**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №1**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “Veb sistemləri və texnologiyaları”

**Mövzu:**  “Kiber Cinayətkarlıq”

**Qrup: “**2441a”

**Tələbə: “**Ələkbərov Emil**”**

**Müəllim: “**Heydərzadə Nübar Azad**”**

**BAKI 2024**

Kibercinayətkarlıq kompüterlərdən və ya internetdən istifadə etməklə həyata keçirilən, çox vaxt fərdləri, təşkilatları və ya hökumətləri hədəf alan cinayət fəaliyyətlərinə aiddir. Bu cinayət kateqoriyasına hakerlik, şəxsiyyət oğurluğu, onlayn fırıldaqçılıq, fişinq, zərərli proqramların yayılması, kiber zorakılıq və bir çox başqaları daxil olmaqla geniş qeyri-qanuni fəaliyyətlər daxildir.

Bəzi ümumi kibercinayətkarlıq növlərinə aşağıdakılar daxildir:

1) Hacking: Məlumatları oğurlamaq, əməliyyatları pozmaq və ya zərər vermək üçün kompüter sistemlərinə və ya şəbəkələrinə icazəsiz giriş.

2) Fişinq: Şifrələr və ya kredit kartı nömrələri kimi həssas məlumatları aşkar etmək üçün şəxsləri aldatmaq üçün qanuni mənbələrdən görünən saxta e-poçt və ya mesajların göndərilməsi.

3) Zərərli proqram: Viruslar, qurdlar, troyanlar, ransomware və casus proqramlar da daxil olmaqla kompüter sistemlərinə sızmaq və zədələmək və ya məlumatları oğurlamaq üçün nəzərdə tutulmuş zərərli proqram.

4) Şəxsiyyət oğurluğu: Fırıldaqçılıq və ya digər cinayətlər törətmək üçün Sosial Müdafiə nömrələri, kredit kartı nömrələri və ya bank hesabı rekvizitləri kimi şəxsi məlumatların oğurlanması.

5) Onlayn fırıldaqlar: Saxta investisiya imkanları, romantik fırıldaqlar və ya lotereya fırıldaqları kimi saxta bəhanələrlə fərdləri pul göndərmək və ya şəxsi məlumat vermək üçün aldatmaq üçün hazırlanmış müxtəlif sxemlər.

6) Kiber zorakılıq: Çox vaxt sosial media platformaları, mesajlaşma proqramları və ya onlayn forumlar vasitəsilə başqalarını təqib etmək, qorxutmaq və ya təhdid etmək üçün elektron ünsiyyətdən istifadə.

7) Məlumatların pozulması: Təşkilatlar tərəfindən saxlanılan həssas məlumatlara icazəsiz giriş və oğurluq, çox vaxt maliyyə itkiləri və fərdlər üçün şəxsi məlumatların oğurlanması ilə nəticələnir.

8) Xidmətdən imtina (DoS) hücumları: Şəbəkənin və ya vebsaytın normal fəaliyyətini pozmaq və istifadəçilər üçün əlçatmaz etmək üçün həddindən artıq trafiklə doludur.

Kibercinayətkarlıq mürəkkəb və daim inkişaf edən təbiətinə görə bütün dünyada hüquq-mühafizə orqanları və kibertəhlükəsizlik mütəxəssisləri üçün əhəmiyyətli problemlər yaradır. Güclü parollardan istifadə, proqram təminatının yenilənməsi, onlayn ünsiyyətdə ehtiyatlı olmaq və təhlükəsizlik proqram təminatından istifadə kimi qabaqlayıcı tədbirlər fərdlərə və təşkilatlara özlərini kiber təhlükələrdən qorumağa kömək edə bilər. Bundan əlavə, beynəlxalq əməkdaşlıq və kibertəhlükəsizlik qanun və qaydalarını gücləndirmək səyləri kibercinayətkarlıqla effektiv mübarizə üçün vacibdir.

Kibercinayətkarlıq rəqəmsal cihazlardan və ya şəbəkələrdən istifadə etməklə həyata keçirilən cinayətkar fəaliyyətlərin geniş spektrini əhatə edir. Bu cinayətlər fırıldaqçılıq, şəxsiyyət oğurluğu, məlumatların pozulması, kompüter virusları, fırıldaqçılıq və digər zərərli hərəkətlərdə genişlənmək üçün texnologiyadan istifadəni əhatə edir. Kibercinayətkarlar kompüter sistemləri və şəbəkələrindəki zəifliklərdən icazəsiz giriş əldə etmək, həssas məlumatları oğurlamaq, xidmətləri pozmaq və fərdlərə, təşkilatlara və hökumətlərə maliyyə və ya nüfuzuna zərər vurmaq üçün istifadə edirlər.

