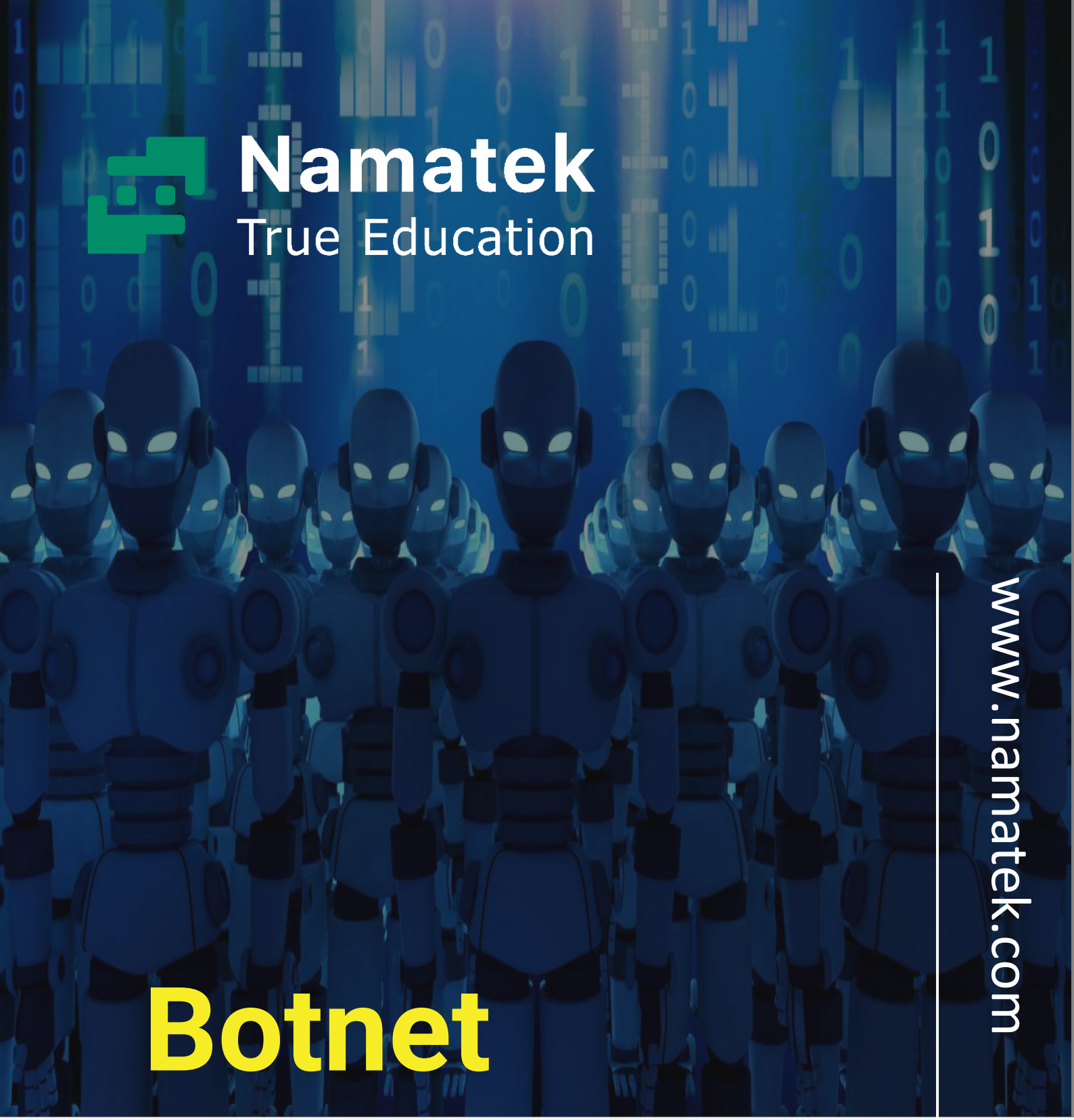


Namatek
True Education

Botnet

www.namatek.com

بات نت چیست؟

فهرست مطالب

آیا تاکنون نام بات نت را شنیده اید، اما نمی دانید در اصل کار بات نت چیست؟ بات نت ها شبکه ای از رایانه ها هستند که می توانند کار های مخرب و حملات اینترنتی انجام دهند. در این مقاله شما را با Botnet ها آشنا خواهیم کرد و به بررسی مشخصات و عملکردشان خواهیم پرداخت. برای کسب اطلاعات در مورد این سیستم تا انتهای مقاله با ما همراه باشید.

