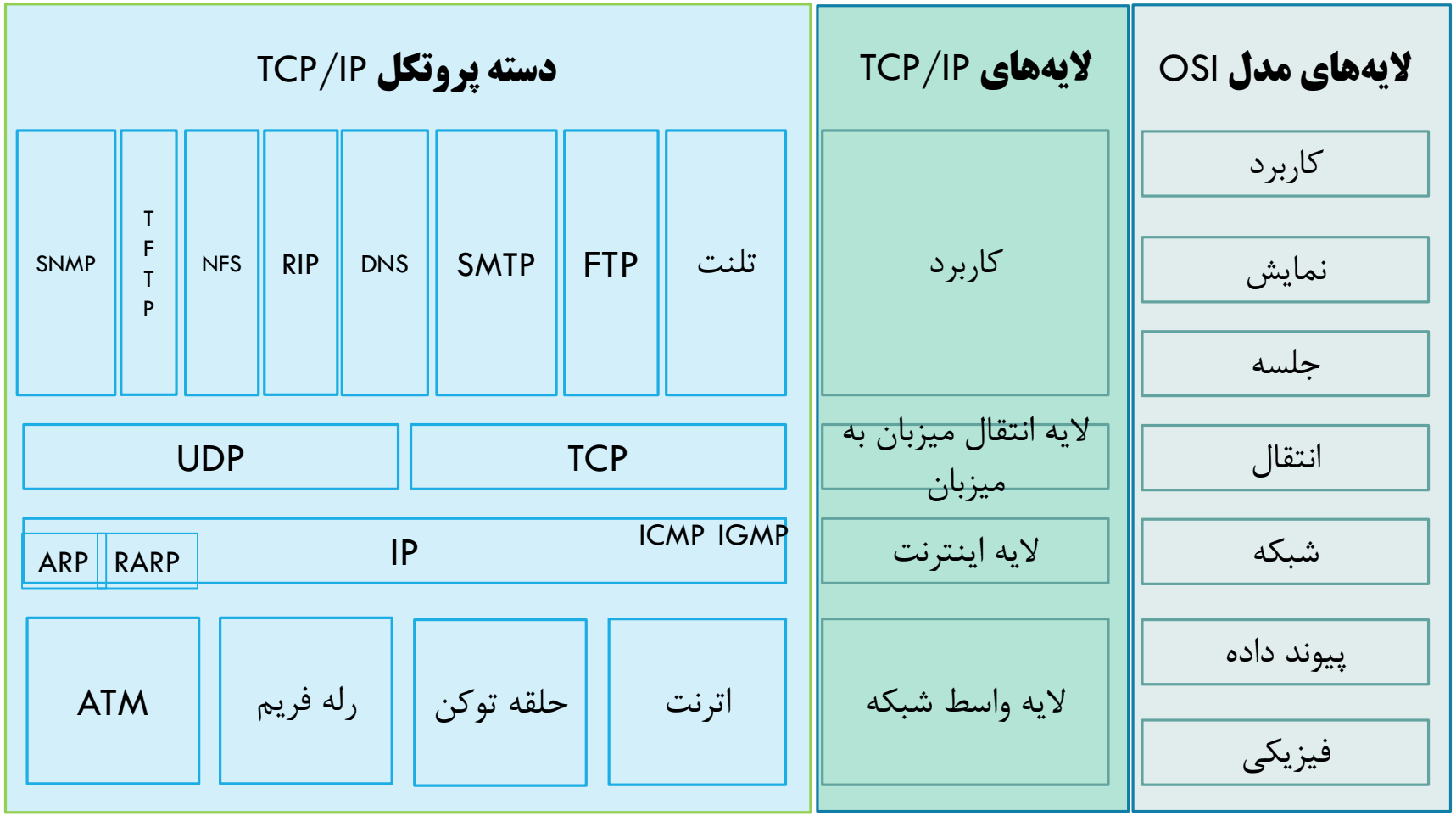
مبانی رایانش امن
نرم‌افزارهای مخرب، حملات معمول

محسن هوشمند
دانشکده تکنولوژی اطلاعات و علم رایانه
دانشگاه تحصیلات تکمیلی علوم پایه زنجان

مدل OSI و TCP/IP



لایه (بین)شبکه

پروتکل اینترنت

- IP
- بدون اطمینان و بی‌اتصال
- بدون وارسی خط و رهگیری
- بسته‌های آی‌پی: دیتاگرم
- ارسال جداگانه و امکان سفر از مسیرهای متفاوت
- امکان دریافت خارج از ترتیب و دریافت چندباره
- عدم رهگیری مسیرها و عدم امکان بازترتیب بسته‌ها
- اجازه افزودن توابع و کارکردهای جدید در صورت لزوم

لایه (بین)شبکه

Address Resolution Protocol (ARP)

- ARP(IP_Address) → Physical_Address
- RARP(Physical_Address) → IP_Address

Internet Control Message Protocol (ICMP)

- گزارش خطا

Internet Group Message Protocol (IGMP)

- مدیریت چندارسالی

ICMP

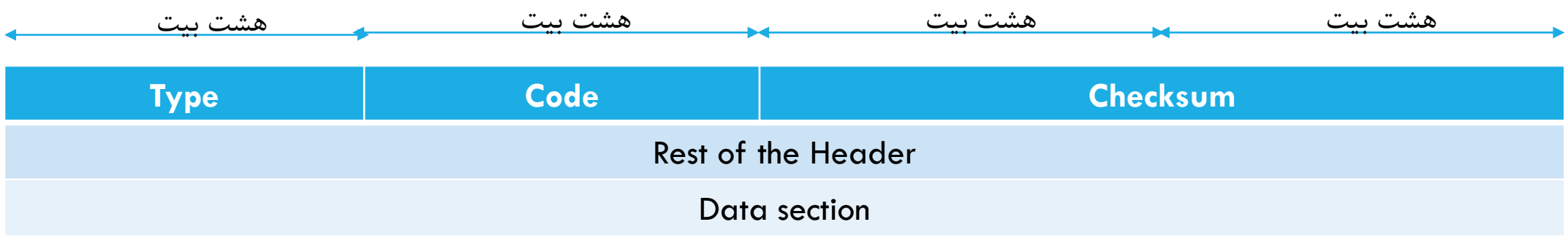
عدم وجود سازوکار کار با خط
- گزارش خطا
- مسئول: ICMP
- پیام‌های ICMP

ICMP Message Type	Description and Important Codes
0: Echo Reply	Answer to a Type 8 Echo Request
3: Destination Unreachable	Error message indicating the host or network cannot be reached. The codes follow: **0**—Destination network unreachable **1**—Destination host unreachable **6**—Network unknown **7**—Host unknown **9**—Network administratively prohibited **10**—Host administratively prohibited **13**—Communication administratively prohibited
4: Source Quench	A congestion control message
5: Redirect	Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway. The codes follow: **0**—Redirect datagram for the network **1**—Redirect datagram for the host
8: Echo Request	A ping message, requesting an Echo Reply
11: Time Exceeded	The packet took too long to be routed to the destination (code 0 is TTL expired)

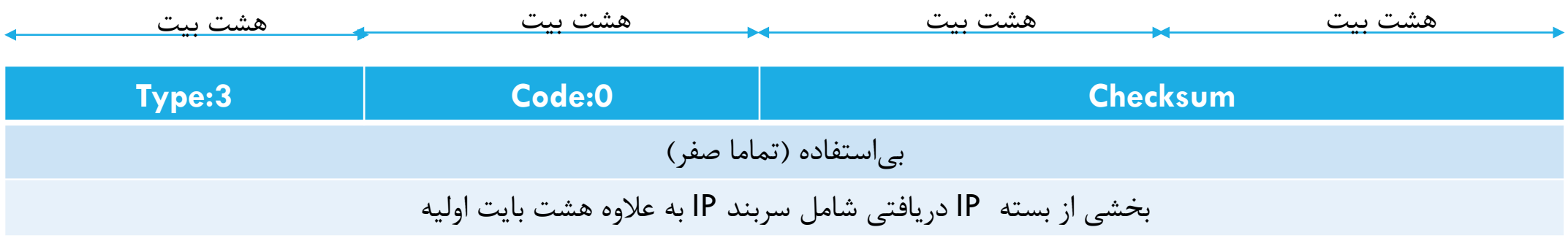
Table 3-2 Relevant ICMP Message Types

پیام‌های درخواستی Query messages	۸ یا 0	درخواست اکو یا پاسخ
	۱۳ یا ۱۴	درخواست استمپ زمانی یا پاسخ

