سیستم های اطلاعات مدیریت پیشرفته

(روش شناسی ایجاد سیستم)

3961220161746

کاوه فرجی گوگردچی(220196542)

بدافزارهای کامپیوتری:

ویروس ها، کرم ها و اسب های تروجان

ویروس ها(Computer virus)

ویروس، یک نوع از بدافزار است که در اغلب مواقع بدون اطلاع کاربر اجرا شده و تلاش می کند خودش را در یک کد اجرایی دیگر کپی کند. وقتی موفق به انجام این کار شد، کد جدید، آلوده نامیده می‌شود. کد آلوده وقتی اجرا شود، به نوبه خود کد دیگری را می‌تواند آلوده کند. این عمل تولید مثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است. معمولاً کاربران رایانه به ویژه آنهایی که اطلاعات تخصصی کمتری درباره کامپیوتر دارند، ویروس‌ها را برنامه‌هایی هوشمند و خطرناک می‌دانند که خود به خود اجرا و تکثیر شده و اثرات تخریبی زیادی دارند که باعث از د ست رفتن اطلاعات و گاه خراب شدن کامپیوتر می گردند در حالیکه طبق آمار تنها پنج درصد ویروس‌ها دارای اثرات تخریبی بوده و بقیه صرفاً تکثیر می‌شوند؛ بنابراین یک ویروس رایانه‌ای را می‌توان برنامه‌ای تعریف نمود که می‌تواند خودش را با استفاده از یک میزبان تکثیر نماید. بنابر این تعریف اگر برنامه‌ای وجود دا شته با شد که دارای اثرات تخریبی با شد ولی امکان تکثیر ندا شته با شد، نمی‌توان آنرا ویروس نامید.

ویروس(Blueborne)

در 13 سپتامبر 2017 سایت dailymail.co.uk از انتقال ویروسی با عنوان blueborne خبر داد. بر اساس اطلاعات این سایت بلوبورن ویرو سی ا ست که از طریق بلوتوث د ستگاه های کامپوتری گسترش پیدا می کند و به همین دلیل می تواند میلیون ها سیستم را به خود آلوده کند. در این سایت آمده است که میلیاردها دستگاه برای حمله از BlueBorne آسیب پذیر هستند. بلو بورن یک ویروس جدید مخرب است که با استفاده از بلوتوث غیر قابل کشف می شود.

کارشناسان امنیتی سایبری می گویند ویروس از ضعف در نرم افزار بلوتوث بهره می برد و می تواند بین دستگاه ها و در سرا سر جهان پخش شود. بر خلاف بسیاری از کد های مخرب، که نیاز به اتصال به اینترنت دارند یا نیاز به یک لینک برای کلیک بر روی آن است ، BlueBorne هوابرد است و نیازی به مجوز ندارد.

تی میلر، مدیر عامل سازمان تهدید اطلاعات ، می گوید که شیوع ویروس BlueBorne به شدت خطرناک است. وی گفته: برآورد شده است که تا بیش از 8 میلیارد دستگاه در سراسر جهان تأثیر بگذارد و این به این دلیل است که توانایی آلوده کردن سیستم های ویندوز، لینوکس، اندروید و iOS تا قبل از iOS 10 را دارد.

این باعث تهدید بیشتری نسبت به نرم افزار WannaCry ransomware است که در ماه مه 2017 کامپیوترهای سراسر جهان را گروگان گرفت. BlueBorne شبیه یک ویروس یا بیماری مسری انسانی از جمله ابولا است و مانند بیماری های عفونی می تواند از طریق انتقال هوایی از کشوری به کشور دیگر انتقال یابد. BlueBorne می تواند هر دستگاه مجهز به بلوتوث، از جمله تلفن های هوشمند، لپ تاپ ها، رایانه های شخصی، پرینتر، تلویزیون های هوشمند، ساعت و تجهیزات پزشکی را آلوده کند.

آزمایشگاه های ارتش ها خطر ویروس جدید را از ماه آوریل هشدار داده اند و اکنون ویدیوهایی برای افزایش آگاهی منتشر شده است. هر چند که شرکت های فن آوری از خطرات احتمالی آگاه هستند اما ویورس blueborne در نوع خود باید سخت تر در نظر گرفته شود. همچنین افرادی که دارای دستگاه یا رایانه ای هستند که به روز نشده اند، می توانند به ویروس آلوده شوند، زیرا کاربران اغلب هشدارها را نادیده می گیرند و یا فراموش کرده اند که پچ ها را نصب کنند.

