++++

Zararli dasturlarning birinchi bosqichi?

====

#Erta bosqichi

====

Tugagan bosqichi

====

Oxirgi bosqichi

====

Ko‘payish bosqichi

====

++++

Bu viruslar o‘zlarining tarqalishi uchun boshqa bir dasturning makro dasturlash tilidan foydalanadigan viruslardir.

====

#Makro viruslar

====

But sektor viuslar

====

Monkey viruslar

====

Brain viruslar

====

++++

Zararli dasturlarning ikkinchi bosqichi?

====

#Erta Windows bosqichi

====

Tugagan bosqich

====

Ko‘payish bosqichi

====

Erta bosqichi

====

++++

Makro viruslar odatda qaysi hujjatlarni zararlaydi?

====

#MS Word, MS Excel

====

Bloknot, Notepad, Paint

====

MS Access, MS PowerPoint

====

C++, Delphi, C#

====

++++

Ikkinchi bosqichning asosiy viruslari?

====

#Brain

====

Pochta qurti

====

Makro qurt

====

Bloknot, Notepad, Paint

====

++++

Bu viruslar o‘zlarini operativ tizim fayllari sifatida ko‘rsatadi?

====

#Rutkit viruslar

====

But sektor viuslar

====

Makro viruslar

====

Monkey viruslar

====

++++

Erta Windows bosqichining asosiy viruslari?

====

#Pochta qurti Makro qurt

====

Makro qurt

====

Brain

====

Makro viruslar

====

++++

Rutkitlar odatda ……….. tomonidan kompyuterga o‘rnatiladi?

====

#Troyanlar

====

Xakerlar

====

Dasturchilar

====

Foydalanuvchilar

====

++++

Zararli dasturlarning uchinchi bosqichi bu

====

#Tarmoq qurtlaring rivojlanishi

====

Makro qurtlarning rivojlanishi

====

Pochta qurtlaring rivojlanishi

====

Troyan viruslarining rivojlanishi

====

++++

O‘zgaruvchan viruslar …………….?

====

#O‘z-o‘zidan ko‘payadi

====

Diskovodani zararlaydi

====

E-mail pochtani buzib kiradi

====

Dasturlarni bloklab qo‘yadi

====

++++

Qaysi zararli dasturlar internetda keng tarqalganidan keyin mashhur bo‘lgan?

====

#Tarmoq qurtlaring rivojlanishi

====

Pochta qurtlaring rivojlanishi

====

Makro qurtlarning rivojlanishi

====

Troyan viruslarining rivojlanishi

====

++++

Muayyan vaqt kelganda ishga tushadigan viruslar?

====

#Vaqt bombasi

====

O‘zgaruvchan viruslar

====

Makro viruslar

====

But sektor viruslar

====

++++

Zararli dasturlarning to‘rtinchi bosqichi?

====

#Rutkitlar va ransomwares rivojlanishi

====

Tarmoq qurtlaring rivojlanishi

====

Makro qurtlarning rivojlanishi

====

Pochta qurtlaring rivojlanishi

====

++++

Ransomwares?

====

#Pul berib qutqarib qolish

====

Suv shaklidagi belgi

====

Pul berib undan voz kechish

====

Pulli dasturiy ta’minot

====

++++

2010 yilgacha eng xavfli zararlantiruvchi dasturlar?

====

#Rukitlar, Ransomwareslar

====

Ransomwareslar

====

Troyanlar

====

Suv shaklidagi belgi

====

++++

Qonuniy foydalanuvchi?

====

#Legal

====

Mantiqiy

====

Noqonuniy

====

Suv shaklidagi belgi

====

++++

IDS?

====

#tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi.

====

xavfsizlik xizmati lokal tarmoqdagi dasturlar va ma’lumotlar vakolatga ega

====

xavfsizlik xizmati lokal tarmoqdagi barcha resurslardan foydalanish jarayonini kuzatib, bo‘lgan žolatlarni qayd etish bilan shug'ullanadi

====

xavfsizlik xizmati global tarmoqdagi dasturlar va ma’lumotlar vakolatga ega

====

++++

"troyan horse" va "kompyuter virusi"so'zlari birinchi marta ishlatilgan.

