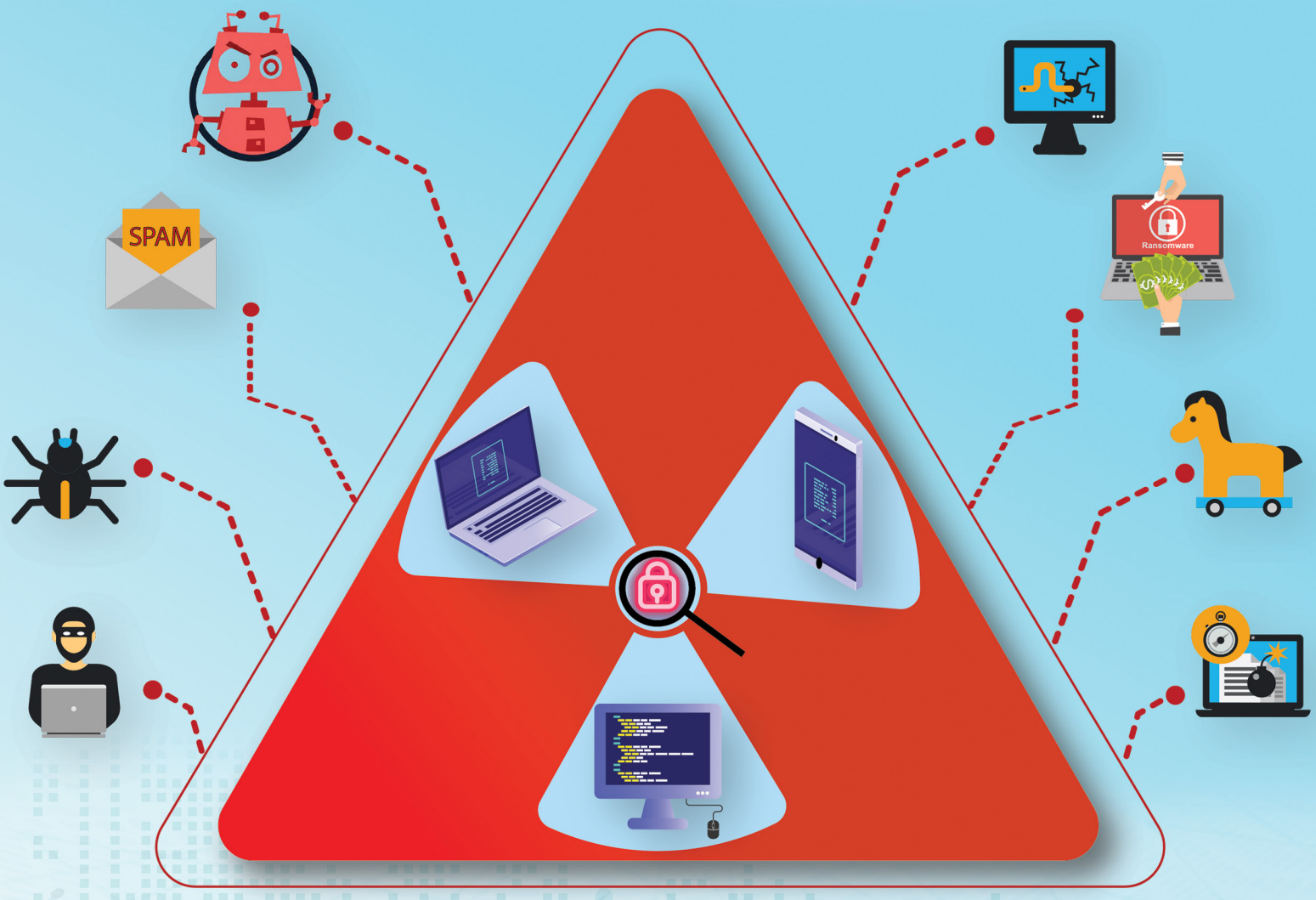
فصل‌نامه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره هشتم/ زمستان ۹۹



- معرفی ابزار OllyDbg
- دفترچه تقلب IDAPRO
- خطرات و تأمین امنیت API ها
- معرفی موتورهای جستجوی آسیب‌پذیری
- معرفی دوره Certified SOC Analyst (CSA)
- توصیه‌های مهم در زمینه امنیت سایبری برای کاربران
- بررسی آخرین گزارش آزمایشگاه تهدیدات مک‌آفی و کسپرسکی