ویروس(WannaCry)

بعلت آلودگی تعداد بسیار زیادی از کامپیوترهای دنیا در عرض زمانی کوتاهی توسط ویروس باجگیر « واناکرای WannaCry » ، آنرا تنها بعد از یک روز پس از انتشار بعنوان بی رحمانه‌ترین ویروس باجگیر تاریخ دنیا می‌شناسند. هدف ویروس باجگیر « واناکرای WannaCry » دقیقاً مشابه ویروس های باجگیر قبلی، رمزنگاری کردن اطلاعات و درخواست باج است. در حال حاضر مبلغ باج حدود یک میلیون و دویست هزار تومان می‌باشد که در صورت عدم پرداخت تا سه روز به دو برابر افزایش پیدا می کند. تفاوت اصلی آن با دیگر ویروسهای باجگیر در نحوه نفوذ آن به کامپیوتر قربانی می‌باشد. ویروسهای باجگیر قبلی برای وارد شدن به کامپیوتر قربانی بیشتر از طریق ایمیل اقدام می کردند و کاربر با اشتباه خود باعث ورود آنها می‌شد اما در مورد این ویروس جدید یعنی « واناکرای WannaCry » نحوه نفوذ از طریق ضعف امنیتی سیستم عامل ویندوز چه در نسخه سروری و چه در نسخه کلاینتی بصورت اتوماتیک و بدون دخالت کاربر صورت می گیرد.

ویروس باجگیر « واناکرای WannaCry » با استفاده از ضعف امنیتی MS17-010 سیستم عامل های ویندوز به کامپیوتر قربانی نفوذ می کند. این ایراد امنیتی که به نام EternalBlue شناخته می شود در تمامی نسخه‌های ویندوز چه از نوع سرور و چه از نوع کلاینت وجود دارد. برنامه نویسان این ویروس باجگیر با دسترسی به اطلاعات محرمانه آژانس امنیت ملی آمریکا این ضعف امنیتی را پیدا و با استفاده از آن ویروس خود را برنامه نویسی کرده‌اند. همانطور

که گفته شد « واناکرای WannaCry » به صورت یک « کرم worm » عمل می کند و بصورت اتوماتیک و بدون دخالت کاربر از طریق ضعف امنیتی سیستم عامل ویندوز به کامپیوتر قربانی نفوذ می کند.

این ویروس ها با استفاده از رمزنگاری تمام فایلهای کامپیوتر قربانی را رمز و غیرقابل استفاده می کند. اطلاعات رمز شده فقط با داشتن کلید انحصاری قابل بازگشت می باشند. در اصل دو کلید وجود دارد یک کلید عمومی و یک کلید اختصاصی که این کلید اختصاصی در سرور سازنده ذخیره می گردد و بعد از پرداخت باج به همراه یک برنامه به قربانی داده می‌شود. به نام هر فایل پسوند WCRY را اضافه می کند.

متن رسمی باجگیری بصورت زیر می باشد که البته یک فایل متنی به نام !Please Read Me!.txt را هم در بیشتر فولدرها می‌سازد:

کرم های کامپیوتری(Worm)

کرم کامپیوتری درست مثل پسر عموی بدذاتش، ویروس، یک نوع بدافزار است. تفاوت کرم با ویروس در این است که کرم‌ها معمولاً خود به خود فایل‌ها را آلوده نکرده و یا تغییر نمی‌دهند. در عوض، به سرعت بارها و بارها خود را کپی کرده و در سراسر شبکه پخش می‌شوند. (مثلاً در اینترنت، شبکه‌های محلی یا شبکه‌ی داخلی شرکت‌ها)

به این صورت، کپی‌ها دوباره تولید و پخش شده، و در یک زمان بسیار کوتاه، خیلی زود می‌توانند تعداد زیادی کامپیوتر را آلوده کنند. برای نمونه، بر اساس تخمین‌ها کرم مشهور ILOVEYOU در عرض فقط ۱۰ روز توانست حدود ۱۰ درصد از کامپیوترهای متصل به اینترنت در جهان را آلوده نماید.

