صاحب‌امتیاز: دانشگاه آزاد اسلامی- مدیرمسئول: محمدامین ایمانجانی- سردبیر: مسعود فروغی
تلفن و فکس: ۶۲۹۹۹۴۹۵ (۰۲۱) کدپستی: ۱۱۳۵۶۳۳۸۱۶
چاپ: چاپخانه دانشگاه آزاد اسلامی
نشانی: خیابان حافظ، پایین‌تر از جمهوری، روبه‌روی ساختمان بورس، ساختمان فرهیختگان، طبقه سوم

ماجرای پرسروصدای هکرها چقدر جدی بود؟

آنانیموس آناناس هم نبود

فرهیختگان همزمان با آغاز ناآرامی‌های اخیر در کشـــور بود که ســـروکله گروه هکرهای آنانیموس پیدا شـــد؛ گروهی از هکرهای ناشـــناس که به شـــکل غیرمتمرکز از سراسر نقاط دنیا دســـت به حملات سایبری علیه دولت‌های مختلف می‌زنند. این گروه که به ادعای خود برای حمایت از زنان و معترضان ایرانی دست به انجام حملات سایبری مختلف علیه شبکه‌ها و زیرساخت‌های حاکمیتی ایران می‌زند در ابتدای ناآرامی‌ها دو پایگاه اینترنتی dolat.ir و iran.gov.ir را مورد حمله سایبری داد و از دسترس خارج کرد، با این حال سایت dolat.ir و درگاه ملی دولت هوشمندساعاتی بعد مجددا به حالت عادی بازگشتند. این گروه همچنین وعده داد که در گام‌های بعدی شمار بالایی از رسانه‌ها و سایت‌های مربوط به دولت را مورد حمله قرار می‌دهد و به همین مناسبت در روزهای اخیر به‌طور مداوم با اخبار حملات سایبری این گروه در حساب‌های توئیتری مرتبط با جامعه هکرهای آنانیموس مواجه هستیم. «فراموش نمی‌کنیم، نمی‌بخشیم، منتظرمان باشید!» عبارتی است که اعضای این گروه عموما در واکنش به اقدامات دولت‌ها می‌نویسند و تکرار می‌کنند اما با توجه به حجم و عمق تاریخچه حملات صورت گرفته از ناحیه اعضای این گروه، به نظر می‌رسد این تهدیدات در میدان عمل آنقدرها نیز جدی و موثر نیست. اکثر پایگاه‌هایی که توسط این گروه هک و از دسترس خارج شده‌اند، در مدت زمان کوتاهی دوباره فعالیت خود را از سر گرفته و به حالت اولیه بازگشته‌اند. به عبارتی حملات این گروه نه آنقدر که در رسانه‌ها و افکار عمومی تبلیغ می‌شود جدی است و نه اقدامات هکرهای آنانیموس در مختل کردن سایت‌ها و پایگاه‌ها و افشای داده‌های حساس منطبق با ادعاهایشـــان بوده و درخور توجهات رسانه‌ای است. با این وجود این روزها مضاف بر محدودیت‌هایی که بر اینترنت سراسر کشور حاکم است، پایگاه‌ها و سایت‌های خدمات عمومی هدف حملات سایبری هستند و به همین مناسبت در این گزارش ضمن معرفی گروه هکرهای آنانیموس و شرح مختصری از تاریخچه شکل‌گیری این گروه و سوابق، میزان جدیت خطر این حملات را مورد ارزیابی قرار داده و به جنبه‌های مختلف فعالیت‌های آنان می‌پردازیم.

