MEASUREMENTS AND MITIGATION OF PEER-TO-PEER-BASED BOTNETS: A CASE STUDY ON STORM WORM

Metin UZUNER
N10228665

İçerik

- Giriş
  - Botnet
  - P2P Botnet
- Makalenin Katkısı
- Botnet Takibi ve P2P Adaptasyonu
- Derinlemesine Storm Worm
- Storm Worm'unun İzlenmesi
- Zararlı ile Mücadele

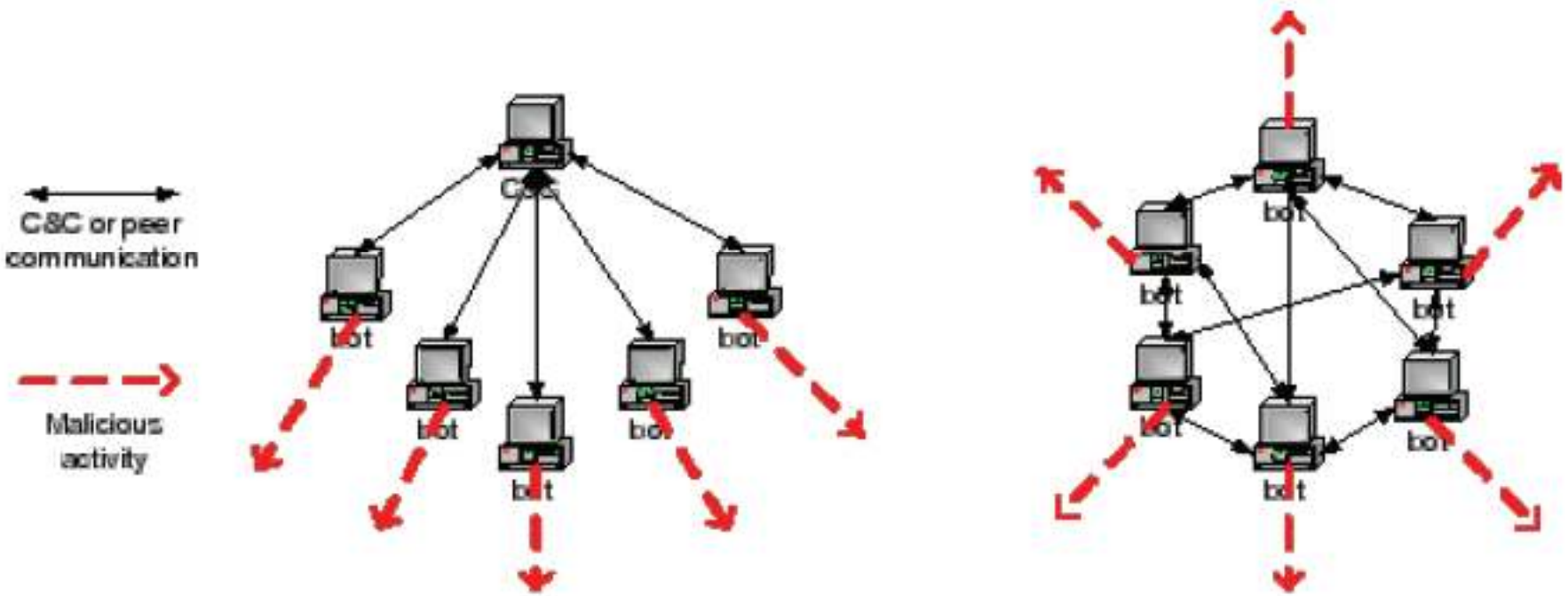
Giriş

- **Bot**: Uzaktan kontrol edilebilen zararlı yazılım yüklü ele geçirilmiş bilgisayar. (Zombi)
  - DDoS
  - Spam mail
  - vb...
- **Botnet**: Tahmin ettiğiniz şey.
- **Botnet Takibi**:
  1. Analiz için bot bir makina ele geçirilir. (Honeypot veya özel yazılımlar ile)
  2. Ele geçirilen bot kullanılarak IRC kanalına girilir.
  3. Toplanan bilgiler yardımıyla IRC sunucusu kapattırılır.

