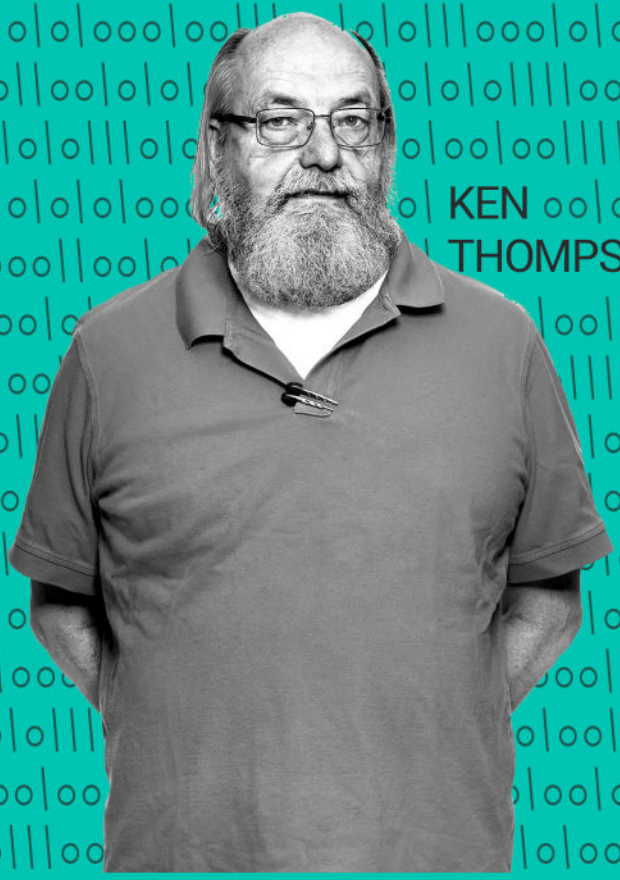
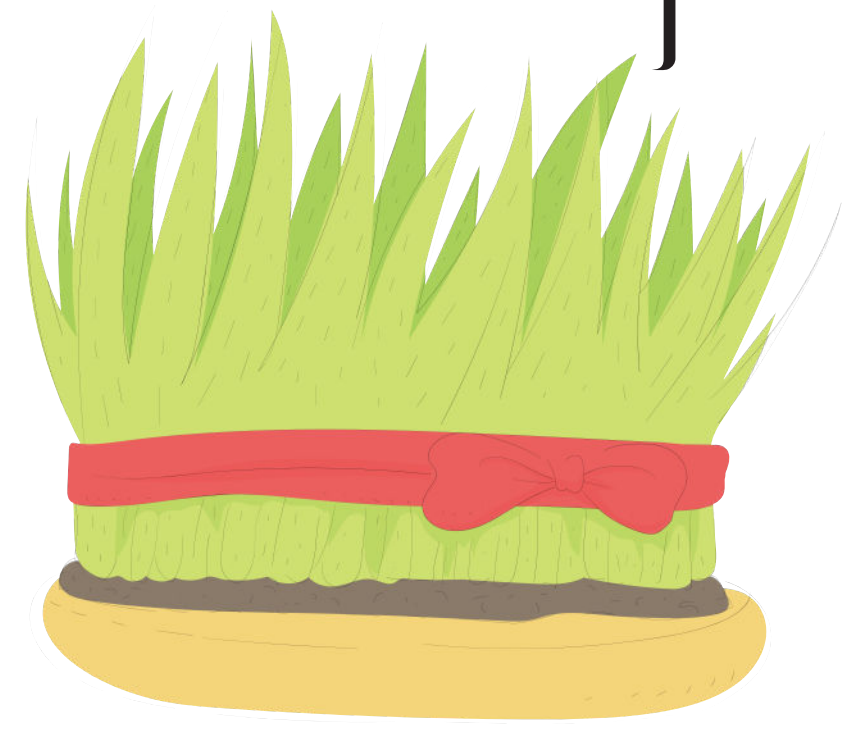
ماتریس

۳

صاحب امتیاز : انجمن علمی مهندسی کامپیوتر
دانشگاه شاهد | اسفند ماه ۱۴۰۳



در این شماره میخوانیم :



بسم الله الرحمن الرحیم

شناسنامه

نشریه ماتریس

صاحب امتیاز: انجمن علمی مهندسی کامپیوتر دانشگاه شاهد

مدیر مسئول: علی بقائی راوری

سر دبیر: فربد فیضی

تیم تحریریه این شماره: محدثه جوان | ساراکاظم زاده عطار | امیرحسین ملکی | محمد مهدی بابابیک | سارا امیرحسینی | فربد فیضی

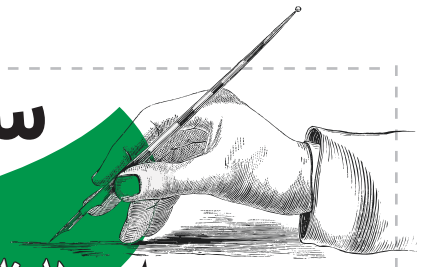
طراح جلد: محمدرضا ناحی داریانی

طراح مجله: علی بقائی راوری

شبکه‌های اجتماعی: @MatrisMagazine

شماره سوم | اسفند ماه ۱۴۰۳

فهرست



سخن مدیر مسئول

به نام به‌روزرسانی کننده ی فصل‌ها و افکار

در آستانه نوروز، فصل نو شدن و شکوفایی، افتخار داریم که شماره‌ای دیگر از ماتریس را پیشکش شما کنیم. آنچه این مسیر را برای ما لذت‌بخش‌تر کرده، نه‌تنها انتشار هر شماره، بلکه بازخوردهای شگفت‌انگیز شما بوده است. از تحسین‌های صمیمانه دانشجویان گرفته تا حمایت و تشویق اساتید، هر پیام و هر بازخورد به ما ثابت کرد که ماتریس نه‌تنها یک مجله، بلکه یک جریان علمی و فرهنگی است که جای خود را در بین شما باز کرده است.

با چنین انگیزه‌ای، تلاش کرده‌ایم این شماره را پربارتر از قبل ارائه دهیم؛ بهاری در دنیای دانش، هم‌زمان با بهاری در طبیعت. این فصل، فرصتی است برای نوزایی ایده ها، خلاقیت و آغازهای تازه و ماتریس نیز با همین نگاه پیش می‌رود.

از همراهی شما سپاسگزاریم و همچنان مشتاق دیدن استعدادها و ایده‌های جدید در ماتریس هستیم. سالی پر از موفقیت و دستاوردهای علمی برایتان آرزومندیم.

علی بقائی راوری

مدیر مسئول

عیدانه ۱۴۰۴

محدثه جوان
سارا کاظم زاده عطار

باز دوباره دم عید شده و جمله ی "پس کی سرت رو از توی اون گوشی/ لپتاپ/ کامپیوتر در میاری؟" از زبون خانواده ها نمیفته.

قضیه از این قراره که خانواده معتقد هستن لحظه ی تحویل سال باید دور سفره ی هفت سین بشینیم، و هر چقدر براشون توضیح میدم که من همین الان هم کنار سفره هفت سین نشستم، قانع نمیشن.

اصلا به همین بهونه هم که شده، بیاید هفت سین یه کامپیوتری اصیل رو براتون توضیح بدم.

در حالت عادی، سین اول سمنو ولی ما به جاش یه هارد SSD NVMe با سرعت بالا میذاریم، چون دیگه کسی حوصله ی آپلود های معمولی رو نداره. اینطوری لودینگ تایممون رو به صفر نزدیک تر می کنیم تا هر چه زودتر، سال تحویل بشه و بریم سراغ پروژه ی بعدی.

سین دوم، سیب که از قضا ما به جاش مک بوک پرو رو داریم. بهش میگن نماد سلامتی ولی بیشتر به نماد خالی شدن حساب بانکی شبیه؛ مخصوصاً برای اونایی که فکر می کنن با داشتن یه سیب گاز زده، خلاقیت شون ۱۰ برابر میشه.

نوبتی هم که باشه، نوبت سنجده که ما به جاش یه الگوریتم یادگیری ماشین داریم که فرزانگی رو از دیتاست های بزرگ برامون استخراج کنه. البته یه وقتایی مثل سنجد واقعی، خروجی بی مزه ای بهمون میده.

سین چهارم، سیر. الحق که یه فایروال قدرتمند که کل سیستم رو از حمله های سایبری و بدافزارهای سمی دور نگه میداره، بهترین جایگزین به. حواستون باشه اگر این سین رو جا بندازید، هکرها کل سفرتون رو DDoS می کنن.

سین پنجم سرکه است که مثل یه باتری UPS، نماد صبر و تحمل در برابر نوسانات و قطعی برقه. ممکنه مثل سرکه واقعی خوشمزه نباشه اما وقتی سیستم

داره کرش میکنه، این باتری تبدیل به قهرمان زندگیت میشه.

از هر چی که بگذریم، سبزه جزء جدا نشدنی از هفت سین عه ولی ما به جاش کدهای سبز صفحه ی ترمینال لینوکس رو داریم، نماد تولد دوباره و امید، البته اگه rm -rf رو نزده باشی، وگرنه دیگه سبزه‌ای باقی نمیمونه!