#۱ بات نت چیست؟ (Botnet)

Botnet برگرفته از Robot Network و به معنای شبکه ای از رایانه های آلوده به بدافزار است. هر ربات در بات نت تحت کنترل یک طرف حمله کننده معروف به bot-herder است. طرف حمله کننده از یک نقطه مرکزی می تواند به هر رایانه در بات نت خود دستور دهد تا دستورالعمل هایی را به صورت هماهنگ و همزمان انجام دهند.

مقیاس یک botnet مهاجم را قادر می سازد اقدامات بزرگی را انجام دهد که قبلا توسط بدافزار غیر ممکن بود (در بسیاری از موارد، بات نت ها از میلیون ها ربات تشکیل شده اند). بات نت ها می توانند از راه دور تحت کنترل یک مهاجم باقی بمانند. از این طریق ماشین های آلوده می توانند به روز رسانی های مورد نظر مهاجم را دریافت کرده و رفتار خود را در حین فعالیت تغییر دهند. در نتیجه، کارایی آن ها برای مهاجم یا bot-herder بیشتر می شود.

#۲ اقدامات رایج بات نت

اقدامات رایج بات نت ها عبارت است از:

۱. ایمیل اسپم (Email Spam): اگر چه امروزه ایمیل به عنوان روش قدیمی برای حمله شناخته می شود؛ اما به این دلیل که بات نت های اسپمینگ وسعت گرفته اند، همچنان مورد استفاده قرار می گیرند. آن ها برای ارسال پیام های اسپم که اغلب شامل بدافزار هستند از تعداد زیادی ربات استفاده می کنند. به عنوان مثال بات نت Cutwail می تواند حداکثر ۷٤ میلیارد پیام در روز ارسال کند.

۲. حملات دیداس (DDoS Attack): روش این نوع از حمله بات نت چیست؟ در این حمله مهاجمان از بات نت برای از کار انداختن شبکه یا سرور مورد نظر استفاده می کنند.
۳. تخلف مالی (Financial Breach): این نوع شامل بات نت هایی است که مخصوص سرقت مستقیم وجوه شرکت ها و اطلاعات کارت اعتباری طراحی شده است. بات نت های مالی، مانند بات نت ZeuS، مسئول حملاتی هستند که میلیون ها دلار به طور مستقیم از چندین شرکت در مدت زمان بسیار کوتاه دزدیده اند.
٤. نفوذهای هدفمند (Targeted Intrusions): بات نت های با وسعت کوچکتر طراحی شده اند تا برای به خطر انداختن سیستم های خاص با ارزش بالا در سازمان ها مورد استفاده قرار بگیرند. در این روش مهاجمان می توانند از حفره های امنیتی اقدام به نفوذ در شبکه کنند.

این نفوذها برای سازمان ها بسیار خطرناک است؛ زیرا مهاجمان به با ارزش ترین دارایی های آن ها دسترسی خواهند داشت؛ از جمله:

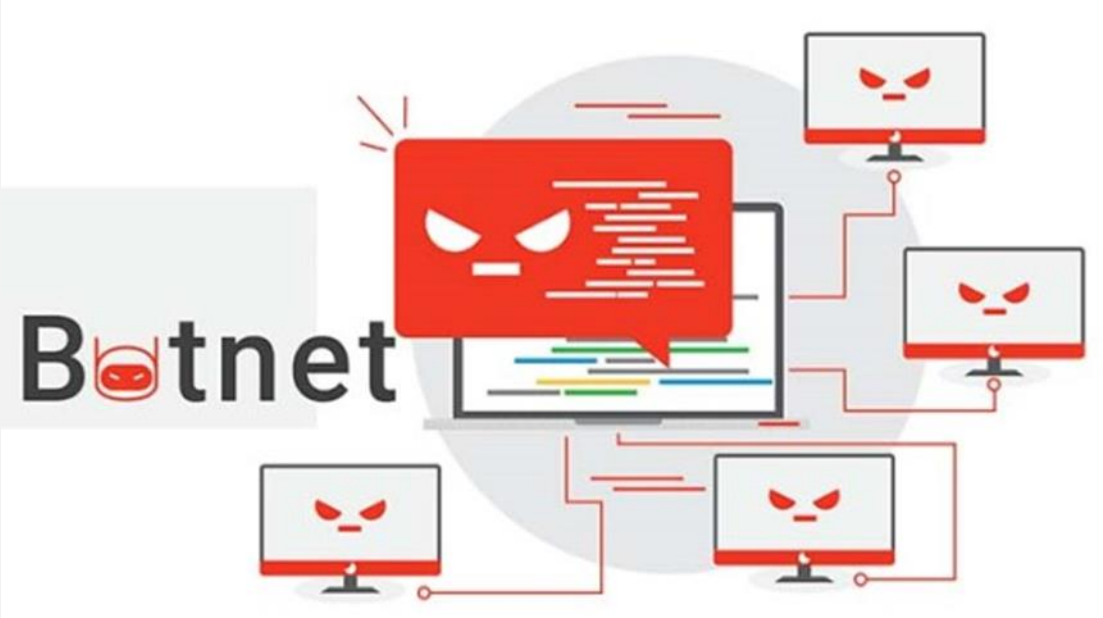
- داده های مالی
- تحقیق و توسعه
- مالکیت معنوی و اطلاعات مشتری