کرم‌های کامپیوتری سنتی ساخته می‌شدند تا پخش شوند. آن‌ها با سرعت بسیار زیاد گسترش می‌یافتند و در پهنای‌باند شبکه اختلال ایجاد می‌کردند، اما عملکرد سیستم‌ها را تغییر نمی‌دادند. این رویه در سال ۲۰۰۴ با ظهور Witty تغییر کرد .Witty کرمی بود که به فایروال و محصولات امنیتی کامپیوترهای یک شرکت خاص حمله می‌کرد و گفته می‌شد اولین کرمی است که Payload (قطعه کدی برای ایجاد آسیب‌های واقعی و ملموس) دارد. از آن زمان، کرم‌های حامل Payload در کل جهان پخش شدند و کارهای مختلفی انجام دادند. مثلاً Nyxem قادر به حذف فایل های مایکروسافت آفیس بود، و Daprosy می‌توانست از قابلیت های کی‌لاگینگ (Keylogging) استفاده کند.

یکی از رایج‌ترین روش‌های پخش شدن کرم‌ها از طریق اسپم‌های ایمیلی است. در قدیم، کرم‌ها می‌توانستند درون متن ایمیل مخفی شوند، اما با آمدن کلاینت‌های جدید ایمیل و مسدود شدن امکان درج داده‌های توکاری شده در سال ۲۰۱۰، احتمال آسیب دیدن به این روش خیلی کم شده است. همه‌ی سیستم عامل‌ها آسیب‌پذیری‌های خودشان را دارند حتی سیستم عامل macOS. برخی از کرم‌ها طوری طراحی شده‌اند تا از این نقاط ضعف استفاده کنند. معروف‌ترین مثال در این مورد احتمالاً Conficker است، کرمی که اولین بار در حالی در سال ۲۰۰۸ شناسایی شد که به آسیب‌پذیری موجود در یکی از سرویس‌های شبکه‌ی ویندوز که در نسخه‌های مختلف آن حمله کرده بود. کرم‌ها، نرم‌افزاری خرابکارند که وقتی PC تان آلوده شد در پی آنند تا هر چه سریع‌تر تکثیر پیدا کنند. برخلاف ویروس‌ها آنها به برنامه‌ی میزبان نیاز ندارند بلکه از طریق ابزارهای ذخیره سازی همچون USB و رسانه‌های ارتباطی همچون ایمیل یا آسیب‌پذیری‌هایتان، خودشان را در سیستم عامل شما پخش می‌کنند. تکثیرشان باعث افت عملکرد PCها و شبکه‌ها می‌شود. همچنین ممکن است به طور مستقیم رفتاری خرابکارانه اجرا کنند.

کرم(Psyb0t or Network Bluepill)

Psyb0t یا Network Bluepill یک کرم رایانه ای است که در ژانویه 2009 کشف شده است. این تصور می شود که این کرم منحصر به فرد است چون می تواند آنتن های فرستنده و مودم های با سرعت بالا را آلوده کند. Psyb0t اولین بار در ژانویه 2009 توسط Terry Baume محقق امنیت استرالیا در ای دی اس ال ها و مودم های Netcomm NB5 ADSL شناسایی شد. سپس، در اوایل ماه مارس، یک حمله DDoS به DroneBL (یک سرویس لیست سیاه IP) اجرا شد. از این حمله، DroneBL تخمین زده است که حدود 100000 دستگاه را آلوده کرده است. این حمله در اوایل ماه مارس توجه خاصی به این امر به همراه داشت که احتمالا اپراتور آن را تعطیل کرد. همچنین DroneBL با موفقیت تلاش کرد تا فرمان و کنترل و سرورهای DNS خود را پایین بیاورد.

دو نسخه شناخته شده وجود دارد. اولین نسخه L2.5 روی روتر / مودم ADSL Netcomm NB5 تاثیر گذاشت. جدیدتر نسخه L2.9 در حال حاضر بیش از 50 مدل توسط Linksys، Netgear و دیگر فروشندگان، از جمله کسانی که در حال اجرا DD-WRT یا سیستم عامل OpenWrt اجرا می شود.