فرمت کلی پیام ICMP



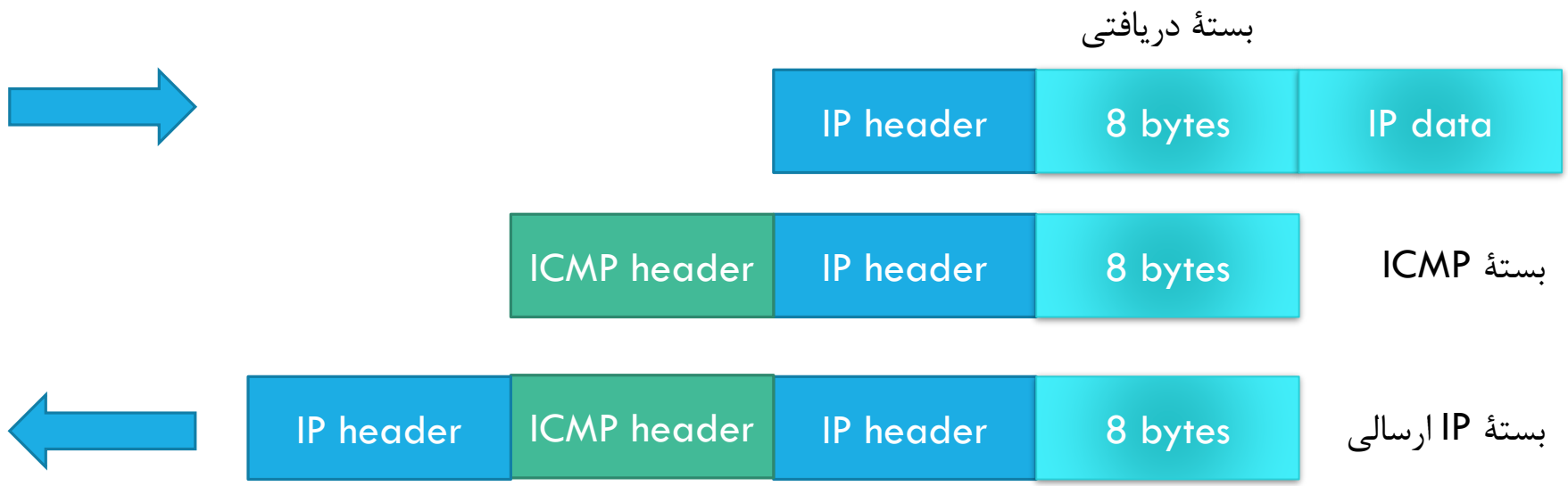
گزارش خطا-مقصد دسترسی‌ناپذیر



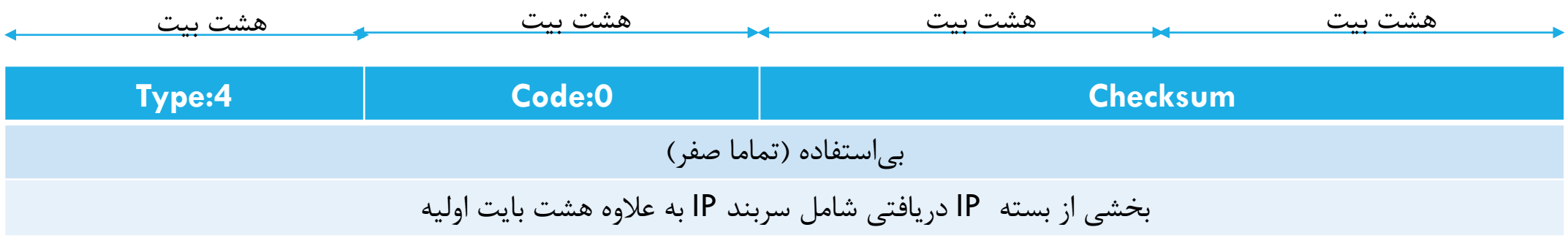
گزارش خطا به مبدا اصلی

انواع گزارش خطا

- مقصد دسترس‌ناپذیر


بستهٔ دریافتی
IP header
8 bytes
IP data
ICMP header
IP header
8 bytes
بستهٔ ICMP
IP header
ICMP header
IP header
8 bytes
بستهٔ IP ارسالی

کاهش سرعت SOURCE QUENCH

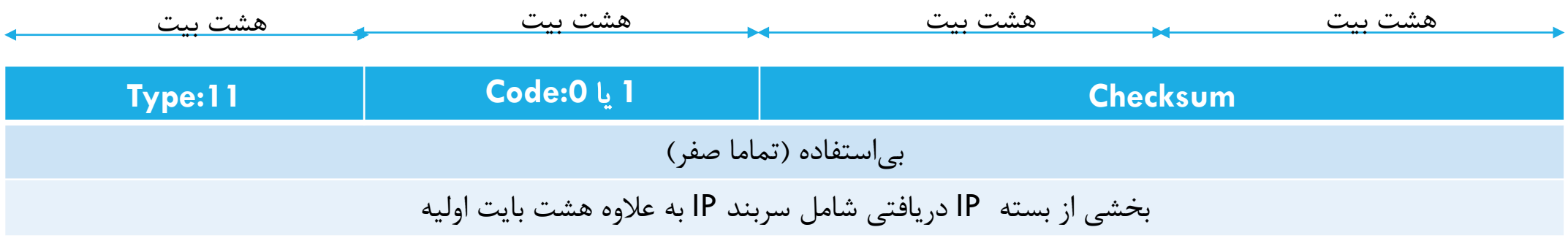


عدم وجود کنترل جریان یا کنترل شلوغی congestion در پروتکل IP

پیام اطلاع کاهش حجم ارسال

- Source quench

زمان زیادی



رسیدن TTL به صفر. حذف بسته و ارسال پیام زمان زیادی به مبدا اصلی: کد صفر

یا عدم دریافت تمامی قطعات- ارسال زمان زیادی پیام و دور ریختن قطعات دریافتی: کد یک

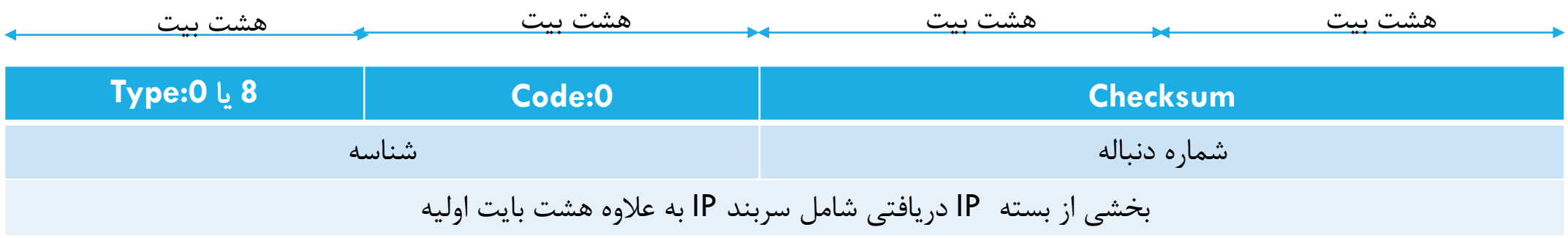
مشکل پارامتر

Type:12	Code:0 یا 1	Checksum
Pointer	بی‌استفاده (تماما صفر)	
بخشی از بسته IP دریافتی شامل سربند IP به علاوه هشت بایت اولیه		

تغییر مسیر پیام

Type:5	Code:0 یا 3	Checksum
نشانی IP مسیریاب هدف		
بخشی از بسته IP دریافتی شامل سربند IP به علاوه هشت بایت اولیه		

پیام درخواست-اکو



با میزبان یا مسیریاب

ارسال پیام پاسخ-اکو از میزبان یا مسیریاب دریافت‌کنندهٔ پیام درخواست-اکو

مشهور به پیام‌های پینگ

ابزاری مدیریتی جهت

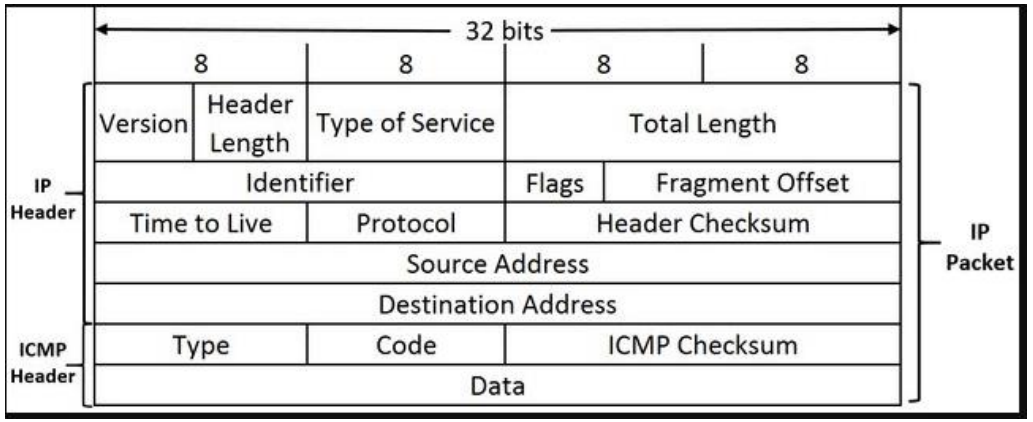
- آزمایش اتصال بین ابزارهای شبکه
- آزمایش تاخیر شبکه و ازدست دادن بسته