====

#1980 yil

====

1982 yil

====

1985 yil

====

1979 yil

====

++++

…….- yil tijorat antivirusining tug'ilgan yili?

====

#1987

====

1980

====

1985

====

1989

====

++++

Saudiya hacker 0XOMAR onlayn 400,000 dan ortiq kredit kartalari tafsilotlari zararlandi bu qaysi yil?

====

#2012

====

2005

====

2010

====

2018

====

++++

Birinchi polimorf viruslari yaratilgan yil?

====

#1990

====

1998

====

1955

====

1966

====

++++

Jinoyat tashkilotlari professional cyberattacks moliyalashtirish boshladi?

====

#2000 yil tahdidlar diversifikatsiya va ko'payishi

====

2000 yil tahdidlar diversifikatsiya, iqtisodiy, injener-texnik

====

Ma’naviy, yaxlitlik, tashkiliy-ma’muriy

====

Huquqiy, tashkiliy-injenerik, ma’muriy-texnik

====

++++

Qaysi yilda AQSh hukumati uchun Markaziy razvedka boshqarmasi sobiq xodimi Edvard Snouden milliy xavfsizlik agentligi (NSA)dan tasniflangan ma'lumotlarni ko'chirib chiqadi.

====

#2013

====

2015

====

2016

====

2020

====

++++

Qaysi yilda zararli xakerlar yahooga kirib, uning 3 milliard foydalanuvchisining hisoblari va shaxsiy ma'lumotlarini buzishdi?

====

#2013-2014

====

2000-2002

====

2011-2013

====

2009-2011

====

++++

WannaCry ransomware bir kunda 230,000 kompyuterlarini zaharlaydi qaysi yilda?

====

#2017

====

2015

====

2016

====

2020

====

++++

bir nechta DDoS hujumlari yangi Zelandiya fond bozorini vaqtincha yopishga majbur qildi?

====

#2019

====

2015

====

2016

====

2020

====

++++

Kompyuter viruslari-…..

====

#Ko‘payish, dasturlarda o‘rnashish, aloqa liniyalari, ma’lumotlarni uzatish tarmoqlari bo‘yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o‘xshash qobiliyatlarga ega

====

Signal bo‘yicha yoki o‘rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infrastrukturalariga o‘rnatiluvchi dasturlanmagan qurilmalar

====

Telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish

====

Snouden milliy xavfsizlik agentligi

====

++++

Intellektual inqilob natijasida ……-yillardan e'tiboran davlatlar kiberdunyo taqdim etgan imkoniyatlardan o‘z harbiy salohiyatlarini rivojlantirish yo‘lida ham foydalana boshladilar.?

====

#1990

====

1997

====

1998

====

1991

====

++++

............ faylni tiklovchi dastur.

====

#Auslogics dasturi

====

Cloud

====

Tools

====

E-Disk

====

++++

Android-antiviruslar ikkita parametrga asoslaymiz bular qaysilar?

====

#Himoya – tahdidlarni samarali aniqlash qobiliyati, Yuzabiliti – mobil qurilmaning ishlashiga ta’siri.

====

Himoya – tahdidlarni samarali aniqlamaydigan qobiliyati, Yuzabiliti – mobil qurilmaning ishlashiga ta’siri.

====

Himoya – tahdidlarni samarali aniqlash qobiliyati, Hujum – mobil qurilmaning ta’siri.

====

Himoya – tahdidlarni samarali aniqlash qobiliyati, tizimli – mobil qurilmaning ishlashiga ta’siri.

====

++++

…. — bu ularning ishlash tamoyili žar bir tekshiriluvchi ob’ektdan (fayldan, yuklovchi sektordan, tizimli reestrdan) nazorat summasini o‘qib olib, uni tegishli ma’lumotlar bazasida saqlashdan iborat.

====

#O‘zgarishlarni qayd qiluvchi revizorlar

====

Skanerlar

====

virus žarakatini cheklovchi blokiratorlar

====

Handy Recovery dasturi

====

++++

SABSA (Sherwood Applied Business Security Architecture) qanday xavfsizlik arxitekturasi ?