درباره مرکز آپا دانشگاه کردستان

آپا مخفف عبارت آگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CSIRT می‌باشد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رسانی، با بکارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان اقدام به انتشار نشریه‌ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.
مخاطبان اصلی نشریه کارشناسان و متخصصانِ فناوری اطلاعات و شبکه، دانشجویان و علاقمندان فضای سایبری است. مطالب این نشریه عموماً محورهای زیر را شامل می‌شود:

- اطلاع‌رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نسبت به آخرین تهدیدات و آسیب‌پذیری ابزارهای فضای مجازی
- آموزش‌های تخصصی و عمومی در جهت ارتقاء دانش امنیت

شایان ذکر است، ویرا، اسم نشریه، واژه‌ای در زبان کردی به معنی صاحب‌فکر و هوشمند است.

صاحب امتیاز: مرکز آپا دانشگاه کردستان
مدیر مسئول: محمد فتحی
سردبیر: هادی گلباغی
سردبیر فنی: محمد حبیبی
ویراستار: نازیلا خسروی
طراحی و صفحه‌آرایی: پرستو مجیدی
نویسندگان (به‌ترتیب مطالب):
محمد حبیبی/ سینا فقیری/ محمد ساروقی
پرستو مجیدی/ هادی گلباغی/ نازیلا خسروی

تلفن مرکز: ۰۸۷۳۳۶۱۱۴۱۵
نشانی مجله: کردستان، سنندج، بلوار پاسداران، دانشگاه کردستان، دانشکده مهندسی، ساختمان شماره ۳، طبقه همکف، مرکز آپا
وب‌سایت: www.cert.uok.ac.ir
ایمیل: apa@uok.ac.ir

راهنمایی:

- در فهرست مطالب می‌توانید با کلیک بر روی هریک از بخش‌ها و مطالب به صفحه مورد نظر منتقل شوید.
- با کلیک بر روی QR کدها می‌توانید مستقیما به لینک‌ها منتقل شوید.

فهرست **مطالب**

مقاله‌های آموزشی

۰۳ معرفی موتورهای جستجوی آسیب‌پذیری

۱۲ خطرات و تامین امنیت API ها

۲۰ مقدمه‌ای بر تحلیل بدافزار و معرفی ابزارهای این حوزه

معرفی ابزار

۳۴ معرفی ابزار Masscan

۳۹ معرفی ابزار OllyDbg

دفترچه تقلب

۴۸ دفترچه تقلب IDAPro

معرفی دوره

۵۵ معرفی دوره Certified SOC Analyst(CSA)

معرفی کتاب

۵۸ کتاب The Pentester BluePrint

مقاله‌های تحقیقاتی

۶۱ بررسی آخرین گزارش آزمایشگاه تهدیدات مک‌آفی و کسپرسکی

۶۷ حمله فیشینگ به مایکروسافت آفیس با میزبانی فایربیس گوگل

امنیت اطلاعات

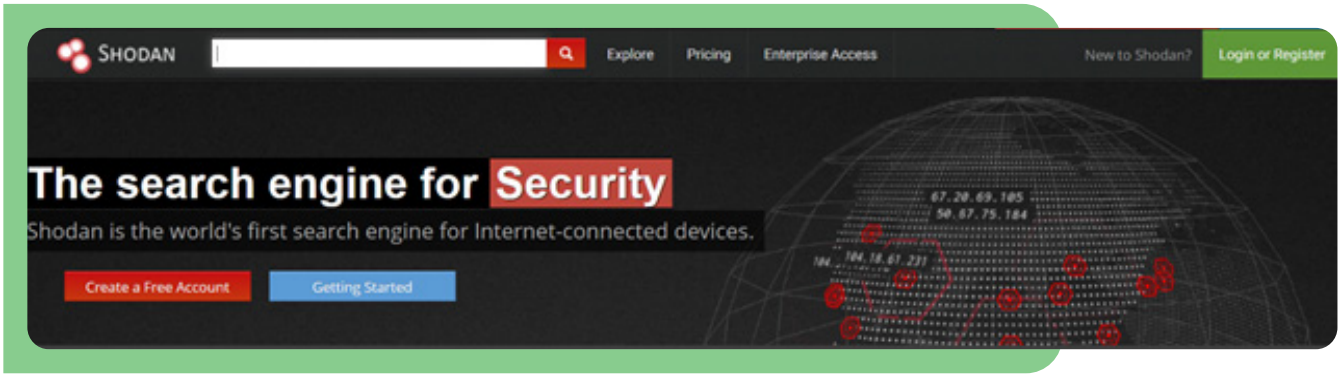
۷۳ توصیه‌های مهم در زمینه امنیت سایبری برای کاربران