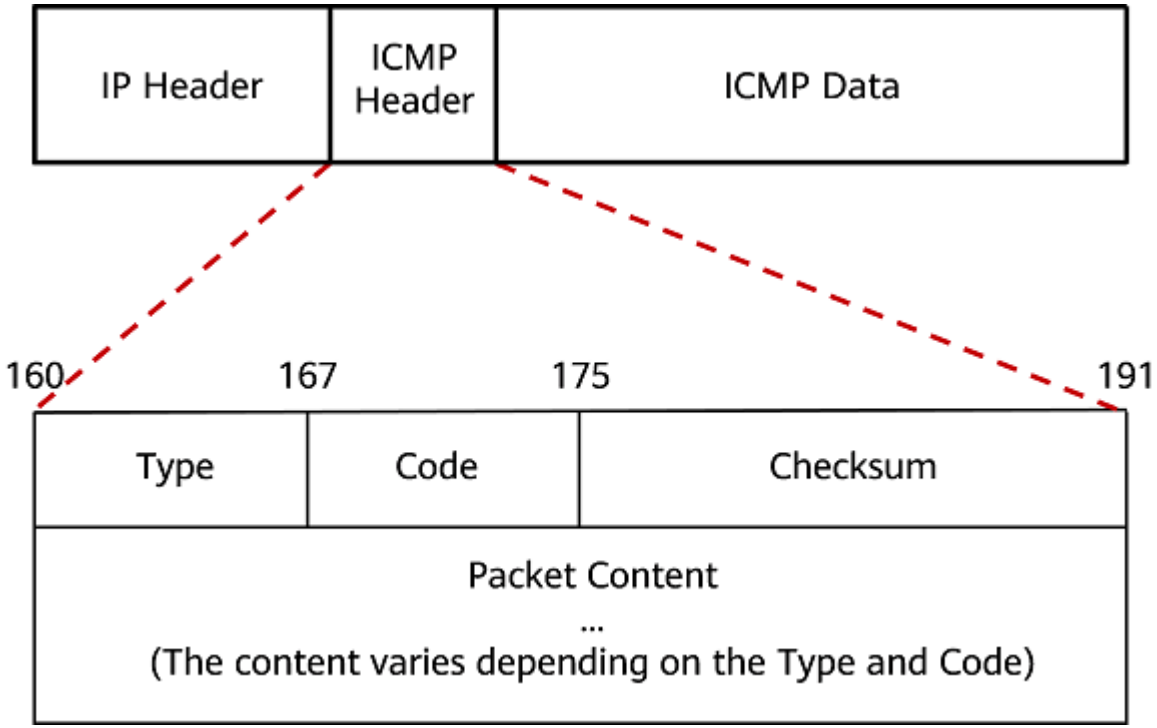
پیام درخواست-استمپ زمانی و پاسخ

Type:13 یا 14	Code:0	Checksum
شناسه		شماره دنباله
بخشی از بسته IP دریافتی شامل سربند IP به علاوه هشت بایت اولیه		
استمپ زمان دریافت		
استمپ زمان ارسال		

مشخص کننده زمانی که پیام ICMP در انتقال صرف می‌کند

نگرانی بابت اشکالات امنیتی





https://info.support.huawei.com/info-finder/encyclopedia/en/ICMP.html

https://www.researchgate.net/publication/316727741_Determining_proximal_geolocation_of_IoT_edge_devices_via_covert_channel/figures?lo=1

مهمترین نمونه‌های معمول تهدیدات امنیتی

کد مخرب

برنامه‌های ناخواسته

طله‌گذاری

هک‌کردن و خرابکاری سایبری

دزدی /کلاهبرداری کارت

جعل

کد مخرب

یا بدافزار

Malicious code یا malware

برنامه‌ای که پنهانی در برنامهٔ دیگری با قصد تخریب داده، اجرای برنامه‌های نفوذ یا مخرب، وارد شده است

گستره‌ای از تهدیدات شامل

- ویروس‌ها
- کرم‌ها
- باج‌افزار
- اسب‌های تروا
- در رو (در پشتی)
- بات‌ها، بات‌نت‌ها (شب‌بات)

طبقه‌بندی با روش انتشار و یا فعالیت و محموله

- انتشار شامل ویروس‌ها و کرم‌ها و تروا‌ها
- محموله شامل تخریب سیستم، طله‌گذاری جاسوسی، موارد دیگر

کد مخرب

دسته‌بندی‌های قدیمی

- تمایز بین انگل‌ها (ویروس‌ها) و مستقل‌ها(کرم‌ها و ترواها و بات‌ها)!
- تمایز بین تولید مثل (ویروس‌ها و کرم‌ها) و عدم تولید مثل(ایمیل هرز، ترواها)

کد مخرب

تطور در مجموعه‌ابزارها

- جرم‌افزارها
- مجموعه ابزار زئوس، بلک-هول، ساکورا، فنیکس

بهره‌جویی و ابزارهای بهره‌جوئی exploit

- استفاده از آسیب‌پذیری نرم‌افزارها
- کیت‌های بهره‌جوئی
- مجموعه بهره‌جوی انگلر angler

۲۰۱۶

- تولید ۳۵۷میلیون بدافزار
  - میانگین نیم‌میلیون در روز!

کد مخرب

قبلا صرفا تک نفره و جهت تضعیف کامپیوتر

امروزه گروه‌های کوچک هک یا شرکت‌های مورد حمایت دولتی

- جهت دزدی ایمیل‌ها و اعتبارات مربوط به اتصال و داده شخصی و اطلاع مالی
- تفاوت بین جرم خرده‌پا (آفتابه‌دزد) و جرم سازمان‌یافته

تحویل بدافزار

- معمولا با پیوستی به ایمیل یا پیوندی در ایمیل
- یا در صفحات ورد و اکسل
- اخیرا اتصال آن به زنجیره تبلیغات برخط
  - بدیغات! Malvertising
- یکی از مهم‌ترین تبلیغات آلوده به بدافزار
  - یاهو ۶,۹ میلیون کاربر بازدیدکنندهٔ روزانه
  - ۲۰۱۶ بنگاه‌های خبری چون نیویورک تایمز و aol و بی‌بی‌سی تبلیغات منتشر در چند شبکه تبلیغی و رسیدن به بنگاه‌های مذکور
    - به دست گرفتن رایانه با کلیک شدن، رمز کردن داده کاربر
- امکان جلوگیری با بلوکه کردن تبلیغات ظاهر شدنی
- استفاده از فلش ادوب
  - جلوگیری مرورگرهای اصلی از اجرای خودکار آن
- زمان فعلی
  - Fileless malware

کد مخرب

پیاده‌کردن از داخل ماشین

- Drive-by download
- بدافزار همراه با فایل درخواستی جهت پیاده
- درخواست آگاهانه یا ناآگاهانه
- از روش‌های شایع آلوده کردن رایانه
- تعبیه در پی‌دی‌اف
- امروزه بیشتر حرفه‌ای و سازمانی تا ناوارد و تازه‌کار
  - سخن‌کوتاه بحث پول

ویروس‌ها، کرم‌ها، تروا‌ها، درهای پشتی

تروا‌ها، درهای پشتی

- دو روش دسترسی به سیستم
- دارای انواع
- اما اشتراک در نیاز به نصب با برنامه دیگر

ویروس‌ها، کرم‌ها

- مخرب برای سیستم‌ها و شبکه‌ها همانند تروا‌ها و درهای پشتی
- حامل تروا‌ها و ممکن‌سازی ایجاد درپشتی برای خرابکاران

ویروس

برنامه رایانه‌ای

- انگلی
- قادر به ایجاد و تولید از خود
- پخش به دیگر فایل‌ها و آلودگی دیگر برنامه‌ها
- تغییر برنامه‌ها
  - تزریق رویه‌ای به کد اصلی جهت امکان تولید ویروس
- امکان ویروس متصل به برنامه به انجام هر کاری که برنامه اجازه آن را دارد.

اجزای ویروس‌ها

- سازوکار آلودگی- ابزارهایی انتشاردهندهٔ ویروس و امکان‌دهی تولید از خود.
- شلیک- رخداد یا شرطی مشخص‌کنندهٔ فعال‌سازی یا تحویل محموله
- اجرای عمل مخربی «محموله» payload
  - آنچه ویروس به جز انتشار انجام می‌دهد
  - از نمایش پیامی یا تصویری تا تخریب فایل‌ها و فرمت‌کردن حافظه جانبی رایانه از کار انداختن یا بدکار کردن برنامه‌ها

ویروس

فازهای دوره زندگی ویروس

- خفتگی dormant
  - غیرفعال بودن ویروس
- انتشار
  - تعبیه نسخه‌ای از خود در برنامه‌ای دیگر یا بخش‌های خاصی از سیستم روی دیسک
  - غالبا همراه با دگردیسی جهت پنهان ماندن
  - برنامهٔ آلودهٔ جدید دارای توده ویروسی قرار گرفته در فاز انتشار
- فاز شلیک
  - فعال شدن ویروس برای اجرای کارکردهای تعریف شده
- فاز اجرا
  - انجام کارکرد،
  - احتمال بی‌خطر بودن مانند نمایش پیام روی صفحه یا خطرداری مانند تخریب برنامه و فایل‌های داده

ویروس

معمولا وابسته به سع

حتی وابسته به سخت‌افزار خاص

سخن کوتاه، طراحی شده جهت انتفاع از جزییات و ضعف‌های سیستم‌های خاص

ویروس ماکرو

- هدف‌گیری انواع خاصی از اسناد مورد استفاده در گستره‌ای از سیستم‌ها

ویروس

- ساختار ویروس اجراپذیر
  - اتصال به ابتدا یا انتهای برنامهٔ اجراپذیر یا تعبیه به دیگر انواع برنامه به انحاء دیگر
  - کلید اجرای برنامه آلوده
  - اجرای کد ویروس در ابتدا و سپس اجرای کد برنامهٔ اصلی

ویروس

- ساختار ویروس اجراپذیر
  - اتصال به ابتدا یا انتهای برنامهٔ اجراپذیر یا تعبیه به دیگر انواع برنامه به انحاء دیگر
  - کلید اجرای برنامه آلوده
  - اجرای کد ویروس در ابتدا و سپس اجرای کد برنامهٔ اصلی
  - کد روبرو

```
program V
1234567;
procedure attach-to-program;
begin
    repeat
        file := get-random-program;
    until first-program-line ≠ 1234567;
    prepend V to file;
end;
procedure execute-payload;
begin
    (* perform payload actions *)
end;
procedure trigger-condition;
begin
    (* return true if trigger condition is true *)
end;
begin (* main action block *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto main;
end;
```