در آخر، سکه رو داریم که قدرتمندانه، جاش رو به یه ولت پر از بیت کوین داده. نمادی از ثروت؛ البته بیشتر برای اونهایی که از ۲۰۱۰ جدی اش گرفتند نمود داره، همونایی که الان لازم نیست مدام کد بزنن.

شاید فکر کنید سفره ی ما همین قدر ساده و بی رنگ و روعه، ولی ما آپشن های دیگه ای هم داریم.

مثلا به جای آینه، یه نمایشگر OLED با رزولوشن 4K میزاریم که زندگی رو حتی خوش رنگ تر از واقعیت بهمون نشون میده.

یا مثلا به جای شمع، لامپ های RGB کیس هست که هر بار ()update رو اجرا کنه، رنگش عوض می‌شه.

از همه مهم تر، یه اپلیکیشن قرآن روی تبلت نصب کردیم که هرجا سیستم به مشکل خورد، با یه دعا ریستش کنیم و سیم اتصالمون به درگاه الهی، همواره وصل باشه.

البته سفره مون یه باگ هایی هم داره. مثلا به جای ماهی، یه ربات متصل به IoT داریم که اگر اینترنت قطع شه، Freeze می شه.

یا مثلا نورپردازیمون با یه کد اسکی رنگی عه که خیلی ملیح توی پس زمینه خودنمایی می کنه، ولی اگر خدایی نکرده حواسمون پرت شه، با یه syntax error کلش بهم می ریزه.

حالا قضاوتش با شما، حق داریم که لحظه ی سال تحویل پشت گجت های دیجیتالی‌مون باشیم یا نه؟

به هرحال، سال نوتون مبارک، باگ هاتون کم و پردازنده هاتون همیشه خنک!

مروری بر مقاله تاریخی کن تامپسون با عنوان تاملی بر اعتماد به اعتماد

امیرحسین ملکی

در این بخش از نشریه ماتریس، نگاهی به یک مقاله تاریخی خواهیم انداخت. کن تامپسون که معرف همه علاقمندان به تکنولوژی و برنامه‌نویسی است. او همانطور که یکی از بنیان‌گذاران یونیکس است، خالق

زبان B و C و Go نیز است.

در هر صورت، او در هنگام دریافت جایزه تورینگ، مقاله‌ای نوشت که لرزه بر پیکره امنیت دیجیتال انداخت. مقاله‌ای تحت عنوان (تأملی بر اعتماد به اعتماد - Reflections on Trusting Trust)، که مانند یک افسانه ترسناک، به ما هشدار می‌دهد که چگونه اعتماد ما به ابزارهای بنیادی می‌تواند دچار فساد شود.

تامپسون در این مقاله نشان داد که چگونه یک «گناه اولیه» در دنیای نرم‌افزار می‌تواند به شکلی ناپیدا در طول سال‌ها و دهه‌ها باقی بماند. او یک حقیقت هولناک را آشکار کرد: اگر یک کامپایلر آلوده باشد، می‌تواند بدون نیاز به تغییر در کد منبع، آلودگی خود را به هر نرم‌افزاری که کامپایل می‌کند، منتقل کند و این یعنی، حتی اگر تمام کدها بررسی شوند، همچنان امکان وجود تهدیدی نامرئی وجود دارد.

• نطفه گناه در دل کامپایلرها

در جهان نرم‌افزار، کامپایلرها به‌عنوان پل ارتباطی میان کدهای انسانی و باینری‌های اجرایی عمل می‌کنند. اما تامپسون نشان داد که اگر اولین کامپایلر دچار نقص یا دستکاری باشد، هر کامپایلر دیگری که از آن ساخته شود نیز آلوده خواهد بود.

این موضوع یک پارادوکس را ایجاد می‌کند:

- اگر نتوان به یک کامپایلر اعتماد کرد، چگونه می‌توان به کامپایلرهای ساخته‌شده توسط آن نیز اعتماد داشت؟

- چه اتفاقی می‌افتد اگر ابزاری که برای تست امنیت استفاده می‌کنیم، خودش آلوده باشد؟

- چگونه می‌توان مطمئن شد که کدی که می‌بینیم، همان چیزی است که اجرا می‌شود؟

این مسئله ما را به یک واقعیت تلخ می‌رساند: بررسی کد منبع به‌تنهایی تضمین‌کننده امنیت نیست. در حقیقت، ما باید تمام تاریخچه کامپایلر را بررسی کنیم، نه فقط خروجی نهایی را.

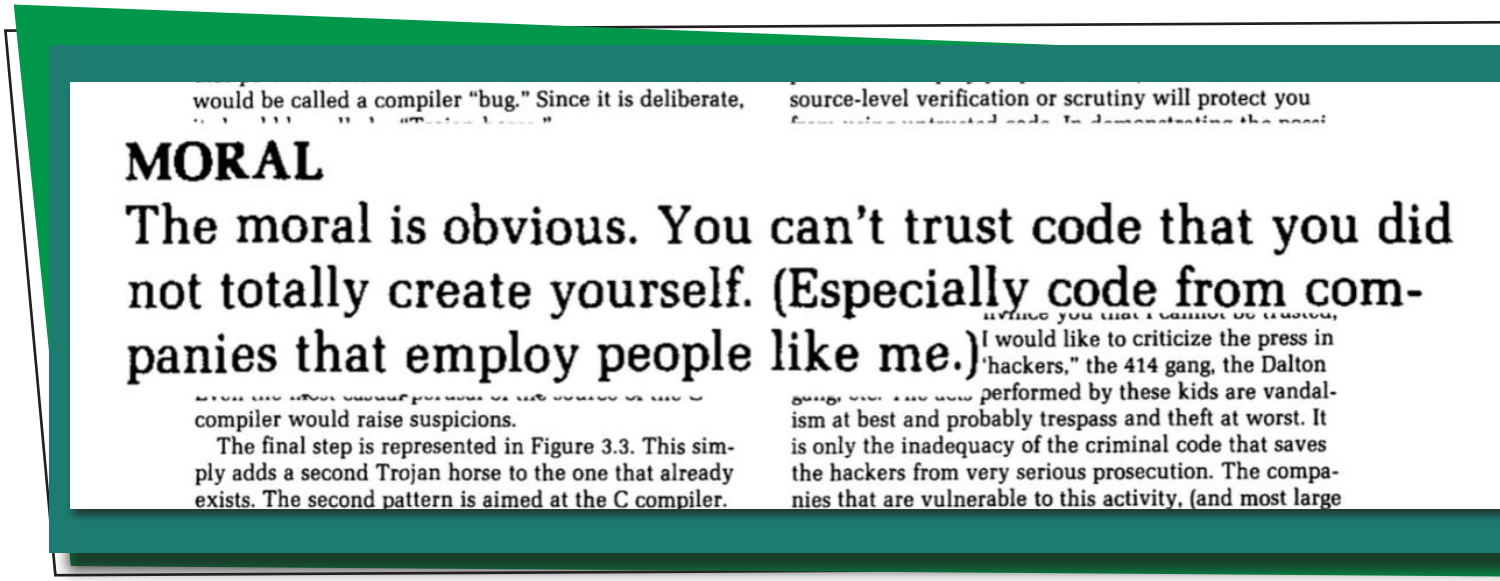
• تاریخ مدرن و درس‌هایی از اعتماد

- ماجرای حفره‌های امنیتی سخت‌افزاری

در سال ۲۰۱۸، دو آسیب‌پذیری بزرگ به نام‌های Spectre و Meltdown کشف شدند که نشان دادند چگونه نقص‌های نهفته در معماری پردازنده‌ها می‌توانند امنیت کل صنعت را به خطر بیندازند. این آسیب‌پذیری‌ها مشابه هشدار تامپسون بودند: چیزی که در سطح بنیادی خراب باشد، در تمام سیستم‌ها اثرگذار خواهد بود.

- رسوایی الگوریتم‌های رمزنگاری ضعیف

در دهه‌ی ۹۰ میلادی، سازمان NSA الگوریتم‌های رمزنگاری ضعیفی را به‌عنوان استاندارد معرفی کرد که بعدها مشخص شد قابل نفوذ هستند. این نمونه‌ای از همان تهدید بود: ابزارهایی که باید امنیت را تأمین کنند، خودشان می‌توانند منبع ناامنی باشند.


would be called a compiler "bug." Since it is deliberate, source-level verification or scrutiny will protect you

MORAL

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)

I would like to criticize the press in 'hackers," the 414 gang, the Dalton performed by these kids are vandalism at best and probably trespass and theft at worst. It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution. The companies that are vulnerable to this activity, (and most large

compiler would raise suspicions.

The final step is represented in Figure 3.3. This simply adds a second Trojan horse to the one that already exists. The second pattern is aimed at the C compiler.

- فجایع زنجیره تأمین نرم‌افزار

حملات به زنجیره‌ی تأمین نرم‌افزار، مانند حمله سولاروینڈز (SolarWinds Attack) در سال ۲۰۲۰، نشان دادند که چگونه یک نقص در یک ابزار بنیادی می‌تواند صدها شرکت را آلوده کند. این همان گناهی است که در دودمان نرم‌افزاری باقی می‌ماند.