مقاله‌های آموزشی

تهیه و تدوین : محمد حبیبی

مقدمه

در این بخش به بررسی موتورهای جستجوی آسیب‌پذیری معروف می‌پردازیم. موتورهای جستجوی آسیب‌پذیری می‌توانند نقش مهمی را در بخش جمع‌آوری اطلاعات از مراحل تست نفوذ ایفا کنند و برای یافتن آسیب‌پذیری‌های سرور یا شبکه هدف، استفاده شوند.
در این بخش سه موتور جستجوی Censys، Shodan و Zoomeye را بررسی می‌کنیم.



موتور جستجوی Shodan

Shodan یک موتور جستجو است که به کاربر امکان جستجوی سیستم‌های مختلف از قبیل وب کم، روترها، سرورها یا سایر تجهیزات IOT متصل به اینترنت را می‌دهد. Shodan معمولاً داده‌هایش را برای وب سرورها (پروتکل‌های HTTP/HTTPS و پورت‌های ۸۰۸۰, ۴۴۳, ۸۴۴۳,۸۰)، پروتکل FTP(پورت ۲۱)، SSH(پورت ۲۲)، Telnet(پورت ۲۳)، SNMP(پورت ۱۶۱)، IMAP(پورت ۱۴۳ یا برای حالت رمزگذاری شده پورت ۹۹۳)،SMTP(پورت ۲۵)، SIP(پورت ۵۰۶۰) و RTSP(پورت ۵۵۴) و پورت‌های تعریف‌شده دیگر جمع‌آوری می‌کند.
Shodan از سال ۲۰۰۹ توسط آقای John Matherly که در سال ۲۰۰۳ ایده جستجوی دستگاه‌های متصل به شبکه‌ی اینترنت را داد، شروع به فعالیت کرد. نام Shodan از یکی از کاراکترها با همین نام از بازی ویدیویی به نام System Shock گرفته‌شده است.
Shodan به‌صورت کلی شبکه اینترنت را برای یافتن دستگاه‌های موجود در اینترنت که به‌صورت عمومی در دسترس هستند جستجو می‌کند و بیشتر تمرکز خود را بر تشخیص سیستم‌های SCADA گذاشته است.
در حال حاضر Shodan به کاربران بدون حساب کاربری، ده نتیجه، به کاربران با حساب کاربری، پنجاه نتیجه و به کاربران که اشتراک Freelancer را تهیه‌کرده‌اند، یک‌میلیون نتیجه در ماه، کاربران Small Business بیست میلیون نتیجه در ماه و برای Corporate هم به‌صورت نامحدود نتایج جستجو را نمایش می‌دهد. هزینه اشتراک Corporate ماهانه ۸۹۹ دلار است و بیشتر برای سازمان‌ها و کمپانی‌های بزرگ در حوزه فناوری اطلاعات کاربرد دارد.
در این بخش سعی می‌کنیم بخشی از فیلترها و دورک‌های مربوط به موتور جستجوی Shodan را معرفی کنیم:

