آرایه

فصل‌نامهٔ علمی‌دانشجویی انجمن علمی مهندسی کامپیوتر دانشگاه شیراز

سال یکم - شمارهٔ ۱ - بهار ۱۳۹۹

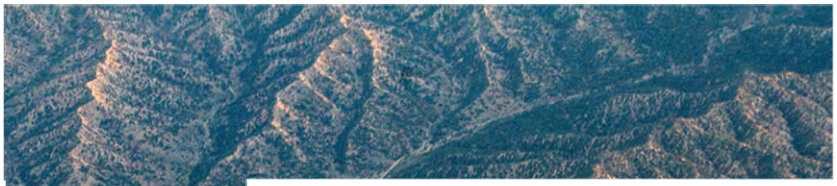
در دنیای کامپیوتر ساعت چند است؟

سه ماه در تلگرام

از مصر باستان تا تلگراف ارتش آلمان

هو المُعلِّم

آ



فهرست

فصل‌نامهٔ علمی‌دانشجویی آرایه

سال یکم، شمارهٔ ۱، بهار ۱۳۹۹

صاحب‌امتیاز: انجمن علمی مهندسی کامپیوتر دانشگاه شیراز

مدیرمسئول: پویا فکری

سردبیر: سیدمحمدحسین هاشمی

استاد مشاور انجمن و ناظر علمی: دکتر سیدمحمدرضا موسوی

با تشکر از: دکتر مرتضی کشتکاران

هیئت‌تحریریه (به ترتیب حروف الفبا):

امیررضا خواجوی (ورودی ۹۸ کامپیوتر)

راضیه زارع (ورودی ۹۶ کامپیوتر)

کوثر شمس (ورودی ۹۷ کامپیوتر)

محسن طهماسبی (ورودی ۹۸ کامپیوتر)

ر.ق.ع (ورودی ۹۸ کامپیوتر)

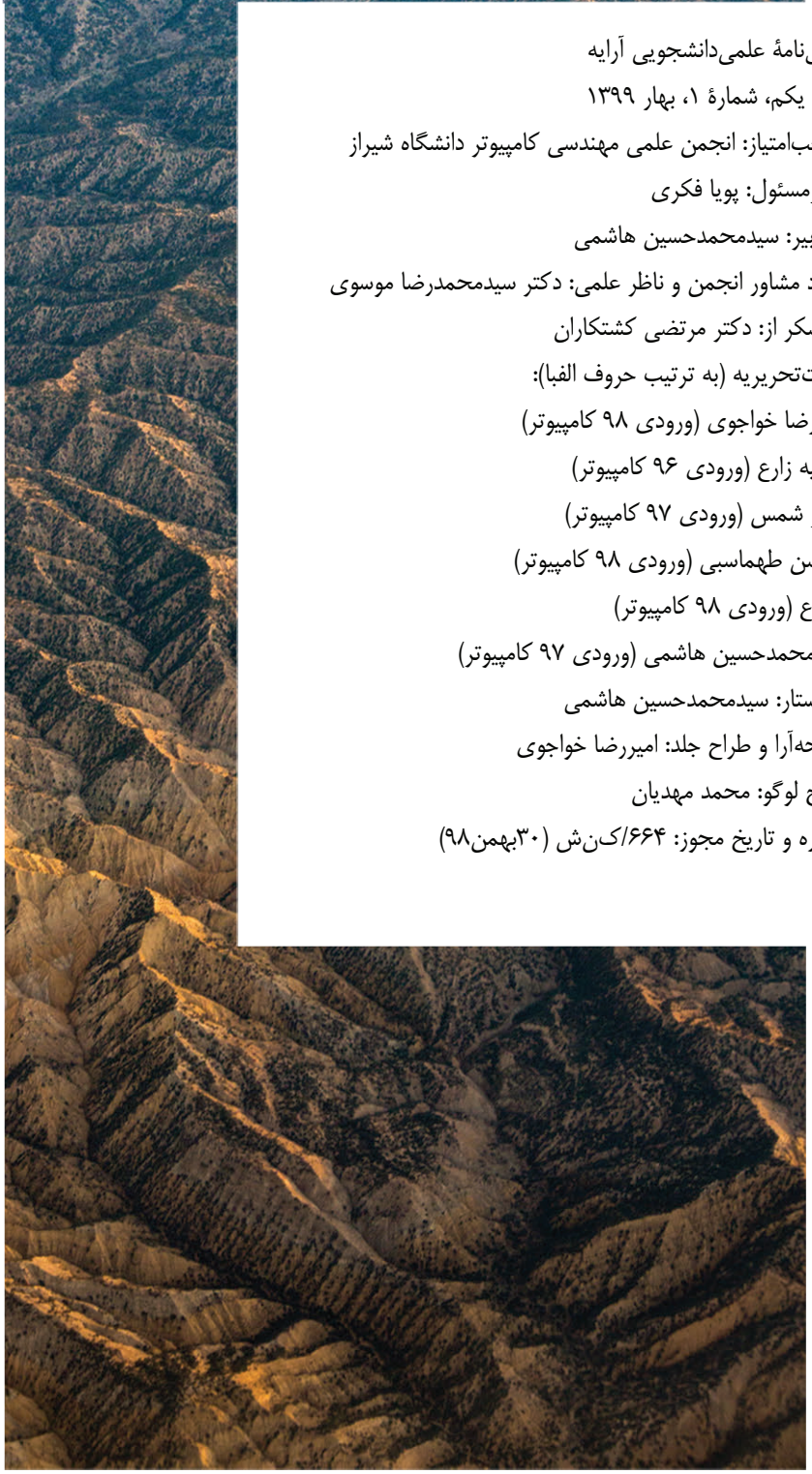
سیدمحمدحسین هاشمی (ورودی ۹۷ کامپیوتر)

ویراستار: سیدمحمدحسین هاشمی

صفحه‌آرا و طراح جلد: امیررضا خواجوی

طراح لوگو: محمد مهدیان

شماره و تاریخ مجوز: ۶۶۴/ک‌ن‌ش (۳۰بهمن۹۸)



سخن سردبیر

قدم اول

روزهـای قرنطینه با همـهٔ بدی‌ها و خسـتگی‌ها و بی‌حوصلگی‌هایش، چیزهـای خوبـی هـم داشـت. مانـدن در خانـه و تعطیلـی بعضـی از کارهـا باعـث شـد تـا وقـت آزاد بیشـتری داشـته باشـیم و در همیـن وقــت آزاد کارهایــی را بکنیــم کــه مدت‌هــا دلمــان می‌خواسـته شـروع کنیـم یـا بـرای بعضی‌هایمـان این شـانس وجود داشـت که تجربه‌های جدیدی داشته باشیم و عادت‌هایی مثل خواندن کتـاب، دیـدن فیلم، ورزش کـردن، گوش‌دادن به پادکسـت و ... را به عادت‌هــای روزانه‌مــان تبدیــل کنیــم. امــا بعضــی از عادت‌هــا فراموش شـده‌اند و ممکن اسـت در چنین موقعیت‌هایی به سراغشـان نرویـم؛ حتـی ممکـن اسـت بعضـی از مـا هرگـز تجربـهٔ آن‌هـا را بـه یـاد نیاوریـم. یکـی از آن عادت‌هـا، خوانـدن مجله و نشریه است.

بیـش از ۱۰ سـال از چـاپ آخریـن شـمارهٔ نشـریهٔ «صفـر و یـک» می‌گـذرد. آخریـن نشـریهٔ دانشـجویی بخـش کامپیوتـر دانشـگاه شـیراز. و حـالا آرایـه، نشـریهٔ جدیـد بخـش کامپیوتـر اسـت. نشـریه‌ای بـا هـدف افزایـش سـطح علمـی بخـش و ایجـاد یـک تریبـون دانشـجویی اختصاصـی بـرای دانشـجویان؛ چیـزی کـه کمبـودش، سـال‌ها حـس می‌شـد. ایـدهٔ نشـریه در سال‌های قبـل هـم مطـرح شـده بـود امـا در عمـل از اوایـل تـرم جـاری امـکان شـروع بـه کار آن بـا حمایـت انجمـن علمـی فراهـم شـد تـا اولیـن شـماره‌اش در ایـن بهـار منتشـر شـود. آرایـه سـعی می‌کنـد محلـی باشـد بـرای گردهمایـی همـهٔ دانشـجویان بخـش. همـهٔ آن‌هایـی کـه حرفـی بـرای گفتـن و دغدغه‌ای برای مطرح‌کردن دارند.

این شماره، قدم اول راه است.

از مصر باستان تا تلگراف ارتش آلمان

راضیه زارع

۵ دقیقه

انسان‌ها از ابتدای آفرینش، درگیر چگونگی برقراری ارتباط با یکدیگر بودند. کمی بعدتر، با تشکیل قبیله و حکومت و سیاست‌گذاری، نیاز بشر به برقراری امنیت در ارتباطات خود افزایش یافت و مفهوم رمزنگاری از همان جا شکل گرفت. روش‌های رمزنگاری و رمزگشایی از حدود ۴۰۰۰ سال پیش، ابداع شدند و در برهه‌های حساس تاریخ از جمله جنگ‌های جهانی، اهمیت یافتند. برخی از این روش‌ها اگرچه منسوخ شده‌اند اما پایه و اساس شکل‌گیری روش‌های رمزنگاری کنونی در دنیای ارتباطات و اطلاعات هستند که به‌طور گسترده در مخابرات، شبکه‌های اینترنتی، رمزهای دیجیتال و اینترنت اشیا[1] کاربرد دارند. رمزنگاری، دانشی است که متن حاوی یک پیام را با کمک یک الگوریتم و یک کلید به‌گونه‌ای تغییر می‌دهد که تنها کسانی که از الگوریتم رمزگشایی و کلید اطلاع دارند، بتوانند به پیام دسترسی داشته باشند.

در این مقاله قصد داریم با برخی از مشهورترین روش‌های رمزنگاری تاریخ آشنا شویم.

تکنیک هیروگلیف[2]

شواهد به‌دست‌آمده هیروگلیف را قدیمی‌ترین روش رمزنگاری می‌داند. مصریان باستان حدود ۴۰۰۰ سال قبل، با نوشتن متونی حاوی کدهای رمزآمیز که تنها کاتبان مورداعتماد دربار از آن آگاهی داشتند، با یکدیگر ارتباط برقرار می‌کردند. هیروگلیف که به معنی «نشانهٔ نوشته‌های مقدس» است، به طور انحصاری در اختیار کاهنان معابد بود. آن‌ها تا حد امکان تلاش می‌کردند از شکل‌هایی مبهم در رسم‌الخط خود استفاده کنند تا دشمنان و بیگانگان از محتوای پیام مُطلع نشوند.

در بین‌النهرین نیز، مردم برای مخفی‌نگه‌داشتن فرمول ساخت ظروف سفالی، با ساخت کدهایی متشکل از کم‌کاربردترین حروف میخی، از رمزنگاری استفاده می‌کردند.

۱- Internet of Things (IoT)

۲- Hieroglyph

هیروگلیف

خط میخی

روش اِسکیتال[1]

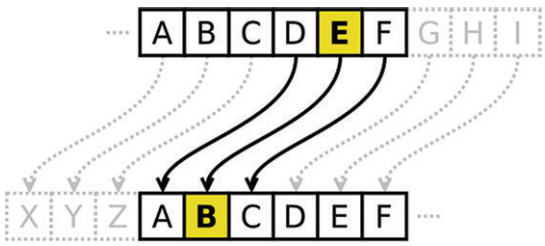
یونانیان باستان با اختراع دستگاهی به نام اسکیتال، به روشی جالب، پیام‌های خود را مخفی می‌کردند. یک چوب بلند که معمولاً استوانه‌ای بود را با نواری نازک از پاپیروس، چرم و یا پوست به صورت اُریب نوارپیچ می‌کردند. سپس پیام را به صورت افقی بر روی این استوانه می‌نوشتند. آنگاه نوار را باز کرده و به پیک می‌دادند تا به گیرنده تحویل دهد. مشخص است که تنها کسی می‌توانست پیام را بخواند که قطر چوب او با چوب کاتب پیام یکی بود. بر اساس شواهدی ابداع این روش به آرشلیوس[2]، شاعر یونانی قرن هفتم قبل از میلاد، منسوب است اما تا حدود ۵۰۰ سال، نوع نگارش این رمز مخفی ماند.

۱- Scytale
۲- Aeschylus
۳- Caesar
۴- Vigenère
۵- Giovan Battista Bellaso

کلید رمزگذاری سزار[3]

این روش ساده، در واقع اولین الگوی رمزنگاری ثبت‌شده در تاریخ به حساب می‌آید. ژولیوس سزار، رهبر نامدار سیاسی و نظامی جمهوری روم در سدهٔ پیش از میلاد مسیح (ع)، با ابداع روشی مبتنی بر جابه‌جایی کاراکترها، پیام‌های ارسالی برای فرماندهان سپاه خود را ایمن کرد. در این روش حروف یک پیام با شماره‌ای توافق شده، رمزنگاری شده و گیرندهٔ این پیام، حروف را با همان شماره تغییر می‌داد تا به پیام اصلی دست پیدا کند. الگوی رمزنگاری ژولیوس سزار برای دورانی که از هر قوم و قبیله به ندرت کسانی بودند که باسواد باشند، به قدر کافی امنیت داشت. در این روش تعداد شیفت حروف الفبا همان کلید رمزنگاری است.

مثال:	a r r a y
رمز:	x o o x v



الگوی رمزنگاری سزار با کلید سه انتقال به چپ (شماره‌ای که خود سزار انتخاب کرده بود.)

تابع جبری رمزگذاری سزار برای ۲۶ حرف الفبا:

$$E_n(x) = (x + n) \bmod 26$$

تابع جبری رمزگشایی سزار برای ۲۶ حرف الفبا:

$$D_n(x) = (x - n) \bmod 26$$

نتیجه، عددی بین ۰ تا ۲۵ است. اگر x–n یا x+n در این بازه نباشند، باید بر ۲۶ تقسیم شوند و باقی‌مانده را لحاظ کرد.

روش ویژنِر[4]

اگرچه ژِئون باتیستا بِلاسو[5] این روش را در سال ۱۵۵۳ شرح داد اما این روش در قرن ۱۹ میلادی به‌اشتباه به ویژنر نسبت داده شد. رمزنگاری ویژنر متشکل از رمز سزار مختلفی است که در دنباله‌ای با ارزش‌های مختلف تغییر می‌یابد.

خط افقی را به عنوان رشته پیام و ستون عمودی را به عنوان کلید در نظر می‌گیریم. هر حرف رشته با حرفی که روبروی کلید معادل آن آمده جابه‌جا می‌شود. کلید نیز به اندازهٔ تعداد حروف پیام تکرار می‌شود.

پیام:	a r r a y
کلید (تکرار به اندازهٔ حروف پیام):	k e y k e
متن رمزشده (براساس جدول ویژنر):	k v p k c

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

جدول ویژنر

در اواخر دهۀ ۱۷۰۰ میلادی، توماس جفرسون[۱]، برپایۀ روش ویژنر یک سیستم رمزنگاری با امنیتی بالاتر ابداع کرد. ماشین اختراعی او از ۳۶ چرخ تشکیل شده است که ۲۶ حرف الفبا به طور تصادفی روی آن‌ها نوشته شده است. هرکدام از این چرخ‌ها یک شمارۀ مشخص دارند. ترتیب قرارگیری این چرخ‌ها روی محور هم، در واقع همان کلید رمزنگاری است.

شیوۀ رمزنگاری در این روش به این صورت است که ابتدا شخص فرستنده، کلید رمزنگاری (ترتیب چرخ‌ها) را تنظیم می‌کند. سپس با چرخش چرخ‌ها، حروف پیام را به ترتیب پیدا می‌کند؛ به‌گونه‌ای که حروف پیام روی محور ظاهر شوند. حالا محور اصلی، حاوی پیام است که رمزنگاری نشده است. باتوجه به این‌که هر چرخ ۲۶ حرف دارد و تنها یکی از این حروف (که یکی از حروف پیام است)، روی محور اصلی قرار گرفته است، پس اکنون ۲۵ ردیف دیگر در بالا و پایین ردیف حاوی پیام (ردیف واقع بر محور)، قرار دارد. هر کدام از این ردیف‌ها می‌توانند پیام رمزشده باشند. فرستنده، متنِ واقع بر یکی از این ردیف‌ها را به عنوان متن رمزشده می‌فرستد. گیرنده که ترتیب قرارگیری چرخ‌ها (کلید رمز) را می‌داند، چرخ‌ها را مرتب کرده و با چرخش چرخ‌ها، پیام رمزشده را روی محور اصلی می‌سازد. سپس، در سایر ردیف‌های چرخ به دنبال عبارتی معنادار می‌گردد. بدیهی است تنها کسی می‌تواند متن رمزشده را رمزگشایی کند که ترتیب چرخ‌ها را بداند. ضعف این روش در آن است که در مواردی نادر، احتمال این وجود دارد که شخص گیرنده دو عبارت معنادار در ردیف‌ها پیدا کند.

این رمزنگاری، بعدها در دهۀ ۱۹۰۰ به‌طور تکامل‌یافته‌تر، در ارتش آمریکا به کار گرفته شد.