====

#amaliy xavfsizlik arxitekturasi

====

nazariy xavfsizlik arxitekturasi

====

amaliy va nazariy xavfsizlik arxitekturasi

====

virus žarakatini cheklovchi

====

++++

Tarmoqlararo žimoya ekrani inglizcha nomini toping

====

#FireWall

====

Network

====

Xavfsiz tarmoq

====

Brandmauer tarmoq

====

++++

Axborotlarni tashkiliy himoyalash elementlari qanday bog‘lovchi omil bo‘lib hisoblanadi?

====

#yagona tizimga

====

sanoqli tizimga

====

sanoqsiz tizimga

====

Xavfsiz tarmoq

====

++++

Kompyuter tizimi (tarmogi)ga ziyon yetkazishi mumkin bo‘lgan sharoit, harakat va jarayonlar uchun nima hisoblanadi.

====

#xavf – xatarlar

====

Himoya va hatarlar

====

Xavfsizlik tizimi

====

Birlashgan tizimlar

====

++++

IT xavflarini o'lchashning alternativ usullari odatda nimalarni uz ichiga oladi?

====

#Tahdidlar, zaifliklar va aktivlar hajmi kabi bog'liq omillarni baholashni o'z ichiga oladi

====

Axborot texnologiyalaridan foydalanish bilan bog'liq har qanday xavf

====

Turli xil hodisalarning yuzaga kelish ehtimoli

====

Zaifliklar va aktivlar hajmi kabi bog'liq omillarni baholash

====

++++

Xavfni minimallashtirish – bu?

====

#tashkilot uchun umumiy xavfni kamaytirish uchun choralar ko'rish

====

Tahdidlar, zaifliklar va aktivlar hajmi kabi bog'liq omillarni baholashni o'z ichiga oladi

====

Axborot texnologiyalaridan foydalanish

====

Turli xil hodisalarning yuzaga keltirish

====

++++

Zaifliklarni tatbiqiy hamda tizimli sathlarda tezdan samarali qidirishni amalga oshiruvchi tarmoq xavfsizligi skaneri. Ushbu skaner har qanday ko‘lamli tarmoqlarda xavfsizlik maqomini nazoratlashning samarali tizimini barpo etadi. Bu qanday Himoyalanganlikni taxlillovchi dastur?

====

#XSpider 7.8

====

Tarmoq revizori

====

Tarmoqlararo ekran texnologiyasi

====

Bitlocker

====

++++

ruxsatsiz foydalanishga urinishlarni bartaraf etishga mo‘ljallangan tarmoq skaneri. Tarmoq revizori TCP/IP steki protokollaridan foydalanuvchi o‘rnatilgan tarmoq dasturiy va apparat ta’minoti zaifliklarini aniqlash uchun ishlatiladi. Bu qanday Himoyalanganlikni taxlillovchi dastur?

====

#Tarmoq revizori

====

XSpider 7.8

====

Skaner BC

====

bitlocker

====

++++

Foydalanuvchilarning Internetdan foydalanishlarini, trafikni qayd etishni va filtrlashni, resurslarni tashqi xujumlardan himoyalashni tashkil etishga mo‘ljallangan.

====

#Usergateproxy&Firewall

====

Trust access

====

Security studio endpoint protection

====

Cisco ids/ips

====

++++

O'g'irlangan ma'lumotlar va shu ma’lumotlarga aloqador kiber jinoyatchilarning mahsulotlarini tarqatish va sotish?

====

#Distribyutorlar

====

Jinoyatchilar

====

Tizim xostlari va provayderlari

====

Tizim xostlari

====

++++

Internet brauzerlarda himoyalangan ulanishlar xavfsizligining muammosini yechish uchun yaratilgan protocol?

====

#SSL

====

UDP

====

FTP

====

HTTP

====

++++

Kiberjinoyat quroli?

====

#internet va eng so’nggi raqamli texnologiyalar.

====

tarmoqlarning foydaluvchilari

====

ishchi stantsiyalar, serverlar, shaxslar

====

professional mutaxassislar ish faoliyati

====

++++

…. - tizimlar va ularda ishlaydigan dasturiy ta'minotdagi xavfsizlik zaifliklarini aniqlash, baholash, davolash va hisobot berish jarayonidir.