فیلترهای جستجوی پایه

فیلتر	مثال	کاربرد
city:	city: "Bangalor "	جستجوی دستگاه‌های موجود در یک شهر
country:	country:"IN"	جستجوی دستگاه‌های موجود در یک کشور
geo:	geo:"56.913055,118.250862"	جستجوی دستگاه‌های موجود در یک منطقه جغرافیایی
hostname:	hostname:"google"	جستجوی دستگاه‌های با یک نام میزبان
net:	net:210.214.0.0/16	جستجو در یک محدوده شبکه
Organization	org:microsoft	جستجو برای یک سازمان خاص
ASN:	asn:ASxxxx	جستجوی یک ASN (Autonomous System Number)
os:	os:"windows 7"	جستجوی دستگاه‌ها بر اساس سیستم‌عامل
SSL/TLS Certificates	ssl.cert.issuer.cn:example.com ssl.cert.expired:true	جستجو بر اساس گواهینامه‌های SSL/TLS
port	port:21	جستجو دستگاه بر اساس پورت‌های باز
Product	product:nginx,product:android	جستجو بر اساس نام محصول
cpe:	cpe:nginx, cpe:cisco	جستجو بر اساس CPE(Customer Premises Equipment)
Server:	server: apache, server: cisco-ios	جستجو بر اساس نام محصول
ssh fingerprints:	dc:14:de:8e:d7:c1:15:43:23:82:25 :81:d2:59:e8:c0	جستجوی ssh fingerprints
PEM Certificates:	http.title:"Index of /" http.html:". pem"	جستجوی گواهینامه PEM
Device Type:	device:firewall, device:pda device:webcam, device:router, device:power	جستجو بر اساس نوع دستگاه

فیلترهای کاربردی برای پیدا کردن سیستم‌های کنترل صنعتی

محصول	فیلتر
Samsung Electronic Billboards	"Server: Prismview Player"
Gas Station Pump Controllers	"in-tank inventory" port:10001
Fuel Pumps	"privileged command" GET (برای دسترسی به ترمینال نیاز به احراز هویت نباشد)
Automatic License Plate Readers	P372 "ANPR enabled"
Traffic Light Controllers / Red Light Cameras	mikrotik streetlight
Voting Machines in the United States	"voter system serial" country:US
Open ATM	NCR Port:"161"
Telcos Running Cisco Lawful Intercept Wiretaps	"Cisco IOS" "ADVIPSERVICESK9_LI-M"
Prison Pay Phones	"[2J[H Encartele Confidential"
Tesla PowerPack Charging Status	http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2
Tesla PowerPack Charging Status	"Server: gSOAP/2.8" "Content-Length: 583"
C4 Max Commercial Vehicle GPS Trackers	"[1m[35mWelcome on console"
Submarine Mission Control Dashboards	title:"Slocum Fleet Mission Control"
CAREL PlantVisor Refrigeration Units	"Server: CarelDataServer" "200 Document follows"
Nordex Wind Turbine Farms	http.title:"Nordex Control"
Maritime Satellites	"Cobham SATCOM" OR ("Sailor" "VSAT") ردیابی کشتی‌ها بر روی نقشه به‌صورت بلادرنگ
DICOM Medical X-Ray Machines	"DICOM Server Response" port:104
GaugeTech Electricity Meters	"Server: EIG Embedded Web Server" "200 Document follows"
Siemens Industrial Automation	"Siemens, SIMATIC" port:161
Siemens HVAC Controllers	"Server: Microsoft-WinCE" "Content-Length: 12581"

فیلترهای کاربردی برای پیدا کردن سیستم‌های کنترل صنعتی

محصول	فیلتر
Door / Lock Access Controllers	"HID VertX" port:4070
Railroad Management	"log off" "select the appropriate"
Tesla Powerpack charging Status	http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2
XZERES Wind Turbine	title:"xzeres wind"
PIPS Automated License Plate Reader	"html:"PIPS Technology ALPR Processors" "
Modbus	"port:502"
Niagara Fox	"port:1911,4911 product:Niagara"
GE-SRTP	"port:18245,18246 product:"general electric"
MELSEC-Q	"port:5006,5007 product:mitsubishi"
CODESYS	"port:2455 operating system"
S7	"port:102"
BACnet	"port:47808"
HART-IP	"port:5094 hart-ip"
Omron FINS	"port:9600 response code"
IEC 60870-5-104	"port:2404 asdu address"
DNP3	"port:20000 source address"
EtherNet/IP	"port:44818"
PCWorx	"port:1962 PLC"
Crimson v3.0	"port:789 product:"Red Lion Controls"
ProConOS	"port:20547 PLC"