تلگراف زیمِرمَن[۲]

در ۱۶ژانویه۱۹۱۷، آرتور زیمرمن، وزیر امور خارجۀ آلمان، تلگرافی رمزی از واشنگتن به سفیر این کشور در مکزیک فرستاد. او در این تلگراف به سفیر آلمان در مکزیک دستور داد که از دولت مکزیک بخواهد به نفع آلمان وارد جنگ شود و در عوض ایالت‌های نیومکزیکو، تگزاس و آریزونا را از آن خود کند اما سرویس اطلاعاتی بریتانیا پیام‌های آلمانی‌ها را رهگیری و رمزگشایی کرد. کشف این تلگراف موجی از خشم بین دوستداران آلمان در آمریکا و محافظه‌کاران ایجاد کرد و این تلگراف به سرعت مشهور شد. رمزگشایی این تلگراف بهانه‌ای شد تا ایالات متحده به صف مخالفان آلمان بپیوندد و سرنوشت جنگ جهانی اول تغییر کند. ارتش آلمان در خلال جنگ جهانی اول، از روشی موسوم به adfgvx برای رمزنگاری پیام‌ها استفاده می‌کرد.

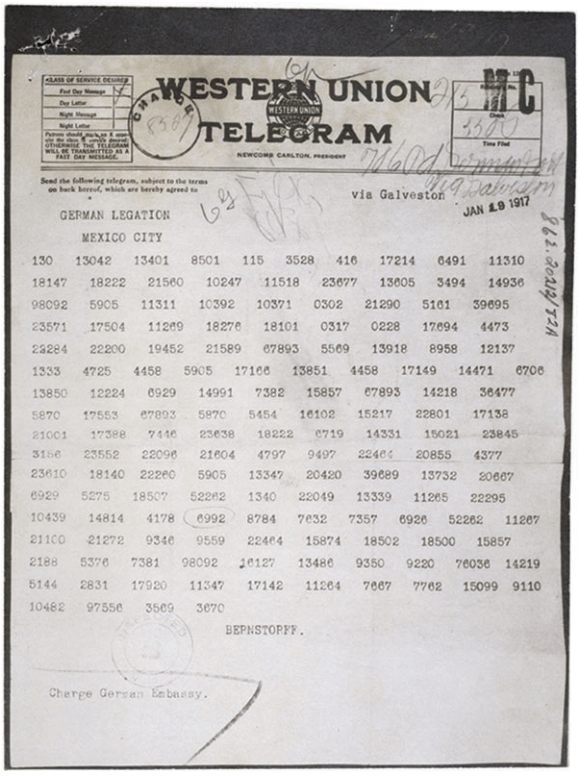
سیستم رمزنگاری adfgvx تلگراف زیمرمن

تمام سیستم رمزنگاری به شش حرف ADFGVX خلاصه می‌شود. با این شش حرف می‌توان تمامی حروف الفبا را پوشش داد. این شش حرف در زبان مورس[۳] شکل‌های کاملاً متفاوتی دارند؛ به‌گونه‌ای که اشتباه‌کردنشان سخت می‌شود.

ماشین رمزنگاری روسی

۱- Thomas Jefferson ۲- Arthur Zimmermann

۳- روشی برای انتقال پیام که در تلگراف به کار گرفته می‌شود.



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3070

BERNSTORFF.

Cherge German Embassy.

تلگراف رمزی زیمرمن به سفارت آلمان در مکزیک

زمانی که پیام‌ها با تلگراف و زبان مورس فرستاده می‌شد، اهمیت داشت که متنی که رمز شده احتمال خطایش در ارسال به زبان مورس تا جای ممکن کم شود؛ زیرا تغییر حتی یک نشانه در متن رمز شده، ممکن بود به تغییر مفهوم کلی عبارت منجر شود.

پیام:	hello world
رمزشده:	DFAXFAFAFG XDFGGDFAAG

برای رمزکردن پیام با رمز ADFGVX از جدولی ماتریسی به نام جدول Polybius که به شکل زیر است، استفاده می‌شود. در شروعِ کارِ ابداعِ این ماتریس حرف V در رمز جدول وجود نداشت و بعدها برای پوشش ارقام و جدا کردن حروف I و J از هم، به این رمز اضافه شد. به طور مثال معادل رمزشدهٔ حرف O در این سیستم، FG است (F ردیف حاوی O و G ستون حاویO) معادل هر دو حرف I و J هم DG می‌شود.

	A	D	F	G	X
A	A	B	C	D	E
D	F	G	H	I/J	K
F	L	M	N	O	P
G	Q	R	S	T	U
X	V	W	X	Y	Z

این سیستم مبنای رمزگذاری پیام‌های ارتش آلمان در جنگ جهانی اول بود که البته با شیوه‌هایی مثل چیدن اتفاقی حروف در ماتریس، استفاده از کلیدواژه‌های خاص در رمز یا تغییر کلید رمزنگاری در زمان‌های مختلف، آن را پیچیده‌تر کردند.

با شکسته‌شدن رمز تلگراف زیمرمن، آلمانی‌ها به فکر الگوریتم‌های قوی‌تر و پیچیده‌تر رمزنگاری افتادند. با شروع جنگ جهانی دوم، ماشینی منسوب به اِنیگما[1] و ماشین بنفش ژاپن[2] به عنوان دو تا از مشهورترین سیستم‌های رمزنگاری، جهت رمزنگاری اسناد محرمانه به‌کار گرفته شدند که در شماره‌های بعدی آرایه، به معرفی و آموزش الگوریتم آن‌ها خواهیم پرداخت.

منابع

۱- Roger A. Prichard. History of Encryption (January 26,2002)
آموزش ریاضیات و رمزنگاری (ircrypt.com)
۱۰فروردین۹۹

۲-۱۱تلگراف سرنوشت‌ساز که روند تاریخ را تغییر دادند! برگرفته از
http://cafekhoondani.com
۱۰فروردین۹۹

۳- عوض‌شدن صحنهٔ جنگ جهانی اول با یک تلگراف برگرفته از
https://www.yjc.ir/fa/news/7027102
۱۰فروردین۹۹

۴- کریپتوگرافی و رمزگذاری داده در گذر زمان برگرفته از
minerscamp.net
۱۰فروردین۹۹

۵- ده سیستم رمزنگاری مشهور برگرفته از
anarshoo.wordpress.com
۱۰فروردین۹۹

۶- اتحاد محکم، امید. مقدمه‌ای بر تاریخچهٔ رمزنگاری برگرفته از
mag.netran.net
۱۰فروردین۹۹

۷- نمونه‌ٔ خط هیروگلیف بر روی یک کتیبه برگرفته از
http://ganjur.loxblog.com
۱۰فروردین۹۹

عکس‌ها:
۱- ترجمهٔ خط میخی: اولین زبان نوشتاری دنیا. از وبلاگ گروه ترجمهٔ آنلاین
۱۰فروردین۹۹

2- Caesar Cipher Left Shift of 3 (13th May 2018)
Retrieved from s4scoding.com
۱۰فروردین۹۹

3- The Secret History of the Zimmermann Telegram(Nov 20, 2018).
Retrieved from history.com
۱۰فروردین۹۹

۱- Enigma

۲- Japan's Purple Encryption Machine

سه ماه در تلگرام

نتایج تحقیق بر روی ۷۵هزار کانال تلگرامی

محسن طهماسبی

۶ دقیقه

چند سالی است که به نوشتن و توسعهٔ خزنده‌های اینترنتی (برنامه‌های کامپیوتری که به جمع‌آوری اطلاعات مشغول‌اند و در محیطی مانند وب یا تلگرام پخش شده و مکان‌های جدیدی را تحت‌نظر می‌گیرند) مشغول هستم.

کرالر موردبحث در این مقاله از ده کانال تلگرامی شروع کرد و تا پایان پروژه بیش از ۹۰هزار کانال را به طور روزانه بررسی می‌کرد.

در ادامه به اطلاعات و آمار جالب حاصل از این تحقیق بر روی محیط تلگرام خواهیم پرداخت که از آنالیز اطلاعات حاصل در این سه ماه (بیش از سی‌میلیون پیام) به دست آمده‌اند. بازهٔ زمانی جمع‌آوری اطلاعات مورد بررسی، اردیبهشت تا مرداد ۱۳۹۸ بوده است.

کرالر یا خزنده چیست؟

قبل از ورود به اصل مطلب، ابتدا لازم است به چیستی کرالر یا خزنده بپردازیم. تا کنون فکر کرده‌اید موتورهای جست‌وجو مثل گوگل چگونه کار می‌کنند؟ موتورهای جست‌وجو با استفاده از برنامه‌هایی به نام کرالر یا خزنده به جمع‌آوری اطلاعات یک محیط مانند وب می‌پردازند. چطور؟

با دادن آدرس یک سایت به خزنده، او شروع به استخراج تمام لینک‌های درون آن صفحه می‌کند و بعد، همین فرایند برای بقیهٔ صفحه‌های استخراج‌شده نیز اجرا می‌شود و به‌مرور یک شبکهٔ بسیار بزرگ از صفحات وب تشکیل خواهد شد.

شما با بررسی داده‌های استخراج‌شده می‌دانید کدام صفحه به چه صفحهٔ دیگری لینک شده، یک سایت شامل چه صفحاتی بوده و البته تعداد بسیار زیادی صفحه وب و سایت را پیدا می‌کنید که در ابتدای کار غیرممکن به نظر می‌رسید!

این خزنده‌ها به وب محدود نمی‌شوند. به‌عنوان مثال در خزندهٔ موردبحث در این پست، برنامه از یک کانال به یک کانال دیگر می‌پرد و ۱۰ کانال اولیه که به بات داده شده در سه ماه تبدیل به ۹۰هزار کانال یکتا می‌شود!

اطلاعات کلی

خزنده در مدت اجرای سه‌ماههٔ خود، بیش از ۷۵هزار کانال فعال (تا زمان جمع‌آوری داده‌های ارائه‌شده) را کشف کرده و مورد بررسی قرار داده است. در این مدت بیش از سی‌میلیون پست تلگرامی، آنالیز و ۷۶۳۷۳ فایل apk استخراج شده است.

تلگرام = ارزش افزوده + فیشینگ و بدافزار + قمار + کپی!

به نظر شما چطور یک تبلیغ در یک زمان مشخص در هزاران کانال قرار می‌گیرد؟ گسترده‌ها شبکه‌های تبلیغاتی تلگرام هستند که تعداد زیادی کانال را تحت پوشش خود دارند. موضوع حتی از سطح گسترده‌ها نیز فراتر رفته و به اتحاد گسترده‌ها می‌رسد، جایی که در نهایت می‌توان تبلیغی را برای میلیون‌ها نفر ارسال کرد.

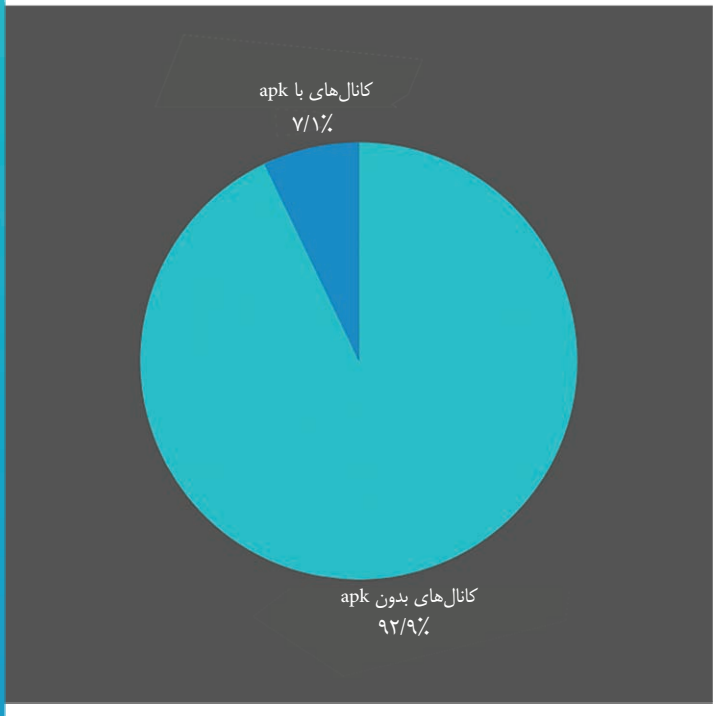
این گسترده‌ها گاهی با بستن چشم خود روی محتوای تبلیغ موجب می‌شوند یک نفر با سرمایهٔ هنگفت، تبلیغ درصد بالایی از این گسترده‌ها را خریده و در هزاران کانال تلگرامی پخش کند. ضریب نفوذ یک تبلیغ که بارها در کانال‌های دنبال‌شدهٔ یک کاربر تکرار شده بسیار بالاست و بدون توجه به محتوای آن، موجب باورپذیری بسیار زیاد در کاربر می‌شود.

تحلیل بر روی پست‌های متنی و چندرسانه‌ایِ کانال‌ها نشان می‌دهد حجم عظیمی از محتوای تلگرام کپی شده است؛ کپی‌هایی که گاهی در زیر یک دقیقه از منبع اصلی صورت می‌گیرد و در موارد بسیاری منبع آن‌ها توییتر بوده است. بر همین اساس، الگوهایی دیده شده که به نظر می‌رسد عده‌ای با شناسایی این نقاط کپی‌خور و تغذیهٔ محتوایی آن‌ها، سعی در کنترل افکار عمومی یا شایعه‌پراکنی دارند که در اینجا بیش از این به آن نمی‌پردازیم.

ارزش‌افزوده، پادشاه برنامه‌های اندرویدی تلگرام

خدمات ارزش‌افزوده[1] در ایران عموماً خدماتی هستند که با ارائهٔ یک سری خدمات، به صورت دوره‌ای از کاربر هزینه ای می‌گیرند. نحوهٔ پیاده‌سازی این سرویس‌ها در ایران معمولاً به این صورت است که در قبال ارائهٔ یک سری خدمات، از اعتبار سیم‌کارت کاربر روزانه مبلغی مانند ۵۰۰ تومان کم می‌شود. این سری خدمات سال‌هاست که در ایران ارائه می‌شوند و ظاهراً تا اینجای کار مشکلی وجود ندارد، اما مشکل از آن‌جا شروع می‌شود که چندین سال پیش سود کلان این پول‌ها توجه عدهٔ زیادی سودجو را به خود جلب کرد و شرکت‌هایی ایجاد شدند که با ارائهٔ خدمات صوری و بی‌ارزش به مردم و حتی خدمات یک‌بارمصرف، تا مدت‌ها از قربانیان روزانه و به طور نامحسوس پول کم می‌کردند. این جریان حتی تا جایی پیش رفت که برنامه‌هایی ایجاد شدند که بدون اطلاع کاربر، آن‌ها را عضو سرویس‌های ارزش‌افزوده کرده و تا مدت‌ها از مردم دزدی می‌کردند.

البته به‌مرور، فضای جولان‌دادن این شرکت‌ها محدود و محدودتر شد و در زمان اجرای این تحقیق، برنامه‌هایی با خدمات نسبتاً بی‌ارزش یا یک‌بارمصرف با تبلیغات زیاد، اقدام به عضویت مردم در این سرویس‌ها می‌کردند. با بسیاری از این عناوین آشنا هستید: چند گیگ اینترنت رایگان و ... .

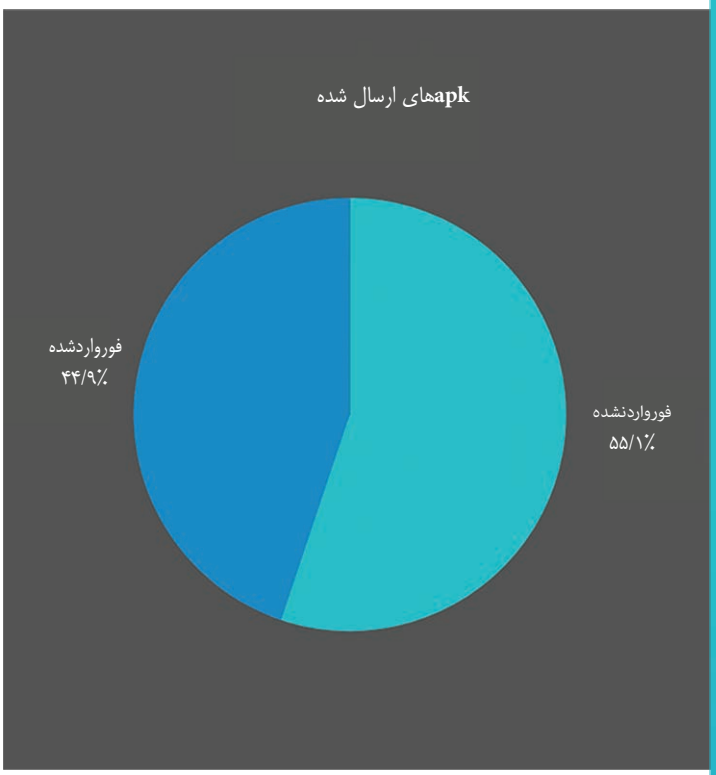


فقط حدود ۷ درصد از کانال‌های رصدشده دارای فایل apk بوده‌اند.