ویروس

- ساختار ویروس اجراپذیر
  - اتصال به ابتدا یا انتهای برنامهٔ اجراپذیر یا تعبیه به دیگر انواع برنامه به انحاء دیگر
  - کلید اجرای برنامه آلوده
  - اجرای کد ویروس در ابتدا و سپس اجرای کد برنامهٔ اصلی
  - کد روبرو
  - سادگی تشخیص

```
program V
1234567;
procedure attach-to-program;
begin
    repeat
        file := get-random-program;
    until first-program-line ≠ 1234567;
    prepend V to file;
end;
procedure execute-payload;
begin
    (* perform payload actions *)
end;
procedure trigger-condition;
begin
    (* return true if trigger condition is true *)
end;
begin (* main action block *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto main;
end;
```

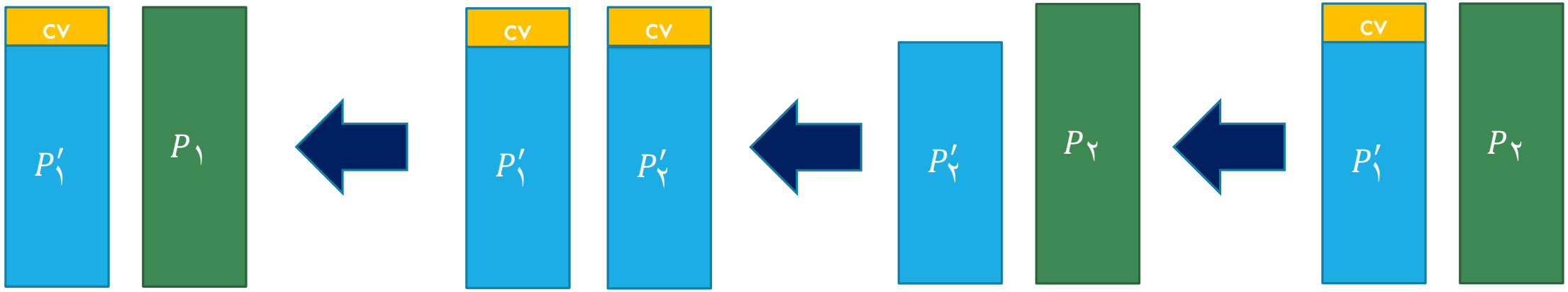
ویروس

- ساختار ویروس اجراپذیر
  - اتصال به ابتدا یا انتهای برنامهٔ اجراپذیر یا تعبیه به دیگر انواع برنامه به انحاء دیگر
  - کلید اجرای برنامه آلوده
  - اجرای کد ویروس در ابتدا و سپس اجرای کد برنامهٔ اصلی
  - کد روبرو
  - سادگی تشخیص
  - راه‌حل- فشرده کردن کد اجراپذیر

```
program V
1234567;
procedure attach-to-program;
begin
    repeat
        file := get-random-program;
    until first-program-line ≠ 1234567;
    prepend V to file;
end;
procedure execute-payload;
begin
    (* perform payload actions *)
end;
procedure trigger-condition;
begin
    (* return true if trigger condition is true *)
end;
begin (* main action block *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto main;
end;
```

ویروس

```
program CV
1234567;
procedure attach-to-program;
begin
        repeat
                file := get-random-program;
        until first-program-line ≠ 1234567;
        compress file; (* t1 *)
        prepend CV to file; (* t2 *)
end;
procedure (* main action block *)
        if ask-permission then attach-to-program;
        uncompress rest of this file into tempfile; (* t3 *)
        execute tempfile; (* t4 *)
end;
```



t_0: آلودگی P'_1 و پاکی P_2

t_1: آلوده شدن P_2 و ایجاد نسخهٔ آلودهٔ P'_2

t_2: الحاق ویروس فشرده به P'_2

t_3: درآوردن از فشردگی P'_1 به برنامه اصلی P_1

ویروس

- طبقه‌بندی ویروس‌ها
  - طبقه‌بندی مبنی بر مقصد
    - آلایندهٔ سکتور راه‌انداز (بوت)
    - آلایندهٔ فایل-
    - ویروس ماکرو-
    - ویروس چندبخشی-
  - طبقه‌بندی مبنی بر روش پنهان شدن
    - ویروس رمزشده
    - ویروس پنهان stealth
    - ویروس چندریختی
    - ویروس دگردیس

کرم

معمولا ویروس‌ها همراه کرم

به جای پخش از فایل به فایل

- طراحی‌شده جهت پخش از رایانه به رایانه
- به دنبال نقاط آسیب‌پذیر در برنامه‌های سرور یا مشتری جهت دسترسی به سیستم‌های جدید
  - استفاده از شبکه جهت انتشار بین رایانه‌ها
  - رسانه‌های اشتراکی مانند کارت حافظه خارجی، دیسک نوری
  - انتشار کرم‌های ایمیلی با تعبیه در کد اسکریپت یا داده‌های پیوست به ایمیل
  - انتقال فایل در پیام‌رسان‌ها

لازم نبودن فعال شدن به دست کاربر

امکان داشتن محموله

کرم

یافتن هدف

- به دنبال سیستم‌های استفاده‌کننده از خدمات آسیب‌پذیر و سپس آلوده کردن آنها
  - ادامه جهت یافتن موارد جدید پس از نصب روی سیستمی
- روش‌های پیمایش نشانی‌های شبکه
  - تصادفی
  - فهرست حمله
  - توپولوژی
  - زیرشبکهٔ محلی

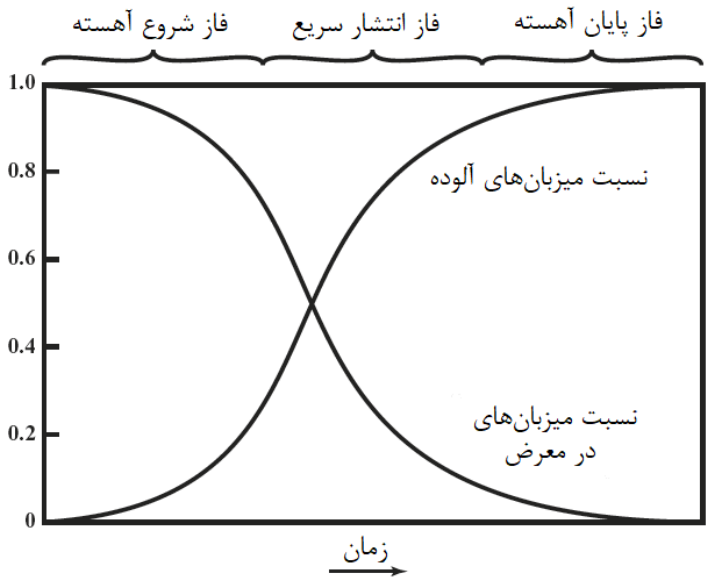
کرم

مدل انتشار

- استفاده از مدل‌های همه‌گیری
  - ساده‌ترین

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

- $I(t)$ تعداد افراد آلوده شده در زمان t
- $S(t)$ تعداد افراد در معرض ولی آلوده نشده در زمان t
- β آهنگ آلودگی
- $N = I(t) + S(t)$ کل جمعیت



کرم

کرم اسلامر Slammer

- از بدنامان محل!
- هدف آن آسیب‌پذیری شناخته شده «پ‌د» در سرور سکیول مایکروسافت
  - آلوده کردن ۹۰ درصد رایانه‌های در سطح دنیا پس از ده دقیقه از انتشار اولیه!
    - از کار انداختن دستگاه‌های خودپرداز بانک امریکا
    - صندوق بقالی‌ها مانند زنجیره پابلیکس در اتلانتا
    - از کار انداختن اتصالات اینترنتی در کره جنوبی و افت بازار سهام

کرم کانفیکر در سال ۲۰۰۸

- پیچیده‌ترین پس از اسلامر تاکنون
  - آلوده کردن ۱۱ میلیون کامپیوتر
- ۲۰۱۷ راه‌اندازی مجدد با باج افزار واناکرای

باج‌افزار

نوعی از بدافزارها (و معمولا از نوع کرم)

- قفل کردن رایانه یا فایل‌ها و جلوگیری از دسترسی شما بدان‌ها
- معمولا نمایش پیامی که دادگستری یا نیروی پلیس فعالیت غیرمجازی بر روی رایانه شما پیدا کرده است
  - درخواست پرداخت جریمه جهت بازکردن رایانه و جلوگیری از پیگیرد قانونی

از انواع

- رمزقفلcryptolocker
  - رمز کردن فایل‌ها با رمزگذاری نامتقارن و درخواست بازگشایی آن مثلا با بیت‌کوین
  - انجام نیافتن در زمان مقرر معمولا منجر به رمز شدن آن برای همیشه
- رمزدفاع Cryptodefense
- رمزدیوار

افزایش ۴۰۰درصدی حملات باج‌افزارها

- مرتبط با رشد ارز مجازی بیت‌کوین

مهم‌ترین واناکرای wannaCry

- آلوده کردن ۲۳۰هزار رایانه در پهنه دنیا
- هدف رایانه‌های استفاده کننده از سیستم‌عامل ویندوز
- رمزکردن داده و درخواست پرداخت بیت‌کوین

درپشتی

Backdoor و همین‌طور trapdoor

ویژگی ویروس‌ها و کرم‌ها و اسب‌های تروا

- موجب‌ساز دسترسی دور به رایانه آلوده شده
- با استفاده از آن دسترسی به سیستم بدون نیاز به عبور از روال‌های دسترسی امنیتی عادی
- نصب به عنوان خدمت شبکه
  - گوش دادن به پورتی غیراستانده که مهاجم با استفاده از آن می‌تواند وصل شود

داون‌اپ

- کرم با درپشتی

ویروت

- ویروس که فایل تایپ‌ها را تغییر می‌دهد
- همچنین دارای درپشتی جهت پیاده و نصب تهدیدات بیشتر

درپشتی

افزودن خدمت جدید

- معمول‌ترین روش پنهان‌کاری درپشتی در سیستم عامل ویندوز
- پیش از نصب
- پیش از نصب بررسی سیستم جهت شناخت خدمات در حال اجرا
- ایجاد خدمت جدید با نام شک‌نینگیز!