2000-ci ildə Birləşmiş Millətlər Təşkilatının Cinayətin Qarşısının Alınması və Cinayətkarlarla Müalicə üzrə onuncu Konqresi kibercinayətləri beş kateqoriyaya ayırdı: icazəsiz giriş, kompüter məlumatlarına və ya proqramlarına zərər vurma, kompüter sisteminin və ya şəbəkənin fəaliyyətinə mane olmaq üçün təxribat, icazəsiz ələ keçirmə. sistem və ya şəbəkə daxilində məlumatlar və kompüter casusluğu.

Beynəlxalq səviyyədə həm dövlət, həm də qeyri-dövlət subyektləri kibercinayətlərlə, o cümlədən casusluq, maliyyə oğurluğu və digər transsərhəd cinayətlərlə məşğul olurlar. Beynəlxalq sərhədləri keçən və ən azı bir milli dövlətin hərəkətlərini əhatə edən kibercinayətlər bəzən kibermüharibə adlanır. Uorren Baffet kibercinayətkarlığın “bəşəriyyətin bir nömrəli problemi”[ olduğunu və bunun “insanlıq üçün real risklər yaratdığını” dedi.

Dünya İqtisadi Forumunun 2020-ci il Qlobal Risklər Hesabatı, mütəşəkkil kibercinayətkar qrupların ABŞ-da onların aşkarlanması və təqib olunma ehtimalının 1 faizdən az olacağını təxmin edərkən, onlayn cinayətlər törətmək üçün güclərini birləşdirdiyini təsdiqləyir. Məxfi məlumat qanuni və ya başqa şəkildə tutulduqda və ya açıqlandıqda kibercinayətkarlıqla bağlı bir çox məxfilik narahatlığı var.

Dünya İqtisadi Forumunun 2023-cü il Qlobal Risklər Hesabatı kibercinayəti bu gün və növbəti 10 il ərzində dünyanın üzləşdiyi 10 əsas riskdən biri kimi sıralayır. Əgər kibercinayətə bir milli dövlət kimi baxılsaydı, kibercinayətkarlıq dünyanın üçüncü ən böyük iqtisadiyyatı hesab olunacaqdı. Rəqəmlərə görə, kibercinayətin 2024-cü ildə dünya üzrə 9 trilyondan çox ziyana səbəb olacağı proqnozlaşdırılır.

**Təsnifatlar**

**Kompüter fırıldaqçılığı**

Kompüter fırıldaqlığı elektron məlumatları götürmək və ya dəyişdirmək və ya kompüterdən və ya sistemdən qanunsuz istifadə əldə etmək üçün kompüterdən istifadə etmək aktıdır. İnternetdən istifadəni əhatə edən kompüter fırıldaqlığına internet fırıldaqçılığı da deyilir. Kompüter fırıldaqçılığının hüquqi tərifi yurisdiksiyaya görə dəyişir, lakin adətən kompüterə icazəsiz və ya icazəsiz daxil olmağı nəzərdə tutur.

Kompüter fırıldaqçılığının formalarına məlumatı dəyişdirmək üçün kompüterlərə müdaxilə, kompüter qurdları və ya virusları kimi zərərli kodun yayılması, məlumatların oğurlanması üçün zərərli proqram və ya casus proqramların quraşdırılması, fişinq və avans ödənişli fırıldaqlar daxildir.

Fırıldaqçılığın digər formaları kompüter sistemlərindən istifadə etməklə törədilə bilər, o cümlədən bank fırıldaqları, kartinq, şəxsiyyət oğurluğu, qəsb və məxfi məlumatların oğurlanması. Bu cür cinayətlər çox vaxt şəxsi və ya maliyyə məlumatlarının itirilməsi ilə nəticələnir.

**Kiberterrorizm**

Kiberterrorizm termini kiberməkan və ya kompüter resurslarından istifadə etməklə törədilən terror aktlarına aiddir. Viruslar, qurdlar, fişinq, zərərli proqram təminatı, aparat və ya proqramlaşdırma skriptləri vasitəsilə kompüter şəbəkələrinin və fərdi kompüterlərin pozulması aktları kiberterrorizmin formaları ola bilər.

Hökumət rəsmiləri və informasiya texnologiyaları (İT) təhlükəsizliyi üzrə mütəxəssislər 2001-ci ilin əvvəlindən şəbəkə problemlərinin və server fırıldaqlarının əhəmiyyətli dərəcədə artdığını sənədləşdiriblər. Birləşmiş Ştatlarda Federal Təhqiqatlar Bürosu (FTB) və Mərkəzi Kəşfiyyat kimi qurumların artan narahatlığı var. Agentlik (CIA).