در بین تبلیغات تلگرامی، درصدی هم به تبلیغات فایل‌های نصبی اندروید (apk) اختصاص دارد. یکی از مهم‌ترین دلایل کم‌بودن تبلیغات apk ترس گسترده‌ها از انتشار بدافزار و عواقب آن است اما در بین همین درصد کم نیز موضوعات جالبی مشاهده شد.

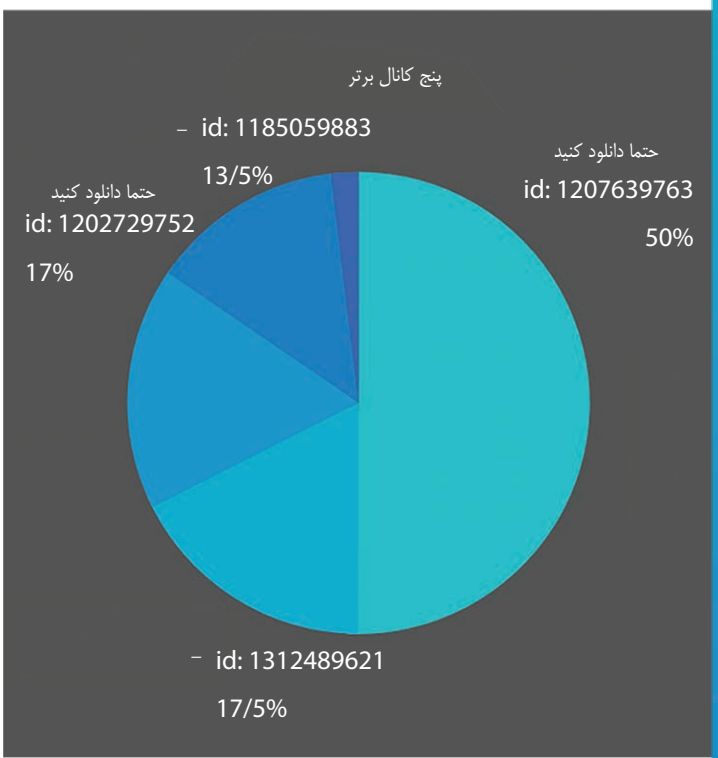
طبقِ اطلاعات جمع‌آوری‌شده، چهار کانال اول در زمینهٔ ارسال apk تماماً به تبلیغات ارزش افزوده اختصاص دارند که خصوصی (Private) هستند و تمام این فعالیت از طریق فوروارد‌کردن برنامه‌ها به کانال‌های دیگر صورت می‌گیرد! در واقع درصد بالایی از فایل‌های تبلیغ‌شده از کانال‌های خصوصی پخش می‌شوند.

۱- Value Added Services (VAS)



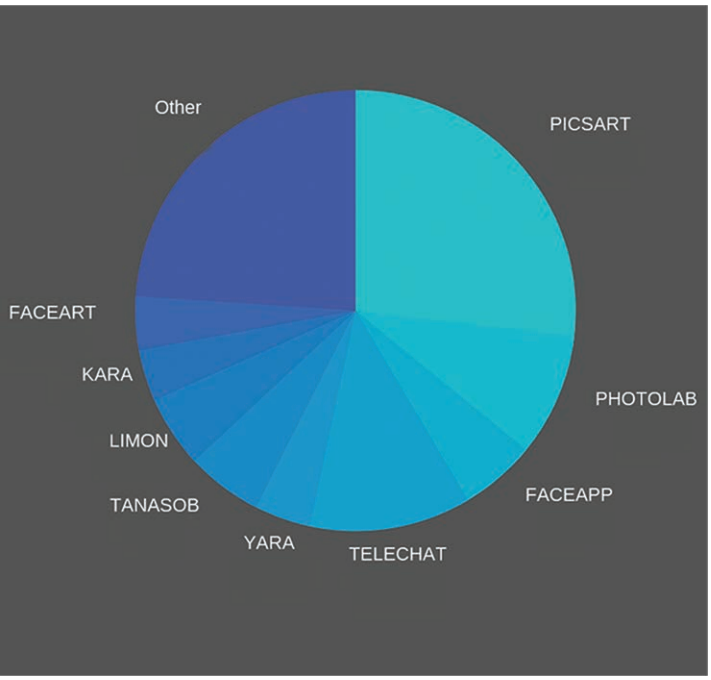
حدود ۴۵ درصد فایل‌های رصدشده فوروارد شده‌اند.

با دقیق‌ترشدن روی این شبکهٔ پخش برنامه‌های ارزش‌افزوده نکات جالبی مشخص شد. تقریباً تمامی این کانال‌ها خصوصی هستند. دو تا از کانال‌های ذکرشده نسخه‌های تکراری برنامه‌های خود را بارها با فایل‌های متفاوت از هم منتشر می‌کردند (احتمالاً به دلایل آماری و جلوگیری از رهگیری فایل‌ها) و اسم این کانال‌ها نیز بعضاً یکسان انتخاب شده تا امکان رهگیری و بررسی فعالیت آن‌ها محدود شود.



کانال‌های متفاوت، با برنامه‌های متفاوت، با اسم‌های مشابه! (پنج کانال برتر ارزش‌افزوده که چهار تا از آن‌ها، چهار تای اول در زمینهٔ پخش apk هستند.)

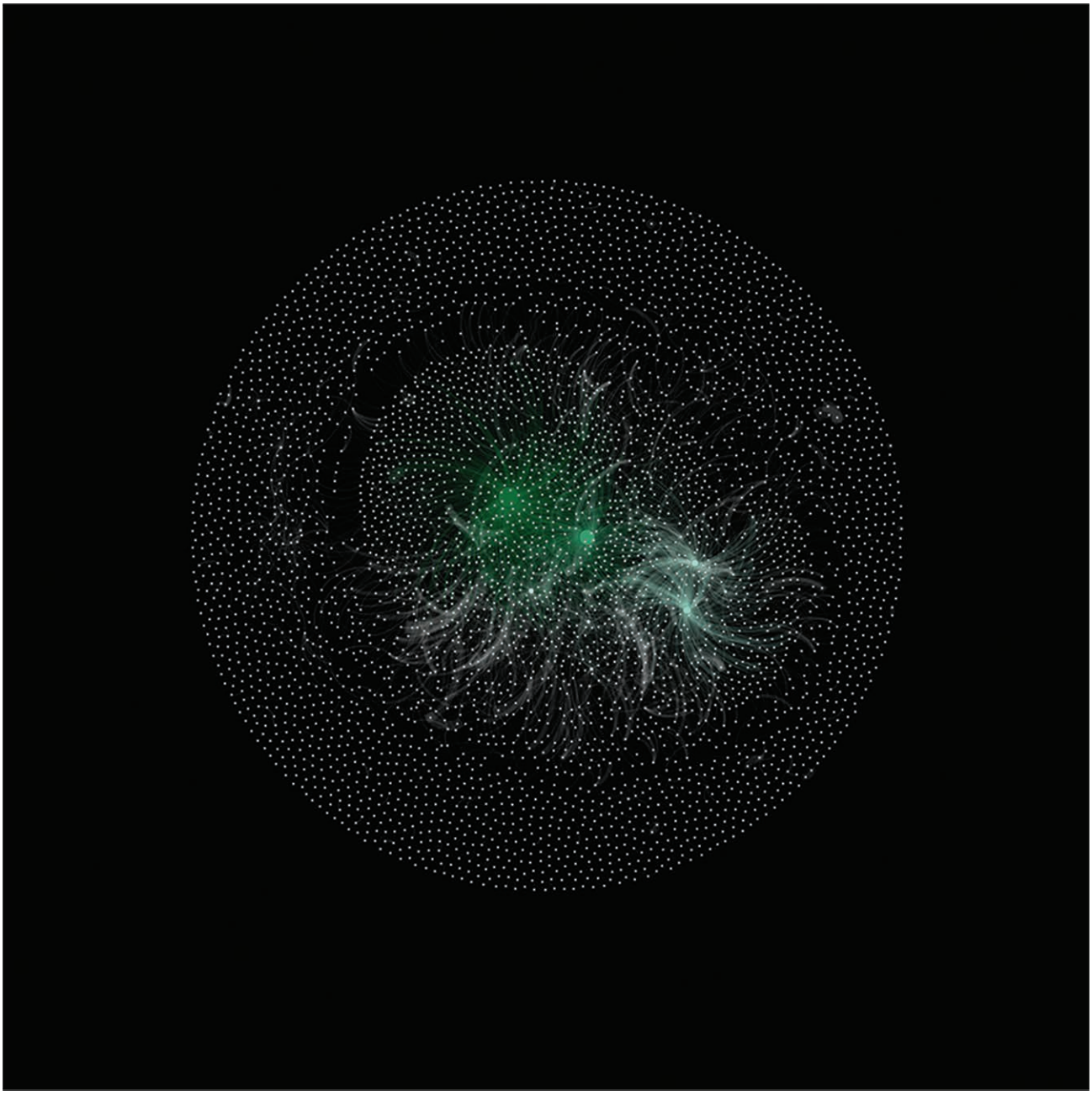
این کانال‌ها هرکدام لیست مجزایی از برنامه‌های ارزش‌افزوده را پخش می‌کردند که بعضی از آن‌ها در مدت کوتاهی تبلیغ شده و بعد از میان رفته‌اند. حتی بعضی از نسخه‌های بررسی‌شده، ابتدا کاربر را عضو سرویس کرده و بعد برنامهٔ اصلی را دانلود می‌کنند!



برنامه‌های تبلیغ‌شدهٔ این کانال‌ها (همگی ارزش‌افزوده)

بسیاری از برنامه‌های نام‌آشنای بالا، در واقع برنامه‌های اصلی نیستند و شرکت‌های ارزش‌افزوده با سوءاستفاده از شهرت نام این برنامه‌ها، برنامه‌های بی‌ارزشی را به همین نام ساخته‌اند و تبلیغ می‌کنند.

برنامه‌های ارزش‌افزوده بدون شک پادشاه برنامه‌های اندرویدی در تلگرام هستند؛ اما ارزش‌افزوده در تلگرام به برنامه‌ها محدود نمی‌شود بلکه فعالیت اصلی سرویس‌های ارزش‌افزوده مانند فعالیت آن‌ها در اینستاگرام بیشتر بر پایهٔ صفحه‌های وب و تبلیغاتی مثل اینترنت رایگان است که البته حجم تبلیغاتشان در تلگرام قابل‌مقایسه با حجم تبلیغاتشان در اینستاگرام نیست.



گراف توزیع فایل‌های apk در تلگرام (نقاط، نشانگر کانال‌ها هستند.)

فیشینگ و بدافزار

برنامه‌های فیشینگ یا کلاه‌برداری، برنامه‌هایی هستند که با جعل فعالیت ادعایی، قربانی را به سمت درگاه‌های بانکی تقلبی هدایت کرده و اطلاعات بانکی آن‌ها را به سرقت می‌برند. البته در زمان انتشار این مقاله و به لطف اجباری‌شدن رمز دوم پویا، این نوع کلاه‌برداری‌ها به‌مراتب کمتر شده‌اند.

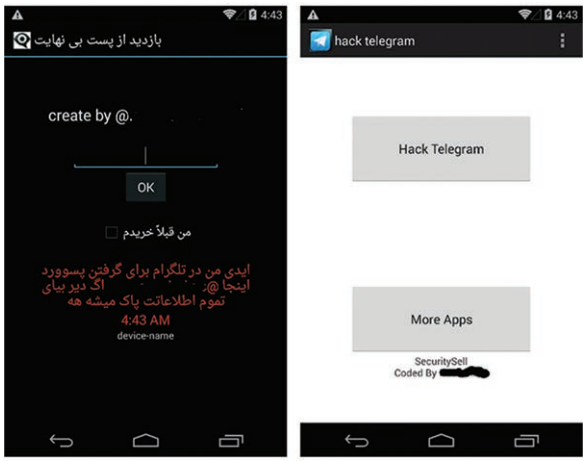
برخلاف برنامه‌های ارزش‌افزوده، بدافزارها و برنامه‌های فیشینگ تا حد امکان غیرمتمرکز بوده و گسترده‌ها یا تک‌کانال‌ها آن‌ها را به صورت پراکنده تبلیغ کرده‌اند. برنامه‌های فیشینگ را به طرز جالبی عموماً برنامه‌سازهای ایرانی ساخته‌اند که بدون نیاز به حتی یک خط برنامه‌نویسی به راحتی و صرفاً با طراحی چند منو، درگاه‌های جعلی را به خورد قربانی می‌دادند و از کارت بانکی او سرقت می‌کردند. در درجهٔ بعدی، بعضی نیز با کپی‌کردن و تغییر سورس‌های آماده، تروجان[1]هایی (بدافزارهای جاسوسی) را می‌ساختند.

همچنان شایع‌ترین نوع بدافزار محیط تلگرام در ایران، بدافزارهای Hiddad یا Hidden app هستند که با نصب‌شدن روی تلفن قربانی و گرفتن دسترسی، از دید کاربر مخفی شده و به تبلیغات آزاردهنده می‌پردازند.

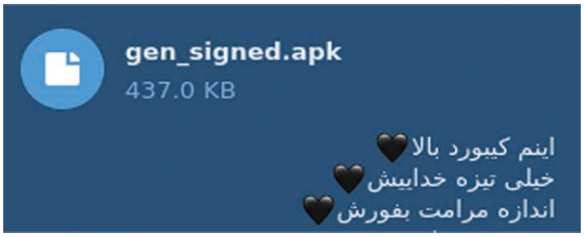
۱- Trojan

ایـن برنامـه بـا سوءاسـتفاده از اعتقـادات مذهبـی مـردم بـه آلوده‌سـازی آن‌هـا و نشـان‌دادن تبلیغـات آزاردهنـده و اجبـاری و نصـب اجبـاری می‌پرداخت. در طـی چندین ماه حدود ۱۳۰۰ بار در کانال‌های مختلف رصد شد.

در ایـن بیـن، بدافزارهـای جدی‌تـری هـم بـه صـورت محـدود در حـال پخـش هسـتند کـه عمومـاً هکرهـای روسـی و چینـی آن‌هـا را نوشـته‌اند. جالـب اینکـه خیلـی از ایـن برنامه‌هـا را کانال‌هـای هـک و ... منتشـر می‌کننـد و به‌راحتـی در دسـترس هرکسی قرار می‌دهند.



چـپ: باج‌افـزار به اسـم «بازدید پسـت». در سیسـتم‌عامل اندروید عمومـاً باج‌افزارها به راحتـی قابـل حـذف و بایپس[1] هسـتند. **راسـت:** ایـن بدافزار پـس از گرفتن دسترسـی به ریست‌فکتوری تلفن قربانی اقدام می‌کند.



برخـی از ایـن بدافزارهـا بـه صـورت آمـاده پخـش شـده و فقـط نیـاز بـه تغییـر چنـد پارامتـر در فایـل apk دارنـد تـا بدافـزار شـخصی شـما آمـاده شـود! (تصویـر یکـی از بدافزارهای پخش‌شده)

و امـا تلگرام‌هـای جعلـی نیـز شـدیداً فعـال بودنـد. بیـش از ۸۰۰ نسـخهٔ تلگـرام جعلـی بـا قابلیت‌هایـی ماننـد تبلیغـات اجبـاری و جاسوسـی کشـف شـدند کـه عمومـاً از کار افتاده‌انـد. عمـوم ایـن بدافزارهـا (تبلیغاتی‌هـا و نصب‌اجباری‌هـا) از سـرویس‌های پوش‌نوتیفیکیشـن[2] ایرانی برای فرستادن دستور به گوشی قربانی‌ها اسـتفاده می‌کنند و سـرویس‌های ایرانی پس از هشـدارهای بسـیار، همچنـان موفـق بـه سـامان‌دهی سیسـتم‌های خـود نشـده‌اند. سـرویس‌های پوش‌نوتیفیکیشـن وظیفـهٔ ارسـال نوتیفیکیشـن بـه کاربـران یـک برنامـه را دارنـد کـه گاهـی بـرای تبلیغـات مجـاز، گاهـی بـرای اطلاع‌رسـانی و البتـه بسـیاری از اوقـات نیـز برای تبلیغات این بدافزارها استفاده می‌شوند.

قمار و شرطبندی

بعیـد اسـت در تلگـرام یـا اینسـتاگرام فعـال باشـید و تبلیغات وسوسه‌کنندهٔ شرطبندی را ندیده باشید. طبق بررسی‌ها روی کمپین‌های تبلیغاتی شـرطبندی، هر چند وقت یک بار اسـم سـایت شرطبندی تبلیغ‌شده تغییر کرده اما دقیقاً با همان گسترده‌ها و الگوی فعالیـت، تبلیغـات صـورت گرفتـه اسـت. در واقـع بـه نظـر می‌رسـد یـک نفر/تیـم پشـت کمپیـن تبلیغاتـی تمـام ایـن سایت‌هاسـت یا حتی تمام این سـایت‌ها (که رصد شـده‌اند) زیر نظر یـک تیـم اجرایـی فعالیـت می‌کننـد. الگـوی تبلیغاتـی سـایت‌های قمـار بسـیار منظم‌تـر از باقـی تبلیغـات بـوده و از نظـر زمان‌بنـدی تبلیغات و بهره‌وری، حساب‌شده‌تر هستند.