تروجان‌های مدیریت راه دور Remote Administration Trojans (RATs)

- دسته‌ای از درهای پشتی مناسب جهت تدسترسی دور به ماشین تسخیر شده
- فراهم کردن کارکردها ظاهری مناسب برای کاربر و باز ردن پرت‌های شبکه رایانه قربانی
- دارای دو فایل سرور و مشتری
  - سرور نصب شده در سیستم مشتری
  - مشتری جهت نفوذ به سیستم تسخیرشده

اسب تروا

جلوهٔ بی‌خطری و سپس انجام عملی غافلگیرکننده
- از موارد مهندسی اجتماعی

ویروس نیست
- عدم توانایی تولید از خود
- اما جاده‌صاف کن ورود ویروس‌ها یا دیگر کدهای مخرب مانند بات‌ها و روتکیت‌ها
- یا حملات بنداوری خدمت توزیعی Distributed Denial of Service (DDOS)

ارسال از طریق پیام‌رسان، IRC، پیوست ایمیل یا برنامه‌های جعلی

دارای برنامهٔ پنهان جهت سرقت گذرواژه‌ها و ارسال آن

دراپرها و پیاده‌سازها و دیگر انواع
- ۱۳۹۰ سونی تجربه بزرگترین نقض داده در زمان خود
  - دستیابی به اطلاعات ۷۷ میلیون کاربرثبت‌شده شامل کارت بانک
- معمولا استفاده در بدافزارهای مالی پخش شده با شبات‌ها
  - زئوس
    - سرقت اطلاعات با بررسی کلیک‌های روی صفحه کلید
    - ۱۰ میلیون رایانه از سال ۲۰۰۷
  - تینبا
    - اولین بار دیده شده در ۱۳۹۱ با فروش اطلاعات اعتباری از طریق حمله هنگامی که کاربر در حال دستیابی به تارمانه بانکی خود است
  - رمنیت
    - جهت سرقت رمزهای بانکی، کلوچک‌های جلسات، داده شخصی

اسب تروا

برنامه‌ها:

Trojan Name	Port	Trojan Name	Port
Emotet	20/22/80/443	Bionet, MagicHound	6667/12349
Dark FTP	21	GateCrasher	6969
EliteWrap	23	Remote Grab	7000
Mspy	68	ICKiller	7789
Ismdoor, Poison Ivy, powerstats	80	Zeus, Shamoon	8080
WannaCry, Petya	445	BackOrifice 2000	8787/54321
njRAT	1177	Delf	10048
DarkComet, Pandora RAT	1604	Gift	10100
SpySender	1807	Senna Spy	11000
Xtreme	1863	Progenic Trojan	11223
Deep Throat	2140/3150/6670/6671	Hack 99 Keylogger	12223
Spygate/Punisher RAT	5000	Evil FTP	23456
Blade Runner	5400–02	Back Orifice 1.20/ Deep BO	31337, 31338
Killer, Houdini	6666	Devil	65000

اسب تروا

کانال‌های Overt و Covert

- کانال **overt** کانال معمول و قانونی که برنامه‌ها با سیتم یا شبکه ارتباط برقرار می‌کنند
- کانال **covert** استفاده از کانال‌های برنامه در راستایی غیر از آنچه اهداف آنهاست.

استفاده تروا‌ها از کانال‌های Covert

- سختی رمزگشایی و فهم آنها
- تکیه بر تونل‌زنی
  - اجازه به پروتکلی جهت استفاده از پروتکل دیگر
  - تونل‌زنی ICMP
    - استفاده از **ICMP echo-request** و **echo-reply** جهت انتاقل داده **payload** مورد نیاز مهاجم
    - ابزار **Loki**

فهرست انواع تروا‌ها

defacement Trojan

proxy server Trojan

- استفاده جهت تونل‌کردن ترافیک یا اجرای حله تهاجمی با سیستم دیگر

botnet Trojans

- Denial of Service Trojans
- استفاده جهت اجرای حمله به خدمت یا بندآوری آن

Remote access Trojans

- Remote Access Trojans RATS
- استفاده جهت دسترسی راه دور به سیستم

e-banking Trojans

Data-sending Trojans

- استفاده جهت یافتن داده روی سیستم و تحویل داده به مهاجم

Destructive Trojans

- استفاده جهت حذف یا تخریب فایل‌های روی سیستم

FTP Trojans

- استفاده جهت ایجاد سرور اف‌تی‌پی به منظور کپی کردن فایل‌ها به سیستم

Security software disabler Trojan

- استفاده جهت از کار آنداختن آنتی‌ویروس

فهرست انواع ترواها

command shell Trojan

- درپی فراهم‌سازی درپشتی به سیستم با استفاده از خط-فرمان
- Netcat
  - باز و بسته کردن پورت‌ها جهت گوش دادن
  - تمرین کار با آن. یک هفته. گزارش هفته بعد و امتیازدهی
  - امکان استفاده از آن
    - جهت ارتباطات دورنی یا بیرونی
    - TCP یا UDP
    - هر پورتی روی ماشین
    - DNS forwarding
    - Port mapping and forwarding
    - Proxying
    - Port scanner

تحلیل بدافزار

فرایند مهندسی معکوس نرم‌افزاری مخبر

جهت یافتن اطلاع از چگونگی کارکرد و ساخت آن

دو دسته روش

- ایستا و پویا
- تحلیل بدافزار ایستا Static malware analysis یا static code analysis
  - بررسی کد اجرایی جهت شناخت بدافزار
- تحلیل بدافزار پویا

بات‌ها

- نصب مخفیانه بر رایانه متصل به اینترنت
- پس از نصب پاسخ به شخص ثالث خارجی
  - شبان‌بات
- استفاده از منابع رایانه مسخر برای اجرای اهداف مهاجم
- شب‌بات (نت‌بات)
  - مجموعه رایانه‌های مسّخر
  - جهت انجام فعالیت‌های مخرب مثل ارسال اسپم، حمله دداس، دزدی اطلاعات از دیگر رایانه‌ها و ذخیره ترافیک شبکه برای مقاصد بعدی
- مشخص نبودن تعداد دقیق اما محتملا هزاران که کنترل‌گر میلیون‌ها کامپیوتر
- تهدیدی بزرگ برای اینترنت و تا
  - به دلیل امکان انجام حملات بسیار بزرگ با استفاده روش‌های متنوع و گسترده

بات‌ها

- کاربردها
  - حملات عدم‌خدمت توزیعی DDoS
  - هرزنامه‌نگاری
  - شنود ترافیک
  - ثبت کلیک «کی‌لاگینگ»
  - پخش بدافزار جدید
  - نصب امکانات تبلیغاتی و اشیای کمکی مرورگر
  - حمله به شبکه‌های گفتگو
  - دستکاری بازی‌ها و نظرسنجی برخط

بات‌ها

- روستوک
  - بزرگترین منبع اسپم‌سازی با تحت انقیاد گرفتن پانصدهزار رایانه
  - کنترل سرورهای واقع در شش محل خدمات‌رسانی در امریکا
    - اطلاعی از اینکه روستوک چه می‌کند نداشتند
  - ۱۳۹۰ اتحاد شبه پلیس فتای امریکا و واحد جرائم دیجیتال مایکروسافت جهت از کار انداختن آن
- ۱۳۹۲
  - مایکروسافت و پلیس فدرال به دنبال از کار انداختن ۱۴۰۰ شبات زئوس محور
  - خالی کردن حساب‌های بانکی نزدیک ۵۰۰ میلیون دلار

TABLE 5.4 NOTABLE EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Emotet	Botnet/ Ransomware	Large botnet that delivers various malicious payloads, including ransomware. First appeared in 2017, became the most prevalent malware in 2018, and continued to have an impact in 2019.
WannaCry	Ransomware/ worm	First appeared in 2017. Exploits vulnerabilities in older versions of Windows operating systems, encrypts data, and demands a ransom payment to decrypt them.
Cryptolocker	Ransomware/ Trojan	Hijacks users' photos, videos, and text documents, encrypts them with virtually unbreakable asymmetric encryption, and demands ransom payment for them.
Citadel	Trojan/botnet	Variant of Zeus Trojan, focuses on the theft of authentication credentials and financial fraud. Botnets spreading Citadel were targets of Microsoft/FBI action in 2012.
Zeus	Trojan/botnet	Sometimes referred to as king of financial malware. May install via drive-by download and evades detection by taking control of web browser and stealing data that is exchanged with bank servers.
Ramnit	Trojan/botnet	One of the most prevalent malicious code families still active. In operation since 2010, but largely disappeared in 2015 after the botnet that spread it was taken down. Reemerged in 2016 to become one of the most common financial trojans.
Conficker	Worm	First appeared in 2008. Targets Microsoft operating systems. Uses advanced malware techniques. Largest worm infection since Slammer in 2003. Used in 2017 in conjunction with various ransomware attacks.
Netsky.P	Worm/Trojan	First appeared in early 2003. It spread by gathering target e-mail addresses from the computers, then infected and sent e-mail to all recipients from the infected computer. It was commonly used by bot networks to launch spam and DoS attacks.
Storm (Peacomm, NuWar)	Worm/Trojan	First appeared in 2007. It spread in a manner similar to the Netsky.P worm. Could also download and run other Trojan programs and worms.
Nymex	Worm	First discovered in 2006. Spread by mass mailing; activated on the 3rd of every month, and attempted to destroy files of certain types.
Zotob	Worm	First appeared in 2005. Well-known worm that infected a number of U.S. media companies.
Mydoom	Worm	First appeared in 2004. One of the fastest spreading mass-mailer worms.
Slammer	Worm	Launched in 2003. Caused widespread problems.
Melissa	Macro virus/ worm	First spotted in 1999. At the time, the fastest spreading infectious program ever discovered. It attacked Microsoft Word's Normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook Address Book.