**Kiber qəsb**

Kiber qəsb vebsayt, e-poçt serveri və ya kompüter sistemi zərərli hakerlər tərəfindən hücumlara məruz qaldıqda və ya hücumlarla təhdid edildikdə baş verir, çox vaxt xidmətdən imtina hücumları. Kiberqəsbçilər hücumları dayandırmaq və “qoruma” təmin etmək vədləri müqabilində pul tələb edirlər. FTB-nin məlumatına görə, kiberqəsbçilər korporativ saytlara və şəbəkələrə getdikcə daha çox hücum edir, onların fəaliyyət qabiliyyətini şikəst edir və xidmətlərini bərpa etmək üçün ödəniş tələb edirlər. Hər ay 20-dən çox hadisə FTB-yə bildirilir və qurbanın adını ictimaiyyətdən uzaq tutmaq üçün bir çoxu barədə məlumat verilmir. Təcavüzkarlar tez-tez paylanmış xidmətdən imtina hücumundan istifadə edirlər. Bununla belə, doksinq və böcək brakonyerliyi kimi digər kiberqəsb üsulları mövcuddur. Kiber qəsb nümunəsi 2014-cü ildə Sony Hack idi.

**Ransomware**

Ransomware, kiberqəsbdə fayllara girişi məhdudlaşdırmaq üçün istifadə edilən, bəzən fidyə ödənilmədikcə məlumatların daimi silinməsini təhdid edən zərərli proqram növüdür. Ransomware qlobal problemdir və 2021-ci ildə dünya üzrə 300 milyondan çox hücum təşkil edir. 2022 Unit 42 Ransomware Threat Report-a əsasən, 2021-ci ildə Norton tərəfindən idarə olunan hallarda orta fidyə tələbi 144 faiz artaraq 2,2 milyon dollara çatıb və 85 faiz olub. Qaranlıq veb məlumat zibilliklərində şəxsi məlumatlarını göstərən qurbanların sayında artım. 2021 və 2022-ci illərdə təxminən 400 milyon dollar itki, fidyə proqramı hücumlarının gündəlik insanlara təsirini göstərən statistik göstəricilərdən yalnız biridir.

**Kompüterlər bir vasitə kimi**

Bir şəxs kibercinayətin hədəfi olduqda, kompüter çox vaxt hədəf deyil, alət olur. Adətən insanın zəif cəhətlərindən istifadə edən bu cinayətlər adətən çox texniki təcrübə tələb etmir. Bunlar oflayn dünyada əsrlər boyu mövcud olan cinayət növləridir. Cinayətkarlara sadəcə olaraq potensial qurbanların sayını artıran və onları izləməyi və yaxalamağı çətinləşdirən alət verilmişdir.

Kompüter şəbəkələrindən və ya cihazlarından başqa məqsədlər üçün istifadə edən cinayətlərə aşağıdakılar daxildir:

* Fırıldaqçılıq və şəxsiyyət oğurluğu (baxmayaraq ki, bu, getdikcə daha çox zərərli proqram, hakerlik və ya fişinqdən istifadə edir və bu, onu "hədəf kimi kompüter" və "alət kimi kompüter" nümunəsinə çevirir)
* İnformasiya müharibəsi
* Fişinq fırıldaqları
* Spam
* Qeyri-qanuni ədəbsiz və ya təhqiredici məzmunun, o cümlədən təqib və hədələrin təbliği

Kommersiya məqsədləri üçün (spam) toplu e-poçtun istənilmədən göndərilməsi bəzi yurisdiksiyalarda qanunsuzdur.

Fişinq əsasən e-poçt vasitəsilə yayılır. Fişinq e-poçtlarında zərərli proqramdan təsirlənən digər vebsaytlara keçidlər ola bilər. Yaxud onlar saxta onlayn bankçılıq və ya şəxsi hesab məlumatlarını oğurlamaq üçün istifadə edilən digər vebsaytlara bağlantılar ehtiva edə bilər.

**Reklam fırıldaqçılığı**

Reklam fırıldaqları kibercinayətkarlar arasında xüsusilə populyardır, çünki bu cür fırıldaqlar gəlir gətirir və mühakimə olunma ehtimalı azdır. Sorbonna Biznes Məktəbinin professoru Jean-Lup Richet kibercinayətkarlar tərəfindən törədilən geniş çeşidli reklam fırıldaqlarını üç kateqoriyaya təsnif etdi: şəxsiyyət fırıldaqçılığı, atribusiya fırıldaqçılığı və reklam fırıldaqçılığı xidmətləri.

Şəxsiyyət fırıldaqçılığı real istifadəçiləri təqlid etmək və auditoriya sayını artırmaq məqsədi daşıyır. Şəxsiyyət fırıldaqçılığı üçün istifadə edilən üsullara botlardan gələn trafik daxildir (hosting şirkəti, məlumat mərkəzindən və ya təhlükə altına alınmış cihazlardan gələn); peçenye doldurulması; yer və brauzer növü kimi istifadəçi xüsusiyyətlərinin saxtalaşdırılması; saxta sosial trafik (sosial şəbəkələrdə istifadəçilərin reklam edilən veb-sayta daxil olması üçün aldadılması); və botu qanuni görünən saxta sosial media hesabları.