Giriş

- P2P Botnet
  - Merkezi bir Command & Control sunucusu bulunmaz
  - Bu nedenle Botnet Tracking ile doğrudan tespit edilemez
- P2P Botnet tespitinde Botnet Tracking'den faydalanma
  1. Bot binary'i elde et.
  2. Ağa sız
  3. Botnet'in kullandığı protokoldeki açıklıkları exploit et.
- Bu işlemi ***aktif*** olarak ***ilk defa*** gerçekleştirebilen çözüm...

P2P vs Merkezi



Makalenin Katkısı

1. Botnet takip yöntemini P2P botnetlerini de kapsayacak şekilde genişletilmesi.
2. Storm Worm'unun etkisizleştirilmesi.
3. P2P botnet'lerinin yayılma aşaması, zararlı aktiviteleri ve diğer özellikleir hakkındaki ilk deneysel çalışmalar.

Botnet Takibi ve P2P Adaptasyonu

- **İncelenen Botnet Sınıfı**
  - Unauthenticated content-based/subscribe style communication.
    - Gnutella, eMule veya BitTorrent
  - Tüm node'lar hem sunucu hem istemcidir.
  - Node'lar bilgileri birbirlerine asla doğrudan göndermezler.
  - İçerik sağlayıcılar sağlanan içeriğin ne olduğunu doğrulamazlar.

Botnet Takibi ve P2P Adaptasyonu

- **Geliştirilmiş Botnet Takibi**
  - 1.Adım: P2P Ağda Yayılma İşleminin Exploit Edilmesi
  - 2.Adım: Ağa sızma ve analiz
  - 3.Adım: Etkisiz hale getirme

Derinlemesine Storm Worm

- **Yayılma Mekanizması**
  - Remote Code Execution
  - E-mail ile yayılmakta
  - Sosyal Mühendislik yöntemleri kullanılmakta.
    - ***Spamtraps*** yardımıyla gönderilen spam e-mail'ler toplanır.
    - 2006 ve 2007 arasında günde 2200 ile 23900 arası spam toplandı.
    - Günlük ortalama spam mail sayısı 8500.
    - Bu trafiğin yaklaşık %10'u Storm'a aittir.
    - Client HoneyPots yardımıyla toplanan linkler analiz edildi.
    - Bazı linklere açıklık bulunduran tarayıcı ile bağlanıldığında Storm zararlısının kendisini bot makinaya kopyalamaya çalıştığı gözlemlendi.
    - Kullanılan zararlının polymorphic yapıda olduğu tespit edilmiş.

Derinlemesine Storm Worm

- **Sistem Seviyesi Davranışları**
  - İleri seviye teknikler
  - Binary packer kullanımı
  - Rootkit kullanımı ile varlılığının gizlenmesi
  - Kernel seviyesinde bileşenler

Derinlemesine Storm Worm

- **Ağ Seviyesi Davranışları**
  - İlk versiyonları P2P Distributen Hash Table (DHT) yönlendirme protokolünü kullanmaktaydı. (OVERNET, Edonkey2000)
  - 2007 de kullanılan iletişim protokolü değiştirildi.
  - Overnet + yeni ileşim protokolü olan Stormnet üzerinden yayılmaya devam etti.
  - **Routing Lookup**:
    - Overnet ve Stormnet ortamından yönlendirme prefix matching'e dayanmakta. XOR distance'a göre hesaplanmakta.
    - Yönlendirme tabloları IP adresi, DHT ID ve UDP dan oluşturulmakta.
    - Unbalanced routing tree
      - Sağında yakın noktadaki nodelar , solunda uzak noktadaki nodelar
    - Mesafeler