بات‌ها

- روستوک
  - بزرگترین منبع اسپم‌سازی با تحت انقیاد گرفتن پان
  - کنترل سرورهای واقع در شش محل خدمات رسانی
  - اطلاعی از اینکه روستوک چه می‌کند نداشتند
  - ۱۳۹۰ اتحاد شبه پلیس فتای امریکا و واحد جرائم
- ۱۳۹۲
  - مایکروسافت و پلیس فدرال به دنبال از کار انداختن
  - خالی کردن حساب‌های بانکی نزدیک ۵۰۰ میلیون

کد مخرب

تهدیدی برای کاربر و سرور

- در سطح سرور
  - اما سرورها معمولا دارای ضدویروس
  - امکان از کار انداختن تارمانه
  - نادر
- در سطح مشتری
  - شایع‌تر
  - امکان انتشار به میلیون‌ها رایانه دیگر

برنامه‌های محتملا ناخواسته

- POTENTIALLY UNWANTED PROGRAMS (PUPS)
  - یا potentially unwanted applications (PUAs)

نصب برنامه‌های ناخواسته و محتملا بدون رضایت مشتری

- انگل‌های مرورگر
  - نظارت و تغییر مرورگر کاربر
- آگهی‌افزار
  - استفاده از تبلیغات ظاهر شدنی
- جاسوس‌افزار
  - رهگیری نوشتن کاربر، ایمیل‌ها، پیام‌ها

معمولا در شبکه‌های اجتماعی و مانه‌های محتوای تولیدی کاربران

- سختی حذف پس از نصب
  - PCProtect
    - جلوه چون ضدبدافزار قانونی در حالی که خود بدافزار

برنامه‌های محتملا ناخواسته

- آگهی‌افزار
  - استفاده جهت نمایش تبلیغات ظاهر شدنی حین بازدید مانه
  - ابزاری مورداستفادهٔ مجرمان سایبری
  - گزارش سیسکو
    - ۷۵ درصد سازمان‌های جستجو شده در سال ۲۰۱۶ آلوده به آگهی‌افزار مخرب
  - گزارش آز مالویربایت
    - تهدید غالب برای مصرف‌کنندگان در ۱۳۹۸
- انگل‌های مرورگر
  - یا ربایندهٔ تنظمیات مرورگر
  - نظارت و تغییر مرورگر کاربر یا ارسال اطلاع مراجعه و بازدید مانه‌ها به رایانه دور
  - معمولا جزوی از آگهی افزار
  - ۱۳۹۴
    - لنوو ارسال لبتاب‌های ویندوزی با آگهی‌افزار نصب‌شدهٔ سوپرفیش
    - موجب خطر ربایش هنگام وصل شدن به شبکه بی‌سیم و جمع‌آوری هر چیزی که در مرورگر تایپ می‌شود
    - غیرقانونی اعلام کردن آگهی افزارها از سوی مایکروسافت
  - Cryptojacking
    - نصب انگل مرورگری بکارگیر قدرت پردازش رایانه جهت کاوش رمزارز
    - ۹ میلیون نشانی میزبان اسکریپت کریپتوجک
- جاسوس‌افزار
  - رهگیری نوشتن کاربر، ایمیل‌ها، پیام‌ها

هک‌کردن، خرابکاری سایبر و هک‌گرائی

هک کردن

- هک‌گر
  - فردی به قصد دستیابی به دسترسی غیرمجاز به رایانه
  - در مقابل کرک‌گر – هک‌گر با قصد جرم
  - دسترسی با یافتن ضعف در رویه‌های امنیتی تارمانه و رایانه
  - قبلا متخصصین عاشق چالش ورود به تارمانه‌های دولتی و شرکتی
  - امروزه به دنبال
    - خرابکاری سایبری
      - برهم زدن، آسیب رساندن، تخریب وب سایت
    - نقض داده
      - سرقت اطلاعات شرکتی و شخصی جهت منافع مالی
      - «بمباران زوم»

هک‌کردن، خرابکاری سایبر و هک‌گرائی

- هک‌گرائی
  - مناصب سیاسی
  - معمولا حمله به دولت‌ها و سازمان‌ها و حتی افراد جهت اهداف سیاسی
  - ویکی‌لیکس و LilzSec و Anonymous
  - Shadow broker
    - مسئول استخراج ابزارهای از آژانس امنیت ملی
    - ایراد اترنال بلو مورد استفاده در حملهٔ باج‌افزار واناکرای
  - گروه‌های ببری
    - تحت استخدام سازمان امنیت شرکت جهت اندازه‌گیری وضعیت امنیتی
    - یافتن مصالح محافظتی
      - کلاه‌سفیدها
        - در خدمت سازمان و یافتن و رفع اشکلات امنیتی
        - انجام کار با انعقاد قرارداد
        - سیب و مایکروسافت
      - کلاه سیاه‌ها
        - همانند سفیدها ولی بدون پرداخت و با هدف ضرر زدن
        - افشای اطلاعات بدست‌آمده
        - اعتقاد به آزاد بودن اطلاعات و افشای اطلاعات محرمانه
- در میانه- کلاه خاکستری‌ها
  - به دنبال خیر بزرگ‌تر با یافتن و آشکار کردن اشکالات امنیتی
  - انتشار اشکالات بدون برهم زدن یا ضرررسانی
  - نام و پرستیژ
  - مظنون

نقض داده

- نقض داده data breach
  - هنگام از دست دادن کنترل سازمان‌ها بر اطلاعاتشان به خوارج
  - ۱۳۹۵ نقض داده و برملایی اطلاعات حدود ۱,۱ میلیارد نفر در ۱۵ نقض بزرگ
  - ۱۰۹۳ نقض داده در سال ۱۳۹۵
  - بیشترین آنها در بخش فیاوری ۴۵ درصد، سپس بخش سلامت ۳۵ درصد
- عوامل اساسی
  - هک‌کردن ۵۵ درصد
  - ایمیل تصادفی/ اینترنت ۹ درصد
  - خطای انسانی/ قصور ۸,۷ درصد
  - دزدی داخلی
- در امریکا بیشترین نقض داده شماره امنیت اجتماعی
- یاهو (سه میلیارد نفر) و اکویفکس (۱۴۳ میلیون نفر) دو مورد از بدنام‌ها

مورد اکویفکس

اکویفکس

- شرکت معتبر در گزارش اعتبار و امتیاز

اعلام در اواخر تابستان ۱۳۹۶

- هک شدن و دسترسی و پیاده‌شدن اطلاعات ۱۴۳ میلیون شهروند امریکائی
- شامل اطلاعات شخصی
- اطلاع در اواسط بهار ولی تاخیر تا زمان مذکور
- انجام ماه‌ها قبل از کشف آن

نامشخص بودن و عدم انتشار اطلاع از نحوهٔ حمله

- سود بردن از ایراد در اپاچی استرات Apache Struts
  - نرم‌افزار متن‌باز جهت ایجاد تعامل در تارمانه‌ها
  - اطلاع دادن بخش امنیت سیسکو به اکویفکس دو روز قبل از انجام نقض داده دربارهٔ ایراد مذکور
  - ادعا بر تولید ولی گزارش‌ها مبنی بر پیاده‌سازی ناکامل

مورد اکویفکس

اعتبار

- شریان اقتصادهای در حال‌توسعه و توسعه‌یافته
- استعفای مدیر عامل

بزرگتر از اکویفکس

- یاهو سه میلیارد
- ای‌بی ۱۴۵ میلیون
  - اما پیچیده‌ترین به دلیل نوع اطلاعات سرقتی
  - ۸۲ درصد تمامی افراد دارای اعتبار
- قبل از استعفا قول مبنی بر برگرداندن امنیت به اطلاعات
  - اما نیاز به صدور جدید کارت‌ها، تعویض شماره‌های ملی، گواهی‌نامه‌ها
  - امنیت بیشتر پد بزرگ در تناقض با کسب و کار

مورد ماریوت

بزرگترین شرکت هتل در جهان

۷۰۰۰ املاک و ۱ میلیون اتاق

پد بزرگ و دارای جزییات از نحوهٔ تحرک افراد

داده شخصی ۴۰۰ میلیون نفر

دزدی/کلاهبرداری کارت

- وقوع دزدی کارت نگران‌کننده‌ترین مورد در اینترنت
  - موجب عدم خرید اینترنتی
  - اما در عمل بی‌مبنا
    - ۰,۹ درصد وبی
    - ۰,۸ درصد تراکنش موبایلی
- سعی بر مبارزهٔ فیاوران با پدیده مذکور
  - روش خودکار تشخیص کلاهبرداری
  - مطالعهٔ انسانیِ سفارشات
  - رد کردن درخواست‌های مظنون
  - نیاز به سطوح بیشتر امنیت مانند نشانی ایمیل و موارد مشابه

دزدی/کلاهبرداری کارت

- تصویب قوانین مصوب و مقصر دزدی
  - کمتر از مقداری، مسئول خود شخص
  - از مقداری بیشتر، مسئول نهاد اعتباری
  - در عوض بانک‌ها گرفتن عوارض بیشتر
  - تجار با گرانتر فروختن محصولات
- تغییر تکنولوژی از مغناطیسی به چیپ‌های کامپیوتری جهت مشکل‌تر شدن نقض داده