====

#Tarmoqdagi zaifliklarni boshqarish

====

Tarmoqdagi zaifliklarni olib tashlash

====

Tarmoqdagi zaifliklarni yuq qilish

====

Tarmoqdagi zaifliklarbosqichlarini aniqlash

====

++++

….. - bu ma'lum operatsiyalarni avtomatik ravishda bajarish uchun mo'ljallangan dasturlar.

====

#Botlar

====

Ransomware

====

Rootkitlar

====

Troyanlar

====

++++

... - uchinchi tomonga kompyuterga masofadan kirish va boshqarish imkonini beradi.

====

#Rootkitlar

====

Botlar

====

Ransomware

====

Troyanlar

====

++++

Texnogen tahdidlarning ichki manbalari berilgan qatorni belgilang.

====

#sertifikatlanmagan va litsenziyalanmagan dasturiy ta'minot, monitoring imkoniyatlari zaif bo'lgan axborot tarmoqlari faoliyatini monitoring qilish vositalari

====

ulanish kanallari, muhandislik-texnik tarmoqlar

====

Internet provayderlari va bulutli texnologiya provayderlari

====

noto'g'ri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar

====

++++

Internet provayderlari va bulutli texnologiya provayderlari, ulanish kanallari, muhandislik-texnik tarmoqlar

====

#binolar va xodimlarni nazorat qilishning sifatsiz vositalari;

====

sertifikatlanmagan va litsenziyalanmagan dasturiy ta'minot, monitoring imkoniyatlari zaif bo'lgan axborot tarmoqlari faoliyatini monitoring qilish vositalari

====

noto'g'ri yoki past sifatli uskunalar, muhandislik-texnik tarmoqlar

====

Internet provayderlari va bulutli texnologiya provayderlari, ulanish kanallari, muhandislik-texnik tarmoqlar

====

++++

SOC (Security Operations Center) tahliliy imkoniyatlarini belgilang.

====

#prognozlash, aniqlash, oldini olish, reaksiya

====

dasturlar va axborot tizimlarini boshqarish

====

texnik jihozlardan foydalanish

====

tayyor dasturiy ta'minotni yuklash, texnik jihozlardan foydalanish

====

++++

Tahdidlarni tahlil qilish uchun asosiy SOC elementi, ya’ni bilimlarni boshqarish bu - …

====

#SOCl mutahassislari tobora murakkablashib borayotgan hujumlarning oldini olish va ularga samarali javob berish uchun raqamli sud ekspertizasi, zararli dasturlarni tahlil qilish

====

Ichki tahdidlar to'g'risidagi ma'lumotlar, ommaviy axborot manbalaridan olingan tahlillar

====

An'anaviy himoya vositalari (xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari, SIEM va boshqalar) bilan aniqlab bo'lmaydigan zararli harakatlar haqida oldindan bilib olishga imkon beradi

====

To'g'ri qurilgan hodisaga javob berish jarayoni, bu zararni cheklash va oqibatlarini bartaraf etish xarajatlarini kamaytirish imkonini beradi

====

++++

Tahdidli ma’lumotlar oqimlaridagi ma'lumotlarni tematik guruhlaridan biri - IP va URL manzillar…

====

#Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud.

====

Tegishli ma'lumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi.

====

Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish mumkin bo'lgan ishonchli fayllar xeshlarini o'z ichiga oladi.

====

xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash imkonini beradi

====

++++

Tahdidli ma’lumotlar oqimlaridagi ma'lumotlarni tematik guruhlaridan biri - Zararli ob'ektlar xeshlari …

====

#Tegishli ma'lumotlar eng xavfli va keng tarqalgan zararli dasturlarni, shu jumladan mobil operatsion tizimlar uchun infektsiyalarni qamrab oladi.

====

Zararli va fishing saytlarining tarmoq identifikatorlari, shuningdek, botnet C&C serverlari (jumladan, mobil qurilmalar uchun) mavjud.

====

Ular uchinchi tomon yechimlari va xizmatlari tomonidan foydalanish mumkin bo'lgan ishonchli fayllar xeshlarini o'z ichiga oladi.