حملات سایبری نه‌چندان خطرناک هکرهای آنانیموس به ایران

یکی از مهم‌ترین اهدافی که اهدافی که گروه آنانیموس مدعی حمله به آن بود، سایت بانک مرکزی ایران است که برای مدت کوتاهی از دسترس خارج شد، سخنگوی این بانک اما اندکی بعد اعلام کرد: «در این نوع حملات موسوم به DDos پهنای باند شبکه با ترافیک جعلی پر می‌شود تا کاربران واقعی از دسترسی محروم بمانند. با قطع دسترسی خارجی در شبکه زیرساخت، این اختلال برطرف شده و سایت بانک مرکزی بدون هرگونه مشکلی، اکنون در دسترس است. بنابراین هرگونه ادعا مبنی بر هک شدن سایت بانک مرکزی تکذیب می‌شود.» سایت بانک مرکزی آخرین هدف این گروه نبود، در روزهای گذشته وب‌سایت پزشکی قانونی ایران، پایگاه داده مجلس شورای اسلامی، دیوان محاسبات کشوری، سازمان اطلاعات ایران، وب‌سایت پلیس ایران، وب‌سایت بانک مرکزی ایران، وب‌سایت سخنگوی دولت، وب‌سایت صداوسیما، سایت فارس‌نیوز و برخی از مراکز دولتی و سایت‌های مختلف دیگر مورد حملات سایبری این گروه قرار گرفتند که گرچه برخی از این ادعاها از سوی مقامات رسمی تکذیب شدند اما به نظر می‌رسد بیشتر این حملات صرفا جنبه تبلیغاتی و عملیات روانی داشته و آن‌طور که این گروه ادعا می‌کرده جدی نبوده‌اند. همان‌طور که گفتیم اهداف این گروه شامل اطلاعات حساس و زیرساخت‌های مهم حاکمیت نمی‌شود و اکثرا درگاه‌ها و پایگاه‌های خدمات عمومی از سوی این هکرها مورد حمله قرار گرفته‌اند. همچنین گفتنی است تمامی سایت‌هایی که هدف حمله قرار گرفته بودند پس از مدت کوتاهی مجددا در دسترس کاربران قرار گرفتند و مشخص شد اطلاعاتی هم که از پایگاه‌های دولتی نظیر سازمان ثبت احوال و مجلس شورای اسلامی در حساب‌های توئیتر این گروه منتشر شده، قبلا در دسترس عموم قرار گرفته بوده و داده‌های حساسی به‌شمار نمی‌رفتند. خوراکیان، سخنگوی مرکز ملی فضای مجازی در همین خصوص و درمورد حملات سایبری روزهای اخیر گفته است: «با توجه به اینکه در شرایط کنونی بسیاری از خدمات عمومی در فضای مجازی به مردم ارائه می‌شود، دشمنان از هر فرصتی سوءاستفاده می‌کنند تا با ایجاد اختلال در این سرویس‌ها و خدمات از طریق حملات سایبری زندگی روزمره مردم را دچار اشکال کنند. با تدابیری که اندیشیده شده و با هماهنگی و همکاری بسیار خوب و تلاش بی‌وقفه‌ای که بین دستگاه‌های مربوطه وجود دارد، اکثر قریب به اتفاق این حملات به‌سرعت رصد شده و خنثی می‌شود. مواردی که بعضا برای مدت کوتاهی موثر واقع می‌شود در کوتاه‌ترین زمان ممکن برطرف شده است، لذا در حال حاضر تقریبا همه مواردی که دچار اختلال شده بود مشغول ارائه خدمات هستند. همچنین با پیش‌بینی‌ها و تلاش‌هایی که انجام شده و تداوم نیز دارد جای هیچ‌گونه نگرانی در این رابطه برای مردم عزیز نیست.»