Atribut saxtakarlığı kliklər və söhbətlər kimi real istifadəçilərin fəaliyyətlərini təqlid edir. Bir çox reklam fırıldaqçılıq üsulları bu kateqoriyaya aiddir: botnetin bir hissəsi kimi qaçırılmış və zərərli proqrama yoluxmuş cihazların istifadəsi; klik təsərrüfatları (az maaşlı işçilərin klikləmək və ya söhbət etmək üçün maaş aldığı şirkətlər); həvəsləndirilmiş baxış; video yerləşdirmədən sui-istifadə (displey banner yuvalarında çatdırılır); gizli reklamlar (həqiqi istifadəçilər tərəfindən heç vaxt baxılmayacaq); domen saxtakarlığı (saxta veb-saytda təqdim olunan reklamlar); və istifadəçinin reklamı tıklamağa məcbur edildiyi klikləmə.

Reklam fırıldaqçılığı xidmətlərinə şəxsiyyət və ya atribusiya fırıldaqçılığı etmək üçün lazım ola biləcək bütün onlayn infrastruktur və hostinq xidmətləri daxildir. Xidmətlər spam veb-saytların yaradılmasını əhatə edə bilər (süni geri bağlantılar təmin edən veb-saytların saxta şəbəkələri); əlaqə qurma xidmətləri; hostinq xidmətləri; və ya məşhur brendi təqlid edən saxta və fırıldaq səhifələri.

**Narkotik maddə ticarəti**

Darknet marketləri əyləncə dərmanlarını onlayn almaq və satmaq üçün istifadə olunur. Bəzi narkotik alverçiləri narkotik qatırları və ya potensial müştərilərlə əlaqə saxlamaq üçün şifrəli mesajlaşma vasitələrindən istifadə edirlər. 2011-ci ildə fəaliyyətə başlayan "Silk Road" qaranlıq internet saytı narkotiklərin ilk böyük onlayn bazarı idi. 2014-cü ildə FTB və Europol tərəfindən həmişəlik bağlanıb. Silk Road 2.0 aşağı düşdükdən sonra Silk Road 3 Reloaded ortaya çıxdı. Bununla belə, bu, İpək Yolu brendinin əvvəlki uğurlarından daha çox məlumat əldə etmək üçün İpək Yolu adından istifadə edən Diabolus Market adlı köhnə bazar idi.

Darknet bazarlarında son illərdə anonim satınalmalar və tez-tez digər alıcılar tərəfindən nəzərdən keçirilən sistem kimi bir çox səbəblərə görə trafikdə artım olmuşdur. Darknet bazarlarının fərdləri maliyyə cəhətdən boşalda bilməsinin bir çox yolu var. Satıcılar və müştərilər onlayn olarkən şəxsiyyətlərini gizli saxlamaq üçün çox səy göstərirlər. Onlayn mövcudluğunu gizlətmək üçün ümumi istifadə olunan vasitələrə virtual şəxsi şəbəkələr (VPN), Tails və Tor Brauzer daxildir. Darknet bazarları müştəriləri rahat hiss etdirərək onları şirnikləndirir. İnsanlar Tor brauzerinə asanlıqla daxil ola bilsələr də, əslində qeyri-qanuni bazara çıxış əldə etmək onu Google ilə olduğu kimi axtarış sistemində yazmaq qədər sadə deyil. Darknet bazarlarında tipik .com, .net və .org domen uzantılarından fərqli olaraq tez-tez dəyişən, .onion ilə bitən xüsusi keçidlər var. Məxfiliyə əlavə olaraq, bu bazarlarda ən çox yayılmış valyuta əməliyyatların anonim olmasına imkan verən Bitcoin-dir.

Bazar istifadəçilərinin bəzən qarşılaşdıqları problem çıxış fırıldaqçılığıdır. Yəni, yüksək reytinqə malik olan satıcı sanki bazarda satış aparır və istifadəçilərə heç vaxt almadıqları məhsullar üçün pul ödəyir. Satıcı daha sonra birdən çox alıcıdan pul aldıqdan və ödənilən pulu heç vaxt göndərmədikdən sonra hesabını bağlayır. Hamısı qeyri-qanuni fəaliyyətlə məşğul olan satıcıların artıq satıcı olmaq istəmədikləri halda çıxış fırıldaqçılığı ilə məşğul olmamaq üçün heç bir əsası yoxdur. 2019-cu ildə Wall Street Market kimi tanınan bütöv bir bazarın 30 milyon dollar bitkoin oğurlayaraq aldadıldığı iddia edilir.