جمع‌بندی

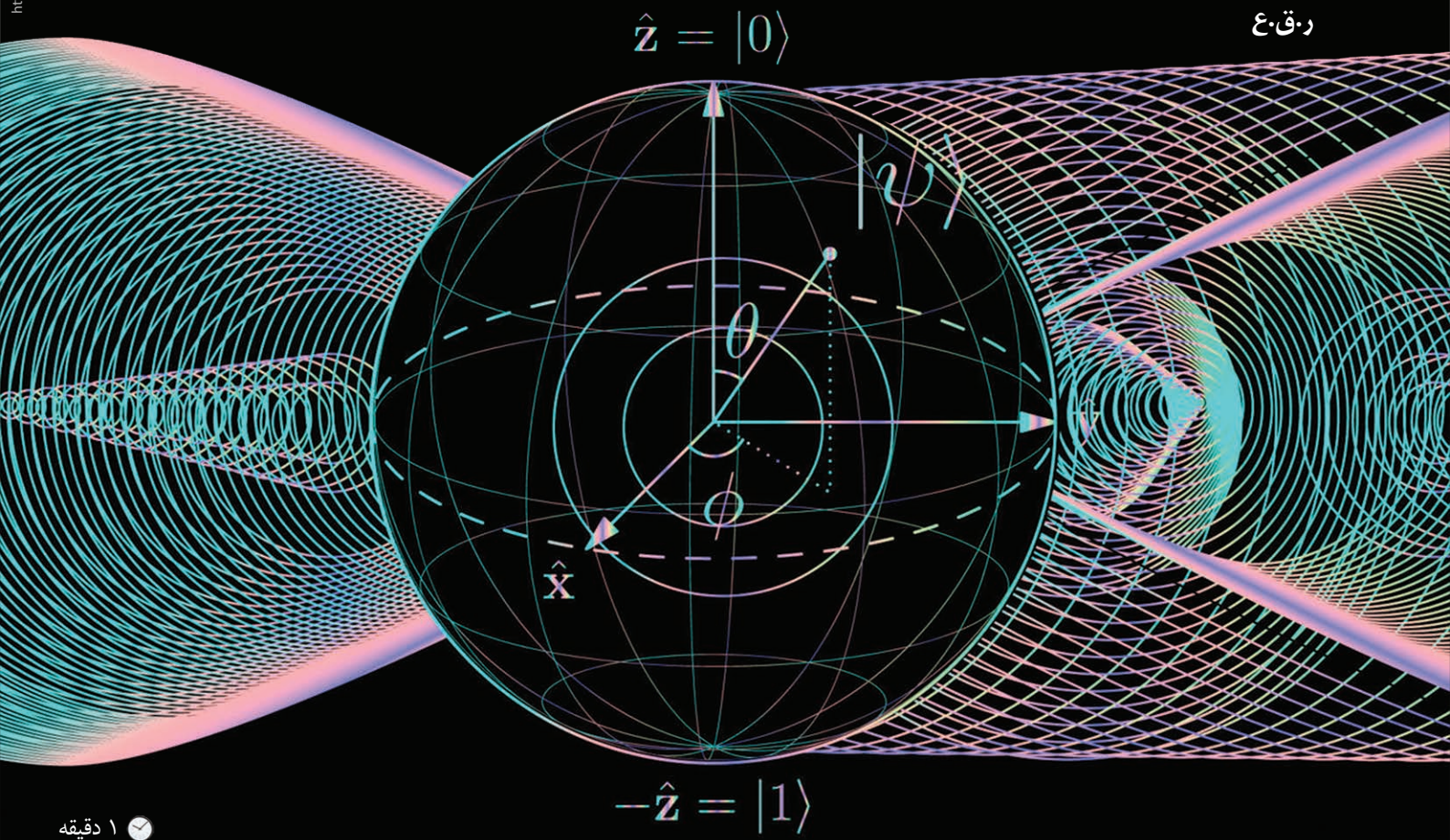
بـا مقایسـهٔ مـوارد گفته‌شـده مشـخصاً حجـم تبلیغـات ارزش‌افزوده (برنامـه و غیربرنامـه) بیشـتر از باقـی مـوارد ذکرشـده اسـت؛ بعـد از آن، تبلیغـات و فعالیـت سـایت‌های شـرطبندی قـرار دارد کـه حساب‌شـده‌تر عمـل می‌کنند و در آخر هم بدافزارها و فیشـینگ قـرار دارنـد که پراکنده‌تـر و مخفیانه‌تـر فعالیت می‌کنند. بـا توجه به آنالیزهـای دسـتی صورت‌پذیرفتـه روی تعـدادی از بدافزارهـای منتشرشـده، به سـختی می‌تـوان گفت بدافـزار یا حملهٔ پیشـرفته‌ای در بسـتر تلگـرام صـورت می‌گیـرد و عمـوم آلودگـی گسـترده از طریق تلگرام، مربوط به بدافزارهای تبلیغاتی ساده است.

تلگـرام حـالا پـس از سـال‌ها، بـه دلایلی مثـل فیلترینگ، بـا وجود پتانسـیل بسـیار بالایـی کـه در ایـن زمینـه دارد، جـای خـود را بـرای فعالیت‌هـای مخـرب بـه اینسـتاگرام داده اسـت. حتـی مهم‌تـر از آن، بعد از خاموش‌شـدن سـرورهای تلگـرام طلایی، تعداد تلگرام‌های جعلی جدید و در حال فعالیت به شـکل شـگفت‌آوری کم شـد. در نهایـت بایـد گفـت ایـن پـروژه در تمـام مـدت فعالیـت بـا امکانـات خیلـی کـم و هزینـهٔ شـخصی بنـده پیـش رفتـه امـا بـا ایـن وجـود، اطلاعـات خـام به‌دسـت‌آمده، پتانسـیل اسـتخراج داده‌های بسـیار جالب‌تری را دارند که متأسـفانه بـه دلایلـی مثـل کمبـود وقـت و امکانـات، تاکنـون صـورت نپذیرفته است.

۱- Bypass
۲- Push Notification

آیندهٔ پردازش‌های کامپیوتری

ر.ق.ع



۱ دقیقه

شواهد نشان می‌دهند که سرعت رشد و بهبود کامپیوترها در حال کاهش است و قانون مور[1] به پایان خود نزدیک می‌شود. طی ۵۰ سال اخیر، رشد خیره‌کننده و سرسام‌آور صنعت کامپیوتر و نیمه‌هادی‌ها، هر چند سال یک بار به مشکلی اساسی برخورد می‌کرد که با راه‌حل‌هایی هوشمندانه رفع می‌شدند و تقریباً هر ۱۰ سال نیز یک تکنولوژی نسبتاً انقلابی وارد صنعت نیمه‌هادی‌ها می‌شد ولی حالا واقعاً در حال نزدیک‌شدن به مرز غیرممکن‌ها هستیم.

تا زمان نگارش این مقاله، بالاترین سطح معماری مورداستفاده در پردازنده‌ها، معماری ۷نانومتری[2] است. البته بعضی از شرکت‌ها به صورت آزمایشی تراشه‌هایی با ترانزیستورهای ۵نانومتری هم تولید می‌کنند ولی پیش‌بینی‌ها حاکی از آن است که حد توانایی کوچک‌کردن ترانزیستورها (البته با صرفهٔ اقتصادی!)، ۳ نانومتر است[3].

پس شیوه‌ای که ۵۰ سال جواب داده بود (کوچک‌کردن ترانزیستورها) دیگر جواب نخواهد داد و باید به دنبال جایگزین‌هایی اساسی بود. بعضی از این جایگزین‌ها هم نه در همهٔ مسائل بلکه در حل مسائل خاصی به کار می‌آیند. در هر صورت در این که کامپیوترهای قرن‌های آینده با انواع امروزی تفاوت فاحشی خواهند داشت، شکی نیست و شاید اصلاً هیچ‌کدام از تکنولوژی‌هایی که امروز به عنوان تکنولوژی‌های نوظهور و انقلابی مطرح هستند، آیندهٔ سیستم‌های پردازشی نباشند بلکه آینده از آن فناوری‌هایی باشد که هنوز حتی ابداع نشده‌اند! ولی بدون شک بسیار هیجان‌انگیز خواهد بود...

در شماره‌های مختلف و در وبلاگ آرایه به آدرس **arraymag.ir** نگاهی خواهیم انداخت به تکنولوژی‌هایی که پتانسیل ایجاد تغییری بنیادی در شیوهٔ پردازش و صنعت کامپیوتر دارند.

در این شماره، «مسئلهٔ گراف همیلتنی در یک قاشق آب‌نمک!» را بخوانید.

۱- گوردون مور، یکی از بنیانگذاران اینتل، این قانون را این‌گونه بیان کرده است: «می‌توان تعداد ترانزیستورها را در یک مساحت ثابت از تراشه، هر ۱۸ الی ۲۴ ماه، دو برابر کرد.»

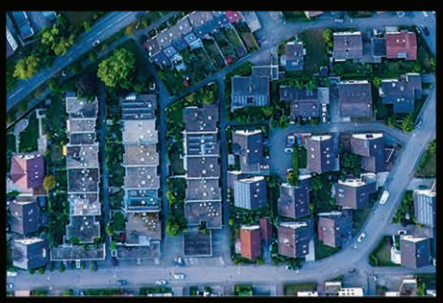
۲- هر نانومتر، یک میلیاردم متر است.

۳- این در صورتی است که اندازهٔ یک اتم سیلیکون مورداستفاده برای ساخت ترانزیستورها تنها ۰/۲۲ نانومتر است. یعنی ترانزیستوری تنها به طول تقریباً ۱۴ اتم!

مسئلهٔ گراف همیلتنی در یک قاشق آب‌نمک!

راضیه زارع

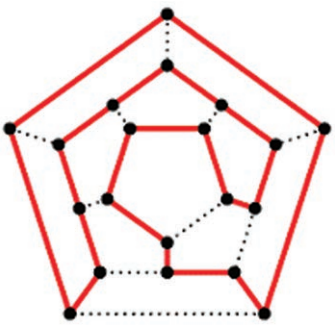
۶ دقیقه



در سدهٔ ۱۸ میلادی، ویلیام همیلتون[۱]، ریاضی‌دان و ستاره‌شناس ایرلندی، مسئله‌ای مطرح کرد که در آن باید برای گره‌های یک گراف، مسیری را پیدا کرد که از گره آغازین گراف شروع شود و در گره پایانی آن خاتمه یابد؛ به شرط آنکه از تمام گره‌های گراف، یک و تنها یک بار عبور کند. از مسیرهای همیلتنی برای حل بسیاری از مسائل دنیای واقعی استفاده می‌شود. این گراف‌ها در نظریهٔ بازی‌ها، گرافیک و بینایی کامپیوتر و رباتیک کاربرد ویژه‌ای دارند.

مسئلهٔ فروشندهٔ دوره‌گرد یکی از مشهورترین انواع این مسائل است. در این مسئله تعدادی شهر و هزینهٔ رفتن مستقیم از هر یک به دیگری داده شده و کم‌هزینه‌ترین مسیری که از یک شهر شروع شود و از تمامی شهرها دقیقاً یک بار عبور کند و به شهر شروع بازگردد، مطلوب است.

این مسئله جزو مسائل سخت NP[۲] محسوب می‌شود.



مسیر قرمز رنگ مداری همیلتنی در یک گراف را نشان می‌دهد.

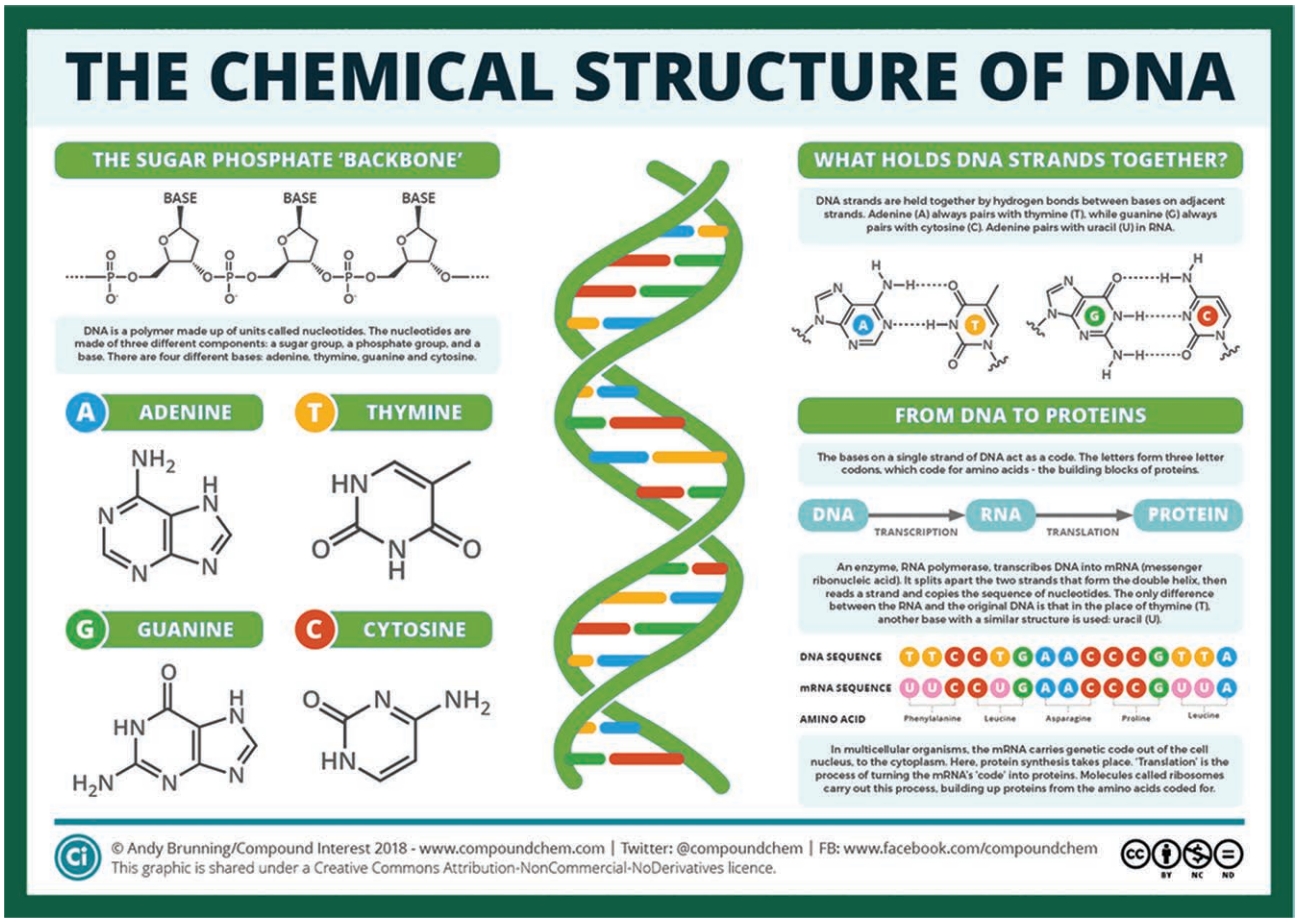
در سال ۱۹۹۴، لئونارد آدِلمَن[۳]، دانشمند علوم کامپیوتر، با ساخت رشته‌های دی‌ان‌ای در آزمایشگاه و قراردادن آن‌ها در لولهٔ آزمایش حاوی آب‌نمک، تلاش کرد مسئلهٔ فروشندهٔ دوره‌گرد مدار همیلتنی را حل کند.

این آزمایش انقلابی در دنیای تکنولوژی ایجاد کرد که منجر به ظهور مفهوم دی‌ان‌ای‌رایانه‌ها شد!

۱- William Hamilton

۲- Nondeterministic Polynomial: مسائلی که الگوریتم بهینه و قابل‌اجرا در زمان معقول (زمان چندجمله‌ای برحسب اندازهٔ ورودی) برای آن‌ها یافت نشده است.

۳- Leonard Adleman



رایانش دی‌ان‌ای مفهومی را معرفی می‌کند که در آن به جای تراشه‌های سیلیکونی، مولکول‌های دی‌ان‌ای محلی برای ذخیره‌سازی داده‌ها و اجرای محاسبات منطقی و ریاضی هستند. در این رایانه‌ها مجموعه‌ای از رشته‌های دی‌ان‌ای، به طور مشخصی با یکدیگر ترکیب می‌شوند تا پاسخ برخی از مسئله‌ها را پیدا کنند. موضوع رایانش دی‌ان‌ای بحثی بسیار پیچیده است و در این مقاله تا حد امکان تلاش می‌کنیم به ساده‌ترین بیان ممکن به آن بپردازیم.

قبل از اینکه با داستان آدلمن و چگونگی سازوکار این رایانه‌ها آشنا شویم، بد نیست کمی راجع به ساختار دی‌ان‌ای بدانیم.