====

xavfsizlik strategiyasini moslashtirish orqali himoya choralarini yaxshilash imkonini beradi

====

++++

… - Kasperskiy laboratoriyasining noyob manbalaridan olingan ichki monitoring ma'lumotlari asosida ma'lum bir mamlakatga qaratilgan zararli dasturlar va kiberhujumlarni tahlil qilish.

====

#Zararli dasturlar va kiberhujumlarni tahlil qilish

====

Tahdid vektorlari ro'yxati

====

Oldindan shartlarni aniqlash

====

Retrospektiv tahlil

====

++++

… - muayyan mamlakatda ma'lumotlarning sizib chiqishi uchun zaruriy shartlarni aniqlash.

====

#Oldindan shartlarni aniqlash

====

Tahdid vektorlari ro'yxati

====

Zararli dasturlar va kiberhujumlarni tahlil qilish

====

Retrospektiv tahlil

====

++++

… - bu kompyuterlar, tarmoqlar yoki ular saqlangan ma'lumotlarga qarshi kompyuterga asoslangan hujumni boshlash orqali hukumatni yoki tashkilotni siyosiy yoki ijtimoiy maqsadlarini ilgari surish uchun qo'rqitadigan yoki majburlaydigan kishi.

====

#Kiberterrorist

====

Kiberetika

====

Kibertahdid

====

Kibermakon

====

++++

Tajovuzkor tomonidan to'g'ridan-to'g'ri tinglash qanday fazifalarni o'z ichiga oladi?

====

#maxfiy eshitish va yodlash; maxfiy eshitish va yozib olish.

====

maxfiy eshitish va yodlash; yozib olish

====

Oshkora ko'rish va maxfiy yozib olish

====

Oshkora ko'rish va maxfiy yozib olish

====

++++

Ma'lumotni tiklash texnikasi?

====

#Bu kompyuterda yo'q qilingan, foydalanib bo'lmaydigan, buzilgan yoki formatlangan ma'lumotlarni, saqlanishda, ularda saqlangan ma'lumotlarga kirishning iloji bo'lmaganda tiklash jarayoni

====

Bu kompyuterda yo'q qilinmagan, foydalanib bo'lmaydigan, buzilgan yoki formatlangan ma'lumotlarni, saqlanishda, ularda saqlangan ma'lumotlarga kirishning iloji bo'lmaganda tiklash jarayoni

====

Bu kompyuterda yo'q qilingan, foydalanib bo'ladigan, buzilgan yoki formatlangan ma'lumotlarni, saqlanishda, ularda saqlangan ma'lumotlarga kirishning iloji bo'lmaganda tiklash jarayoni

====

Bu kompyuterda yo'q qilingan, foydalanib bo'lmaydigan, buzilgan yoki formatlangan ma'lumotlarni, saqlanishda, ularda saqlangan ma'lumotlarga kirishning iloji bo'lganda tiklash jarayoni

====

++++

Ìa'lumotni yo'qotish xavfi hamma uchun bir xilmi?

====

#Bir xil

====

Bir xil emas

====

Barchasida har xil

====

Individual

====

++++

Xavfsizlikka tahdid qaysi sinfga bolinadi?

====

#Uyushtirilgan va Tasodifiy tahdid

====

Oldindan o’ylangan va oldindan o’ylanmagan tahdid

====

Uyushtirilmagan va uyushtirilgan tahdid

====

Uyushtirilgan va Tasodifiy tahdid

====

++++

... - josuslik, buzg'unchilik, sabotaj, suiqasd va hujumlarini amalga oshirishi mumkin bo'lgan xorijiy razvedka tashkilotlari va terrorchilar qaysi darajaliga kiradi.

====

#1-darajali tahdid

====

5-darajali tahdid

====

3-darajali tahdid

====

4-darajali tahdid

====

++++

Axborotning buzilishi yoki yo‘qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan xarakatlar kanday nomlanadi?

====

#Tahdid

====

Zaiflik

====

Hujum

====

Butunlik

====

++++

Axborotni qanday ta’sirlardan himoyalash kerak?

====

#Axborotdan ruxsatsiz foydalanishdan, uni buzilishdan yoki yo‘q qilinishidan

====

Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki sotishdan

====

Axborotdan qonuniy foydalanishdan, uni qayta ishlash yoki foydalanishdan o’rganishi

====

Axborotdan tegishli foydalanishdan, uni tarmoqda uzatishdan

====

++++

Anomaliyani aniqlashda uchta 3 asosiy yondashuv qanday?