فیلترهای کاربردی برای زیرساخت‌های شبکه

عنوان	فیلتر
Routers which got compromised	hacked-router-help-sos
Redis open instances	hacked-router-help-sos
Find Citrix Gateway	title:"citrix gateway"
Weave Scope Dashboards	title:"Weave Scope" http.favicon. hash:567176827
Older versions of MongoDB that insecure by default	"MongoDB Server Information" port:27017 authentication
Mongo Express Web GUI	"Set-Cookie: mongo-express=" "200 OK"
Jenkins CI	"X-Jenkins" "Set-Cookie: JSESSIONID» http.title:"Dashboard"
Jenkins Unrestricted Dashboard	x-jenkins 200
Docker APIs	"Docker Containers:" port:2375
Docker Private Registries	"Docker-Distribution-Api-Version: registry" "200 OK" -gitlab
Pi-hole Open DNS Servers	
Already Logged-In as root via Telnet	"root@" port:23 -login -password -name -Session
Telnet Access	port:23 console gateway
Polycom video-conference system no-auth shell	"polycom command shell"
NPort serial-to-eth / MoCA devices without password	nport -keyin port:23
Android Root Bridges	"Android Debug Bridge" "Device" port:5555
Lantronix Serial-to-Ethernet Adapter Leaking Telnet Passwords	Lantronix password port:30718 -secured
Citrix Virtual Apps	"Citrix Applications:" port:1604
Cisco Smart Install	"smart install client active"
PBX IP Phone Gateways	PBX "gateway console" -password port:23

فیلترهای کاربردی برای زیرساخت‌های شبکه

محصول	فیلتر
Polycom Video Conferencing	http.title:"- Polycom" "Server: lighttpd" "Polycom Command Shell" -failed port:23
Telnet Configuration	"Polycom Command Shell" -failed port:23
Bomgar Help Desk Portal	"Server: Bomgar" "200 OK"
Intel Active Management CVE-2017-5689	port:623,664,16992,16993,16994,16995 "Active Management Technology"
HP iLO 4 CVE12542-2017-	HP-ILO4- !"HP-ILO2.53/4-" !"HP-ILO2.54/4-" !"HP-ILO2.55/4-" !"HP-ILO2.60/4-" !"HP-ILO2.61/4-" !"HP-ILO2.62/4-" !"HP-iLO2.70/4-" port:1900
Lantronix ethernet adapter's admin interface without password	"Press Enter for Setup Mode port:9999"
Misconfigured Wordpress Sites (wp-config.php if accessed can give out the database credentials)	html:"def_wirelesspassword"

فیلترهایی برای پیدا کردن وب کم‌ها در سطح اینترنت

محصول	فیلتر
D-Link webcams	"d-Link Internet Camera, 200 OK"
Hipcam	"Hipcam RealServer/V1.0"
Yawcams	"Server: yawcam" "Mime-Type: text/html"
webcamXP/webcam7	("webcam 7" OR "webcamXP") http.component:"mootools" -401
Android IP Webcam Server	"Server: IP Webcam Server" "200 OK"
Security DVRs	html:"DVR_H264 ActiveX"
Surveillance Cams	NETSurveillance uc-httpd Server: uc-httpd 1.0.0

فیلترهایی برای پیدا کردن چاپگر و دستگاه‌های کپی

فیلتر	محصول
"Serial Number:" "Built:" "Server: HP HTOK"	HP Printers
ssl:"Xerox Generic Root"	Xerox Copiers/Printers
"SERVER: EPSON_Linux UPnP" "200 OK" "Server: EPSON-HTTP" "200 OK	Epson Printers
"Server: KS_HTTP" "200 OK" "Server: CANON HTTP Server"	Canon Printers
title:"OctoPrint" -title:"Login" http. favicon.hash:1307375944	OctoPrint 3D Printer Controllers