Psyb0t با 6000 نام کاربری مشترک و 13،000 کلمه عبور مجهز شده است که در ترکیب های مختلف برای دسترسی به شبکه خانگی خود تلاش می کند. بیشتر روترهای(Router) خانه ای به شما توانایی نامحدودی برای بدست آوردن نام کاربری و گذرواژه صحیح می دهند و این دستگاه ها یک هدف ایده آل برای آلوده شدن هستند.

همچنین، بر خلاف کامپیوتر شما، روتر و مودم شما 24 ساعت شبانه روز کار می کنند، این بدین معنا است که psyb0t دارای زمان نسبتا نامحدودی جهت دسترسی است. در حالی که تهدید psyb0t ممکن است بالا نباشد، اقدامات احتیاطی علیه این نوع حمله بسیار مهم است. بهترین راه برای محافظت در برابر این کرم این است که مطمئن شوید که از گذرواژه و نام کاربری پیشفرض که با تجهیزاتتان مرتبط است استفاده نمی کنید.

برای دریافت راهنمایی در مورد چگونگی تغییر نام کاربری و رمز عبور خود، از دستورالعمل دستگاه یا وب سایت تولید کننده خود مطلع شوید. اگر نگران هستید که آلوده شده اید، یک بازگردانی به حالت تولید کارخانه می تواند دستگاه شما را از آلودگی این کرم پاک گرداند

کرم (Koobface)

Koobface یک کرم شبکه ای است که به مایکروسافت ویندوز، مک OS X و سیستم عامل لینوکس حمله میکند. این کرم در ابتدا کاربران وب سایت هایی مانند فیس بوک، اسکایپ، یاهو مسنجر و وب سایت های ایمیل مانند Gmail، Yahoo Mail و AOL Mail را هدف قرار داد. این ویروس همچنین شبکه های دیگر مانند Myspace، Twitter را هدف قرار می دهد و می تواند دستگاه های دیگر را در یک شبکه محلی آلوده کند.

Koobface نهایتاً تلاش می کند تا اطلاعات ورود برای سایتهای FTP، فیس بوک، اسکایپ و دیگر سیستم عامل های اجتماعی و همچنین اطلاعات مالی حساس را جمع آوری کند. سپس با استفاده از رایانه های همتراز برای ساخت یک بوت نت استفاده می کند. یک کامپیوتر همتراز به دیگر کامپیوتر ها برای دریافت فرامین به صورت ذنجیره وار متصل می شود.

Koobface اصولا با ارسال پیام های فیس بوک به افرادی که "دوستان" یک کاربر فیس بوک هستند و رایانه آن ها آلوده شده است، منتشر می شود. پس از دریافت، پیام گیرندگان را به یک وب سایت شخص ثالث (یا دیگر رایانه آلوده Koobface) هدایت می کند، جایی که از آنها خواسته می شود که آنچه را که باعث به روز رسانی Adobe Flash player می شود دانلود کنید. اگر آنها فایل را دانلود و اجرا کنند، Koobface می تواند سیستم خود را آلوده کند. پس از آن می تواند موتور جستجوی کامپیوتر را در دست بگیرد و آن را به وب سایت های آلوده منتقل کند. همچنین می تواند تو سط لینک هایی که به سایت های ثالث متصل می شوند یا پیامی با مضمون LOL یا YOUTUBE را نشان دهد که اگر لینک باز شود، ویروس تروجان کامپیوتر را آلوده می کند و کامپیوتر تبدیل به یک کامپیوتر زامبی یا میزبان خواهد شد.

در میان اجزای دانلود شده توسط Koobface یک برنامه فیلتر DNS است که دسترسی به وب سایت های شناخته شده امنیتی و یک ابزار پروکسی را که مهاجمین را مجبور به سوء استفاده از کامپیوتر آلوده می کند، متوقف می کند. در یک زمان باند Koobface نیز از Limbo، یک برنامه سرقت رمز عبور استفاده کرد.

در ژانویه سال 2012، نیویورک تایمز اعلام کرد که فیس بوک قصد دارد اطلاعاتی در مورد باند کوبفیس را به اشتراک بگذارد و نام هایی را که به اعتقاد او مسئول است، معرفی کند. که نهایتا در 17 ژانویه این کار را انجام داد.