====

#Nazoratli, Nazoratsiz, Yarim nazorat ostida

====

Nazoratli, Nazoratsiz,

====

Nazoratsiz, Yarim nazorat ostida

====

Nazoratli, Nazoratsiz, Yarim nazorat ostida

====

++++

… - bu standart bo‘lishi mumkin bo‘lmagan hodisalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisaga aytiladi

====

#Insident (mojoro, hodisa) -?

====

Axborotni himoyalash

====

Xavfsizlikni amalga oshirish vaqti meüyorlari

====

Axborotni himoyalash bosqichlari

====

++++

Korxona ichidagi individual foydalanuvchilarning rollari asosida tarmoqqa kirishni cheklash qaysi model?

====

#RBAC modeli

====

Azure modeli

====

Amazon modeli

====

Kirishni boshqarish

====

++++

Amazon ec2 nima?

====

#bulutdagi xavfsiz va qayta o’lchash qobiliyatini ta’minlaydigan web xizmat

====

dasturlash tillarida texnologiyalarida ishlab chiqilgan web-ilova

====

xavfsiz obyektlarga kirish yoki boshqarish tizimining turli vazifalarini bajarish qobiliyati

====

NET, PHP, Windows tomonidan qo’llab-quvvatlaydigan dasturlash tillarida, texnologiyalarida ishlab chiqilgan web-ilova

====

++++

Bajariladigan fayllarni ko’rsating

====

#exe, com, bat

====

exe, txt, doc

====

bas, exe, excel

====

rar, text, bat

====

++++

FTPS -?

====

#FTP xavfsizligi

====

FTP rozetkasi

====

FTP SSH

====

FTP Ba'zi

====

++++

SFTP -?

====

#SSH FTP

====

Soket ftp

====

Xavfsiz FTP

====

Ba'zi ftp

====

++++

\_\_\_\_\_\_ - xavfsiz ulanishni nazarda tutadigan kriptografik protokolning xavfsiz darajasi.

====

#SSL

====

SSH

====

FTP

====

HTTP

====

++++

Arxivli fayllarni ko’rsating

====

#arj, zip, rar

====

rar, zip, pas

====

pas, bas, rar

====

kar, ogg, doc

====

++++

Mantiqiy bombalar-….

====

#Signal bo‘yicha yoki o‘rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infrastrukturalariga o‘rnatiluvchi dasturlangan qurilmalar

====

Ko‘payish, dasturlarda o‘rnashishmaslik, aloqa liniyalari, ma’lumotlarni uzatish tarmoqlari bo‘yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o‘xshash qobiliyatlarga ega

====

Telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish

====

Ob’ekt dasturiy boshqaruv kanallarida axborotni soxtalashtirish

====

++++

............ faylni tiklash (avval Auslogics Favqulodda tiklash) tasodifan o'chirilgan fayllarni tiklaydi.

====

#Auslogics dasturi

====

MiniTool Power Data Recovery dasturi

====

Handy Recovery dasturi

====

Recovery

====

++++

Viruslar haqida dastlabki ma’lumotlar amerikalik …………….. fantastik asarida uchraydi.

====

#T. J. Raynning 1977-yilgi

====

K. J. Raynning 1977-yilgi

====

T. J. Raynning 1978-yilgi

====

T. J. Raynning 1967-yilgi

====

++++

Dunyodagi birinchi virus dasturi 1988 -yili Karnell Universiteti aspiranti ……….. (kichik) tomonidan Internet tarmog’iga joylashtirilgan.

====

#Robert Moris

====

T. J. Ray

====

Maks Moris

====

Lio Moris

====

++++

Virus faoliyati asosan nechta fazaga ega?

====

#4

====

5

====

3

====

6

====

++++

…………. – Bu viruslar kompyuterning ishlay boshlashi (zagruzka) uchun foydalaniladigan qattiq diskning maxsus qismini ishdan chiqaradi.