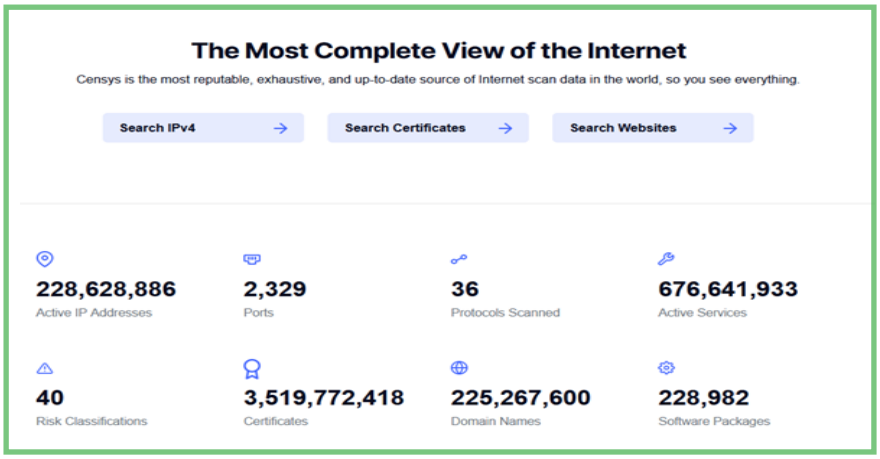
فیلترهای مربوط به پایگاه داده

کاربرد	مثال	فیلتر
جستجوی پایگاه داده‌های MySQL	"product:MySQL"	MySQL
جستجوی پایگاه داده‌های MongoDB	"product:MongoDB"	MongoDB
جستجوی پایگاه داده‌های elastic	port:9200 json	elastic
جستجوی پایگاه داده‌های Memcached	"product:Memcached"	Memcached
جستجوی پایگاه داده‌های CouchDB	"product:CouchDB"	CouchDB
جستجوی پایگاه داده‌های PostgreSQL	"port:5432 PostgreSQL"	PostgreSQL
جستجوی پایگاه داده‌های Riak	"port:8087 Riak"	Riak
جستجوی پایگاه داده‌های Redis	«product:Redis"	Redis
جستجوی پایگاه داده‌های Cassandra	"product:Cassandra"	Cassandra

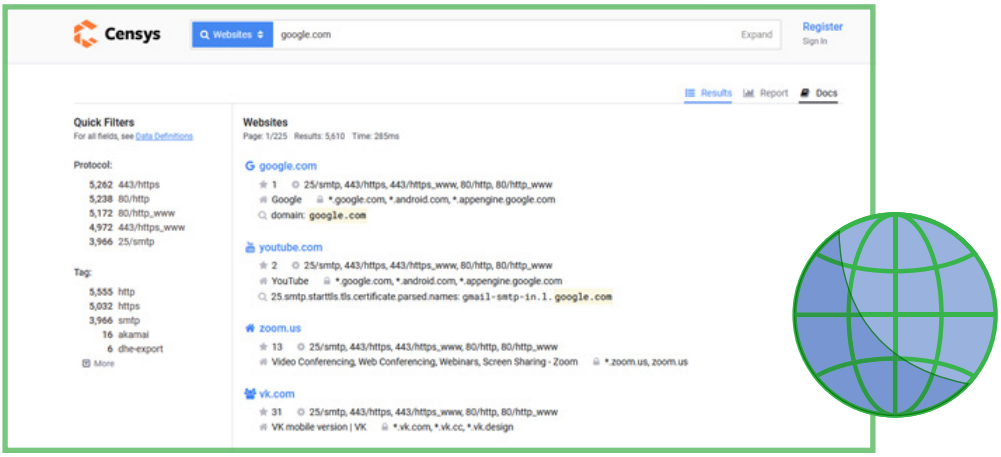
موتور جستجوی Censys

Censys توسط تیمی از محققین امنیتی در سال ۲۰۱۷ با هدف آگاهی‌رسانی به عموم در زمینه شناخت کامل ریسک‌ها و تهدیدات امنیتی در حوزه دیجیتال تأسیس شد. Censys یکی از رقبای قدرتمند وب‌سایت Shodan شناخته می‌شود و چون در حال حاضر محدودیتی برای نمایش نتایج جستجو ندارد محبوبیت بالایی در بین محققین حوزه امنیت سایبری کسب کرده است.

به‌صورت کلی کاربران در وب‌سایت Censys می‌توانند جستجوهای خود را با استفاده از IP آدرس ورژن چهار (IPv4)، certificates یا نام دامنه (Domain) هدف انجام دهند. در تصویر زیر بخش جستجوی وب‌سایت آورده شده است و همان‌طور که قابل‌مشاهده است اسامی IP-آدرس‌های فعال، پورت‌ها، certificates ها، پروتکل‌های اسکن شده، سرویس‌های فعال و غیره نیز آورده شده است.