راهکاری برای شکستن چرخه آلودگی: کامپایل متنوع دوگانه

- کامپایل متنوع دوگانه (Diverse Double-Compiling) یکی از راه‌های مقابله با این مشکل است.

در این روش:

۱. یک برنامه را با دو کامپایلر کاملاً مستقل کامپایل می کنند .

۲. اگر خروجی‌های باینری دقیقاً یکسان باشند، احتمال آلودگی کاهش می‌یابد.

این تکنیک بر این فرض استوار است که دو کامپایلر از دو منبع مختلف، احتمالاً حاوی همان بدافزار نخواهند بود. اما همچنان تضمینی مطلق نیست.

نتیجه‌گیری: آیا می‌توان واقعاً به نرم‌افزارها اعتماد کرد؟

آنچه تامپسون به ما نشان داد، چیزی فراتر از یک هشدار درباره امنیت کامپایلرها بود. این یک حقیقت عمیق درباره ماهیت اعتماد در دنیای دیجیتال است. امروزه، اعتماد صرف به ابزارهای نرم‌افزاری و سخت‌افزاری کافی نیست. باید منشأ، تاریخچه و وابستگی‌های آنها را بررسی کرد. زنجیره تأمین نرم‌افزار و سخت‌افزار نیاز به کنترل و نظارت بیشتری دارد. هیچ راهکار مطلقی وجود ندارد، اما روش‌های تحلیلی مانند کامپایل متنوع دوگانه می‌توانند خطرات را کاهش دهند.

شاید بزرگ‌ترین درس این باشد که در دنیای مدرن، اعتماد باید نه بر اساس کد، بلکه بر اساس بررسی دقیق تمام زنجیره‌ها و فرآیندها بنا شود و در نهایت، این پرسش همچنان پابرجاست: آیا می‌توان به ابزارهایی که ابزارهای ما را می‌سازند، اعتماد کرد؟

و در نهایت نقل قولی از تامپسون:

«نتیجه واضح است: شما نمی‌توانید به کدی که خودتان به‌طور کامل ننوشته‌اید، اعتماد کنید. (به‌ویژه کدهایی که از شرکت‌هایی می‌آیند که افرادی مثل من را استخدام می‌کنند.)»

جنگ تراشه‌ای آمریکا و چین: رقابت ژئوپلیتیکی بر سر فناوری

محمدمهدی بابابیک

جنگ تکنولوژیک میان آمریکا و چین بر سر صنعت نیمه‌هادی‌ها همچنان تشدید می‌شود. این رقابت نه‌تنها آینده ی نوآوری جهانی را تحت تأثیر قرار داده، بلکه به‌عنوان یک منازعه ی ژئوپلیتیکی کلیدی نیز شناخته می‌شود.

آغاز تحریم‌ها

وزارت بازرگانی آمریکا در مه ۲۰۲۰ محدودیت‌هایی علیه هواوی اعمال کرد که منجر به قطع همکاری TSMC، بزرگ‌ترین تولیدکننده تراشه‌های این شرکت شد. این تحریم‌ها کاهش سود سالانه ۷۰ درصدی برای هواوی را در پی داشت و آغازگر تنش‌های بیشتر در صنعت نیمه‌هادی شد.

دلایل استراتژیک آمریکا

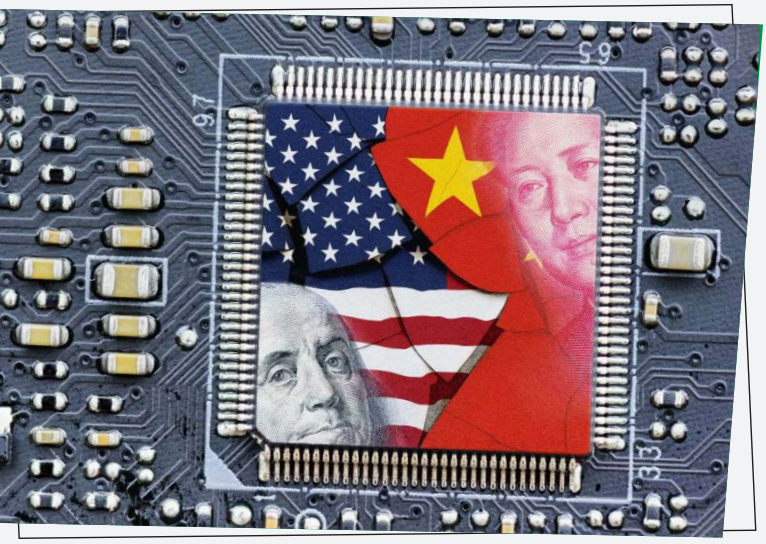
ایالات متحده برتری فناوری را امری حیاتی برای امنیت ملی خود می‌داند. سیاست «ادغام نظامی-مدنی» چین، که هدف آن هم‌گرایی فناوری‌های تجاری با توسعه نظامی است، نگرانی‌های بیشتری برای آمریکا ایجاد کرده است. از دیدگاه واشنگتن، این سیاست می‌تواند برتری نظامی چین را تقویت کند.

تحریم‌های گسترده نیمه‌هادی‌ها

در اکتبر ۲۰۲۲، آمریکا صادرات تجهیزات و تراشه‌های پیشرفته به چین را محدود کرد. قوانین جدید، که در ۲۰۲۳ تشدید شدند، هدف‌شان جلوگیری از دسترسی چین به فناوری‌های حیاتی مانند هوش مصنوعی و ابرکامپیوترها بود. این اقدامات بر شرکت‌هایی مانند انویدیا تأثیر گذاشته و میلیاردها دلار از بازار این شرکت را به خطر انداخته است.

اقدامات متقابل چین

چین نیز در واکنش به این تحریم‌ها، محدودیت‌هایی بر صادرات مواد اولیه مهمی مانند گالیوم و ژرمانیوم اعمال کرد. این عناصر برای تولید تراشه‌های پیشرفته ضروری‌اند و چین بیش از ۶۰ درصد بازار جهانی آن‌ها را در اختیار دارد. این اقدام منجر به افزایش قیمت تراشه‌ها و تأثیرگذاری بر زنجیره تأمین جهانی شده است.



نتیجه‌گیری

درحالی‌که رقابت چین و آمریکا بر سر تراشه‌ها شدت می‌گیرد، تأثیرات آن بر صنایع جهانی، اقتصاد دیجیتال، و امنیت ملی دو کشور غیرقابل انکار است. این جنگ تکنولوژیک نه‌تنها بر قیمت و عرضه تراشه‌ها اثر گذاشته، بلکه مسیر آینده فناوری‌های نوظهور را نیز شکل خواهد داد.

جدال در هسته لینوکس: استعفای یک رهبر، بحران Rust و سایه سنگین فرسودگی در جامعه متن‌باز

سارا امیرحسینی

دراماهای کرنل لینوکس.....

هکتور مارتین، رهبر پروژه Asahi Linux ، صبح جمعه ۱۴ فوریه به وقت استاندارد ژاپن از این پروژه استعفا داد. او دلیل این تصمیم را فرسودگی شغلی، فشار بیش از حد کاربران، و نحوه مدیریت لینوس تورووالدز در خصوص ادغام Rust در کرنل متن‌باز لینوکس اعلام کرد.

در یک پست طولانی، مارتین توضیح داد که تصمیمش تا حدی ناشی از عدم حمایت تورووالدز بوده است. تورووالدز در انتقادی عمومی از مارتین به دلیل آنچه «اعمال فشار اجتماعی» نامید، او را مورد سرزنش قرار داد. این اختلاف نظر بر سر درایورهای Rust باعث شد که مارتین در اوایل فوریه از نقش خود به عنوان نگهدارنده کد کرنل لینوکس برای مک‌های مبتنی بر پردازنده ARM اپل کناره‌گیری کند.

Asahi Linux یک توزیع لینوکس برای مک‌های اپل با پردازنده‌های ARM است. مارتین تا پیش از استعفای خود، هم روی کرنل لینوکس برای این دستگاه‌ها و هم روی توسعه این توزیع کار می‌کرد.

مارتین: مدیریت تورووالدز در ادغام Rust یک شکست بزرگ بود

مارتین در پست خود نوشت:

«مشکلاتی که پروژه Rust for Linux در فرآیند پذیرش در کرنل لینوکس با آن مواجه بوده، به‌خوبی مستند شده است، بنابراین نیازی به تکرار آن‌ها نمی‌بینم. اما باید بگویم که من مدیریت لینوس در این زمینه را یک شکست بزرگ رهبری می‌دانم.»

طبق گزارش‌های قبلی، وصله‌ای که تیم Rust for Linux پیشنهاد داده بود، با مخالفت کریستوف هلوینگ، از نگهدارندگان هسته کرنل لینوکس، مواجه شد. هلوینگ تمایلی به پذیرش مدل انتزاعی ارائه‌شده برای درایورهای Rust نداشت. این موضوع باعث بحث‌های داغی در فهرست ایمیل‌های توسعه‌دهندگان کرنل لینوکس شد. مارتین از تورووالدز خواست تا در این مورد تصمیم‌گیری کند، اما تورووالدز به‌جای آن، او را به‌شدت مورد انتقاد قرار داد و از فرآیند مدیریت جامعه لینوکس دفاع کرد.