ساختمان دی‌ان‌ای

دی‌ان‌ای یک ساختار دو رشته‌ای متشکل از ۴ نوکلئوتید (گونه‌ای از مولکول‌های ترکیبات آلی) است. این نوکلئوتیدها آدنین(A)، گوانین(G)، سیتوزین (C) و تیمین (T) نامیده می‌شوند. این ۴ نوکلئوتید با تشکیل پیوند، به شکل دو دنبالهٔ خطی، ساختمان دی‌ان‌ای را می‌سازند. البته برای تشکیل مارپیچ‌های دوگانهٔ دی‌ان‌ای، A فقط با T و C فقط با G تشکیل پیوند می‌دهند. بنابراین، هر رشتهٔ دی‌ان‌ای یک مکمل مشخص دارد که به ازای هر نوکلئوتید متناظر جفت‌شوندهٔ آن نوکلئوتید وجود دارد.

اگر در مجموعهٔ جوابی که کار می‌کنیم، رشتهٔ مکمل یک رشته موجود باشد، این دو رشته با هم جفت می‌شوند و ساختمان مارپیچ دی‌ان‌ای را می‌سازند.

به طور مثال نوکلئوتید A از یک رشتهٔ دی‌ان‌ای با نوکلئوتید مکمل آن یعنی T در رشته‌ای دیگر می‌تواند تشکیل پیوند دهد اما با نوکلئوتیدهای C و G جفت نمی‌شود. حالا اگر مکمل تمام نوکلئوتیدهای یک رشته در رشتهٔ دیگر یافت شوند، آن دو رشته با هم جفت می‌شوند و ساختمان مارپیچ به وجود می‌آید.

راه‌حل آدلمن برای مسئلهٔ مسیر همیلتنی با کمک دی‌ان‌ای‌رایانه

آدلمن گرافی همیلتنی را مورد بررسی قرار داد که متشکل از ۷ گره و ۱۴ یال جهت‌دار بود. یعنی میان هر دو گره یک مسیر مستقیم برای رفت و یک مسیر مستقیم برای برگشت وجود دارد.

آدلمن برای نمایش نام شهرها (گره‌های گراف) از دنباله‌ای ۸تایی متشکل از نوکلئوتیدهایی تصادفی که در شرایط آزمایشگاهی با روش نوترکیبی ژنتیک بر رشته‌های دی‌ان‌ای قرار گرفتند، استفاده کرد. برای مثال برای شهر (گره) A دنبالهٔ ACTTGCAG، شهر (گره) B دنبالهٔ TCGGACTG و شهر (گره) C دنبالهٔ

GGCTATGT را تعریف کرد که نیمهٔ اول دنباله، به عنوان بخش اول نام شهر و نیمهٔ دوم دنباله، بخش دوم نام شهر معرفی شد. به طور مثال برای شهر A، ACTT نیمهٔ اول نام شهر A و GCAG نیمهٔ دوم نام شهر A است. اهمیت تقسیم نام شهر به دو نیمه را در ادامه خواهید دید. با ترکیب نیمهٔ دوم شهر مبدأ با نیمهٔ اول شهر مقصد نیز، مسیر میان آن دو شهر (یال) مشخص می‌شود. به طور مثال، مسیر میان دو شهر A و B (A مبدأ و B مقصد، یال AB) به صورت GCAGTCGG (GCAG نیمهٔ دوم شهر (گره) مبدأ A و TCGG نیمهٔ اول شهر مقصد یعنی گره B است) و مسیر (یال) BC به صورت ACTGGGCT است. همان طور که گفته شد هر رشتهٔ دی‌ان‌ای، مکمل خود را دارد. آدلمن رشتهٔ مکمل نام شهرها را نیز در شرایط آزمایشگاهی تولید کرد. او $۱۰^{۱۴}$ مولکول از رشته‌های متفاوت را در یک لولهٔ آزمایش قرار داد. برای نزدیک‌کردن شرایط لولهٔ آزمایش به سلول موجود زنده مقداری آب‌نمک به لوله افزود (نمک سدیم یکی از عناصر اصلی مایع اطراف سلول‌ها است.) آدلمن ۱ ثانیه بعد، در محلولی با حجم کمتر از یک‌پانزدهم قاشق چای‌خوری، جواب مسئله را داشت!

تا اینجا، گره‌ها و یال‌ها (مسیر میان دو شهر) ساخته شده‌اند. برای یافتن مسیر همیلتنی، باید شروع به حرکت از مسیرهای مختلف کنیم یا به عبارت دیگر در هنگام کار با رشته‌های دی‌ان‌ای، رشته‌های مختلف را به یکدیگر وصل کنیم تا در نهایت از همهٔ گره‌ها یا همان شهرها عبور کنیم.

آدلمن چگونه به جواب رسید؟

با توجه به شیوهٔ کدکردن، مثلاً مسیر (یال) میان دو شهر A و B (رشتهٔ GCAGTCGG) و مکمل شهر (گره) B (رشتهٔ AGCCTGAC) ممکن است به طور اتفاقی با هم روبرو شوند. بر اساس طراحی کدها، رشتهٔ اول (یال AB) به TCGG ختم و رشتهٔ دوم (مکمل شهر B) با AGCC آغاز می‌شود؛ از آنجا که نوکلئوتیدهای این دو بخش مکمل یکدیگرند، به هم خواهند چسبید (و رشتهٔ طولانی‌تر GCAGTCGG AGCCTGAC تشکیل خواهد شد.) اگر نتیجهٔ حاصل با رشتهٔ حاوی مسیر BC (ACTGGGCT) رودررو شود، این رشته نیز به مجموعهٔ رشتهٔ حاصل از اتصال قبل، خواهد چسبید؛ چون انتهای رشتهٔ حاصل از اتصال قبل یعنی TGAC مکمل شروع رشتهٔ BC (ACTG) است. به همین ترتیب، طول ترکیبات

لئونارد آدلمن

با چسبیدن مسیرها به هم با استفاده از مکمل نام شهرها افزایش می‌یابد. در نهایت لولهٔ آزمایش سرشار از رشته‌هایی خواهد بود، که مسیرهای کدشدهٔ تصادفی میان شهرهای مختلف هستند. از آنجا که تعداد مولکول‌های اولیه بسیار زیاد بود و تعداد شهرها نیز بسیار کم است، می‌توان گفت که تمام مسیرهای ممکن میان شهرها (گره‌ها) ساخته شده و با یک اطمینان تقریبی حداقل یکی از این مسیرها، همان مسیر همیلتنی موردِنظر است.

متأسفانه همان طور که آدلمن مسیر همیلتنی را در لولهٔ آزمایش داشت، ده‌ها تریلیون مسیر دیگر نیز در آزمایش وجود داشتند که همیلتنی نبودند و آدلمن باید آن‌ها را جداسازی می‌کرد. غربالگری رشته‌های دی‌ان‌ای از یکدیگر نیز، طی فرآیندهایی جالب با به‌کارگیری خواص زیستی شیمیایی رشته‌های دی‌ان‌ای رخ داد، که بحث پیرامون آن از حوصلهٔ مطلب خارج است[۱].

در نهایت آدلمن موفق به جداسازی رشتهٔ دی‌ان‌ای حاوی مسیر همیلتنی، از رشته‌های نامرتبط شد و این آزمایش موفق، سرآغازی برای پژوهش در زمینهٔ رایانش دی‌ان‌ای شد.

۱- جهت مطالعه در این زمینه روش Polymerase Chain Reaction و پل الکتروفورز را جست‌وجو کنید.

در ادامه به بحث راجع به مفهوم کلی رایانش دی‌ان‌ای، که با آزمایش آدلمن شکل گرفت، مزایای استفاده از این نوع رایانه‌ها و پیشرفت‌ها و چالش‌های آن می‌پردازیم.

رایانش دی‌ان‌ای

در رایانه‌هایی که از رایانش دی‌ان‌ای استفاده می‌کنند، به جای استفاده از سیگنال الکتریکی برای نمایش یک بیت اطلاعات، از خواص شیمیایی مولکول‌های دی‌ان‌ای استفاده می‌شود. درواقع الفبای ۴کاراکتری نوکلئوتیدها، جایگرین الفبای باینری شده است. دی‌ان‌ای‌رایانه از نوکلئوتیدهای آدنین(A)، گوانین(G)، سیتوزین (C) و تیمین (T) به جای صفر و یک متداول در الفبای باینری استفاده می‌کند. ورودی الگوریتم، یک یا چند رشته مولکول دی‌ان‌ای است و رایانش در فضای یک لولهٔ آزمایش یا اسلاید شیشه‌ای صورت می‌پذیرد. این رایانش در واقع آزمایشی بر روی مولکول‌های دی‌ان‌ای است؛ آزمایش‌هایی از قبیل مرتب‌سازی رشته‌ها بر اساس طول آن‌ها یا برش بخشی از رشته‌ها که حاوی ترکیب یا پیوند خاصی از نوکلئوتیدها هستند. با اعمال این تغییرات رشتهٔ نهایی در واقع به عنوان رشتهٔ خروجی معرفی می‌شود. برای مثال در آزمایش آدلمن، این تغییرات، همان اتصال رشته‌های مکمل به یکدیگر برای تشکیل مسیرهای مختلف و جداسازی رشته‌ها از رشته‌های نامربوط بود. خروجی برنامه هم رشتهٔ حاوی مسیر همیلتنی بود.

چرا دی‌ان‌ای‌رایانه؟

مهم‌ترین دلیل برای انتخاب دی‌ان‌ای‌رایانه‌ها، ظرفیت بسیار بالایی است که این رایانه‌ها در مقایسه با رایانه‌های سیلیکونی برای ذخیرهٔ اطلاعات دارند. ذخیرهٔ این حجم بالای اطلاعات در فضایی کم، به معنی چگالی فوق‌العاده بالای این رایانه‌هاست. ۱ بیت در دی‌ان‌ای به اندازهٔ یک نانومتر مکعب فضا اشغال می‌کند در حالی که در حافظه‌های سخت‌افزاری موجود، ۱ بیت را می‌توان در 10^{12} نانومتر مکعب ذخیره کرد.

از دلایل دیگر می‌توان به دردسترس‌بودن همیشگی منابع دی‌ان‌ای اشاره کرد. به عبارتی تا زمانی که موجود زنده در جهان وجود دارد می‌توان رایانه ساخت!

این عرضهٔ وسیع دی‌ان‌ای قیمت آن را بسیار ارزان کرده است.

بر خلاف مواد سمی که برای ساخت ریزپردازنده‌های سیلیکونی استفاده می‌شوند، زیست‌تراشه‌های دی‌ان‌ای می‌توانند به صورت تمیز ساخته شوند.

یکی از مزایای جالب دی‌ان‌ای‌رایانه‌ها قابلیت اجرای عملیات‌های موازی است. یک لولهٔ آزمایش می‌تواند حاوی ۱۰ تریلیون رشتهٔ دی‌ان‌ای باشد؛ هر رشته یک محاسبهٔ منطقی یا ریاضی را پردازش کند و در یک زمان، تنها در یک لوله آزمایش، ۱۰ تریلیون محاسبه پردازش شود!

پیشرفت‌ها

علی‌رغم نوپا بودن دی‌ان‌ای‌رایانه‌ها دستاوردهای جالبی در این زمینه حاصل شده است. از ذخیره‌سازی اطلاعات در سلول‌های موجودات زنده (DNA Storage)، تا ساخت گیت‌های منطقی عملگر بر رشته‌های DNA.

چگالی بالای ذخیره‌سازی اطلاعات در رشته‌های دی‌ان‌ای و قابلیت موازی بودن فعالیت‌ها در آن‌ها، رایانش دی‌ان‌ای را تبدیل به یک زمینهٔ تحقیقاتی داغ در قرن بیست‌ویکم کرده است.

در این مقاله سعی شد به طور خلاصه و ساده به مقدمات رایانش دی‌ان‌ای پرداخته شود. مسلماً بحث پیرامون این موضوع بسیار وسیع است و در این حجم نمی‌گنجد. جهت مطالعهٔ بیشتر در این زمینه می‌توانید به منابع زیر مراجعه کنید.

منابع

1- Bonsor, Kevin. "How DNA Computers Will Work". Retrieved from computer.howstuffworks.com

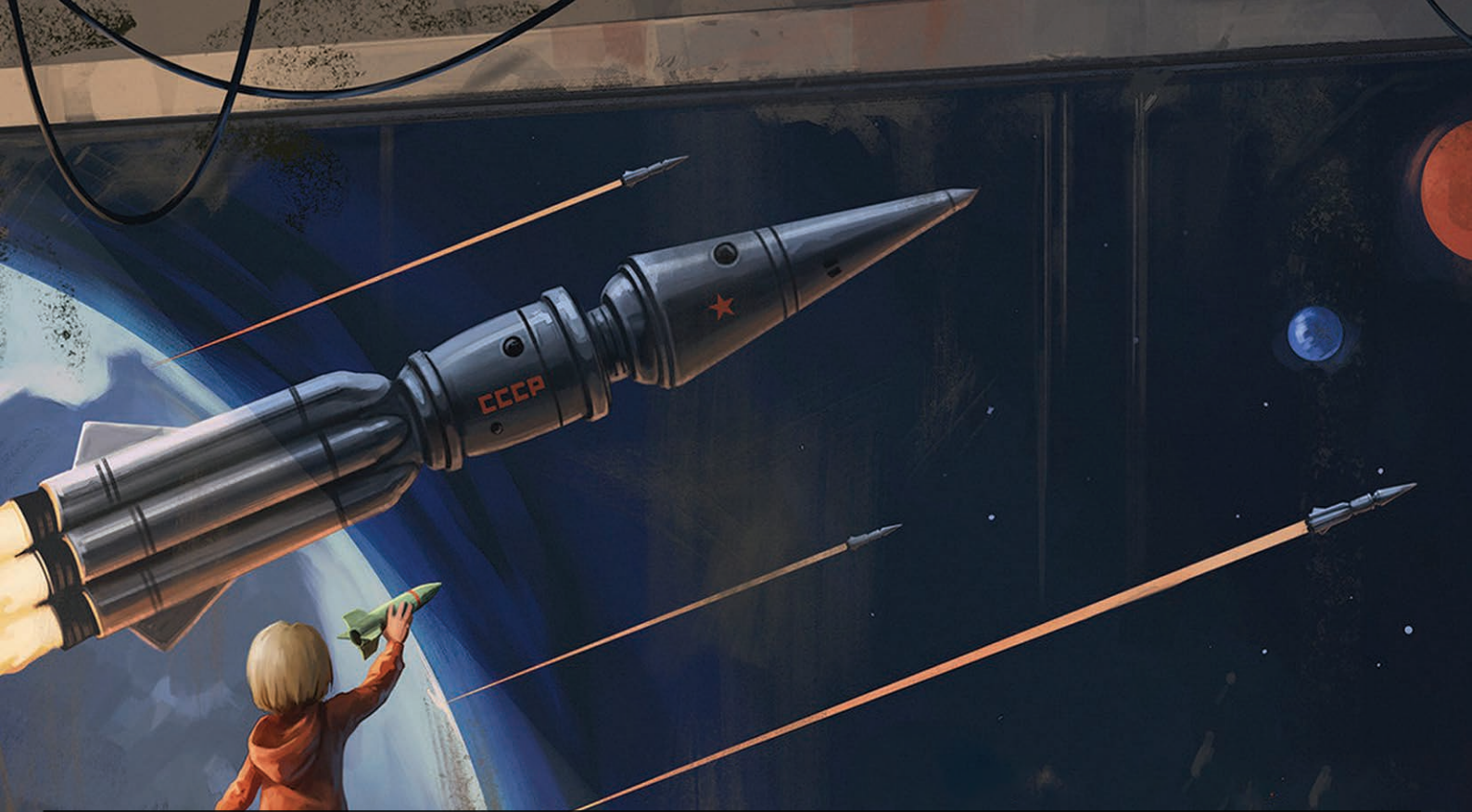
2- Adleman, Leonard M. "Computing with DNA", Scientific American, August, 1998.

3- Shouse, Ben." First Automated DNA Computer Boots Up", May,2001.

4- Wang,Fei &others. "Implementing digital computing with DNA-based switching circuits", NatureCommunications, January 2020.

عکس:

درویش متولی، محمد. گراف همیلتونی به زبان ساده برگرفته از مجلهٔ فرادرس ۱۴فروردین۹۹



از بمب دست‌ساز تا کارابین

کوثر شمس

۶ دقیقه

استارت‌آپ را شرکت نوپا ترجمه کرده‌اند و برداشت غلطی که گاهی دیده می‌شود آن است که معمولاً زمینهٔ کار استارت‌آپ، مرتبط با تکنولوژی یا زمینه‌هایی از این دست است. در حالی که عنصر مشترک استارت‌آپ‌ها خلاقیت و داشتن ایده های نو است؛ خلاقیتی که توانسته است مشکل را به هوشمندانه‌ترین روش به راه‌حل وصل کند. در این مقاله سعی داریم به یکی از استارت‌آپ‌های موفق ایرانی بپردازیم؛ چراکه شاید شرایط و مشکلاتشان برای ما قابل‌لمس‌تر شود.