دزدی/کلاهبرداری کارت

- دلیل اصلی هک‌کردن و تاراج سرورهای شرکت
  - دستیابی به اطلاعات ذخیره شده میلیون‌ها کارت
  - البرت گونزالز ۱۳۸۹
    - سازمان‌دهی بزرگترین دزدی تعداد کارت اعتباری در امریکا
    - همراه چند همکار روسی
    - ورود به سیستم رایانه مرکزی بارنز و نوبل، بی‌جی و چند شرکت دیگر
    - دزدیدن ۱۶۰میلیون کارت اعتباری
    - موجب ضرر ۲۰۰ میلیون دلاری
    - محکوم به ۲۰ سال زندان

دزدی/کلاهبرداری کارت

- سفارشات بین‌المللی دارای خطر بالاتر کلاهبرداری
- مشکل اصلی امنیت
  - پیچیدگی تعیین هویت کاربر
  - عدم وجود فناوری با درجهٔ مطلق جهت تعیین هویت شخص
  - تا یافتن چنین فناوری فروش اینترنتی متضررتر از فروش سنتی
    - امضای الکترویکی
    - اجازه چند عاملی
    - تشخیص اثر انگشت
    - امکان هک شدن پد اثر انگشت

سرقت/کلاهبرداری هویت

- سرقت هویت Identity Fraud
  - دسترسی و استفاده غیرمجاز به اطلاعات شخصی غیرْ جهت سود مالی غیرقانونی
    - شماره امنیت
    - گواهینامه
    - شماره کارت
    - کاربری و گذرواژه
  - وام! خرید، دریافت خدمات دیگر
  - تمامی روش‌های اشاره شده خاصه نقض داده
  - در سال ۲۰۱۶ حدود پانزده میلیون امریکایی تجربهٔ سرقت هویت
    - ضرر ناشی حدود ۱۶ میلیارد دلار

تارمانه‌های جعل، سدمه، اسپم

- جعل Spoofing
  - تلاش برای مخفی‌سازی هویت واقعی با استفاده از ایمیل غیر یا نشانی آی‌پی دیگر
  - تغییر بسته‌های تی‌سی‌پی‌آی‌پی
  - مسیریاب‌ها مجهز به موانعی برای این گونه موارد
  - مرتبط با سدمه pharming
    - تغییر مسیر خودکار پیوند وبی به نشانی دیگر، به مذاق هک‌کننده
      - مستقیما خطری ندارند ولی تهدیدی برای یکپارچگی مانه
      - انحراف به جایی جعلی منجر به جمع‌آوری اطلاعات و دزدی فیاوری
      - یا در صورت قصد برهم‌زدن تغییر سفارش‌ها
      - عدم رضایت مشتری یا عدم موجودی
    - تهدید اعتبار
      - چی راست است و چه دروغ

تارمانه‌های جعل، سدمه، اسپم

- تارمانه‌های اسپم (هرز) و آت و آشغال spam(junk) websites
  - پیشنهاد مجموعه‌ای از تبلیغات برای دیگر مانه‌ها
  - احتمال داشتن کد مخرب
    - امریکا آب و هوا
    - ایران آهنگ

- هرزنامه‌ها
  - ایمیل‌های ناخواسته
  - هزینه بر زیرساخت
  - امکان ارسال از سرور ایمیل یا شبات‌ها و سیستم‌های مسخر کاربران
  - معمولا تبلیغات
  - پیوست‌های بدافزار
    - هدایت به مانه‌های جعلی

حمله‌های نشسته در میان و شنود (بویشگری)

- شنود(بوینده) sniffing
  - برنامهٔ استراق سمع
  - امکان یافتن مشکلات شبکه
  - استفاده قانونی موجب تشخیص گلوگاه‌ها
  - امکان استفاده جهت جرائم و اطلاعات تملیکی
  - بسیار ضررآفرین و سخت جهت تشخیص
- ۱۳۹۲ محکومیت پنج هک‌گر در پی سرقت اطلاعات فروشگاه‌های زنجیره‌ای خرده‌فروشی ۷-یازده و شرکتی فرانسوی

حمله‌های نشسته در میان و شنود

- فال‌گوشی! ایمیل email wiretap
  - نوعی از خطر شنود
  - نگهداری و ضبط اطلاعات ایمیل‌ها در سطح سرور ایمیلی
  - امکان نصب روی کامپیوتر و سرور
  - کارمندان یا دستگاه‌های دولتی
  - قانون پاترویت امریکا
  - اجازه به پلیس فدرال
- حملهٔ نشسته در میان man-in-the-middle (MitM) attack
  - نوعی استراق سمع اما فعالتر!
  - تبدیل از انفعالی به فعال
  - مهاجم در میان راه است و ارتباطات بین دو بخش را تغییر می‌دهد
    - در حالی که دو بخش خیال می‌کنند مستقیم با هم در ارتباطند
    - امکان تغییر محتوا
    - Ettercap

نرم‌افزارهای با ضعف طراحی

گاهی ضعف در سیستم عامل و گاهی در نرم‌افزارهای کاربردی مانند مرورگرها

عوامل شکاف‌های نرم‌افزاری و آسیب‌پذیری‌ها

- افزایش پیچیدگی و اندازهٔ برنامه نرم‌افزاری
- درخواست‌های تحویل زمان‌بر به بازارها

حملات تزریق سکیول

- بهره‌بردن از آسیب‌پذیری‌های ناشی از کاربردهای وبی با طراحی کد ضعیف
  - ضعف در تائیداعتبار درست یا فیلتر داده‌های ورودی کاربر در صفحه
  - موجب ورود کد برنامه مخرب به سیستم و شبکهٔ شرکت
  - استفادهٔ حمله‌کننده از این ضعف‌ها جهت ارسال پرسش سکیولی به پد
  - جهت دستیابی به آن، کارگذاشتن کد مخرب یا دسترسی به سیستم‌های دیگر در شبکه
  - کاربردهای وبی بزرگ دارای صدها محل ورودی داده کاربر
  - هرکدام عامل ایجاد فرصت حملهٔ تزریق سکیول
  - وجود ابزارهای بررسی کاربر وبی برای این نوع آسیب‌پذیری‌ها

نرم‌افزارهای با ضعف طراحی

- یافتن هزاران نقاط آسیب‌پذیر در مرورگرهای اینترنتی،رایانه‌ها، نرم‌افزار لینوکس،کاربردها و سیستم‌عامل همراه
- ۱۳۹۵
  - ده‌هزار گزارش نقطه آسیب‌پذیر
  - بیش از ۲۰ درصد اسیب‌پذیری وبی
    - اسکریپت‌نویسی بین مانه و خطرات سکیول
  - آسیب‌پذیری روز-صفر
    - قبلا گزارش نشده و فعلا نبود وصله
  - گزارش ۴۰۰۰ آسیب‌پذیری در سال مذکور
    - با تعداد کمتری حملهٔ مرتبط با آنها
- طراحی رایانه با درگاه‌های باز جهت ارسال و دریافت با رایانه‌های دیگر
  - معمولا درگاه‌های ۴۴۵ تی‌سی‌پی، ۸۰، ۴۴۳
- شرکت سوفوس
  - گزارش یافتن آسیب‌پذیری روز صفر در افیس مایکروسافت
    - پروتکل تبادل دادهٔ پویای مایکروسافت
    - استفاده برای اشتراک داده بین کاربردها
    - امکان استفاده برای تحویل تروای‌های دسترسی از راه دور

نرم‌افزارهای با ضعف طراحی

- ۱۳۹۳ ایراد در سیستم رمزگذاری اپن‌اس‌اس‌ال
  - مورداستفادهٔ میلیون‌ها تارمانه
  - باگ خونریزی قلبی
  - اجازه به رمزگشایی جلسه اس‌اس‌ال و یافتن نام کاربر، رمزها، اطلاعات دیگر
  - با استفاده از اپن‌س‌س‌ل
    - در همکاری با ضربه قلب برای تسهیل در تماس ماندن کاربر دور پس از اتصال به سرور وب
    - امکان درز یافتن بخشی از محتوای حافظهٔ سرور محتملا دارای رمز و کلید رمزگذاری
  - همچنین shellshock بر لینوکس و یونیکس و س‌ع مک
  - امکان استفاده از CGI جهت افزودن کد مخرب

مسائل امنیتی شبکه اجتماعی

شبکه‌های اجتماعی مکانی برای

- ویروس‌ها
- دزدی هویت
- بدافزارها
- طله‌گذاری
- اسپم

کلاهبرداری اشتراک

- اشتراک بی‌اطلاع و دستی ویدئوها و داستان‌ها و تصاویر دارای نشانی به مانه‌های مخرب

پیشنهادات جعلی، دگمه‌های پسند جعلی،کاربردهای جعلی

مسائل امنیتی شبکه اجتماعی

دارای نظارت و دقت کمتر

- موتورهای جستجو دارای فهرستی از نشانی‌های مخرب و بررسی آنها در مانه‌ها

باز

- هر کس دارای امکان ایجاد صفحهٔ شخصی حتی مجرمان

بیشترین حملات

- حملات مهندسی اجتماعی
- ترغیب بازدیدکننده به کلیک نشانی‌های به نظر علیه سلام

مسائل امنیتی بستر موبایلی

گوشی همراه منبع اطلاعات شخصی و مالی افراد

- استفاده جهت انجام تراکنش‌ها از خرید خرده تا بانک همراه

دارای خطرات مشابه ابزار اینترنتی

- امکان هک کردن بی‌سیم‌های عمومی
- یافتن خطا در پروتکل امنیت بی‌سیم WPA2
  - ایجاد امکان دزیدن رمزها و ایمیل و ترافیک شبکه‌های بی‌سیم
  - بیش از ۴۰ درصد اندرویدی‌ها