مارتین نوشت:

«من کسی نیستم که در برابر بی‌عدالتی‌ها سکوت کنم. وقتی دیدم که یکی از نگهدارندگان قدیمی پروژه تلاش می‌کند تا مانع پیشرفت Rust for Linux شود، اعتراض کردم. اما واکنشی که دریافت کردم، باعث شد که به نقطه شکست برسم. از نقش خود به‌عنوان نگهدارنده کرنل لینوکس برای ARM اپل استعفا دادم، زیرا دیگر نمی‌خواهم بخشی از این جامعه باشم.»

فرسودگی شغلی و بحران در جامعه توسعه متن باز

مارتین استدلال می‌کند که پروژه لینوکس برای بقا نیاز به حمایت بازیگران کلیدی صنعت دارد. اما مدیریت غیرمداخله‌ای توروالدز به برخی از نگهدارندگان اجازه داده است که بدون هیچ عواقبی، به سوءاستفاده از موقعیت خود بپردازند. او به استعفای ودسون آلمیدا فیلیو، یکی از مهندسان مایکروسافت و نگهدارنده Rust for Linux، در آگوست گذشته به‌عنوان یک نمونه اشاره کرد.

توروالدز به صراحت در مواجهه با توسعه‌دهندگان رفتار تندی داشته است. به‌عنوان مثال، سال گذشته، او به یکی از توسعه‌دهندگان گوگل گفت: «کد تو آشغال است!»، که واکنش‌هایی درباره فرسودگی شغلی در جامعه لینوکس به دنبال داشت.

این فرسودگی شغلی در جوامع متن‌باز سال‌هاست که مشکل‌ساز شده و دلایل آن مشخص است: سوءرفتارهای کلامی، کمبود قدردانی از کار داوطلبانه، و فشار کاری بیش از حد. این مسئله چنان جدی شده که سازمان جهانی بهداشت آن را به‌عنوان یک پدیده شغلی طبقه‌بندی کرده است.

بحران منابع و مشکلات مالی در نرم‌افزارهای متن باز

برایان فاکس، هم‌بنیان‌گذار Sonatype، می‌گوید که نرخ فرسودگی در بین توسعه‌دهندگان نرم‌افزارهای متن‌باز به سطح نگران‌کننده‌ای رسیده است. او هشدار می‌دهد که این مسئله می‌تواند زنجیره تأمین نرم‌افزار را به خطر بیندازد.

«بررسی‌های ما نشان می‌دهد که از سال ۲۰۲۰، تعداد بروزرسانی‌های پروژه‌های متن‌باز یا متوقف شده یا کاهش یافته است، که نشانه‌ای از فرسودگی شغلی یا کمبود منابع در این پروژه‌هاست. تا سال ۲۰۲۴، بیش از ۳۰۰,۰۰۰ پروژه دچار کاهش سرعت توسعه یا تعطیلی کامل شده‌اند.»

فاکس تأکید می‌کند که جامعه سالم پایه و اساس یک اکوسیستم نرم‌افزاری موفق است و این نیازمند تأمین مالی است.

«نرم‌افزارهای قدیمی که متروکه شده یا به‌درستی نگهداری نمی‌شوند، باعث ایجاد حفره‌های امنیتی بزرگی می‌شوند که سازمان‌ها را در معرض خطر قرار می‌دهند. پرداخت به نگهدارندگان پروژه‌ها و استخدام توسعه‌دهندگان جدید می‌تواند شروع خوبی باشد، اما از آنجا که بسیاری از این پروژه‌ها توسط بنیادهای غیرانتفاعی مدیریت می‌شوند، شرکت‌ها و کاربران بزرگ نیز باید منابع مالی خود را به این پروژه‌ها اختصاص دهند.»

ترک Asahi Linux؛ خیانت و آزارهای شخصی

مارتین می‌گوید که در سال گذشته سعی کرده بود با محدود کردن ساعات کاری خود روی پروژه کرنل از فرسودگی جلوگیری کند. اما مسائل شخصی، از جمله تهدیدها و حملات برخی افراد علیه خودش و خانواده‌اش، وضعیت را برای او دشوارتر کرده است.

او می‌گوید که پس از انتقاد توروالدز متوجه شد برخی از افراد در جامعه لینوکس «بازی دوگانه» انجام می‌دادند: ظاهراً از او و پروژه Asahi Linux حمایت می‌کردند، اما در پشت پرده علیه او موضع می‌گرفتند.

«من فهمیدم که یکی از این افراد، که در چندین پروژه مهم جایگاه بالایی دارد، نه‌تنها از افرادی که من را مورد آزار و اذیت قرار داده‌اند حمایت کرده، بلکه همچنان از آن‌ها طرفداری می‌کند.»

در حالی که مارتین از جامعه لینوکس کناره‌گیری کرده است، پروژه‌های Rust for Linux و Asahi Linux همچنان به کار خود ادامه خواهند داد.

سیکادای رازآلود

فربد فیضی

سیکادا۳۳۰۱ به جد یکی از جذاب‌ترین داستان‌های عصر اینترنت است. این پروژه به مانند چالشی نبوغ‌آزما طراحی شده بود که با معماهایی شگفت‌انگیز و درهم‌تنیده، ذهن افراد علاقه‌مند به رمزگشایی را به چالش می‌کشید.

هدف ظاهری این پروژه، شناسایی «باهوش‌ترین‌ها» برای عضویت در یک گروه مخفی و مرموز بود. اما جذابیت اصلی داستان به همین جا ختم نمی‌شود؛ سیکادا۳۳۰۱ نه‌تنها شامل پازل‌های دیجیتال مانند رمزنگاری و پنهان‌نگاری بود، بلکه حتی سرنخ‌های فیزیکی مانند مختصات جغرافیایی را در سراسر جهان به‌کار می‌برد.

در دل این پروژه‌ی اسرارآمیز، پیام‌هایی نیز درباره‌ی ارزش‌های حفظ حریم خصوصی، مقابله با سانسور و آزادی اطلاعات دیده می‌شود که ارتباط احتمالی سیکادا با جنبش‌های مرتبط با کریپتو-آنارشیست‌ها را تقویت می‌کند.

«سلام. ما دنبال افراد بسیار باهوش می‌گردیم. برای پیدا کردن آن‌ها، آزمونی طراحی کرده‌ایم. در این تصویر، پیامی نهفته است. پیدایش کنید تا شما را به مسیری به سمت ما هدایت کند. ما مشتاقانه منتظر دیدار با تعداد اندکی از شما هستیم که موفق به رسیدن به آخر مسیر خواهند شد. موفق باشید.»

عکس منتشرشده، متنی سفید بر پس‌زمینه‌ای سیاه و حاوی این پیام بود:

این پیام با امضای اسرارآمیز «۳۳۰۱» تکمیل شد. طراحی این متن، از نظر بصری ساده اما از لحاظ معنا عمیق بود. پیام به گونه‌ای نوشته شده بود که کنجکاوی عمیقی را برانگیزد و کاربران را دعوت کند تا سفری ناشناخته به دنیای رمزها و پازل‌های پیچیده را آغاز کنند.

تحلیل من این است که همین سادگی مینیمالیستی به همراه حس ابهامی که ایجاد می‌کرد، بخش مهمی از موفقیت این چالش در جذب توجه بود.

در آن دوران، معمای سیکادا۳۳۰۱ سؤال‌های متعددی را برانگیخت. کاربران 4chan که با این پیام مواجه شدند،

در ابتدا بین تردید و کنجکاوی گیر کردند. عده‌ای این پیام را به‌عنوان یک شوخی اینترنتی یا حتی حرکتی در راستای بازاریابی تصور کردند. برخی دیگر فکر می‌کردند شاید این معما نوعی روش غیرمتعارف برای جذب نیروی انسانی در پروژه‌های فناورانه و سری است.

اما واقعیت این بود که پیچیدگی معماها فراتر از چیزی بود که به‌سادگی بتوان آن را فقط یک شوخی یا تبلیغ تلقی کرد. اینجا بود که گروه کوچکی از افراد علاقه‌مند به رمزگشایی، این چالش را جدی گرفتند. تلاش آن‌ها به آغاز سفری پر از هیجان و رمز و راز انجامید، و معماهای ۳۳۰۱ به یکی از جنجالی‌ترین و در عین حال جذاب‌ترین پروژه‌های اینترنتی تاریخ تبدیل شد.

جالب است که نام «سیکادا۳۳۰۱» با گذشت زمان به نمادی از این معماها تبدیل شد. در سال‌های ۲۰۱۲، ۲۰۱۳ و ۲۰۱۴، این گروه ناشناس با انتشار معماهای جدید، جامعه‌ای از رمزگشاها و علاقه‌مندان به حل معما را به خود جذب کرد. هر مرحله از این معماها به تخصص‌هایی در زمینه‌هایی مانند رمزنگاری، استگانوگرافی، دانش تاریخی و ادبی نیاز داشت.