Derinlemesine Storm Worm

- **Ağ Seviyesi Davranışları**
  - **Yayınlama ve Arama**
    - Key olarak adlandırılan tanımlayıcılar ile bilgi alışverişi gerçekleştirilir.
    - Aranan key'i bulunduran host routing lookup yöntemi ile bulunur.
      - Hello, IP Adress, DHT ID – bildirimde bulunur
      - Route request/response(kid) – DHT ID kid'e yakın olan eşler aranır
      - Publish request/response – bilgi yayınlanır.
      - Request/response(key) – key ile eşleşen bilgi aranır.
    - Storm iletişiminde ele geçirilen botlar belirli bir key aramaktadırlar.
    - Kontrolcüler botlar tarafından aranan key'lerin ne olduğunu bilirler ve bu aramaların sonucunda istedikleri komutları yayınlarlar.
    - Bu anahtarlar kontrolcülerin ve botların üzerinden önceden anlaştığı buluşma noktası yada postakutusu olarak görülebilirler.

Derinlemesine Storm Worm

- **Ağ Seviyesi Davranışları**
  - **Storm Worm İletişimi**
    - Bu anahtar değeri f(d,r) fonsiyonuna göre oluşturulur.
      - d: o anki zaman
      - r: 0-31 arasında bir sayı
    - Böylece 32 farklı anahtar kullanılmaktadır.
    - Reverse engineering ile f fonksiyonu bulunabilir.
      - Saldırgan fonksiyonu değiştirebilir.
    - Black box test ile key defalarca aynı şekilde üretilerek tüm aranan anahtar değerleri listelenebilmektedir.

    Ayrıca anahtar değerini hesaplayan f fonksiyonu değiştirilse bile honeypot da incelenen botun üreteceği anahtar değeri ile kullanılacak anahtarlar bilinebilmektedir.