با این وصف

- اطلاع کم عموم مردم از خطرات دستگاه همراه

مسائل امنیتی بستر موبایلی

بدافزار تلفن سلولی همراه

- کاربردهای همراه مخرب
- کرم بلوتوث در سرع سیمبین
- عامل جستجوی بدون وقفه دیگر موبایل
  - خالی شدن سریع باتری
- آیفون
  - تاثیر بر قفل‌شکسته‌ها و تبدیل آن به ابزارهای‌شب‌بات
  - با استفاده از کرم iKee.B

مسائل امنیتی بستر موبایلی

۱۳۹۵

- یافتن هژده میلیون آلودگی بدافزاری همراه‌ها
- به سمت تحت تاثیر قرار دادن پرداخت همراه و کاربردهای بانک همراه
- گزارش سیمانتک بر یافتن بدافزاری اندرویدی
  - یافتن پیام‌های متنی با کدهای تایید بانکی و رد کردن آن‌ها به حمله‌کننده
  - بویش پیامک

- ایفن
  - سه خطر روز-صفر
- کاربردهای همراه استارباکس (کاربرد پرداخت با بیشترین امار پرداخت در امریکا)
  - ذخیرهٔ نام کاربری و گذرواژه و ایمیل در متن معمولی
  - امکان دسترسی هر کس به آن با وصل کردن گوشی به رایانه
  - اشتباه گرفتن تاکید بر راحتی و استفادهٔ آسان در طراحی کاربرد با مسائل امنیتی

مسائل امنیتی بستر موبایلی

طله صوتی vishing

- پیام‌های صوتی جهت کمک به کودکان قطحی‌زده هائیتی

طله متنی Smishing

هلیغات madware

گمان بر امن بودن گوشی هوشمند

دلخوشی به حفاظت گوگل یا اپل

اما امکان استفاده از گوشی هوشمند همچون هر ابزار اینترنتی دیگر

درخواست فایل بدون اطلاع کاربر

حذف فایل

انتقال فایل

نصب برنامه و اجرا در زمینه جهت پایش و جمع‌اوری اطلاعات کاربر

تبدیل به بات

کاربردها محتمل‌ترین مکان نقض امنیت

شبکه‌های ناامن

استفاده از ضعف‌های سیم‌کارت

مسائل امنیتی ابر

حرکت به خدمات ابری موجب خطرات امنیتی

حمله بندآوری توقف در دسترسی خدمات ابر

- ۱۳۹۵ داین dyn موجب بر هم خوردن خدمات ابری در امریکا
- بیشتر حملات حمله‌های کاربرد وب
- خطر بیشتر برای شرکت‌های با شبکهٔ هیبرید
- دراپباکس و امکان دسترسی به فایل‌ها در آن بدون اجازه
- انتشار عکس‌های خصوصی چهره‌ها
  - حمله‌های تک-پایین در راستای رمز و دسترسی
  - لاورنس و آی‌کلاود
- اتصال بیشتر دستگاه‌ها و کاربردها با خدمات ابری
  - استفاده از فضای ابری جهت اتصال به حساب‌های وصل شده
  - مثال هونان

عدم امتحان و بررسی زیرساخت

نداشتن رمزگذاری و رویه‌های قوی امنیتی در ابرها

مسائل امنیتی اینترنت اشیاء

محیطی پرچالش جهت حفاظت

۱۳۹۴

- جیپ چروکی
  - کنترل از دور و موجب از کار انداختن ترمز، خاموشی موتور، و فرمان چرخ
- فیات کرایسلر

وسایل پزشکی

داین

- پانصدهزار دستگاه اش

شب‌بات

مسائل امنیتی اینترنت اشیاء

محیطی پرچالش جهت حفاظت

حجم عظیم نشانی‌های متصل به هم

دستگاه‌های تقریبا مشابه با عمر طولانی خدمت‌رسانی

بدون ویژگی‌های بروزکردن

دید کم نسبت به نحوهٔ کار و داده و امنیت

CHALLENGE	POSSIBLE IMPLICATIONS
Many IoT devices, such as sensors, are intended to be deployed on a much greater scale than traditional Internet-connected devices, creating a vast quantity of interconnected links that can be exploited.	Existing tools, methods, and strategies need to be developed to deal with this unprecedented scale.
Many instances of IoT consist of collections of identical devices that all have the same characteristics.	Magnifies the potential impact of a security vulnerability.
Many IoT devices are anticipated to have a much longer service life than typical equipment.	Devices may "outlive" the manufacturer, leaving them without long-term support that creates persistent vulnerabilities.
Many IoT devices are intentionally designed without the ability to be upgraded, or the upgrade process is difficult.	Raises the possibility that vulnerable devices cannot or will not be fixed, leaving them perpetually vulnerable.
Many IoT devices do not provide the user with visibility into the workings of the device or the data being produced, nor alert the user when a security problem arises.	Users may believe an IoT device is functioning as intended when, in fact, it may be performing in a malicious manner.
Some IoT devices, such as sensors, are unobtrusively embedded in the environment such that a user may not even be aware of the device.	Security breach might persist for a long time before being noticed.

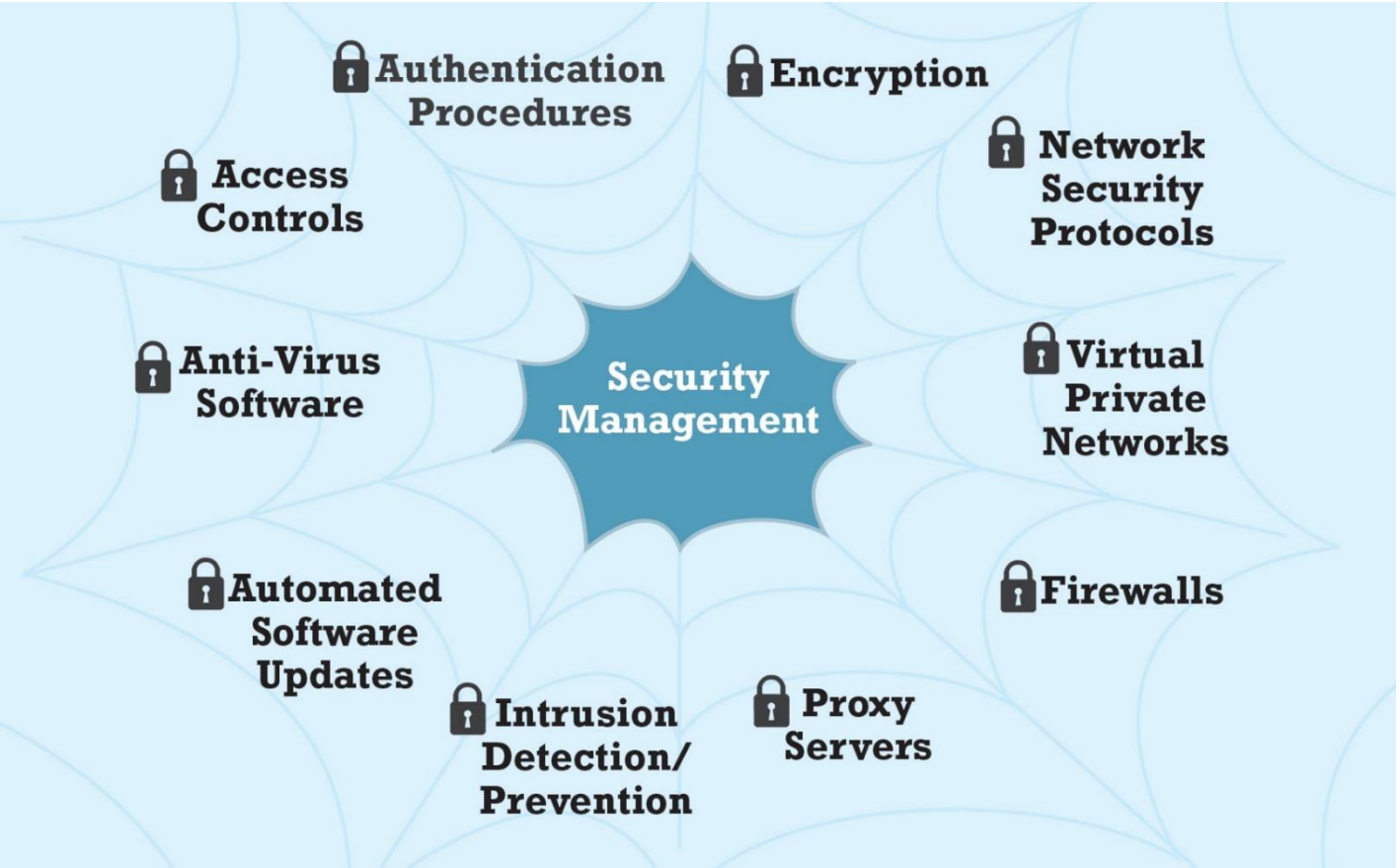
راه‌حل؟

فناوارنه

سیاست‌گذاری

راه‌حل‌های فناوری

استفاده از مجموعه ابزارهایی که حمله یا تخریب خارجی به مانه را مشکل می‌کند



راه‌حل‌های فناوری

حفاظت از ارتباطات اینترنتی

- محتمل‌ترین محل تهدید اینترنتی
- متفاوت از شبکهٔ خصوصی
- مهم‌ترین راه- رمزگذاری

امن‌سازی کانال‌های ارتباطی

شبکه‌های محافظ

- دیوارآتش
- سرور پراکسی

حفاظت از سرورها و مشتری‌ها

- امنیت سیستم عامل
- نرم‌افزار ضدویروس

منابع

[لاودن]

[استالینگز]