چهره پنهان آنارشیسم پشت نقاب‌های آنانیموس

آنانیموس یک گروه غیرمتمرکز از هکرهای بین‌المللی است که عمدتا به دلیل حملات سایبری مختلف خود علیه چندین دولت، نهادهای و سازمان‌های دولتی، شرکت‌ها و زیرساخت‌های مختلف آنها شناخته شده‌اند. این گروه در سال ۲۰۰۳ و در سایت chan4 ایجاد شد اعضای ناشناس این گروه (معروف به آنون‌ها) گاهی اوقات با پوشیدن ماسک‌های معروف گای فاکس که آنها را در فیلم «وی مثل وندتا» دیده‌ایم از عموم مردم متمایز می‌شوند. برخی از انون‌ها نیز صدای خود را از طریق تغییردهنده‌های صدا یا برنامه‌های تبدیل متن به گفتار پنهان می‌کنند. از زمان اکران فیلم «وی مثل وندتا»، در سال ۲۰۰۵، استفاده از ماسک‌های گای فاکس در سطح بین‌المللی و در میان گروه‌های معترض علیه سیاستمداران، بانک‌ها و موسسات مالی رواج یافته است. به اعتقاد این گروه این نقاب‌ها هم هویت را پنهان می‌کنند هم تعهد آنها را به یک هدف مشترک نشان می‌دهند، آنارشیسم علیه دولت‌ها! این گروه در شکل اولیه خود به‌عنوان یک جامعه آنلاین غیرمتمرکز شکل گرفت که به‌طور ناشناس و به شیوه‌ای هماهنگ عمل می‌کرد، معمولا علیه یک هدف کاملا مورد توافق اعضای خود اقدام می‌کرد و عمدتا بر مسائل و موضوعات مرتبط با سرگرمی متمرکز بود. تا اینکه در سال ۲۰۰۸ و در مجرای اعتراضات مردم و گروه‌های مختلف به کلیسای ساینتولوژی در آمریکا، گروه آنانیموس برای اولین بار خود را در قالب کنونی‌اش نشان داد. ماجرایی که نام این گروه را بر زبان بسیاری از رسانه‌های دنیا انداخت و جایی که برای اولین بار و همزمان با اعتراضات گروه هکتیویسم آنانیموس علیه کلیسای ساینتولوژی، اعضای این گروه از این ماسک استفاده کردند، کلیسای ساینتولوژی سازمانی است که با هدف ترویج عقاید کلیسای بین‌الملل ساینتولوژی، مدیریت این کلیساها را برعهده دارد. در آن سال این کلیسا پلتفرم یوتیوب را مجبور کرد تا ویدئویی از تام کروز، بازیگر هالیوودی که درمورد سازمان ساینتولوژی بحث می‌کرد و برای استفاده داخلی در کلیسا ساخته شده بود را حذف کند. به دنبال این اقدام بسیاری از کاربران به کلیسای ساینتولوژی اعتراض کردند. آنانیموس نیز یکی از گروه‌هایی بود که با ورود به این دعوا به روش‌های مختلف اعتراضات خود را به اقدام کلیسای ساینتولوژی نشان داد و معترضان را تشویق کرد که چهره‌های خود را زیر این نقاب‌ها پنهان کنند. با ادامه یافتن این اعتراضات، معترضان بیشتری شروع به استفاده از ماسک گای فاکس کردند، اقدامی که درنهایت جنبه‌ای نمادین به خود گرفت و شهرت این گروه با این ماسک‌ها پیوند خورد.

جامعه هکرهای پنهان در دنیا به دنبال چیست؟

نزدیک به دو دهه است که آنانیموس به‌عنوان یکی از بدنام‌ترین گروه‌های هکری جهان در سراسر نقاط دنیا مشغول فعالیت است، گروه آنانیموس، حملات سایبری هماهنگ‌شده‌ای را علیه دولت‌های مختلف جهان، شرکت‌ها یا سایر گروه‌ها به کار می‌گیرد که اغلب به دلایل اجتماعی یا سیاسی است. افرادی که ادعا می‌کنند با این گروه در ارتباط هستند، ادعا می‌کنند اهداف این گروه هکتیویسم ناشناس شامل سازمان‌های دولتی آمریکا، رژیم صهیونیستی، تونس، اوگاندا و همچنین دولت‌های اسلامی است. همچنین سایت‌های پورنوگرافی کودکان، آژانس‌های حمایت از کپی‌رایت و شرکت‌هایی مانند پی‌پال، مسترکارت، ویزا و سونی شماری از اهدافی بودند که مورد حملات این گروه قرار گرفته‌اند. حملات سایبری این گروه طی سال‌های اخیر علیه سازمان‌های دولتی، رسانه‌ها، شـــرکت‌ها، پیمانکاران و پرسنل نظامی و افسران پلیس آمریکا منجر به افزایش توجهات رســـانه‌ای به فعالیت‌های این گروه شد. پس از حمله روسیه به اوکراین در اواخر سال قبل، یک حساب توئیتر با ۷,۹ میلیون دنبال‌کننده به نام «آنانیموس» علیه روسیه و رئیس جمهور آن، ولادیمیر پوتین، «جنگ ســـایبری» اعلام کرد. از آن زمان، این گروه مســـئولیت حملات ســـایبری مختلفی را که باعث از کار انداختن وب‌ســـایت‌ها و افشـــای داده‌های آژانس‌های دولتی روسیه، و همچنین خبرگزاری‌ها و شرکت‌های دولتی شده، برعهده گرفته است. در توئیتی حساب کاربری آنانیمـــوس که به گفته خـــود: «نمی‌تواند ادعا کند که از طرف کل گروه صحبت می‌کند» از هکرها در سراسر جهان، از جمله در روسیه، خواست تا به سخنان ولادیمیر پوتین و جنگ در اوکراین نه بگویند. به‌طور کلی، گروه آنانیموس به ادعای خود مخالف دولت‌ها و شرکت‌هایی است که به نظر آنها در سانسور یا ترویج نابرابری شرکت می‌کنند. از آنجایی که این گروه غیرمتمرکز است، هیچ ساختار یا سلسله‌مراتب واقعی و مشخصی ندارد، بنابراین اینکه ایده و هدف واقعی این گروه چیست هنوز به‌طور جدی محل بحث است. توئیتی در سال ۲۰۱۹ از یک حساب مرتبط با گروه آنانیمـــوس ادعا کرد که این گروه متعلق به «مردم طبقه کارگر که به دنبال آینده‌ای بهتر برای بشـــریت هستند» است. به ادعای همین منبع اصول این گروه از قرار ذیل اســـت: «آزادی اطلاعات، آزادی بیان، پاسخگویی برای شرکت‌ها و دولت‌ها، حریم خصوصی و ناشناس ماندن برای شهروندان» همه اینها در حالی است که اقدامات آنانیموس از جمله هک کردن ســـایت‌های دولتی و خصوصی، ایجاد اخلال در پایگاه‌های اینترنتی و دزدیدن داده‌های حساس در تمامی نظام‌های حقوقی موجود در کشورهای دنیا جرم بوده و رسانه‌های سرتاسر دنیا علی‌رغم پرداختن به مقاصد و اهداف این گروه آنان را مجرم می‌دانند.