====

#Boot sektor viruslari (Bootsector viruses) dasturi

====

Auslogics dasturi

====

Handy Recovery dasturi

====

Recovery dasturi

====

++++

Dunyodagi birinchi virus dasturi …… -yili Karnell Universiteti aspiranti Robert Moris(kichik) tomonidan Internet tarmog’iga joylashtirilgan.

====

#1988

====

1987

====

1989

====

1986

====

++++

Virus faoliyati asosan 4 ta fazaga ega bular qaysilar?

====

#uxlash fazasi, ko’payish fazasi, ishga kirishish fazasi, vayron qilish fazasi.

====

uxlash fazasi, ko’payish fazasi, ishga kirishish fazasi, vayron qilmaslik fazasi.

====

ishga kirishish fazasi, vayron qilish fazasi va bazasini tuzish

====

ishga kirishish fazasi, vayron qilmaslik fazasi

====

++++

Virus bilan asosan qaysi turdagi fayllar zararlanishi mumkin

====

#COM va EXE ko’rinishidagi fayllar

====

Docx va EXE ko’rinishidagi fayllar

====

SOM va PDF ko’rinishidagi fayllar

====

EXE ko’rinishidagi fayllar

====

++++

……………….. - Bu viruslar kompyuteringizning operativ xotirasida (RAM) yashaydi va zararli harakatini amalga oshiradi.

====

#Memory Resident Viruses )

====

COM va EXE ko’rinishidagi fayllar

====

Docx va EXE ko’rinishidagi fayllar

====

Handy Recovery

====

++++

"Hosiyatsiz sovg’a” degan ma’noni bildiradigan zararli dasturni ko’rsating?

====

#Troyanlar (trojan horses)

====

Chuvalchang viruslar (Worms)

====

Boot sektor viruslari (Bootsector viruses)

====

Fishing

====

++++

Troyan dasturlar odatda nima orqali tarqaladi.

====

#Internet

====

Fleshka

====

Qattiq disk

====

Bootsector

====

++++

… – o’zlarining tarqalishi uchun boshqa bir programmaning makro dasturlash tilidan foydalanadigan viruslardir. Ular odatda Microsoft Word yoki Excel xujjatlarini zararlaydi.

====

#Makro viruslar (Macro viruses)

====

Boot sektor viruslari (Bootsector viruses) dasturi

====

Auslogics dasturi

====

Handy Recovery dasturi

====

++++

… - bu rezident dasturlar, skanerlarning takomillashgan ko‘rinishi bo‘lib, real vaqt oraliƒida fayllarni avtomatik tarzda tekshiradilar.

====

#Monitorlar

====

o‘zgarishlarni qayd qiluvchi revizorlar

====

Skanerlar

====

virus harakatini cheklovchi blokiratorlar

====

++++

Bu viruslar orasida o’zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi.

====

#Rootkit viruslari (Rootkit viruses) dasturi

====

Makro viruslar (Macro viruses) dasturi

====

Boot sektor viruslari (Bootsector viruses) dasturi

====

Handy Recovery dasturi

====

++++

Simsiz tarmoqlar xavfsizligi protokollari qaysilar?

====

#LLC, SSH, SSL/TLS

====

802.1x, SSH, SSL/TLS Dox

====

WPA , IPSec, 802.11 pdf

====

SSL/TLS , , 802.11, IEEE 802.11 Word

====

++++

Vakolatga ega bo‘lgan foydalanuvchining tarmoqqa kirishi uchun belgilangan parol ma’lumotini qo‘lga kiritishga qaratilgan harakatlar?

====

#Parollarga qaratilgan hujumlar

====

Parollarga qaratilmagan hujumlar

====

Parollarga qaratilgan imkoniyatlar

====

Loginga qaratilgan hujumlar

====

++++

- bu ma'lumotni ruxsatsiz foydalanuvchi tomonidan osonlikcha ochib bo'lmaydigan o'qib bo'lmaydigan holda himoya qiladigan texnologiya?

====

#Diskni shifrlash

====

Faylni shifrlash

====

Rasmni shifrlash

====

Videoni shifrlash

====

++++

360 Total Security 5 ta antiviruslardagi himoya qismlari bilan keng ko'lamli virusga qarshi himoya tashkil qilingan bular qaysilar?