سیکادا۳۳۰۱ به‌خوبی شایسته ی عنوان «پیچیده‌ترین و مرموزترین معمای عصر اینترنت» است. این پروژه از زمان آغاز خود توانسته ذهن هزاران نفر را در سراسر دنیا به خود مشغول کند و همچنان بدون پاسخی قطعی باقی بماند. قرار گرفتن در فهرست معماهای حل‌نشده‌ای که توسط واشنگتن‌پست ارائه شد، جایگاه آن را به‌عنوان یکی از نمادهای اسرارآمیز دنیای دیجیتال تثبیت کرده است.

اما آنچه سیکادا را متمایز می‌کند، نه‌تنها پیچیدگی معماها بلکه رازآلودگی کامل درباره اهداف، هویت طراحان و حتی انگیزه اصلی پشت این پروژه است. ۱۲ سال از اولین پیام این گروه می‌گذرد و هنوز سوالاتی اساسی بی‌پاسخ مانده‌اند: این معما برای چه هدفی طراحی شده بود؟ آیا به‌راستی یک سازمان زیرزمینی پشت آن است، یا صرفاً نمایشی از خلاقیت و هوش؟

پروژه‌ی سیکادا۳۳۰۱ بدون شک مرزهای تعریف شده‌ی بازی‌های واقعیت جایگزین (ARG) را بازتعریف کرده است. در حالی که بسیاری از بازی‌های ARG با هدفی مشخص، از جمله تبلیغات، سرگرمی یا حتی اهداف تجاری طراحی می‌شوند و در نهایت پایان‌بندی روشنی دارند، سیکادا۳۳۰۱ گامی فراتر نهاده است و همگان را در یک سفر اسرارآمیز و بی‌پایان فرو برده.

این پروژه که شامل معماهایی پیچیده و فراتر از مرزهای آنلاین است، شباهت‌هایی با ARG دارد؛ چرا که بازیکنان را مجبور می‌کند تا در فضای مجازی و حتی دنیای واقعی، به دنبال سرنخ‌هایی باشند که می‌توانند شامل تماس‌های تلفنی مرموز، مختصات جغرافیایی، یا حتی پوسترهای فیزیکی باشند. اما آنچه سیکادا را از دیگر پروژه‌ها متمایز می‌کند، این است که حتی پس از گذشت سال‌ها از آغاز آن، هویت بنیان‌گذاران، اهداف نهایی و مفهوم اصلی آن همچنان ناشناخته باقی مانده است.

به نظر می‌رسد که سیکادا فراتر از یک چالش سرگرم‌کننده عمل کرده و ذهن افراد را به طرز عمیقی مشغول کرده است. از دید من، این پروژه ممکن است تلاشی برای ایجاد یک جامعه نخبه و اختصاصی از افرادی باشد که توانایی حل چالش‌هایی در سطحی فراتر از انسان‌های عادی دارند. اگرچه هنوز سوالاتی درباره اینکه این جامعه چه کاربردی دارد یا چه هدفی را دنبال می‌کند بی‌پاسخ مانده است.

سیکادا۳۳۰۱ با ترکیب شگفت‌آوری از راز و دانش، موفق شد تا ذهن‌های خلاق و تحلیل‌گر را به یک ماجراجویی پیچیده دعوت کند. انتشار تصویری که در آن پیام‌ها در عمق پنهان شده بودند، نقطه آغاز این سفر مرموز بود. این پیام‌ها و معماها طوری طراحی شده بودند که تنها افراد باهوش و متفکر بتوانند آن‌ها را رمزگشایی کنند و مسیر را به‌سمت هدفی ناشناخته پیش ببرند.

معماهای سیکادا۳۳۰۱ از ابزارها و تکنیک‌هایی استفاده می‌کردند که در دنیای فناوری و علوم، همچنان به‌عنوان

چالش‌های خاص شناخته می‌شوند. از رمزنگاری و استگانوگرافی گرفته تا ارجاع به دانش کهن و روش‌های کلاسیک مانند رمز سزار و سایفر کتاب. هر مرحله، هوشمندی بیشتری طلب می‌کرد و بازیکنان را به کاوش عمیق‌تر در دنیای دیجیتال و واقعی مجبور می‌کرد.

بسیاری از معماها از سرنخ‌هایی بهره می‌بردند که به‌ظاهر ساده بودند، اما در واقعیت، پیچیدگی بالایی داشتند. مثلاً تبدیل یک متن یا کد به مختصات جغرافیایی، یا استفاده از نرم‌افزارهای پیشرفته برای کشف پیام‌های پنهان در تصاویر. این روند مرحله به مرحله طراحی شده بود تا بازیکنان به تدریج به عمق معما نفوذ کنند.

مرحله اول:معماهای سال ۲۰۱۲

بخش اول پروژه سیکادا۳۳۰۱ در سال ۲۰۱۲، به‌عنوان نقطه‌ی آغاز یکی از هیجان‌انگیزترین معماهای اینترنتی، توجه کاربران کنجکاو و علاقه‌مند به حل معما را جلب کرد. این ماجرا با انتشار تصویری در فروم **/b/** وب‌سایت **4chan** شروع شد که حاوی یک پیام چالش‌برانگیز بود: «در این عکس پیامی نهفته است. پیدایش کنید.»

با کشف اولین سرنخ، کاربران به رشته‌ای از اعداد و حروف برخورد کردند که عبارت زیر در آن نمایان بود:

```
TIBERIVS CLAVDIVS CAESAR says «lxx-
t>33m2mqkyv2gsq3q=w]02ntk
```

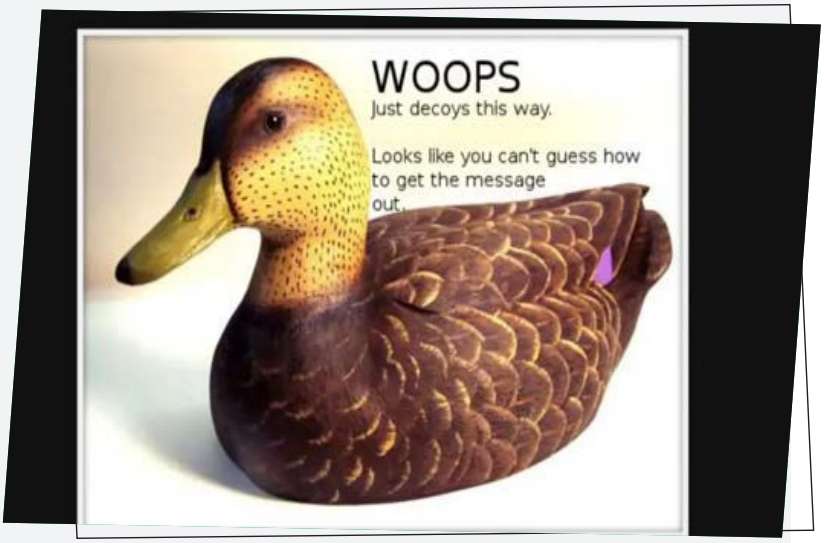
کلمه‌ی CAESAR به‌عنوان سرنخی کلیدی، کاربران را به سوی الگوریتم رمزنگاری «شیفت سزار» هدایت کرد. این روش رمزنگاری، نیازمند جابه‌جایی حروف الفبا به تعداد مشخصی گام به عقب یا جلو است. با توجه به اینکه تیبریوس کلادیوس، چهارمین امپراتور روم بود، کاربران فرض کردند که باید این عبارت را با چهار گام به عقب رمزگشایی کنند. این رمزگشایی منجر به نمایش آدرسی URL به شکل زیر شد:

```
http://i.imgur.com/m9sYK.jpg
```

که با کلیک روی آن، تصویر زیر نمایان شد:

این بار سرنخ در این جمله بود:

Looks like you can't guess how to get the mes-.
sage out



در این مرحله از معما، جمله‌ی «Looks like you can't guess how to get the message out» بیش از آنچه در ابتدا به نظر می‌آمد، حاوی نکاتی پنهان بود. دو کلمه‌ی «guess» و «out» مانند چراغ راهنما عمل کردند و کاربران را به سمت نرم‌افزار استگانوگرافی OutGuess هدایت کردند. این ابزار برای آشکارسازی پیام‌های مخفی در فایل‌های تصویری طراحی شده است.

وقتی کاربران عکس اول را در نرم‌افزار OutGuess باز

کردند، پیام جدیدی کشف شد که درواقع معمای بعدی را آشکار می‌کرد:

این پیام بیانگر هوش طراحان سیکادا بود؛ چراکه آن‌ها توانسته بودند معما را طوری طراحی کنند که هر مرحله نه‌تنها مهارت تحلیل و تفکر خلاق را بسنجد، بلکه کاربران را به‌طور فزاینده‌ای به ابزارها و روش‌های تخصصی‌تر هدایت کند.

با کلیک روی لینک، کاربران وارد فرومی در ردیت شدند که مکان جدیدی برای ادامه‌ی این ماجراجویی مرموز بود.

در این فروم، چندین پست متنی و دو تصویر با نام‌های «Welcome» و «Problems» به چشم می‌خوردند.

هر دو تصویر، حاوی پیام‌هایی نهفته بودند که برای آشکارسازی آن‌ها، کاربران به استفاده از نرم‌افزار استگانوگرافی OutGuess نیاز داشتند. با رمزگشایی این تصاویر، سرنخ‌های جدیدی پدیدار شد.