مبارزان سایبری آنانیموس رابین هود هستند یا تروریست؟

حامیان شـــان این گروه را «مبـــارزان آزادی» و رابین هودهای دیجیتال نامیده‌اند، درحالی که منتقدان از آنها به‌عنوان «تروریست‌های سایبری» یاد کرده‌اند. در سال ۲۰۱۲ مجله تایم، گروه آنانیموس را یکی از «۱۰۰ شـــخص تاثیرگذار» در جهان نامید. شهرتی که تا سال ۲۰۱۸ به شکل قابل توجهی کاهش یافت اما بعدتر و با مجموعه‌ای از جریانات در سال ۲۰۲۰ از جملـــه اعتراضات به قتل جورج فلوید در آمریکا، نام هکرهای آنانیموس دوباره بر ســـر زبان‌ها افتاد. جرمیا فاولر، یکی از بنیانگذاران شرکت امنیت سایبری Security Discovery، در اظهارنظری به شبکه CNBC گفته اســـت: «حامیان آنانیموس احتمالا این گروه را تا حدودی یک «رابین هود ســـایبری» می‌دانند که دولت‌ها و شرکت‌های قدرتمند را به نام اهداف عمومی مورد حمله قرار می‌دهد. شما می‌خواهید اقدام کنید، عدالت می‌خواهید و من فکر می‌کنم گروه‌هایی مانند آنانیموس و هکتیویست‌ها این رضایت فوری را به مردم می‌دهند.» یک وب‌سایت مرتبط با این گروه حتی آنانیموس را به‌عنوان «یک گردهمایی اینترنتی» باساختار فرماندهی بسیار شل و سست و غیرمتمرکز توصیف کرده‌است که بیشتر فعالیت‌هایشان ضدیت و اعتراض به سانسور و اعمال نظارت و کنترل دولت‌ها بر اینترنت است. اما بسیاری بر این باورند که تاکتیک‌های در ظاهر هوشـــیارانه این گروه افراطی و بالقوه خطرناک است. در سال ۲۰۱۲ آژانـــس امنیت ملی، گروه آنانیمـــوس را را تهدیدی برای امنیت ملی دانست. همچنین پارمی اولسون، روزنامه‌نگاری که در سال ۲۰۱۲ کتابی ۴۱۵ صفحه‌ای در مورد این گروه نوشت، در آن زمان اظهار داشت که حتی حامیان این گروه نیز باید میراث آن را مجموعه‌ای از اقدامات مفید و همچنین مضر و آسیب‌رسان بدانند. وی در این باره گفته است: «آیا این گروه در راســـتای منافع مردم جهان خوب عمل کرده است؟ در برخـــی موارد، بله. اما من آزار و اذیت بی‌مورد مردم را به‌عنوان یک چیز بد طبقه‌بندی می‌کنم. هک کردن وب‌ســـایت ســـیا، سرقت اطلاعات مشـــتریان و ارسال آنها به‌صورت آنلاین صرفا برای خندیدن و خندیدن چیز خوبی نیست.»

