin i itakavyosonga mbele itaachiwa uchunguzi wa siku za usoni.

Kuhusu Ashley Taylor

	Mtekelezaji, mjasiriamali na mtafiti, Ashley Taylor amejitumbuk iza mzima kwenye mwingiliano wa teknolojia dijitali na usalam a wa kimataifa. Kwa kuwa mwanachama wa kizazi cha kwanza cha wajasiriamali wa blokicheni, Taylor ameng'amua mapema madhara yanayoweza kutokana na mawasiliano yanayosimbw a na teknolojia za leja zinazosambazwa kwenye uadilifu wa bia shara na maendeleo ya kijamii. Kwa kufanya kazi na mashirika ya teknolojia na fedha, sasa anashughulika kuunda mpangilio wa kibinadamu unaohusisha teknolojia mpya na vigezo vya ute kelezaji vinavyounga mkono udumishaji wa amani na usalama kimataifa.