#۳ بات نت چگونه عمل می کند؟

دارندگان بات نت می توانند همزمان به چندین هزار رایانه دسترسی داشته و برای انجام فعالیت های مخرب به آن ها دستور دهند. مجرمان سایبری در ابتدا با استفاده از ویروس های ویژه Trojan و حمله به سیستم های امنیتی رایانه ها، به آن ها دسترسی پیدا کنند. اما وظیفه ربات در بات نت چیست؟

هر دستگاه یا رایانه هک شده به عنوان یک ربات عضوی از یک گروه بات نت شده و آن ها را قادر به انجام فعالیت های مخرب در مقیاس بزرگ می کند. این فعالیت ها می توانند به صورت خودکار نیز انجام شوند.

در حملات سایبری یک نفر یا حتی یک تیم کوچک از هکرها می تواند اقدامات زیادی را از طریق دستگاه های محلی خود انجام دهد؛ اما با کمترین هزینه و اندکی وقت صرف شده، آن ها می توانند هزاران ماشین اضافی را برای کارایی بیشتر به دست آورند. پس از ساخت شبکه ای از ربات ها (بات نت) مهاجم یا bot-herder با دستورات از راه دور و برنامه نویسی آن ها را هدایت می کند. بسیاری از مهاجمان صاحب بات نت، آن ها را به قیمت های قابل توجهی در بازار سیاه اجاره می دهند.



#۴ مراحل ساخت botnet

مراحل اساسی ساخت botnet را می توان در چند مرحله ساده بیان کرد:

۱. آماده سازی (Prep and Expose): این مرحله با پیدا شدن آسیب پذیری توسط هکرها در یک وب سایت، برنامه یا رفتار انسانی آغاز

می شود. در واقع هکر از یک حفره امنیتی یا آسیب پذیری در سیستم رایانه ای برای قرار دادن بدافزار (malware) در آن ها استفاده می کند.

۲. آلوده کردن (Infect): در این مرحله سیستم رایانه ای با انجام روش های مختلفی که دستگاه وی را به خطر بیندازد، به بدافزار botnet آلوده می شود. بسیاری از این روش ها متقاعد کردن کاربران از طریق مهندسی اجتماعی برای بارگیری ویروس Trojan است. همچنین ممکن است با مراجعه به سایت ناامن و بارگیری فایل آلوده شوند. در نهایت دستگاه ها به بدافزاری آلوده شده اند که مهاجمان به راحتی می توانند آن ها را کنترل کنند.

۳. فعال سازی (Activate): در این مرحله رایانه ها به صورت کامل در اختیار مهاجمان قرار می گیرند. به طور معمول مجرمان اینترنتی به دنبال آلوده و کنترل کردن هزاران، ده ها هزار، یا حتی میلیون ها کامپیوتر هستند. در نهایت دستگاه های آلوده برای انجام حملات در یک گروه بزرگ که با نام بات نت شناخته می شود، بسیج می شوند.