اگر اسم حسین توحیدی را بدون پسوند اختراعش در اینترنت جست‌وجو کنیم، در وهلهٔ اول ممکن است شک کنیم که آیا اسم او را درست نوشته‌ایم؟ اصلاً اسمش را درست به خاطر سپرده‌ایم؟ چون «حسین توحیدی»هایی که در صفحهٔ اول می‌آیند هیچ ارتباطی به خالق یک ایدهٔ نو یا مدیر یک استارت‌آپ ندارند ولی پسوند «کارابین»، تگی است که می‌تواند «حسین توحیدی» مدنظر ما را از بین تودهٔ مطالب پیدا کند.

حسین توحیدی متولد ۱۳۶۲ در تهران است ولی تا قبل از شروع دورهٔ راهنمایی به دلیل شغل پدرش زندگی در شهرهای مختلفی را تجربه کرده است. فرازوفرودهای زندگی حسین، از همان کودکی شروع شد. قبل از اتمام دورهٔ ابتدایی، دو بار ضربه‌مغزی شده بود: یک بار با دوچرخه و یک بار هم وقتی عرض خانه را می‌دوید با گیجگاه زمین خورد. به قدری شرایطش بعد از ضربه‌مغزی دوم عجیب و ناپایدار بود که پدر و مادرش مجبور بودند هر شب که می‌خوابید هر چند ساعت بیدارش کنند و اسمش را بپرسند تا مبادا خوابش عمیق شود؛ چون خواب عمیق ممکن بود باعث به کما رفتنش بشود. شیطنت‌های حسین متناسب با سن و سالش بیشتر و بیشتر می‌شد تا جایی که در دورهٔ دبیرستان یک بار تصمیم گرفت با راه انداختن آتش‌بازی کوچکی در کلاس زبان، حال و هوای همه را که از «ریپیت افتر می»های دبیر زبان خسته شده بودند، عوض کند و یک بمب دست‌ساز در میز معلم کار بگذارد!

از لحاظ درسی، می‌توان گفت تقریباً هیچ‌وقت جزو دانش‌آموزان نمونه نبوده است و در دورهٔ راهنمایی بین ۹۳ نفر دانش‌آموز، نفر نودم بوده است ولی این مسئله ناشی از بهرهٔ هوشی کم نبود و روشش این بود که کمبود نمره‌های هنر و ادبیات را با ریاضی و علوم جبران کند.

آشنایی با یکی از فارغ‌التحصیلان دبیرستانشان که دانشجوی فیزیک بود، باب علاقهٔ حسین به فیزیک را هم گشود و سال ۱۳۸۰، با رتبهٔ ۲۲۲۵ کنکور، ادامهٔ تحصیل در رشتهٔ فیزیک دانشگاه تهران را انتخاب کرد. دو ترم اول را با شروعی طوفانی آغاز کرد تا حدی که ترم ۲، ۲۳ واحد را با معدل ۱۹ پشت سر گذاشت. یکه‌تازی او به قدری مشهود شده بود که دکتر علی محمدی او را ملاک و معیار برای زمان امتحان هایش قرار داده بود و هر وقت حسین برگه‌اش را تحویل می‌داد یعنی وقت استاندارد به پایان رسیده بود و بقیه فقط ۱۵ دقیقهٔ دیگر زمان داشتند. تصور حسین از فیزیک، حرکت روی لبه‌های علمی بود که قرار است دنیا را تکان دهد و به همین علت تصمیم داشت تحصیل در مقاطع بالاتر را در کشورهای دیگر ادامه دهد که این امکان برایش بیشتر دردسترس باشد و به همین علت هم بود که در دانشگاه درس را به همه چیز ترجیح داده بود.

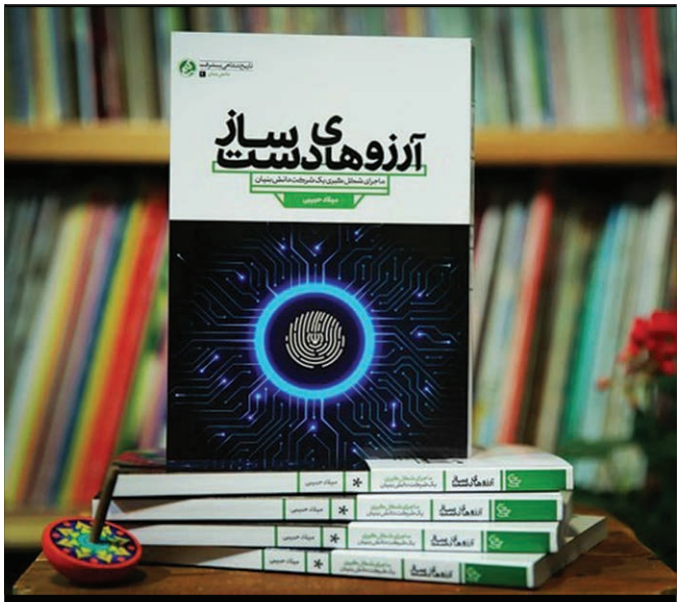
همه چیز خوب و بی‌دردسر پیش می‌رفت تا وقتی یکی از اساتید خاطره‌ای از فایمن[1] (که یکی از برندگان جایزه نوبل بود) نقل کرد و همه چیز عوض شد و توحیدی در ایران ماندگار شد. خود او این خاطره را این‌طور بیان می‌کند: «فایمن روزی برای سخنرانی به دانشگاه آرژانتین دعوت می‌شود. در حین سخنرانی، از دانشجوها می‌پرسد: «شما چرا همان کاری را می‌کنید که ما در آمریکا می‌کنیم؟ وضعیت کشور ما طوری است که باید روی لبهٔ علم حرکت کنیم، اما شما که کشورتان مشکلات متعددی دارد، بروید و مشکلات خودتان را حل کنید؛ نه این که به علومی بپردازید که شاید صد سال آینده هم به دردتان نخورد.»

همین کلیدواژهٔ «مشکلات» ورق را برگرداند. از آن روز، دید حسین به خودش و حتی فیزیک تغییر کرد. تصمیمش این شد که از آن به بعد به‌جای سقوط در درهٔ مطالب تئوری (که آخر آن دره، هیچ چیزی در انتظارش نبود به جز تکه‌کاغذی به اسم مدرک) و شاهد رخوت حاکم بر دانشگاه بودن، به دنبال این برود که مشکلاتی را که می‌بیند، پیدا کند و برای آن‌ها راه‌حل ارائه دهد. تصمیم گرفت برعکس اکثر هم‌دوره‌ای‌هایش که بعد از اتمام تحصیل در ایران یا خارج از کشور به دنبال روشن‌کردن گوشه‌های تاریک فیزیک روی کاغذ بودند، دست به کاری بزند که نتیجه‌اش را برای مردمش ببینند. برای متنوع‌ترشدن نگرش‌ها و استفاده از نظرات مختلف، تصمیم گرفت این بحث را به گروه‌های دانشجویی‌شان بکشاند. ذهن‌های خلاقشان داشت کم‌کم از زیر انبوه کاغذ و جزوه‌ها جوانه می‌زد و اولین ثمره‌اش شد ایدهٔ «بانک همراه»، که دستگاهی باشد برای آنکه مردم بتوانند با آن پرداخت‌های آنلاین و آفلاین داشته باشند. شاید این ایده برای الان که هرکدام از ما حداقل یک کارت بانکی داریم و با ستاره‌مربع‌ها در کوتاه‌ترین زمان مبالغ موردنظرمان را پرداخت می‌کنیم، جذابیتی نداشته باشد ولی باید توجه داشت که برای سال های ۸۲ و ۸۳ ایدهٔ درخشانی بوده است چراکه کارت‌های بانکی حدود ۴ سال بعد یعنی سال ۸۶ تازه رواج پیدا کردند.

به‌دلیل حساسیت بالای زیرساخت‌های اقتصادی و بی‌اعتمادی و ترس از ریسک‌کردن سیستم بانکی، با «بانک همراه» نتوانستند راه به جایی ببرند. ایدهٔ بعدی که مطرح شد طرحی بود به اسم «چشم مردم» که در واقع شد سرآغاز کار پلیس‌های نامحسوس و دوربین‌های ثبت تخلفی که در جاده‌ها می‌بینیم. جرقهٔ ایده وقتی در ذهنشان زده شد که دوستشان، برادرش را در یک تصادف رانندگی از دست داد ولی نمی‌توانستند اثبات کنند که طرف مقابل در تصادف مقصر بوده است. در ابتدای کار ایده‌شان این بود که هر خودرویی بتواند تخلف خودروی دیگر را ثبت کند و دیگر رعایت قوانین محدود به زمان حضور و دیدن شخص مأمور پلیس نباشد. آن‌ها نمی‌توانستند با رابطه‌های محاسبهٔ سرعتِ فیزیک، مچ ماشین‌هایی را که سرعت مجاز نداشتند، بگیرند و پلاکشان را بخوانند پس کم‌کم به سمت یادگیری پردازش تصویر[2] و بینایی ماشین[3] رفتند تا بتوانند خودشان ایده‌شان را پیاده‌سازی کند. سال ۸۵ برای اینکه به رسمیت شناخته بشوند و بتوانند در مناقصه‌ها شرکت کنند، شرکت «پویا فناوران کوثر» را با ۵ عضو ثبت کردند. حالا کم‌کم روی سختِ خلاق و دغدغه‌مندبودن خودش را به حسین نشان می‌داد و به قدری وقتش صرف ایده‌شان شد و از فضای درس‌های اصلیش دور شد که به هر روشی متوسل شد تا به دلیل افت تحصیلی از دانشگاه اخراجش نکنند! دیگر کارنامهٔ تحصیلی‌اش هم ردیف ۱۹ و ۲۰ ترم‌های اول و دوم نبود بلکه ۲ ترم مشروطی

۱- Richard Feynman
۲- Image Processing
۳- Machine Vision

داشت و برای فرار از سربازی، ۲ ترم هم مرخصی گرفته بود! بالاخره «چشم مردم» را (که حالا شده بود «دوربین سرعت‌سنج و ثبت تخلفات خودرویی» و در واقع همان دوربینی بود که روی ماشین‌های پلیس نامحسوس نصب می‌شد)، با ناجا پیش بردند و در نهایت سودش برایشان شد هیچ! در واقع بعد از تسویه با بقیهٔ اعضای مهمان تیم، تنها تفاوتشان با قبل از شروع پروژه، یک سابقهٔ کار بود و یک شرکت که روی کاغذ ثبت شده بود؛ به‌اضافهٔ یک چک ۵۰هزارتومانی که جایزه‌ای بود که در طرح جوان خوارزمی سال ۸۷ برنده شده بودند و آنقدر کم بود که تنها کاربردش، این بود که یادگاری نگهش دارند. اما نتیجهٔ کارشان چیزی بود که هیچ‌کدام از مدیرانی که نمی‌خواستند ریسک کارکردن با آن‌ها را بپذیرند، توقعش را نداشتند: آن‌ها توانستند دوربین‌هایی را بسازند که نه‌تنها در ایران نمونه‌اش را کسی نساخته بود، بلکه تا آن زمان (سال ۸۹)، در جهان نمونه‌ای با این سطح از دقت در پردازش تصاویر وجود نداشت! ایدهٔ بعدی‌شان ثابت‌کردن همان دوربین‌ها در جاده‌ها بود که نتیجه‌اش «دوربین‌های ثبت تخلف جاده‌ای» بود که امروزه در بیشتر بزرگ‌راه‌ها و آزادراه‌ها دیده می‌شود. بعد از اتمام این پروژه، وضعیتشان مجدداً شد همان چیزی که قبل بود و شرایط اقتصادی شرکت به قدری سخت شد که تصمیم گرفتند روند کاریشان را از پروژه‌های صنعتی به پروژه‌های کوچک ولی پرسودتر تغییر بدهند که یک نمونه‌اش ساخت دستگاهی بود که خیارهای یک مزرعه را برای فروش در بازار داخلی و صادرات دسته‌بندی می‌کرد و در سبدهای جداگانه می‌ریخت. با پیاده‌سازی «سورتر خیار»، شرکت توانست کم‌کم به مرحلهٔ سودآوری برسد و آن‌ها بتوانند به پروژه‌هایی که دوست داشتند فکر کنند؛ چون از این جا به بعد عملاً سرمایه‌ای داشتند و دیگر نیازی به کارکردن با سازمان‌های دولتی نبود و دستشان بازتر می‌شد. اولین پروژه‌ای که با این سَبک داشتند، تولید دوربین های embedded بود. تصمیم گرفته بودند با تجاربی که داشتند این بار دوربین‌ها را با تمام نرم‌افزارها و سخت‌افزارهایی که لازم بود آماده کنند و در جعبه‌ای شُسته‌رُفته، در اختیار مشتری قرار بدهند تا وابسته به نیاز خودش از آن به صورت ثابت یا متحرک استفاده کند. تصمیم بر این شد که نام اختراعشان را «کارابین» بگذارند که ترکیبی بود از «car» و «دوربین». بالاخره در سال ۱۳۹۵،گواهی‌نامه‌های لازم، مثل گواهی‌نامهٔ CE، را برای کارابین گرفتند و در همان سال برندهٔ مقام نخست جشنوارهٔ بین‌المللی خوارزمی شدند که جایزهٔ ۱۵سکه‌ای آن، برخلاف جایزهٔ پنجاه‌هزارتومانی جوان خوارزمی، برایشان کارآمدتر بود. امروز کارابین‌های توحیدی و تیمش در ۸۰۰ نقطهٔ ایران نصب شده‌اند و علاوه بر آن توانسته‌اند ۳۰ طرح تحقیقاتی را نیز به پایان برسانند و تولیدات دیگری را نیز بر مبنای بینایی ماشین و پردازش تصویر (مثل پلاک‌خوان پارکینگی یا سیستم تخمین حجم بار خودروهای سنگین در حین حرکت)، به بازار عرضه کنند. ضمن اینکه توانایی و استعدادشان در بسیاری از زمینه‌های راداری، موشکی و ... به کمک نهادهای مختلف آمده است و اکنون نام شرکتشان جزو شرکت‌های پیمانکاری تأییدصلاحیت‌شدهٔ وزارت نفت، وزارت نیرو و سازمان راهداری و حمل‌ونقل جاده‌ای کشور است.



این مقاله با استفاده از کتاب «آرزوهای دست‌ساز»، نوشتهٔ میلاد حبیبی، نوشته شده است که جلد اول از مجموعهٔ کتاب‌های «تاریخ شفاهی پیشرفت» انتشارات «راه یار» است که سال ۱۳۹۸ به چاپ رسیده است و با استقبال خوب دانشجویان رشته‌های مهندسی و فنی‌وحرفه‌ای مواجه شده است. خود نویسنده علت را این طور بیان می‌کند که «روایتِ پیشرفت و تجربهٔ زیسته‌ای از جنبش دانشجویی» و «فعالِ دانشجویی بودن اعضای این شرکت» باعث شده است که با استقبال خوب جوانان و دانشجویان و دانش‌آموزان (به ویژه در رشته‌های فنی و مهندسی و فنی‌وحرفه ای) مواجه شود. چرا که مخاطبان جوان و دانشجو دراین کتاب می‌خوانند که چگونه تعدادی دانشجو برخلاف فضای رخوت‌انگیز و نامطلوب برخی دانشگاه‌ها، می‌توانند اهداف و آرمان‌های خودشان را دنبال کنند و به موفقیت برسند.

حکایت همچنان باقیست! داستان بمب دست‌ساز، ماجرای مفصل ساخت «چشم مردم» و روایت‌های خالقان کارابین از مشکلاتشان را، می‌توانید در وبلاگ آرایه به آدرس arraymag.ir بخوانید.

کالبدشکافی کنسول‌بازی PS4

محسن طهماسبی

برای فهم بهتر این مقاله بهتر است آشنایی اولیه‌ای با کِرنل، ممـوری و امنیـت داشـته باشـید.

۶ دقیقه

از ابتدای ظهور کنسول‌ها و پلتفرم‌های بازی‌های ویدیویی همواره یکی از مخاطبان فعال و دردسرساز آن‌ها، هکرها و گیک‌های کنجکاوی بودند که در طی سال‌ها تاریخ بازی‌های ویدیویی، کشفیات و پیشرفت‌های بسیاری را (در کنار خراب‌کاری‌هاشان) به ارمغان آورده‌اند.

کنسول پلی‌استیشن ۴ یکی از پرطرفدارترین پلتفرم‌های بازی در دنیاست که مانند پیشینیان خود، از کنجکاوی هکرها در امان نمانده است.

نسل قبلی کنسول‌های بازی به لطف ضعف‌های امنیتی سخت‌افزاری و هکرها، در مدت زمان نسبتاً کوتاهی به اصطلاح جیل‌بریک[۱] شدند و در کشورهایی مثل ایران به دلیل عدم امکان خرید بازی‌های اورجینال و قیمت آن‌ها، بسیار مورداستقبال قرار گرفتند.

اما با روی‌کارآمدن نسل هشتم کنسول‌ها و درس‌گرفتن شرکت‌ها از تجربیات قبلی، هک کنسول‌ها و دست‌کاری آن‌ها حالا بیش از هر زمان دیگری سخت شده است؛ با این حال گاهی اشتباهاتی کوچک باعث پیداشدن روزنه‌ای برای نفوذ و بررسی قلب این پلتفرم‌های بسیار امن و بسته شده‌اند. یکی از این تلاش‌ها، تلاش CTurt (نام مستعار)، محقق امنیتی مایکروسافت بود که در فریمور[۲] معروف ۱.۷۶، موجب نفوذ کامل و دستیابی به بالاترین سطح دسترسی گردید که در ادامه نگاهی اجمالی به آن خواهیم انداخت.