تصویر «Welcome» حاوی پیامی بود که اعلام می‌کرد از این پس تمام پیام‌های سیکادا با استفاده از امضای رمزنگاری‌شده‌ی PGP ارائه خواهد شد. این اقدام برای اطمینان از اصالت پیام‌ها و جلوگیری از انتشار پیام‌های جعلی طراحی شده بود.

در تصویر «Problems» نیز پیامی بود که می‌گفت: «کلید همیشه جلوی چشمان‌تان بوده است. این معما تلاشی برای پیدا کردن جام مقدس نیست. اینقدر آن را دشوارتر از چیزی که هست، نکنید.» این پیام بر اهمیت توجه به جزئیات ساده و رویکرد منطقی تأکید داشت.

رمزگشایی از تصویر اصلی، به‌جز هدایت به لینک صفحه‌ی ردیت، با رویکردی نوآورانه شامل سایفر کتاب همراه بود. این شیوه‌ی رمزنگاری که نیازمند استفاده از کتاب یا متنی خاص به‌عنوان کلید است، یکی از روش‌های قدیمی اما به‌شدت هوشمندانه برای پنهان‌سازی پیام‌های سری به شمار می‌رود.

در سایفری که سیکادا ۳۳۰۱ به کار گرفته بود، دستورالعمل رمزگشایی به این صورت بود که دو عدد، جداشده با دونقطه، به ترتیب به شماره‌ی خط و شماره‌ی کاراکتر در متن مرجع اشاره می‌کردند. این رویکرد، دقت و صبر بالایی را از کاربران می‌طلبید و به‌نوعی ذهن آنان را به چالش می‌کشید تا با ترکیبی از مهارت‌های جستجو و تحلیل، پیام پنهان را کشف کنند.

هدر صفحه ردیت با استفاده از اعداد مایا، پیچیدگی بیشتری به این معمای رمزنگاری اضافه کرد. هر نقطه معادل عدد یک، هر خط معادل عدد پنج و علامت راگبی‌شکل به‌عنوان عدد صفر در نظر گرفته شد. با ترجمه این اعداد، رشته‌ای به‌صورت زیر به‌دست آمد:

۱۰-۲-۱۴-۷-۱۹-۶-۱۸-۱۲-۷-۸-۱۷-۰-۱۹

مقایسه این اعداد با عنوان صفحه (a2e7j6ic78h-0j7eiejd0120) نشان داد که ارقام کمتر از ۱۰ بین این دو رشته مشترک هستند. سپس حروف الفبا به این اعداد مرتبط شدند؛ برای مثال، عدد ۱۰ معادل حرف a، عدد ۱۴ معادل e، و به همین ترتیب تا عدد ۱۹ معادل j شد.

با گسترش این روش به کل عنوان، اعداد متناظر با حروف به رشته زیر رسیدند:

۱۰-۲-۱۴-۷-۱۹-۶-۱۸-۱۲-۷-۸-۱۷-۰-۱۹-۰-۷-۱۴-۱۸-۱۴-۱۹-۱۳-۰-۱-۲-۰

این اعداد، کلیدی برای استفاده در سایفر کتاب بودند که به رمزگشایی متون منتشرشده در صفحه ردیت کمک کردند. این فرآیند پیشرفته و مرحله‌به‌مرحله، کاربران را به کشف پیامی هدایت کرد که آن‌ها را فراخواند:

Call us at US telephone number two one four three nine oh nine six oh eight

این پیام، شماره‌ای در ایالت تگزاس را معرفی کرد که کاربران می‌توانستند با آن تماس بگیرند.

این شماره تلفن (۲۱۴۳۹۰۹۶۰۸) که در تگزاس است، حالا غیرفعال شده؛ اما اگر آن روزها به این شماره زنگ می‌زدید، این پیام ضبط‌شده را می‌شنیدید:

لینک و متن پیام صوتی:
بسیار خوب. کارت خوب بود. سه عدد اول مورد نظر است که به تصویر اول final.jpg مربوط می‌شود.

۳۳۰۱ یکی از آن‌ها است. باید دوتای دیگر را پیدا کنی. هر سه تای آن‌ها را در هم ضرب و به آن com. اضافه کن تا قدم بعدی را پیدا کنی. موفق باشی. خدانگهدار.

این جزئیات نشان‌دهنده دقت و عشق سیکادا ۳۳۰۱ به مفاهیم ریاضی و رمزنگاری است. استفاده از اعداد اول در ابعاد تصویر (۵۰۹ و ۵۰۳)، هم‌چنین ارجاع غیرمستقیم به ویژگی خاص عدد ۳۳۰۱ که عددی اول

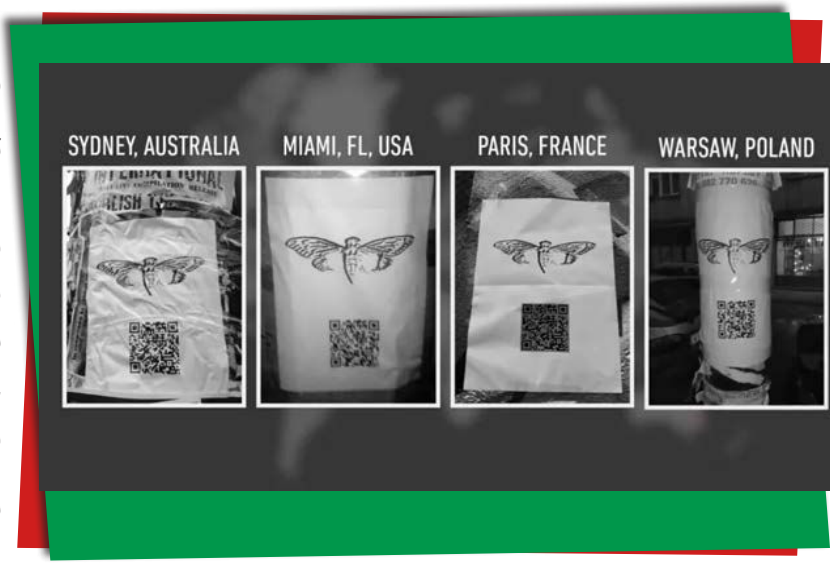
$$509 \times 503 \times 3301 = 845145127$$

دوقلو است، توجه خاص این پروژه به ساختار ریاضی را آشکار می‌کند. این ویژگی‌ها به نوعی حس نظم و هوشمندی طراحان سیکادا را بازتاب می‌دهند.

ضرب سه عدد مرتبط و اضافه کردن «.com» نیز کاربران را به آدرس `http://845145127.com` هدایت کرد. هرچند این وب‌سایت دیگر در دسترس نیست، اما نسخه پشتیبان آن بازتاب روش مرحله‌بندی سیکادا برای هدایت کاربران است. جالب اینجاست که بعد از باز کردن این لینک، تصویری از سیکادا (زنجره) به همراه شمارش معکوس دیده می‌شد که به نوعی منتظران را به مرحله بعدی معما هدایت می‌کرد.

این شمارش معکوس سرانجام به نمایش مختصات GPS منتهی شد که کاربران ماجراجو را به مکان‌هایی در سراسر دنیا، از جمله اسپانیا، روسیه، آمریکا و ژاپن، هدایت کرد. چنین اقدامی، یعنی ترکیب فضای مجازی و دنیای واقعی، هیجان خاصی به این پروژه می‌بخشید و تجربه‌ای واقعیت‌محور از یک معمای دیجیتال ارائه می‌کرد.

افراد شجاعی که تصمیم گرفتند به محل این مختصات بروند، روی تیرهای برق پوسترهایی پیدا کردند که روی آن‌ها تصویر سیکادا و کد OR بود.



مرحله‌ی اسکن کدهای **QR** یکی از لحظات هیجان‌انگیز پروژه سیکادا۳۳۰۱ بود. دو پیام که از این کدها نمایان شدند، نمایانگر هوشمندی و عمق طراحی این معماها بودند.

پیام اول، هشداری علیه همکاری افراد در حل معماها بود و تأکیدی واضح داشت که سیکادا به دنبال فردیت و خودکفایی در حل این چالش‌هاست. این هشدار، اصل مهمی از سیکادا را روشن کرد: تنها کسانی که به‌طور مستقل توانایی حل معماها را دارند، شایسته پیوستن به اهداف این گروه مرموز هستند.

سیکادا در این پیام، کاربران را به کتاب آگریپا (کتاب مردگان) نوشته‌ی ویلیام گیبسون ارجاع می‌داد. این کتاب که به‌شکلی خاص بر روی فلاپی دیسک منتشر شده بود، ویژگی منحصربه‌فردی داشت؛ بعد از یک بار خوانده شدن، به‌طور خودکار رمزگذاری می‌شد تا هیچ‌کس دیگر نتواند به آن دسترسی پیدا کند. این ویژگی، حس رمزآلود و ناپایداری اطلاعات را به اوج می‌رساند.

رمزگشایی از نسخه دیجیتال کتاب و آشکارسازی لینک sq٦wmgv٢zcsrix٦t.onion، ورود به دنیای تاریک‌تر و پیچیده‌تر معمای سیکادا۳۳۰۱ را نشان می‌دهد. این لینک که مخصوص دسترسی از طریق شبکه‌ی ناشناس تور بود، نمادی از چالش‌های عمیق‌تر و خصوصی‌تر این پروژه بود. این اقدام، سطحی از هیجان و رمزآلودگی را اضافه کرد که تنها مناسب افراد سریع و آماده بود.