اسب های تروجان(Trojan horse)

اسب تروجان یا تروجان یک برنامه نفوذی است که از نوع بدافزار است که به سیستم عامل، دسترسی سطح بالا پیدا کرده است در حالیکه به نظر می‌آید یک کار مناسب را در حال انجام است. یک داده ناخواسته روی سیستم نصب می‌کند که اغلب دارای یک در پشتی برای دسترسی غیرمجاز به کامپیوتر مقصد است.[۱] این در پشتی‌ها گرایش به دیده نشدن توسط کاربران دارند اما ممکن است باعث کند شدن کامپیوتر شوند. تروجان‌ها تلاش برای تزریق به فایلها مانند ویروس‌های کامپیوتری را ندارند تروجانها ممکن است اطلاعات به سرقت ببرند یا به کامپیوتر میزبان صدمه بزنند.[۲] تروجانها ممکن است به وسیله دانلود نا خواسته یا نصب بازیهای آنلاین یا برنامه‌های تحت شبکه یا به کامپیوتر هدف دسترسی داشته باشند. این موضوع از داستان اسب تراجان گرفته شده است و نوعی از مهندسی اجتماعی است.

شرکت امنیتی پاندا در گزارش تازه خود که به بررسی وضع امنیت سایبر در سال ۲۰۱۱ اختصاص دارد، تصویر کاملی از تحولات مرتبط با امنیت در فضای مجازی ارایه کرده است. نکته مهمی که در این گزارش به چشم می‌خورد، افزایش دامنه فعالیت تروجان‌های مخرب است، به گونه‌ای که از میان انواع بدافزارها شامل ویروس، کرم، تروجان و... این تروجان‌های نفوذگر هستند که بخش عمده تهدیدات سایبری را به خود اختصاص داده‌اند.

تروجان ها از طرق مختلفی وارد سیستم ها می شوند که می توان از آن جمله به موارد زیر اشاره کرد:

- دانلود کردن نرم‌افزار: شما نرم‌افزاری را دانلود می‌کنید و تروجان در پس این نرم‌افزار پنهان شده و وارد سیستم شما می‌شود.
- سایت‌های مخرب: وقتی شما وارد سایتی می‌شوید سایت یک برنامه را روی سیستم شما اجرا می‌کند و تروجان را وارد سیستم شما می‌کند.
- ایمیل:احتمال دارد همراه با ایمیل فایلی باشد که اگر شما آن را باز کنید تروجان وارد سیستم شما می‌شود.
- استفاده از نقص نرم‌افزارها: تروجان از طریق نقص‌هایی که در نرم‌افزارهایی مثل مرورگر وجود دارد وارد سیستم شما می‌شود.
- از طریق دیسکت‌ها

تروجان(CryptoLocker)

حمله CryptLocker ransomware یک حمله سایبری با استفاده از CryptLocker ransomware است که از 5 سپتامبر 2013 تا اواخر ماه مه 2014 رخ داده است. این حمله به یک تروجان رایانه ای که مایکروسافت ویندوز را هدف قرار داده است نسبت داده شده است و اعتقاد بر این بود که برای اولین بار در 5 سپتامبر 2013 به اینترنت فرستاده شده.

این ویروس از طریق پیوست های ایمیل آلوده، و از طریق یک بوت نت Gameover ZeuS پخش شده است. هنگامی که فعالیت آغاز شد، بدافزار انواع خاصی از فایل های ذخیره شده در درایوهای محلی و مجهز به شبکه را با استفاده از رمزنگاری کلید عمومی RSA رمزگذاری می کند و با کلید خصوصی تنها در سرورهای کنترل بدافزار ذخیره می کند. پس از آن بدافزار پیامی را نشان می دهد که در صورت پرداخت با یک مهلت اعلام شده، رمزگشایی داده ها را ارائه می دهد و در صورتی که مهلت تمام شود، تهدید می شود که کلید خصوصی حذف شود. اگر مهلت مقرر تمام شود، بدافزار پیشنهاد می دهد که از طریق سرویس آنلاین ارائه شده توسط اپراتورهای مخرب، با قیمت بالاتری در واحد بیت کوین رمزگشایی را انجام خواهد داد. هیچ تضمینی وجود ندارد که پرداخت محتوی رمز شده را آزاد کند.