امنیت در PS4

کنسول نسل هشتمی سونی از پردازنده‌ای با معماری مرسوم X86_64 استفاده می‌کند که به مدد شهرتش، تحقیقات بسیاری بر روی آن صورت گرفته است و ابزارهای فراوانی برای تحقیق روی آن وجود دارد.

سونی و مایکروسافت با درس‌گرفتن از اشتباهات خود در سطح سخت‌افزار (به خصوص JTAG)، این بار با امن‌سازی و محدودسازی هرچه بیشتر پل‌های ارتباطی سخت‌افزار، راه را برای این‌چنین تلاش‌ها و نفوذهایی تا حد بسیار موفقی بسته‌اند.

سیستم‌عامل PS4 که Orbis OS نام دارد، بر پایهٔ FreeBSD 9 توسعه یافته است و از جهات بسیاری به این سیستم‌عامل شباهت دارد که می‌تواند سبب شناخت نسبی و کلی ما نسبت به درون ابعاد تاریک PS4 شود. اما شناخت ما نسبت به درون سیستم‌عامل PS4 محدود به FreeBSD و معماری پردازندهٔ آن نیست. طیف وسیعی از ابزارها و برنامه‌های متن‌باز[۳] در PS4 استفاده شده‌اند که از جملهٔ آن‌ها می‌توان به Webkit اشاره کرد، یک موتور رندر[۴] برای مرورگرهای وب که آن را اپل توسعه داده است و در محصولات اپل نیز کاربرد وسیعی دارد.

۱- Jailbreak
۲- Firmware
۳- Open Source
۴- rendering engine

اما Webkit به دلیل پیچیدگی‌های نالازم و متن‌بازبودن، باگ‌های امنیتی نسبتاً زیادی را در سال‌های اخیر از خود به ثبت رسانده، از جمله CVE-2012-3748 که در نسخه‌هایی از Webkit وجود دارند که PS4 نیز در فریمور ۱.۷۶ از آن استفاده نموده است.

ورود به دنیای تاریک PS4

این باگ امنیتی که در یک متد جاوا اسکریپت قابل سوءاستفاده است، اجازهٔ دسترسی به بخش‌های غیرمجاز حافظه را به هکر می‌دهد، اما برخلاف سالیان گذشته که دستیابی به یک باگ Memory Overflow به معنی دسترسی سطح بالا در قربانی بود، در دنیای امروز شیوه‌هایی امنیتی مورد استفاده قرار می‌گیرند که کار را برای هکرها بسیار سخت می‌کنند.

یکی از این راهکارهای امنیتی، Data Execution Protection یا DEP است. این شیوهٔ امنیتی در سطح کرنل، مجوزها و دسترسی‌های نواحی مختلف حافظه را به شیوهٔ خاصی کنترل می‌کند که در نتیجهٔ آن، بخش‌هایی از حافظه که قابل‌نوشتن هستند مجاز به اجراشدن نیستند و بخش‌هایی که قابل اجراشدن هستند، مجوز بازنوشته‌شدن را ندارند. در نتیجه نمی‌توان پس از دستیابی به یک باگ Memory Overflow به راحتی یک پیلود را در حافظهٔ قربانی لود و اجرا کرد، گرچه می‌توان کدهایی که در حال حاضر در نواحی قابل‌اجرای حافظه لود شده‌اند را اجرا کرد.

بازی با گجت ها: ROP[1]

یکی از راه‌های دورزدن این مکانیزم امنیتی، شیوه‌ای به نام ROP است. در این روش، هکر با آنالیز کدهای لودشده در حافظه، دستورات اسمبلی موردنیاز خود را به گونه‌ای که بلافاصله پس از آن‌ها دستور ret آمده، پیدا می‌کند و با تشکیل یک زنجیره از این دستورات، پیلود موردنظر خود را پیاده‌سازی می‌کند. به هرکدام از این دستورات، یک گجت گفته می‌شود.

با استفاده از باگ امنیتی مذکور و تکنیک ROP، می‌توان تا حدی به اجرای کدهای موردنظر پرداخت و سیستم‌عامل را کاوش کرد. با کاوش‌های بیشتر و بررسی بخش‌هایی از حافظهٔ لودشده، نتایج جالبی از نیمهٔ تاریک سیستم‌عامل PS4 آشکار شد؛ از جمله لیست system callها که شباهت بسیار زیادی به نمونه‌های مشابه در FreeBSD دارد.

پس از روزها دست‌وپنجه‌نرم‌کردن با محدودیت‌ها و مشکلات برقراری ارتباط با کرنل از مرورگر وب، سرانجام لیست دقیق‌تری از system callها به دست آمد. به جز system callهای استاندارد FreeBSD، چندین system call ناشناس جدید را هم سونی پیاده‌سازی کرده است.

با بهره‌گیری از ابزارهای ذکرشده امکان اجرای طیف وسیعی از عملیات‌ها و کاوش‌ها فراهم شد. اما این ماجراجویی خیلی زود به بن‌بست مهمی خورد: Jailها.

زندان‌ها یا Jailها مکانیزم استاندارد FreeBSD برای Sandboxing و ایزوله‌سازی و از قابلیت‌های مهم این سیستم‌عامل هستند.

با وجود این مانع جدی، دسترسی پردازهٔ میزبان حمله (Webkit) به‌شدت در یک محیط ایزوله و جعلی محدود می‌شود. تلاش برای پیداکردن و خواندن فایل‌هایی که مطمئناً روی PS4 وجود دارند با شکست مواجه شد و این دلیلی بر وجود Sandboxing بود، چرا که سیستم‌عامل یک File System جعلی با حداقل فایل‌ها را به پردازه نشان می‌دهد.

ارتقای دسترسی و نفوذ به کرنل

باگ CVE-2014-9322 معروف به BADIRET یک باگ خطرناک در کرنل است که اولین بار در لینوکس کشف شد و مدتی بعد مشخص گردید که روی FreeBSD نیز قابلیت پیاده‌سازی دارد. این باگ به هکر امکان dosکردن سیستم‌عامل و فراتر از آن، توانایی ارتقای سطح دسترسی را می‌دهد. این باگ ابتدا در قالب CVE-2014-9090 کشف شد که باعث kernel panic و crashکردن سیستم می‌شد.

کرنل لینوکس با مدیریت اشتباه double faultهای مربوط به SS (Stack Segment) در معماری X86، باعث می‌شد در شرایط خاصی که اکسپلویت ایجاد کرده و با به‌وجودآمدن faultهای حساب‌شده، با اجرای یک system call به نام modify_ldt، کرنل panic کرده و سیستم کاملاً از کار بیفتد.

در ابتدا این باگ صرفاً به dosکردن سیستم‌عامل محدود بود و به همین جهت توجه خاصی به آن نمی‌شد اما پس از مدتی و بررسی بیشتر متخصصین، مشخص شد با استفاده از همین اِشکال در هندل‌کردن کرنل، می‌توان سطح دسترسی به کرنل را ارتقا داد که منجر به ثبت‌شدن باگ CVE-2014-9322 شد.

۱- Return-oreinted Programming

پیاده‌سازی اکسپلویت این باگ دشواری‌های فراوانی داشت و به همین دلیل مجدداً موردتوجه قرار نگرفت و سرانجام با منتشرشدن یک گزارش تخصصی دربارهٔ این باگ، توجه متخصصین را جلب کرد.

یکی از مهم‌ترین دشواری‌های پیاده‌سازی اکسپلویت این باگ، رفتار پردازشگرهای معماری X86 در مواجهه با triple fault است. در صورت اشتباه اکسپلویت و رخدادن triple fault، پردازشگر، فارغ از وضعیت سیستم نسبت به راه‌اندازی مجدد اقدام می‌کند.

از طرفی، در اکسپلویت‌های کرنل به‌خصوص ارتقای سطح دسترسی، بازگرداندن وضعیت کرنل (مانند وضعیت رجیسترها، جداول و ...) چالش مهمی محسوب می‌شود و هرگونه خطا در این عمل باعث panic در کرنل می‌شود.

به همین جهت و به‌دلیل درصد خطا در عملکرد هر بار اجرای اکسپلویت، توسعهٔ آن و فراهم‌سازی بستر اجرا امری مهم محسوب می‌شود.

با تطابق نحوهٔ اجرای حمله بر روی لینوکس با سیستم عامل FreeBSD و پورت‌کردن اکسپلویت این حمله به FreeBSD، مشخص شد کرنل این ورژن از فریمور PS4 نیز به این حملات آسیب‌پذیر است.

با اجرای این حمله و دست‌کاری سطح دسترسی پردازه و غیرفعال‌کردن Jail، بالاخره و بعد از چالش‌های فراوان دسترسی نسبتاً کاملی به نیمهٔ تاریک PS4 فراهم شد و این اولین باری بود که دسترسی مستقیم به کرنل Orbis OS ممکن شد.

پس از نفوذ

سرانجام و پس از نفوذ موفقیت‌آمیز با سطح دسترسی کرنل، محیط بسیار مناسب‌تری برای ماجراجویی در سیستم‌عامل PS4 فراهم شد. هکر پس از بازیابی وضعیت کرنل و اجرای موفق اکسپلویت، دسترسی بسیار وسیعی به کنترل های سیستم‌عامل از جمله مکانیزم‌های امنیتی و محدودکننده پیدا می‌کرد.

از جملهٔ آن‌ها فعال‌کردن درگاه UART و اتصال مستقیم سخت‌افزاری به کنسول سیستم‌عامل و همچنین غیرفعال‌سازی انواع مکانیزم‌های امنیتی مانند Jailing و Sandboxها و در نهایت، تغییر سطح دسترسی پردازهٔ میزبان برای کاوش در Userland بود. نتیجهٔ دسترسی‌های بالا، نگاهی جزئی و دقیق برای اولین بار به File system واقعی PS4 و کاوش سیستم‌عامل و ماژول‌های آن بود اما محدود به این موضوع نشد.

یکی از تفریحات و چالش‌های بسیار فنی هکرها پس از نفوذ به یک سیستم بسته مانند PS4، اجرای سیستم‌عاملی جدای از سیستم‌عامل اصلی روی دستگاه است که معمولاً تلاش‌ها در جهت بوت‌کردن لینوکس بر روی پلتفرم هدف است.

قبل و بعد از این نفوذ، تلاش‌های بسیاری برای بوت‌کردن لینوکس روی PS4 صورت گرفته که طیف وسیعی از روش‌ها را برای دست‌یابی به این هدف شامل می‌شود، تلاشی که در صورت موفقیت کامل آن، با توجه به قدرت سخت‌افزاری بالای PS4 می‌تواند بستر بسیار مناسبی برای بازی‌های کپی و بدون لایسنس باشد.

سخن پایانی

عموم محققینی که روی چنین تکنیک‌ها و نفوذهایی کار می‌کنند علاقه‌ای به Jailbreak کردن یا به اصطلاح، کپی‌خورکردن کنسول ندارند و به همین دلیل، بخش‌های مهم و بسیاری از جزئیات تلاش‌های آن‌ها بر عموم مخفی می‌ماند یا پس از سال‌ها عمومی می‌شود.

این حمله یا به اصطلاح Exploit chain از آن جهت حائز اهمیت است که به خوبی، یک ماجراجویی و کاوش در یک پلتفرم بسیار بسته را به علاقه‌مندان نشان می‌دهد. آنالیز و روشن‌سازی نقاط تاریک این پلتفرم بسته با حداقل دسترسی‌ها و پیداکردن مسیری برای ارتقای دسترسی، زنجیره‌ای از اقدامات بسیار مهم هوشمندانه است که می‌تواند الگوی خوبی برای علاقه‌مندان این حوزه باشد.

باگ‌هایی مانند BADIRET و باگ اشاره‌شده در Webkit، موجب توسعهٔ مکانیزم‌های جدیدتر امنیتی شده که با محدودکردن دسترسی‌ها و دامنهٔ اجرای پردازه‌های جانبی، سعی در جلوگیری از اجرای حمله حتی در صورت وجود باگ دارند.

باید منتظر بود و دید که آیا راهکارهای امنیتی جدید می‌توانند جلوی ماجراجویی هکرها را بگیرند؟

منبع

Hacking the PS4: Introduction to PS4's security, and userland ROP, Userland code execution, Kernel exploitation

https://cturt.github.io/ps4.html

۱فروردین۹۹

دردنیای کامپیوتر ساعت‌چنداست؟

نگاهی به اثرات متقابل ویروس کرونا و دنیای کامپیوتر و تکنولوژی

سیدمحمدحسین هاشمی

۷ دقیقه

امروز دیگر صحبت دربارهٔ ویروس کرونا بحث جدیدی نیست. کلیدواژه‌های کرونا، قرنطینه، ماسک و ... کلماتی هستند که هر روز به گوشمان می‌خورند. اثر چنین بیماری همه‌گیری را همه احساس کرده‌ایم اما این روزها برای غول‌های تکنولوژی دنیا چگونه می‌گذرد؟ کرونا چطور روند تولید و توزیع کالاهای دیجیتال را تحت تاثیر قرار داده است؟ تکنولوژی و علم کامپیوتر چگونه می‌توانند به مقابله با این بیماری برخیزند؟

در چه حالیم؟

شیوع یک بیماری ویروسی همه‌گیر مانند کرونا مساوی است با محدودشدن فعالیت‌های اجتماعی و کارهایی که نیاز به تجمع افراد دارند و این یعنی تعطیلی کارخانه‌های تولید انبوه مانند صنایع تولید سخت‌افزار یا ابزارهای دیجیتالی. فاکس‌کان[1] که بزرگ‌ترین تولیدکنندهٔ قطعات الکترونیکی در دنیا و شرکتی با ۴۶ سال سابقه است هم در مقابل شیوع کرونا تسلیم شده است و مدتی پس از شیوع کرونا تمام خطوط تولید خود را تعطیل کرد. با وجود آنکه بعد از مدتی این شرکت دوباره کار خود را با بخشی از کارگران و خطوط تولید خود از سر گرفت اما اعلام کرد مدتی طولانی زمان خواهد برد تا به توان تولیدی کامل خود برسد. جالب است که این کارخانهٔ بزرگ تولید محصولات دیجیتال، از مدتی پیش بخشی از خطوط تولید خود را به تولید ماسک اختصاص داده است. نمایندگی‌های فروش و خدمات پس‌ازفروش کارخانه‌های بزرگ ازجمله اپل هم برای چند هفته در سراسر دنیا تعطیل بودند. بعضی از آن‌ها هنوز هم به طور کامل تعطیل هستند.

بیایید کمی عمیق‌تر به موضوع نگاه کنیم. شرکت‌های تولید سخت‌افزار یا ابزارهای هوشمندی مثل تلفن‌های همراه، تبلت‌ها یا رایانه‌های شخصی از رَویهٔ خاصی در تولید استفاده می‌کنند که «تولید به‌هنگام»[2] نامیده می‌شود. این اصطلاح یعنی برنامه‌ریزی کارخانه به شکلی صورت می‌گیرد که همواره کمترین تعداد قطعات خام و محصول تولیدشده در انبارهای کارخانه موجود باشد؛ دلیل اصلی آن هم کاهش هزینه‌ها و مشکلات انبارداری در درازمدت است. این روش با وجود داشتن مزایای زیاد، در مواردی مثل شیوع بیماری‌های فراگیر و تعطیلی‌های اجباری، بسیار آسیب‌پذیر است و این به این دلیل است که موجودی انبارهای کارخانه‌های تولیدی بسیاری از محصولات دیجیتالی، بسیار کمتر از چیزی است که ممکن است تصور کنیم. مشکل به همین جا ختم نمی‌شود و وقتی جدی‌تر به نظر می‌رسد که بدانیم برای مثال یک کارخانهٔ تولید تلفن همراه با دهها کارخانهٔ تولیدکنندهٔ

۱– Foxconn
۲– Just-In-Time Manufacturing

قطعات تلفن همراه در ارتباط است؛ بنابراین شروع به کار آن کارخانه مستلزم شروع مجدد تولید کارخانه‌های تولید قطعات است. ویروس کرونا فقط رَویه‌های تولید و توزیع محصولات دیجیتال را دچار اختلال نکرده است. گوگل در میانه‌های اسفند ۹۸، به دلیل شیوع این ویروس، کنفرانس I/O 2020 را که قرار بود بین ۲۳ تا ۲۵ اردیبهشت ۹۹ برگزار شود، لغو کرد. البته گوگل صرفاً کنفرانس حضوری را لغو کرده است و ممکن است این کنفرانس را به صورت آنلاین برگزار کند. پیش از این هم نمایشگاه MWC (بزرگ‌ترین نمایشگاه موبایلی که همه‌ساله در شهر بارسلون برگزار می‌شود) و کنفرانس F8 فیس‌بوک هم لغو شده بودند.