طریقه برخورد دولت‌های مختلف با هکرهای آنانیموس

از سال ۲۰۰۹ ده‌ها نفر به دلیل دست داشتن در حملات سایبری گروه آنانیموس، در کشورهایی ازجمله آمریکا، بریتانیا، استرالیا، هلند، اسپانیا و ترکیه دستگیر شده‌اند. اعضای این گروه اما عموما به این پیگردها اعتراض می‌کنند و این افراد را شهدای جنبش می‌خوانند. اولین فردی که به دلیل شرکت در یک حمله DDoS این گروه به زندان فرستاده شد، دیمیتری گوزنر ۱۹ ساله از آمریکا بود. او در نوامبر سال ۲۰۰۹ به جرم ایجاد اختلال غیرمجاز در یک کامپیوتر محافظت‌شده اعتراف کرد و به ۳۶۶ روز حبس در زندان فدرال آمریکا محکوم شد. در ۱۳ ژوئن ۲۰۱۱ نیز مقامات ترکیه ۳۲ نفر را دستگیر کردند که گفته می‌شود در حملات DDoS به وب‌سایت‌های دولتی ترکیه دست داشته‌اند. این افراد در شهرهای مختلف ترکیه ازجمله استانبول و آنکارا دستگیر شدند. به گفته مجله پی سی، این افراد پس از حمله به مجموعه‌ای از وب‌سایت‌ها در پاسخ به درخواست دولت ترکیه که از ارائه‌دهنده‌های خدمات اینترنتی خواسته بود برای پیاده‌سازی فیلترینگ در اینترنت این کشور اقدام کنند، دستگیر شدند. همچنین کریس دویون با نام مستعار فرمانده X، یکی از رهبران ناشناس این گروه، در سپتامبر ۲۰۱۱ به دلیل انجام یک حمله سایبری به وب‌سایت سانتا کروز، در کالیفرنیا دستگیر شد. او در فوریه ۲۰۱۲ به قید وثیقه از حبس بیرون آمد و از مرزهای زمینی به کانادا گریخت. در سپتامبر ۲۰۱۲ نیز روزنامه‌نگاری به نام بارت براون که به دلیل صحبت با رسانه‌ها مورد حمله قرار گرفته‌اند. همچنین گفتنی است تمامی سایت‌هایی که هدف حمله قرار گرفته بودند پس از مدت کوتاهی مجددا در دسترس کاربران قرار گرفتند و مشخص شد اطلاعاتی هم که از پایگاه‌های دولتی نظیر سازمان ثبت احوال و مجلس شورای اسلامی در حساب‌های توئیتر این گروه منتشر شده، قبلا در دسترس عموم قرار گرفته بوده و داده‌های حساسی به‌شمار نمی‌رفتند. خوراکیان، سخنگوی مرکز ملی فضای مجازی در همین خصوص و درمورد حملات سایبری روزهای اخیر گفته است: «با توجه به اینکه در شرایط کنونی بسیاری از خدمات عمومی در فضای مجازی به مردم ارائه می‌شود، دشمنان از هر فرصتی سوءاستفاده می‌کنند تا با ایجاد اختلال در این سرویس‌ها و خدمات از طریق حملات سایبری زندگی روزمره مردم را دچار اشکال کنند. با تدابیری که اندیشیده شده و با هماهنگی و همکاری بسیار خوب و تلاش بی‌وقفه‌ای که بین دستگاه‌های مربوطه وجود دارد، اکثر قریب به اتفاق این حملات به‌سرعت رصد شده و خنثی می‌شود. مواردی که بعضا برای مدت کوتاهی موثر واقع می‌شود در کوتاه‌ترین زمان ممکن برطرف شده است، لذا در حال حاضر تقریبا همه مواردی که دچار اختلال شده بود مشغول ارائه خدمات هستند. همچنین با پیش‌بینی‌ها و تلاش‌هایی که انجام شده و تداوم نیز دارد جای هیچ‌گونه نگرانی در این رابطه برای مردم عزیز نیست.»