====

#Bitdefender; Avira; QVMII; Bulutli hisoblash; tizimni ta'mirlash

====

Bitdefender; Avast; QVMII; Bulutli hisoblash; tizimni ta'mirlash

====

Bitdefender; Avira; QVMII; Bulutli hisoblash; tizimni buzish

====

Bitdefender; Nod; QVMII; Bulutli hisoblash; tizimni ta'mirlash

====

++++

360 Total Security nechinchi yil tashkil topgan?

====

#2008 yil

====

2001 yil

====

2009 yil

====

2010 yil

====

++++

Kasperskiyning Laboratoriyasi qaysi davlat informatsion hafsizligi sohasida eng yirik programma ta'minoti ishlab chiqaruvchisidir.

====

#Rossiya

====

Angliya

====

Xitoy

====

Germaniya

====

++++

……. - bu ularning ishlash tamoyili fayllarda, xotirada, yuklovchi sektorlarda virus signaturasini, ya’ni virusning o‘ziga xos dasturiy kodini izlab topishdan iborat.

====

#Skanerlar

====

Monitorlar

====

Immunizatorlar

====

o‘zgarishlarni qayd qiluvchi revizorlar

====

++++

Bu viruslar muayyan sana yohud payt kelganida yoki foydalanuvchi tomonidan muayyan harakat amalga oshirilganida ishga tushadigan viruslardir.

====

#Vaqt bombasi viruslari (Time or Logic Bombs)

====

O’zgaruvchan viruslar (Polymorphic viruses)

====

O’zgaruvchan viruslar (Rootkit viruses)

====

Fishing

====

++++

Bu viruslar nafaqat o’z-o’zidan ko’payadi, balki ko’paygan paytda o’zlarining kodlarini ham o’zgartirib turishadi.

====

#O’zgaruvchan viruslar (Polymorphic viruses)

====

O’zgaruvchan viruslar (Rootkit viruses)

====

Vaqt bombasi viruslari (Time or Logic Bombs)

====

Handy Recovery

====

++++

ESET kompaniyasi tomonidan ishlab chiqarilgan antivirus mahsulotlari to'plamini ko’rsating.

====

#Internet MONitor (IMON), E-mail MONitor (EMON),Document MONitor (DMON) Zaùita ot fishinga, Enhanced Media Control, ESET Social Media Scanner

====

Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Kaspersky Anti-Spam, Kaspersky Internet Zaùita ot fishinga, Enhanced Media Control, ESET Social Media Scanner

====

Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Kaspersky Anti-Spam, Kaspersky Internet Security, Kaspersky Linux Security, Avast

====

Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Internet MONitor (IMON), E-mail MONitor

====

++++

ESET NOD32 - ESET kompaniyasi tomonidan birinchi versiyasi nechinchi yil oxirida chiqarildi.

====

#1987 yil oxirida chiqarildi

====

1983 yil oxirida chiqarildi

====

1988 yil oxirida chiqarildi

====

1986 yil oxirida chiqarildi

====

++++

Kasperskiy Laboratoriyasi asosiy mahsulotlarini toping?

====

#Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Kaspersky Anti-Spam, Kaspersky Internet Security, Kaspersky Linux Security, Kaspersky Hosted Security

====

Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Kaspersky Anti-Spam, Kaspersky Internet Security, Kaspersky Linux Security, Avast

====

Kaspersky Anti-Virus, Kaspersky Anti-Hacker, Internet MONitor (IMON), E-mail MONitor

====

Internet MONitor (IMON), E-mail MONitor (EMON), Document MONitor (DMON)

====

++++

1997 yilning nechinchi iyulida mustaqil kompaniya sifatida Evgeniy Kasperskiy tashkil qilgan.

====

#21-iyulida

====

22-iyulida

====

23-iyulida

====

24-iyulida

====

++++

Mak-Elis kriptotizimida qanday tuzatuvchi kodlar ishlatiladi?

====

#Xatoliklarni tuzatuvchi kodlar ishlatiladi

====

Xatoliklarni tuzatuvchi kodlar ishlatilmaydi

====

Xatoliklarni tuzatmaydigan kodlar ishlatiladi

====

Xato kodlar ishlatilmaydi

====