پس از آلوده شدن، یک کامپیوتر آلوده (ربات) اجازه دسترسی به فعالیت در سطح مدیر سیستم را به مهاجم می دهد؛ اما هدف از این کار در یک بات نت چیست؟

- خواندن و نوشتن داده در سیستم
- جمع آوری اطلاعات شخصی کاربر
- ارسال پرونده ها و سایر داده ها

- نظارت بر فعالیت های کاربر
- جستجو برای یافتن آسیب پذیری در دستگاه های دیگر
- نصب و اجرای هرگونه برنامه کاربردی

#۵ چند ربات در Botnet وجود دارد؟

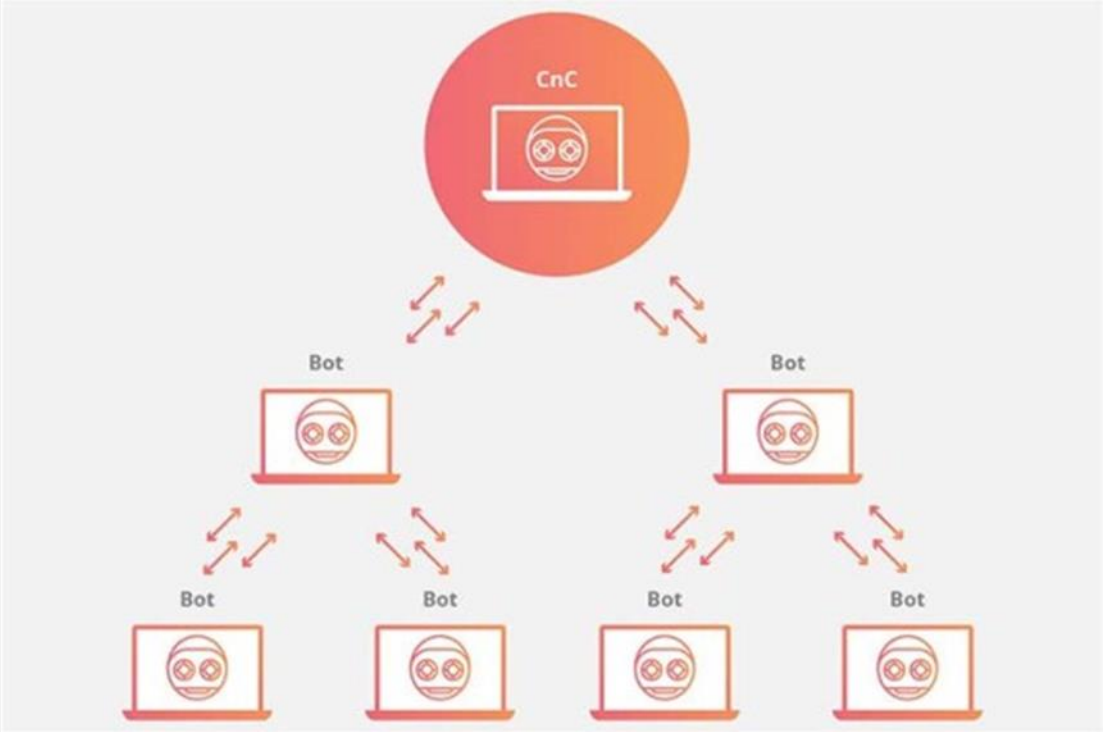
تعداد ربات ها در هر botnet متفاوت است و به توانایی مهاجم در آلوده کردن دستگاه های محافظت نشده بستگی دارد. ممکن است در حمله DDoS از یک بات نت با بیش از ۷۵۰۰۰ ربات استفاده شود که هر کدام از آن ها می توانند صدها درخواست در ثانیه به سرور ارسال کنند.

بر این اساس اثرات حمله بات نت چیست؟

اثرات حمله botnet می تواند بسیار ویرانگر باشد. از عملکرد کند دستگاه تا قبض های گسترده اینترنت و سرقت داده های مهم و شخصی. علاوه بر این پیامدهای قانونی را نیز باید در نظر گرفت. به عنوان مثال، اگر از رایانه شما به عنوان بخشی از حمله botnet استفاده شود، ممکن است از نظر قانونی مسئول عواقب هرگونه فعالیت مخربی باشید که از دستگاه شما نشات گرفته است.

#۶ روش کنترل بات نت چیست؟

شاید برایتان جالب باشد که روش هکرها برای مدیریت بات نت چیست! صدور دستورات بخش مهمی از کنترل بات نت است؛ اما ناشناس بودن برای مهاجم نیز به همان اندازه مهم است. به همین دلیل، بات نت ها از طریق برنامه نویسی از راه دور کار می کنند.