Derinlemesine Storm Worm

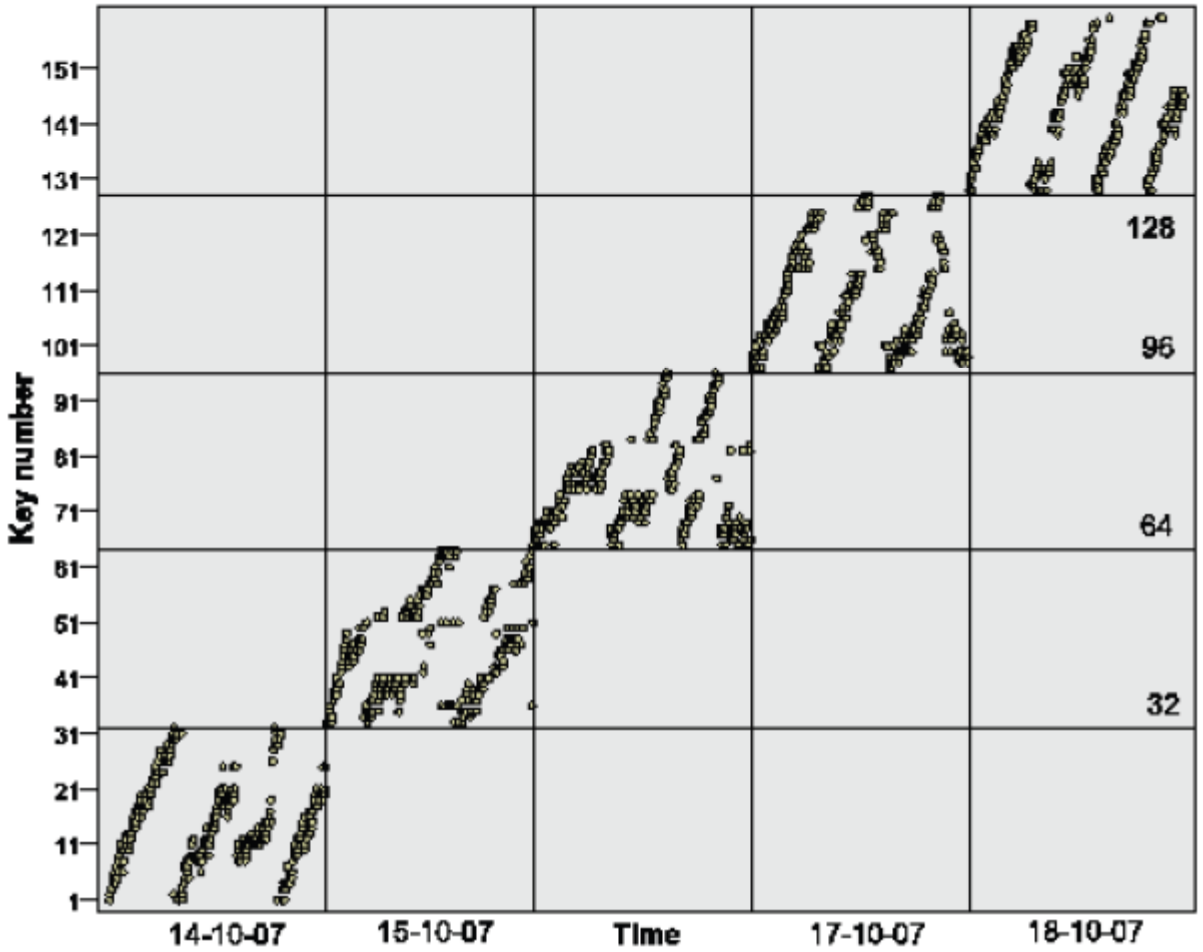


Figure 1: Keys generated by Storm in order to find other infected peers within the network (October 14-18, 2007)

Derinlemesine Storm Worm

- **Ağ Seviyesi Davranışları**
  - **Storm Worm İletişimi**
    - Keyler çalıştırılacak komutların bulunmasında kullanılmaktadır.
    - Bu anahtarlara karşılık gelen içerikler saldırganlar tarafından önceden yayınlanmaktadır.
    - Overnet üzerinden bu keylere karşılık gelen gerçek içerik bilgisinin ***.mpg;size=*;** olduğu görülmüştür.
    - Yıldızlı alanlar 16 bit sayıdan oluşmaktadır ve botların bu sayılardan komut alacakları kontrol düğüme bağlandıkları tahmin edilmektedir.
    - Fakat bu sayılardan IP ve Port numarası bilgisini nasıl çıkardıkları henüz billinmemektedir. Bu bilgi yalnızca Stormnet'e katılan botlar tarafaından hesaplanabilmektedir.

Storm Worm'unun İzlenmesi

- **Yayılma Aşamasının Exploit Edilmesi**
  - Öncelikle bot binary örneği elde edilir.
  - Bunun için smaptraps ve honeypot sistemleri kullanılabilir.
  - Spam maillerle gelen URL'ler tıklanılarak zararlı kodun bir örneği elde edilir.
  - Black-box analiz yöntemi ile aranan key değerleri bulunur.
    - Botlar emir alacakları komutları aramak zorundadır, bu arama zorunluluğu key değerlerini bulmak için exploit edilir.
    - Bu şekilde güncel arama keylerinin en azından bir altkümesi elde edilebilir.
    - Honeypot ortamında aranan 32 key tespit edilebilmiştir.

Storm Worm'unun İzlenmesi

- **Ağa Sızma ve Analiz**
  - Elde edilen keyler ve kullanılan iletişim protokolleri bilgisi ile ağa sızılır.
  - Analiz aşamasına ağın boyutları tespit edilerek başlanabilir.

Storm Worm'unun İzlenmesi

- **Ağ Haritasının Çıkarılması (Crawling)**
  - Geliştirilen ve kodlanan iki asenkron thread kullanılarak tüm ağ dolaşılır.
  - Bu sayede ağdaki tüm eşlerin haritası çıkartılabilir. Bu işlem yaklaşık 40 saniye sürmekteymiş.