تنها تعداد اندکی از کسانی که به‌موقع وارد این وب‌سایت شده بودند، توانستند به مرحله آخر این دور از معماها دست یابند. این مرحله به‌نوعی گزینش نهایی برای جدا کردن بهترین‌ها از میان هوشمندترین‌ها بود. رویکرد سیکادا در این مرحله، تأکیدش بر سرعت عمل، دقت و کنجکاوی بی‌حدوحصر را بیشتر نمایان می‌کند.

به نظر می‌رسد این لایه عمیق‌تر از معماها و روش انحصاری انتخاب، فلسفه سیکادا را در تعیین اولویت برای فردیت و شایستگی منحصربه‌فرد تأیید می‌کند.

دومین پیام به‌دست‌آمده از اسکن کدها که به ویرایش یازدهم دانشنامه بریتانیکا اشاره داشت، اهمیت دانش و اطلاعات عمیق را بازتاب می‌داد. افرادی که موفق به ورود به لینک تور شدند، با خواسته‌ای خاص مواجه شدند: ساخت ایمیل جدید و ارسال آن برای دریافت دستورالعمل‌های بیشتر.

پیامی که پس از این فرآیند منتشر شد، تأکید مجددی بود بر دیدگاه سیکادا: «ما دنبال بهترین‌ها هستیم، نه پیروان.» این جمله، فلسفه‌ی فردیت‌گرایانه و گزینشی سیکادا را به خوبی بیان می‌کرد. اما جالب‌ترین قسمت این مرحله، هشدار شدید به افراد درباره درز نکردن جزئیات بود. پیام به‌وضوح اعلام می‌کرد که هرگونه افشاگری منجر به حذف فرد از مراحل بعدی خواهد شد.

(درحالی‌که برخی از کاربران نتوانستند در برابر وسوسه‌ی افشای محتوای ایمیل خود مقاومت کنند، این اقدام پیامدهای مشخصی داشت و مسیر آن‌ها را به پایان رساند. چنین کنترل سختگیرانه‌ای از اطلاعات، نظم و قدرت طراحی سیکادا را به نمایش می‌گذارد.)

این مرحله از معماهای سیکادا۳۳۰۱، اوج پیچیدگی و چالشی بزرگ برای شرکت‌کنندگان بود. استفاده از روش شکستن رمزنگاری به روش کلید عمومی (RSA)

که یکی از سخت‌ترین پروتکل‌های رمزنگاری است، به نوعی آزمون نهایی برای افراد بود. ترکیب این رمزنگاری با فایل MIDI موسیقی، رویکردی خلاقانه و بی‌سابقه داشت که نه‌تنها دانش رمزنگاری بلکه توانایی تجزیه و تحلیل موسیقی را نیز به چالش کشید.

تبدیل فایل MIDI به متن با استفاده از برنامه‌ی پایتون، پیامی آشکار کرد که دستورالعمل‌های بیشتری برای ادامه‌ی مسیر معما ارائه می‌داد. اما همچنان، اطلاعات دقیقی درباره‌ی افرادی که موفق به حل این مرحله شدند در دسترس نیست؛ انگار که این نخبگان در سایه و به‌دور از دید عموم عمل کرده‌اند.

یک ماه پس از این مرحله، تصویری که در فروم ردیت منتشر شده بود، به پیامی تغییر یافت که پایان این مرحله را اعلام می‌کرد. این پیام همچنین به کسانی که موفق به تکمیل معما نشده بودند، امیدواری داد که در آینده معماهای بیشتری منتشر خواهد شد.

به نظر می‌رسد سیکادا ۳۳۰۱ همواره رویکردی ساختاریافته داشته که علاوه بر گزینش بهترین‌ها، حس انتظار و تعلیق را در میان علاقه‌مندان زنده نگه می‌داشت.

این داستان در نسخه بعدی ماتریس ادامه دارد...

سفر در زمان با کامپیوتر: از ۱۹۷۰ تا ۲۰۳۸، رازهایی که زمان یونیکس فاش می‌کند

امیرحسین ملکی

هکِ زمان

اگر شما هم از آن دسته دانشجوهایی هستید که عاشق باگ‌های عجیب و غریب تکنولوژی‌اید، حتماً این صحنه برایتان جالب است: نصب یک سیستم عامل جدید، ریست شدن زمان گوشی به اول ژانویه ۱۹۷۰، و یک لحظه سکوت پر از حیرت

چرا ۱۹۷۰؟! مگر این تاریخ چه رازی دارد؟

جواب این سؤال، یک نام آشناست: Unix Time یا همان «زمان یونیکس»؛ مفهومی که دنیای نرم‌افزار را از ابتدا تا امروز شکل داده و حتی آینده را هم تهدید می‌کند!

ماجرای ۱۹۷۰: تولد یک اَبَرستاره!

همه‌چیز از پروژهٔ یونیکس شروع شد. مهندسان آن زمان تصمیم گرفتند زمان در کامپیوترها را با شمارش

ثانیه‌ها از یک نقطهٔ ثابت محاسبه کنند و این نقطه را «Unix Epoch» نامیدند. اما چرا ۱ ژانویه ۱۹۷۰؟!

- برخی میگویند این تاریخ، شروع نمادین عصر کامپیوترهای مدرن بود.

- برخی دیگر شوخی می‌کنند که توسعه‌دهندگان یونیکس آنقدر غرق کدنویسی بودند که فراموش کردند سال نو را جشن بگیرند و تاریخ را روی ۱۹۷۰ قفل کردند!

به هر حال، این عدد جادویی «۰» در زمان یونیکس است: `۱ January ۱۹۷۰ ۰۰:۰۰:۰۰ UTC`.

حالا هر وقت سیستم عامل‌ها (مثل PostMarketOS) در تشخیص زمان شکست می‌خورند، به این نقطهٔ صفر برمی‌گردند و گوشی شما را به ماشین زمان ارزان‌قیمت تبدیل می‌کنند!

۲۰۳۸: فاجعهٔ زمانی بعدی در راه است!

شاید فکر کنید این یک شوخی بی‌ضرر است، اما زمان یونیکس یک بمب ساعتی هم دارد! سیستم‌های ۳۲-بیتی زمان را با عددی ۳۲-بیتی ذخیره می‌کنند که در سال ۲۰۳۸ به حداکثر ظرفیت خود می‌رسد. وقتی این عدد از `۲,۱۴۷,۴۸۳,۶۴۷` ثانیه بگذرد، به طور جادویی به ۲,۱۴۷,۴۸۳,۶۴۷- تبدیل می‌شود و تاریخ به ۱۹۰۱ برمی‌گردد!

- این باگ که به Problem Y۲۰۳۸ معروف است، می‌تواند سیستم‌های بانکی، ماهواره‌ها و حتی دستگاه‌های پزشکی را دچار اختلال کند.

- راه حل؟ مهاجرت به سیستمهای ۶۴-بیتی که تا ۲۹۲ میلیارد سال دیگر کار می‌کنند! (احتمالاً تا آن زمان، خورشید هم تبدیل به کوتولهٔ سفید شده باشد!)

چرا این موضوع برای شما مهم است؟

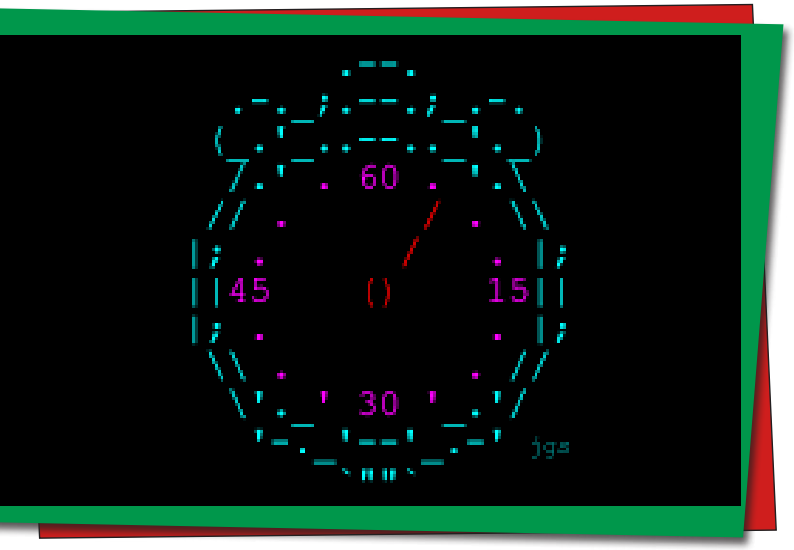
۱. یادگیری زمان یونیکس مثل یادگیری الفبای دنیای برنامه‌نویسی است. هر API، دیتابیس، یا سیستم عاملی با این مفهوم سروکار دارد.

۲. اشکالات زمانی (مثل ۱۹۷۰ یا ۲۰۳۸) آزمونی برای مهارت‌های عیب‌یابی شما هستند. تصور کنید رزومه‌تان بنویسید: نجات جهان از فاجعهٔ ۲۰۳۸ !