بزرگنمایی حملات سایبری گروه آنانیموس در رسانه‌ها و افکار عمومی

در توضیح اینکه چرا حملات هکرهای آنانیموس آنقدر که در رسانه‌ها بزرگنمایی شده جدی نیستند، محمود ورداسبی، کارشناس حوزه امنیت سایبری اخیرا در اظهارنظری پیرامون حملات سایبری گروه آنانیموس به پایگاه‌های اینترنتی ایران گفته است: «همان‌گونه که مرکز ملی فضای مجازی اعلام کرده است ما آسیب زیرساختی ندیده‌ایم. اصطلاحا به این حملاتی که در حال انجام است ddos می‌گویند. این حملات صرفا درخواست‌های بسیار زیادی به سمت سرورها و سایت‌های دولتی می‌فرستند و سایت‌های دولتی چون توان پاسخگویی به این حجم از درخواست را ندارند، از دسترس خارج می‌شوند. این گروه که در این مدت این اقدامات را انجام می‌دهد، درواقع هک واقعی انجام نداده است و صرفا یک عملیات رسانه‌ای و روانی برای مردم انجام می‌دهند. چنین مساله‌ای سبب می‌شود که گمان شود اطلاعات از دسترس خارج یا منتشر شده اما هنوز این اتفاق رخ نداده و عملا با این کار زندگی روزمره مردم را به هم ریخته‌اند زیرا به سایت‌هایی که حمله می‌شود، سرویس‌دهی به مردم را مختل می‌کنند یا در چند روز اخیر سایت‌هایی را که به مردم خدمات ارائه می‌دهند و از دسترس خارج کرده‌اند، در حال آسیب دیدن هستند، نه زیرساخت‌ها و سازمان‌های دولتی.» این کارشناس امنیت سایبری همچنین معتقد است اقدامات هکرهای آنانیموس جنبه روانی دارد، ویس در این باره گفته است: «به‌طور کلی هیچ دسترسی‌ای به اطلاعاتی رخ نداده است و به دو سه مورد مانند اطلاعات قدیمی یکی از دانشگاه‌های کشور و نیز یکی از رسانه‌های کشور که نرم‌افزار کوچکی بوده دسترسی پیدا کرده‌اند و کلا ماجرا بعد روانی و رسانه‌ای این مساله است که تاکنون متاسفانه به این مساله پرداخته نشده تا از جو روانی آن کاسته شود. هنوز سایتی دچار اختلال کلی نشده است، یعنی اگر سایتی هک شده و اطلاعات آن درز پیدا کرده، باید منتشر شود؛ هک کردن به‌صورت کلی یا برای باج‌گیری است که اطلاعات منتشر نمی‌شود یا برای درخواست‌هایی است که خودشان مطرح می‌کنند که بلافاصله منتشر می‌شود. اما طی ۱۰ روز گذشته که ما درگیر زیرساخت هستیم، اطلاعاتی مبنی بر اینکه سایتی هک شده منتشر نشده است. حتی سایت‌هایی که گفته شده توسط گروه هکری آنانیموس هک شده‌اند، بعد از یک الی دو دقیقه دوباره در دسترس قرار می‌گیرند، پس عملا هکی انجام نشده است. به‌صورت دقیق‌تر حمله‌ای که از دستگاه‌های آلوده صورت می‌گیرد، می‌تواند اپلیکیشن‌های بازی که توسط میلیون‌ها کاربر نصب شده، باشد و فرضا هکر به آنها دستوری ارسال می‌کند که به طور مثال سایتی را باز کنند و قطعا سرویس‌ها و زیرساخت سایت مورد نظر که روزانه و طبق پیش‌بینی باید به صدهزار کاربر پاسخ دهند، به‌صورت ناگهانی با ۵۰ میلیون درخواست مواجه می‌شوند و درنتیجه سرورها و سرویس‌هایش قدرت پاسخگویی به این حجم از درخواست را ندارند و عملا از دسترس خارج می‌شوند.»