Storm Worm'unun İzlenmesi

Algorithm 1: send thread (is executed once per crawl)

```
Data: peer: struct{IP address, port number, DHT ID}
Data: shared list Peers = list of peer elements
/* the list of peers filled by the receive thread and
   worked on by the send thread                          */
Data: int position = 0
/* the position in the list up to which the peers have
   already been queried                                  */
Data: list ids = list of 16 properly chosen DHT ID elements
1 Peers.add(seed); /* initialize the list with the seed peer */
2 while position < size(Peers) do
3     for i=1 to 16 do
4         dest DHT ID = Peers[position].DHT ID ⊕ ids[i]; /* normalize
              bucket to peer's position                  */
5         send route requests (dest DHT ID) to Peers[position];
6     position++;
```

Storm Worm'unun İzlenmesi

Algorithm 2: receive thread (waits for the `route response` messages)

```
Data: message mess = route response message
Data: peer: struct{IP address, port number, DHT ID}
Data: shared list Peers = list of peer elements
/* the list shared with the send thread                    */
1 while true do
2     wait for (mess = route response) message; foreach peer ∈ mess do
3         if peer ∉ Peers then
4             Peers.add(peer);
```

Storm Worm'unun İzlenmesi

- **Overnet ve Stormnet İçi Casusluk**
  - Sybil saldırısı
  - Amaç: Biri tarafından merkezi olarak kontrol edilebilen nodeları P2P ağların stratejik yerlerine konumlandırmak.
  - Böylece ağın bir kısmının ya da tamamının kontrolünü ele geçirmeye çalışmak.
  - Overnet ve Stormnet'e sızmak ve bilgi toplamak için gerçekleştirilir.
  - Ne tarz içeriğin yayınlandığını ve ne arandığının takibi yapılabilir.

Storm Worm'unun İzlenmesi

- **Sybil Gerçekleştirimi:**
  - Aktif olan P nodları DHT ID uzayı kullanılarak crawler aracılığıyla bulunur.
  - Bulunan P nodlarına **hello request** gönderilerek yönlendirme tabloları casus nodeları gösterecek şekilde **zehirlenir**.
  - Böylece casus olmayan bir P nodeunun **route request** talebinin casus nodea da iletimi sağlanır. Bu talebe DHD ID'si hedef nodea yakın olan casus nodeların bilgisi ile karşılık verilir. P node'u hedef sisteme yeterince yakın olduğunu hissettiğinde **publish request** ya da **search request'te** bulunur ve bunların tamamı casus nodelar tarafından da görülür.
  - Bu şekilde gerçekleştirilen **tüm route request**'ler, **publish request** ve s**earch request'ler** casus nodelara da ulaşır.
  - Tüm içerik daha sonra analiz edilmek üzere veritabanında saklanır.

Storm Worm'unun İzlenmesi

- **Dolaşma ve Casusluk Sonucu**
  - 45.000 ve 80.000 arası online eş Overnet üzerinde
  - 426,511 farklı DHT ID ve 1,777,886 farklı IP adresi
  - %75'i bir NAT sisteminin arkasında çalışmadığı
  - 210 farklı ülke