۳. این تاریخ‌های عجیب، طنز پنهان تکنولوژی را نشان می‌دهند: گاهی پیشرفت‌های انسان، به سادگی «یک شمارش ثانیه» است که از کنترل خارج میشود!

حالا نوبت شماست!

- گوشی قدیمی‌تان را روشن کنید. اگر تاریخ آن ۱۹۷۰



است، شما یک مسافر زمان ناخواسته هستید!

- کد بزنید و زمان یونیکس را به تاریخ خوانا تبدیل کنید (چالش: بدون استفاده از کتابخانه‌های آماده!).

- منتظر ۱۹ ژانویه ۲۰۳۸ باشید؛ روزی که تاریخ تکرار می‌شود... یا نه؟!

پ.ن: هروقت سیستم عامل جدید نصب می‌کنید، یک شمع برای ۱۹۷۰ روشن کنید؛ آغازگر تمام ثانیه‌های دیجیتال ماست!

و در آخر زمان، تنها متغیری است که نمی‌توانید آن را بازنویسی کنید... یا شاید هم بتوانید!؟

گروه هکتیویستی Dark Storm

فربد فیضی

گروه هکتیویستی Dark Storm به‌طور فزاینده‌ای در فضای سایبری شناخته شده است. این گروه به‌ویژه به دلیل استفاده از تاکتیک‌هایی که شباهت بسیاری به گروه هکری KillNet دارند، توجه بسیاری را جلب کرده است. Dark Storm در ابتدا به‌عنوان یک گروه مستقل با هدف حمله به کشورهای غربی و سازمان‌های حامی اوکراین فعالیت می‌کرد، اما به‌مرور زمان تبدیل به یک سرویس اجاره‌ای برای حملات سایبری به اهداف مختلف شده است.

همچنین این گروه از حامیان مردم مظلوم فلسطین و کشور فلسطین نیز هست.

گروه‌های هکتیویستی (Hacktivist) گروه‌هایی هستند که از مهارت‌های هک و فناوری برای پیشبرد اهداف سیاسی، اجتماعی یا ایدئولوژیک استفاده می کنند .

(Anonymous) یکی از شناخته‌شده‌ترین گروه‌های هکتیویستی که در موضوعات مختلفی از جمله آزادی اینترنت و مقابله با فساد فعالیت کرده است.

این گروه‌ها گاهی به عنوان قهرمانان دیجیتال دیده می‌شوند، اما فعالیت‌های آن‌ها می‌تواند بحث‌برانگیز باشد، زیرا ممکن است قوانین را نقض کنند.

تاریخچه و پیدایش گروه Dark Storm

گروه Dark Storm برای اولین بار در سال ۲۰۲۳ مشاهده شد. از آن زمان این گروه به‌سرعت حملات سایبری خود را گسترش داده و به‌ویژه در حملات DDoS(Distributed Denial of Service) و باج‌افزار (Ransomware) مشهور شده است. هدف‌گذاری‌های اصلی این گروه شامل کشورهای عضو ناتو، رژیم صهیونیستی و ایالات متحده آمریکا بوده است. این گروه به‌طور خاص به زیرساخت‌های حیاتی و سازمان‌های کلیدی در این کشورها حمله کرده و در برخی موارد، اقدام به دزدی اطلاعات مهم و حساس کرده است.

تاکتیک‌ها و شباهت با گروه KillNet

یکی از ویژگی‌های برجسته گروه Dark Storm، استفاده از تاکتیک‌های مشابه گروه KillNet است که آن‌ها نیز به‌طور گسترده به‌عنوان یک گروه هکتیویستی مستقر در روسیه شناخته می‌شوند. گروه KillNet پیش از Dark Storm فعالیت‌های زیادی در زمینه حملات DDoS علیه کشورهای غربی و سازمان‌های نظامی و دولتی انجام داده بود. شباهت‌های موجود بین این دو گروه باعث می‌شود که این‌گونه حملات پیچیده‌تر و هماهنگ‌تر به نظر برسند.

حملات DDoS:

یکی از تاکتیک‌های اصلی گروه Dark Storm، انجام حملات DDoS است که باعث اشباع و از کار انداختن سرورها و خدمات آنلاین می‌شود. در این نوع حملات، گروه‌های هکری با استفاده از یک شبکه بزرگ از دستگاه‌های آلوده به بدافزار (که به آن‌ها «BotNet»

گفته می‌شود)، سرورها یا سایت‌های هدف را با حجم زیادی از درخواست‌ها پر می‌کنند تا منابع سیستم‌ها را مصرف کرده و سرویس‌های آنلاین را متوقف کنند.

حملات باج‌افزار (Ransomware) :

در کنار حملات DDoS، گروه Dark Storm از باج‌افزار نیز برای هدف‌گذاری سازمان‌ها و کشورهای خاص استفاده کرده است. در این نوع حملات، بدافزار با رمزگذاری داده‌های سیستم‌های آلوده به‌طور پنهانی اطلاعات حساس را قفل کرده و پس از آن، هکرها درخواست‌هایی برای دریافت پول به‌عنوان باج برای بازگرداندن دسترسی به داده‌ها ارسال می‌کنند. این حملات باعث ایجاد تلفات مالی قابل توجه و به خطر افتادن داده‌های حساس می‌شوند.

هدف‌گذاری‌ها و پیامدهای حملات

گروه Dark Storm به‌طور عمده کشورهایی را هدف قرار می‌دهد که در موضوعات جغرافیایی و سیاسی خاص، از جمله حمایت از اوکراین در برابر تجاوزات روسیه، فعال هستند. این گروه به‌ویژه به زیرساخت‌های حیاتی مانند شبکه‌های دولتی، سیستم‌های انرژی، شرکت‌های بزرگ و دیگر سازمان‌های کلیدی حمله کرده است.

حملات به رژیم صهیونیستی و کشور های عضو ناتو:

کشورهای عضو ناتو و رژیم صهیونیستی از جمله اصلی‌ترین اهداف حملات گروه Dark Storm هستند. این حملات معمولاً به‌منظور ایجاد اختلال در عملیات‌های سیاسی، نظامی و اقتصادی این کشورها انجام می‌شود. تأثیرات این حملات نه تنها بر زیرساخت‌های فناورانه این کشورها، بلکه بر اعتماد عمومی به امنیت آنلاین و قابلیت‌های دفاعی سایبری آنها نیز تأثیرگذار است.

حملات به ایالات متحده:

گروه Dark Storm همچنین به زیرساخت‌های کلیدی ایالات متحده آمریکا، از جمله سیستم‌های انرژی، نهادهای دولتی و شبکه‌های ارتباطی این کشور، حملات سایبری انجام داده است. این حملات می‌تواند به‌طور مستقیم بر امنیت ملی ایالات متحده تأثیر بگذارد و منجر به خسارات مالی و از دست رفتن اطلاعات حساس گردد.

پیچیدگی و حرفه‌ای بودن حملات

شباهت‌های موجود بین Dark Storm و KillNet به وضوح نشان‌دهنده پیچیدگی و حرفه‌ای بودن این گروه‌ها در طراحی و اجرای حملات سایبری است. این گروه‌ها به‌طور خاص توانایی هماهنگی و اجرای حملات با مقیاس بزرگ را دارند که می‌تواند آسیب‌های قابل توجهی به زیرساخت‌های حیاتی کشورهای هدف وارد کند. هماهنگی حملات، استفاده از بدافزارهای پیچیده و ابزارهای پیشرفته، نشان‌دهنده توانایی این گروه‌ها در انجام حملات پیچیده و گسترده است.

گروه هکتیویستی Dark Storm در یکی از جدیدترین اقدامات خود، مسئولیت حمله سایبری به پلتفرم X (که پیش‌تر با نام توییتر شناخته می‌شد) را از طریق کانال تلگرامی خود پذیرفت. این گروه در پستی اعلام کرد که «توییتر توسط تیم Dark Storm آفلاین شده است.» در این گزارش، گروه Dark Storm به‌طور مشخص از نام قدیمی توییتر استفاده کرده است، که این امر ممکن است به‌عنوان نشانه‌ای از عدم احترام یا حتی مخالفت با ایلان ماسک، مالک جدید پلتفرم، تفسیر شود.

اعلام مسئولیت در کانال تلگرام:

گروه Dark Storm به‌طور رسمی از طریق کانال تلگرام خود مسئولیت این حمله را بر عهده گرفت. در این پست، گروه ادعا کرده است که توانسته پلتفرم X را آفلاین کند. استفاده از نام قدیمی توییتر، در حالی که این پلتفرم اکنون به نام X شناخته می‌شود، ممکن است به‌طور عمدی برای نشان دادن نوعی بی‌احترامی یا مخالفت با تغییرات جدید در پلتفرم توسط ایلان ماسک باشد.

همکاری در نشریه ی ماتریس

نشریه ی ماتریس در جهت ارتقای کیفیت نشریه و مشارکت همه دانشجویان در سه تیم تحریریه، ویراستاری و طراحی گرافیک عضو همکار می پذیرد.

جهت ارتباط با روابط عمومی نشریه و همکاری در تهیه نشریه با ما در ارتباط باشید.

@MatrisMagazine