هر botnet را می توان توسط دستورات به طور مستقیم یا غیر مستقیم در مدل های زیر قرار داد:

- مدل های کلاینت/سرور متمرکز شده (Centralized client-server:)

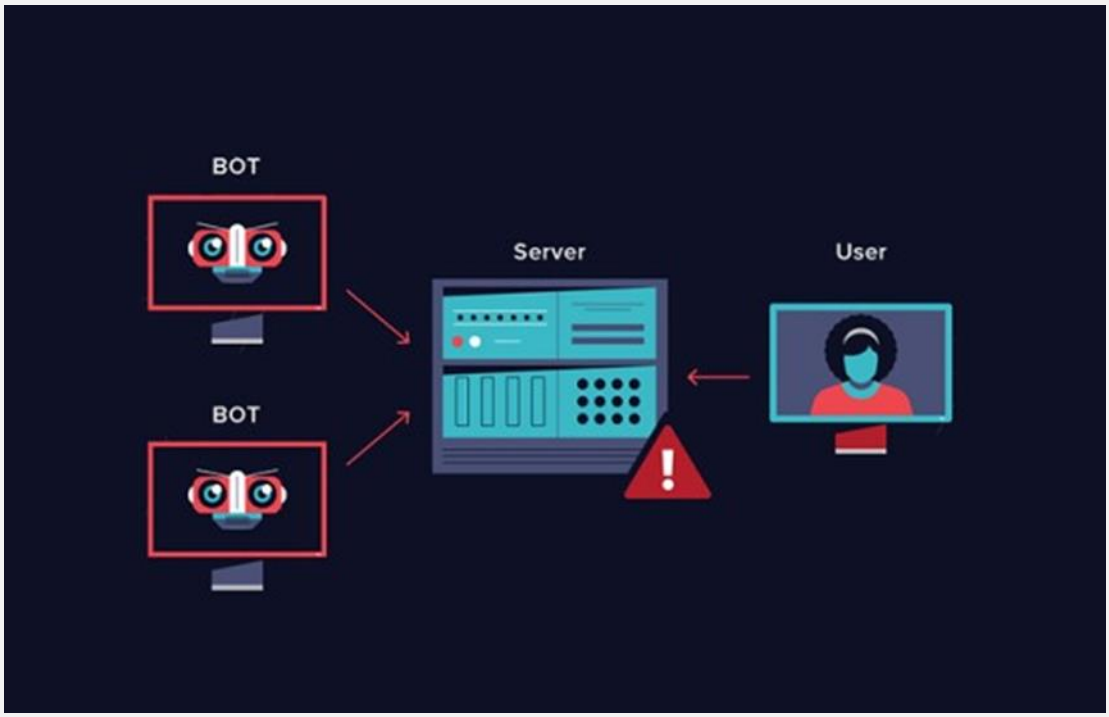
مدل های متمرکز توسط یک سرور ربات اداره می شوند. در این مدل ممکن است سرورهای دیگری را به عنوان sub-herders یا پروکسی در بات نت قرار دهند. این زیرمجموعه بخشی از وظایف سرور اصلی را انجام می دهد و بر اساس سلسله مراتب، همه دستورات را از سرور اصلی به سمت ربات ها ارسال می کند.

- مدل های غیر متمرکز نظیر به نظیر (P2P یا Decentralized peer-to-peer:)

مهاجمان در مدل های غیرمتمرکز، مسئولیت ها و دستورالعمل ها را در همه رایانه های آلوده شده تعبیه می کنند. در این مدل تا زمانی که یک ربات بتواند با هر یک از رایانه های آلوده دیگر تماس بگیرد، می تواند دستورات را به او و سایرین منتقل کند.

ساختار نظیر به نظیر بیشتر هویت مهاجم اصلی را پنهان می کند. به همین دلیل امروزه رواج بیشتری دارد.

#۷ هدف مهاجمان از ایجاد بات نت چیست؟



- سرقت مالی: با اخاذی یا سرقت مستقیم پول
- سرقت اطلاعات: برای دسترسی به حساب های حساس یا محرمانه

- خرابکاری در سرویس دهی: با آفلاین کردن سرورهای سرویس دهنده و یا وب سایت ها
- استخراج ارز رمزنگاری شده: با استفاده از قدرت پردازش سیستم کاربران مختلف برای استخراج ارز رمزنگاری شده
- فروش دسترسی به مجرمان دیگر: اجاره بات نت به مجرمان دیگر

بیشتر انگیزه های ساخت بات نت شبیه سایر جرایم اینترنتی است. در بسیاری از موارد، این مهاجمان یا می خواهند چیز ارزشمندی را بدزدند یا برای دیگران دردسر ایجاد کنند.