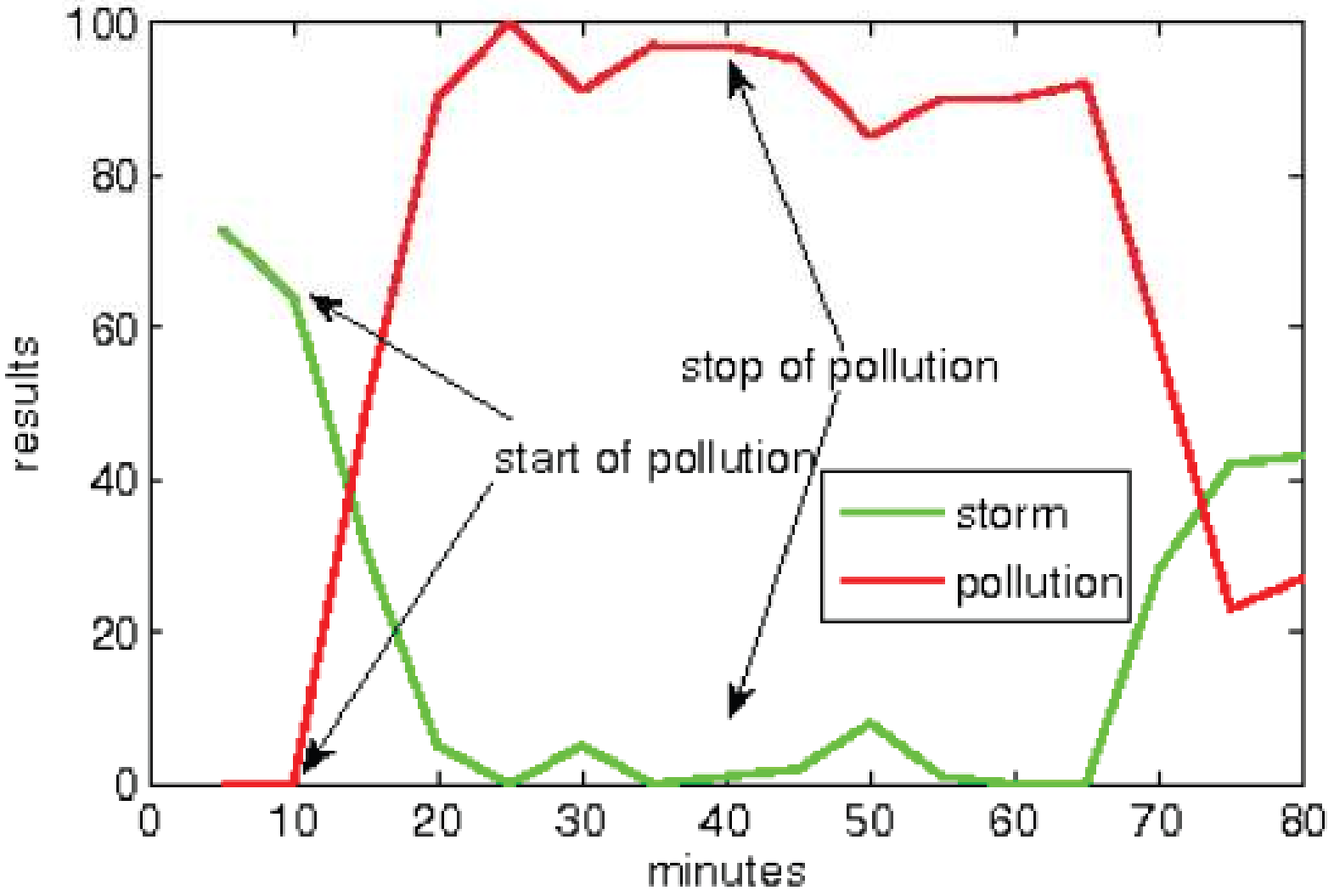
Zararlı ile Mücadele

- **Eclipsing Content**
  - Sybil saldırısı gibi
  - Bir K anahtarına benzer anahtar üretiler.
  - Yönlendirme tablosu zehirlenir.
  - Bu şekilde tüm **route requestler** elde edilmeye çalışılır.
  - Overnet ve Stormnet'te kullanılan içeriğin anahtar bilgisi tüm hash uzayı için gönderilmesi ve uzayın belili bir K anahtarı etrafında sınırlanamaması nedeniyle bir K arama anahtarının tamamıyla örtülmesi *gerçekleştirilememektedir*.

Zararlı ile Mücadele

- **Kirletme (Polluting)**
  - Belirli bir K anahtarı için gerçekleştirilen aramaların sonucuna ulaşılmaması için, K anahtarı kullanılarak çok büyük boyutlu içerik dosyaları yayınlanır.
  - Burada amaç K anahtarı ile saldırgan tarafıdan daha önce yayımlanan içeriğin yeni yayınlanan içerik tarafından bastırılmasını sağlamaktır.
  - Storm botları da K anahtarı için içerik yayınlayacakları için saldırıyı kontrol etmeye çalışan grup ile saldırıyı gerçekleştiren makinalar arasında bir yarış durumu oluşacaktır.

Zararlı ile Mücadele



1