CryptoLocker معمولا به عنوان یک پیوست به یک ایمیل به ظاهر بی ضرر ایمیل فرستاده می شود، که به نظر می رسد توسط یک شرکت مشروع ارسال شده است. فایل زیپ موجود در ایمیل ارسال شده که شامل یک فایل پی دی اف است. به هنگامی که برای اولین بار اجرا می شود، payload خود را در پوشه پروفایل کاربر نصب می کند و یک کلید به رجیستری ایجاد می کند که باعث می شود تا هنگام اجرای آن اجرا شود.

پس از آن تلاش می کند با یکی از سرورهای فرماندهی و کنترل تعیین شده تماس بگیرد؛ یک بار متصل شده، سرور یک جفت کلید RSA 2048 بیتی تولید می کند و کلید عمومی را به کامپیوتر آلوده می فرستد. سرور ممکن است یک پروکسی محلی باشد و از طریق دیگران به کار رود، اغلب در کشورهای مختلف نقل مکان می شود تا ردیابی آنها را دشوارتر کند.

در دسامبر 2013، ZDNet یک آدرس چهار بیت کوین را که توسط کاربران CryptoLocker آلوده شده بود، ردیابی کرد و تلاش کرد تا هزینه های اپراتور را ارزیابی کند. این چهار آدرس نشان داد که BTC 41.928 بین 15 اکتبر و 18 دسامبر در حدود 27 میلیون دلار در آن زمان حرکت می کند.

تروجان(Regin)

Regin (همچنین به عنوان Prax یا QWERTY شناخته می شود) یک ابزار پیچیده نرم افزارهای مخرب و هکینگ است که توسط آژانس امنیت ملی ایالات متحده و همتای انگلیسی آن، ستاد ارتباطات دولتی (GCHQ) استفاده می شود. Regin یک بدافزار است که در نوامبر 2014 توسط شرکت سیمنتک کشف شده است. این حفره امنیتی احتمالاً توسط یک نهاد دولتی طراحی شده و برای شش سال اهدافی را در سراسر جهان هدف قرار داده است و پس از نفوذ به رایانه شخصی می‌تواند از صفحات عکس بگیرد، رمزهای عبور را بدزدد و فایل‌های حذف شده را پیدا کند. دافزار رجین اولین بار توسط کمپانی کاسپرسکی، سیمانتک و دی اینترسپت، در نوامبر 2014 منتشر شد. این بدافزار کامپیوترهایی با سیستم عامل مایکروسافت را مورد حمله قرار می‌دهد و با سازمان‌های آژانس جمع‌آوری اطلاعات ایالات متحده (NSA) و همتای آن بریتانیایی آن GCHQ مرتبط است.

کسپراسکای می گوید که برای اولین بار در بهار 2012 از بدافزار آگاه گردیده است، اما ظاهراً سرنخ‌هایی از اولین نمونه‌های این بدافزار در سال‌های 2003 در کامپیوترها وجود داشته است.از میان کامپیوترهای آلوده شده توسط Regin، 28 در صد سهم روسیه،24 در صد عربستان سعودی،9 در صد سهم هریک از کشورهای مکزیزک و ایرلند و 5 درصد برای هریک از کشورهای ایران، افغانستان، بلژیک، اتریش، پاکستان و هند می‌باشد.

کسپر اسکای قادر به مشخص کردن هدف حمله نیست. اما این بدافزار افراد مخصوص و شرکت‌های تجاری کوچک و مخابرات را مورد حمله قرار می‌دهد. این بدافزار با بدافزار استاکس نت مقایسه می‌شود از این نظر که توسط تیمی قدرتمند نوشته شده و احتمالاً توسط یک دولت غربی به عنوان یک ابزار جمع‌آوری اطلاعات توسعه داده شده است.

Regin به خوبی برای جاسوسی بر روی یک کامپیوتر مشخص طراحی شده است.داده‌های Regin در سیستم آلوده ذخیره نمی شود، بلکه به نظر می‌رسد رجین از ماشین رمزگذاری مجازی خود یک فایل به میزبان می‌فرستند که این فایل با یک عدد و نه یک نام شناخته می‌شود.ماشین رمزگذاری مجازی نوع دیگری از رمز نگاری است که به ندرت در رمزنگاری RC5 استفاده می‌شود.

ارتباطات رجین درون کوکی‌های HTTP جاسازی شده و از پروتکل‌های TCP و UDP به همراه دستورهای کنترل سرور که می‌تواند عملیات، آپلود و محموله‌های اضافی را کنترل کند بهره می‌برد.