عادت می‌کنیم

اما این همهٔ ماجرا نیست و زندگی هنوز ادامه دارد. انسان وفق‌دادن خود با شرایط را خوب بلد است. بسیاری از شرکت‌های بزرگ تکنولوژی (مثل خیلی از کسب‌وکارهای دیگر)، با فراهم‌کردن بسترهای دورکاری برای کارمندانشان سعی کرده‌اند شرایطشان را بهبود بخشند. در راستای کمک به همین امر، گوگل و مایکروسافت قابلیت‌های غیررایگان نرم‌افزارهای Hangout Meets و Teams را برای مدتی رایگان کرده‌اند. البته شکی نیست که این رایگان‌کردن می‌تواند تبلیغی هم برای این نرم‌افزارها باشد. در همین بین، اپل از جدیدترین آیفون SE خود رونمایی کرد. همچنین چندی پیش سایت بلومبرگ اعلام کرد آیفون ۱۲ بدون تأخیر راهی بازار خواهد شد (هرچند که خبرهای ضدونقیضی دراین‌باره شنیده می‌شود.) شیائومی هم به عنوان یک شرکت چینی، مدتی قبل از تلفن همراه و مچ‌بند هوشمند جدید خود رونمایی و عرضهٔ ایربادز جدید خود را به بازار چین شروع کرد. همهٔ این‌ها نشان از این دارند که شرکت‌های بزرگ تکنولوژی سعی کرده‌اند خودشان را با شرایط همراه کنند و شاید همین یکی از دلایل موفقیت بزرگ‌ترین کسب‌وکارهای دنیا باشد.

شرایط بهتر هم می‌شود

مسئله به همین جا ختم نمی‌شود. علاوه بر اینکه بسیاری از شرکت‌ها و کارخانه‌ها در بحران کرونا به کار خود (هر چند با توانی کمتر از حالت معمول) ادامه می‌دهند، این بحران برای بعضی از کسب‌وکارها سودمند هم بوده است. فروشگاه‌های آنلاین در سراسر دنیا از آن مواردی هستند که با رونق جدی کارشان روبه‌رو شده‌اند. یکی از نمونه‌های وطنی آن‌ها یعنی دیجی‌کالا هم از این قاعده مستثنا نیست. با تعطیل‌شدن بیشتر فروشگاه‌ها و مراکز فروش در سطح شهرهای سراسر کشور، دیجی‌کالا یکی از چندین فروشگاه آنلاین بود که با اقبال عمومی زیادی روبه‌رو شد؛ تا حدی که به مدت چند هفته به دلیل عدم توانایی در پردازش و ارسال حجم بالای سفارش‌ها، از پذیرش سفارش در بعضی از شهرها خودداری می‌کرد که در نوع خود اتفاق عجیبی است.

رشد می‌کنیم

روبه‌روشدن با حجم بالای سفارش‌ها تنها دغدغهٔ دیجی‌کالا نبود. در بحران کرونا این شرکت می‌بایست در جهت سلامت کارمندانش، تعداد افراد حاضر در واحدهای عملیات در هر ساعت از شبانه‌روز را کاهش می‌داد. همچنین برای رعایت پروتکل‌های بهداشتی، ضدعفونی‌کردن بسته‌های ارسالی برای مشتریان، باعث می‌شد فرایند پردازش کالا طولانی‌تر شود. در این شرایط حساس، دیجی‌کالا با استخدام بیش از ۱۰۰۰ کارمند جدید توانست اندکی بر این بحران غلبه کند. انتظار می‌رود این عادتِ مردم به خرید آنلاین بعد از پایان دوران قرنطینه هم ادامه داشته باشد که نتیجهٔ آن رشد جدی فروشگاه‌های آنلاین خواهد بود.

هوش مصنوعی، دلسوزِ انسان طبیعی

در ۳۱ دسامبر ۲۰۱۹ شرکت بلودات[1] که در تورنتو مستقر است و از هوش مصنوعی برای ردیابی گسترش بیماری‌های عفونی استفاده می‌کند، مجموعه‌ای از موارد غیرمعمول ذات‌الریه را اطراف بازاری در ووهان چین تشخیص داد. سازمان بهداشت جهانی ۹ روز بعد کشف این ویروس را تأیید کرد. بلودات که از تخصص انسانی و هوش مصنوعی برای ردیابی بیماری‌های عفونی از جمله کرونا استفاده می‌کند، توانسته است اطلاعات مفیدی را از شیوع این بیماری در اختیار مشتریانش که شرکت‌ها و دولت‌ها هستند، قرار دهد. استفاده از هوش مصنوعی می‌تواند در آینده هم برای تشخیص زودهنگام بیماری‌هایی مثل کرونا به دولت‌ها کمک کند. اما کمک هوش مصنوعی به مقابله با ویروس کرونا به همین جا ختم نمی‌شود و قرار است کمک‌حال پزشکان هم باشد. به دلیل کمبودها و محدودیت‌های کیت‌های تشخیص بیماری کرونا، یکی از روش‌های تشخیصی، استفاده از تصاویر گرفته‌شده از قفسهٔ سینه با اشعهٔ ایکس یا سی‌تی‌اسکن است اما ازآنجایی‌که تشخیص تفاوت کرونا و دیگر عفونت‌های ریوی مانند آنفولانزا از روی عکس‌های پزشکی ساده نیست، محققان هوش مصنوعی امیدوارند بینایی کامپیوتری که می‌تواند بسیار دقیق‌تر از چشم انسان عمل کند به تشخیص کرونا از روی عکس‌های پزشکی کمک کند. این اولین باری نیست که دانشمندان، برای استفاده از هوش مصنوعی در پزشکی تلاش می‌کنند. یکی از چالش‌های همیشگی بر سر راه دانشمندان هوش مصنوعی، نبود تعداد زیادی نمونهٔ پزشکی است که با توجه به تعداد بالای مبتلایان به کرونا، این بار این مشکل کمتر احساس می‌شود. یکی از تلاش‌ها در همین زمینه، یک سیستم یادگیری عمیق[2] متن‌باز[3] به نام COVID-NET است که DrawnAI و دانشگاه واترلو آن را ایجاد کرده‌اند. برای این پروژه از پایگاه دادهٔ COVIDx استفاده شده است که شامل ۱۶۷۵۶ رادیوگرافی از قفسهٔ سینهٔ مبتلایان به کرونا و دیگر عفونت‌های ریوی است. این تنوع داده‌ها به مدل یادگیری عمیق در تشخیص بیماری‌ها کمک می‌کند.

اتحاد غول‌ها

در این میان گوگل و اپل هم برای جلوگیری از شیوع کرونا شروع به همکاری کرده‌اند. آن‌ها برای مبارزه با شیوع کرونا می‌خواهند از روشی موسوم به «ردیابی تماس» استفاده کند. این روش به این صورت کار می‌کند که اگر دو نفر به مدت ۱۰ دقیقه یا بیشتر با هم صحبت و معاشرت رودررو داشته باشند، در این مدت تلفن‌های همراه این دو نفر از طریق سیگنال‌های بلوتوثی با هم ارتباط برقرار می‌کنند و اطلاعات این اصطلاحاً «تماس» را ذخیره می‌کنند. اگر پس از مدتی یکی از آن‌ها به کرونا مبتلا شود، با موافقت خودش اطلاعات بلوتوثی ۱۴ روز گذشته‌اش را که حاوی اطلاعاتی دربارهٔ تماس‌های نزدیک او با دیگران است، به سرور ارسال می‌کند؛ سرور هم به همهٔ افرادی که در ۱۴ روز گذشته با او در ارتباط بوده‌اند پیامی ارسال می‌کند تا از این موضوع آگاه شوند. مهندسان اپل و گوگل قصد دارند در نهایت چنین مشخصه‌ای را در سیستم‌عامل‌های اندروید و ios پیاده‌سازی کنند اما فعلاً قرار نیست برنامه‌ای ساخته شود بلکه آن‌ها درصدد طراحی یک API هستند که برنامه‌های دیگر بتوانند از امکانات آن استفاده کنند.

یک نرم‌افزار ایرانی هم با عملکردی مشابه و به کوشش مهندسان دانشگاه‌های امیرکبیر، شهید بهشتی و شریف به نام «ماسک» و برای ردیابی مبتلایان به ویروس کرونا طراحی شده است. در این برنامه که قابل‌نصب بر روی تلفن‌های همراه اندرویدی است، می‌توان از امکاناتی نظیر تست اولیهٔ ابتلا به کرونا، اطلاع از سلامت افرادی که با آن‌ها تماس داشته‌اید، مشاهدهٔ نقشهٔ کشوری شیوع کرونا، دریافت محتوای آموزشی بهداشتی و ... استفاده کرد.

۱- BlueDot
۲- Deep Learning
۳- open source

ثروت در خدمت انسانیت

میلیاردرهای عرصه‌های تکنولوژی و نرم‌افزار هم به جبههٔ مقابله با کرونا پیوسته‌اند. در این میان احتمالاً شاخص‌ترین خبر مربوط به جک دورسی، مدیرعامل توییتر است. او یک میلیارد دلار یعنی تقریباً معادل یک چهارم سرمایهٔ خالص خود را برای کمک به مقابله با ویروس کرونا اهدا کرده است. همچنین تا امروز جف بزوس، مالک آمازون و بیل گیتس، مؤسس مایکروسافت که ثروتمندترین افراد جهان به‌شمار می‌آیند، هر یک ۱۰۰ میلیون دلار و مارک زاکربرگ، موسس فیس‌بوک ۲۵ میلیون دلار جهت کمک به جلوگیری از شیوع کرونا کمک کرده‌اند. راک‌استارگیمز[۵] هم اعلام کرده است که به مدت دو ماه، بخشی از درآمدهای حاصل از بازی‌های آنلاین خود را به سازمان‌های مرتبط با ویروس کرونا اهدا خواهد کرد.

جک دورسی

در خانه بمانیم

شاید جدی‌ترین راهکار پیشگیری از ابتلا به کرونا و مقابله با این ویروس، همین کار سادهٔ «در خانه ماندن» است. آن هم در روزهایی که همه چیز دست‌به‌دست هم داده‌اند تا این قرنطینهٔ خانگی راحت‌تر سپری شود؛ از فروشگاه‌های اینترنتی تا آموزش مجازی و وبینارهای آنلاین. از جمله اتفاقات عجیب این روزها که به لطف اینترنت و فضای مجازی ممکن شده است، اکران آنلاین بعضی از فیلم‌ها قبل از اکرانشان در سینماست. در ایران ابراهیم حاتمی‌کیا در در این کار پیش‌قدم شده است و فیلم خروج او تا امروز توانسته است فروش خوبی داشته باشد.

۱- Rockstar Games

از طرفی مدتی قبل سونی هم اعلام کرد بازی‌های Journey و Uncharted Collection به مدت محدود برای همهٔ کاربران پلی‌استیشن ۴ به صورت رایگان قابل‌خرید است و بعد از دریافت، برای همیشه در حساب کاربری آن‌ها باقی خواهد ماند. محمدجواد آذری جهرمی، وزیر ارتباطات، هم که قبل از عید با دادن هدیهٔ اینترنت ۱۰۰ گیگابایتی به مشترکین اینترنت خانگی به ماندن مردم در خانه کمک کرده بود، مدتی قبل اعلام کرد قرار شده است پهنای باند تمامی مشترکین اینترنت خانگی در جهت استفاده از محتوای دیجیتال و به خصوص محتوای آموزشی دیجیتال به ۱۶ مگابیت‌درثانیه افزایش پیدا کند. البته از آنجایی که پهنای باند سرویس‌دهندگان اینترنت حد مشخصی دارد باید دید در صورت پیروی سرویس‌دهندگان اینترنت، این اقدام با چه تبعاتی در زمینهٔ افت کیفیت اینترنت همراه خواهد بود.

جمع‌بندی

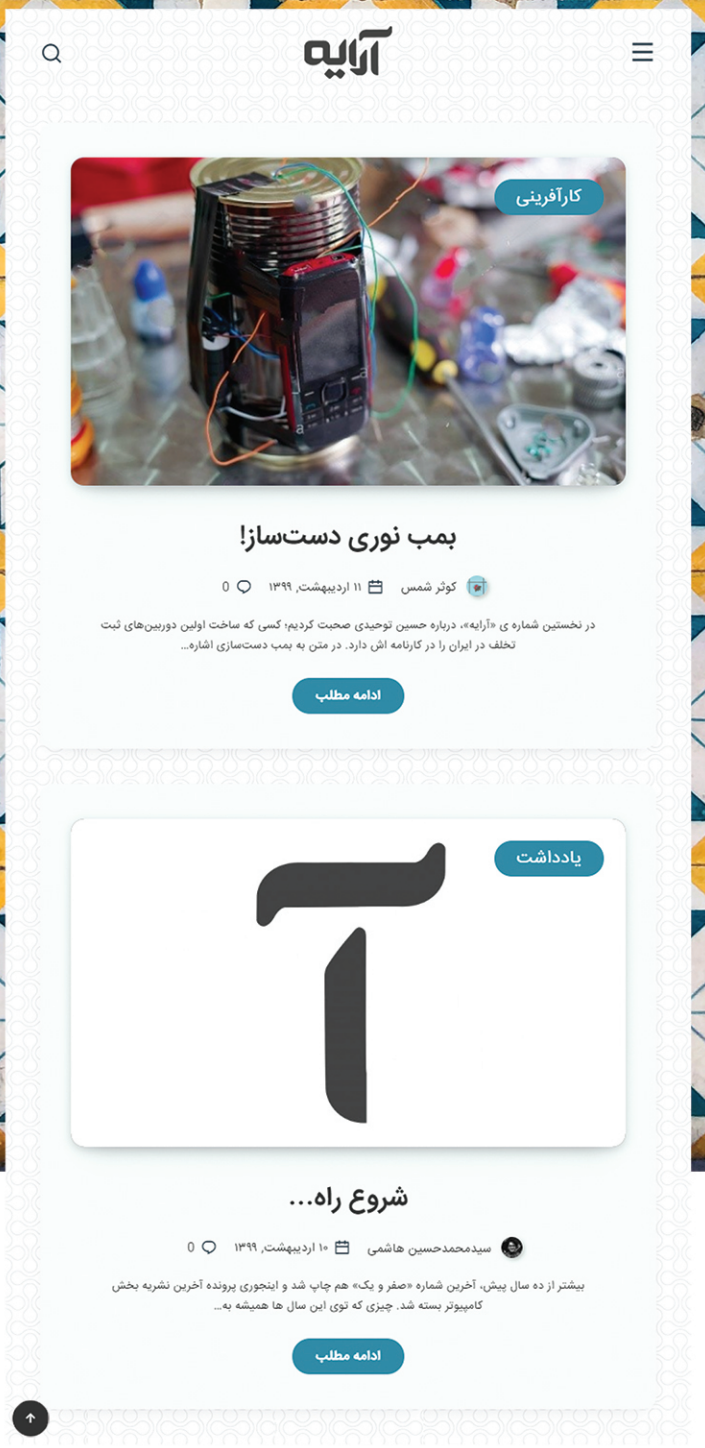
بحران کرونا مانند هر بحران دیگری گذراست و روزی به پایان خواهد رسید و در این میان افراد و سازمان‌هایی که بتوانند خودشان را با شرایط وفق دهند و روند روبه‌رشد خود یا حداقل شرایط فعلی‌شان را حفظ کنند می‌توانند از این بحران با موفقیت بیرون بیایند. حتی این شرایط می‌تواند برای بسیاری از افراد یا سازمان‌ها مفید هم باشد و باعث رشد آن‌ها شود. به هر حال احتمالاً بعد از عادی‌شدن شرایط تغییراتی جدی را در زمینهٔ فناوری‌های نوین شاهد خواهیم بود. مثلاً ممکن است توجه بیشتری به رابطهای کاربری بدون‌نیازبه‌لمس شود؛ یا محققین روی روش‌های کنترل بیماری‌ها با استفاده از داده‌های کلان و اینترنت اشیا بیشتر تمرکز کنند؛ یا اینکه کسب‌وکارها تکیهٔ بیشتری روی ربات‌ها داشته باشند یا ... . چیزی که واضح است نیاز به برداشتن قدم‌هایی در جهت تقویت زیرساخت‌های دیجیتالی (مخصوصاً در ایران) است. همهٔ این اقدامات برای این خواهد بود که از این به بعد در برابر چنین بحران‌هایی مقاوم‌تر باشیم چراکه بحران کرونا اولین بحران همه‌گیر بشر نبوده است و آخرین آن‌ها هم نخواهد بود.

منابع

لیست کامل و دقیق منابع را در لینک زیر ببینید:

1- www.digikala.com/mag
2- www.Bloomberg.com
3- www.apple.com
4- www.cnbc.com
5- www.irna.ir

با ما در ارتباط باشید...



جای شما در آرایه خالی است...

برای مشارکت در تولید آرایه می‌توانید از راه‌های ارتباطی زیر استفاده کنید:

arraymag.ir

t.me/arraymag

arraymagcontact@gmail.com

منبـع عکس‌هـای گرافیکـی ایـن شـماره
https://unsplash.com

عکـس روی جلـد، تصویـری از اتـاق تمیـز اینتـل برگرفتـه از سـایت
https://newsroom.intel.com