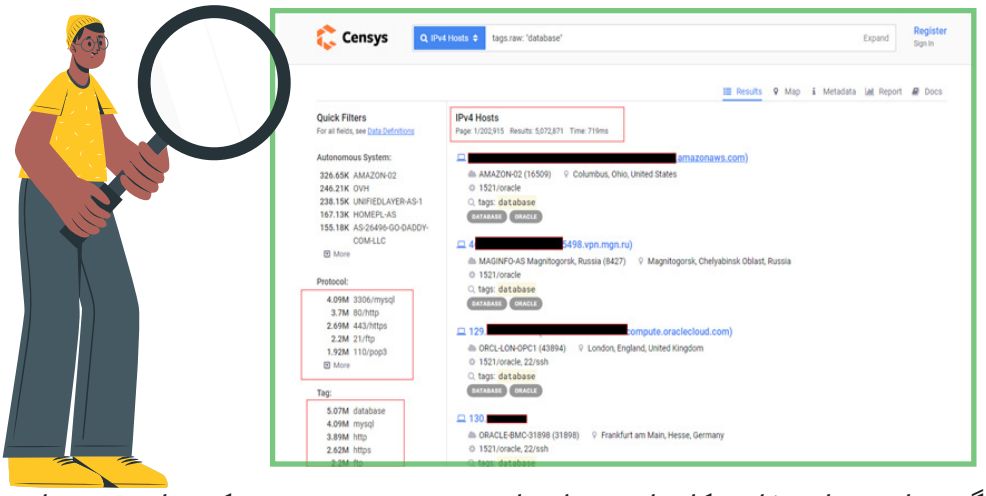
در تصویر زیر خروجی جستجو برای دامنه Google.com آورده شده است. در این خروجی در سمت چپ لیستی از پروتکل‌ها و Tag ها آورده شده است. Tag ها مقادیر خاصی هستند که به برخی از میزبان‌ها متصل و کاربر با جستجوی هر Tag میزبان‌هایی که آن Tag را دارند مشاهده می‌کند.



برای دسترسی به آخرین به‌روزرسانی از Tag ها و دسترسی به جزئیات دستگاه‌های آن‌ها می‌توان از لینک زیر استفاده کرد.Tag ها نقطه شروع مناسبی برای محققین حوزه امنیت سایبری هستند که با استفاده از آن‌ها می‌توانند سرویس، پروتکل یا نرم‌افزار خاصی را در فضای اینترنت جستجو کنند.

https://censys.io/ipv4/report?q=*&field=tags.raw&max_buckets=1000

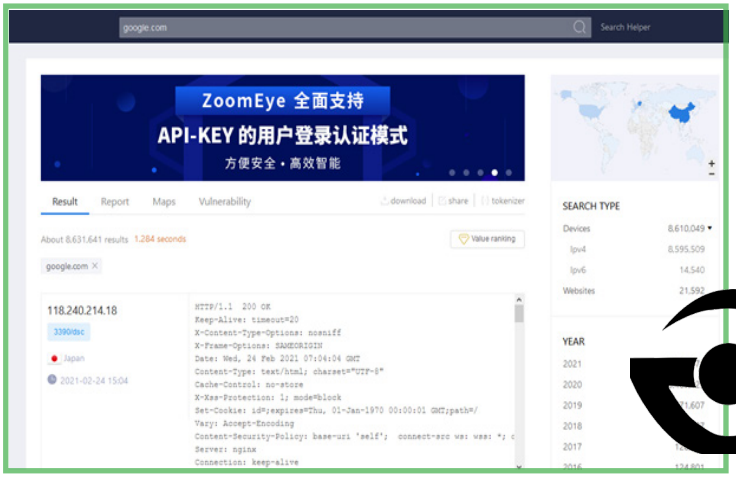
به‌عنوان‌مثال خروجی تگ database در تصویر زیر آورد شده است که شامل ۵,۰۷۲,۸۷۱ نتیجه می‌باشد.



ابزار censys برای جلوگیری از سوءاستفاده، کاربران مهمان را محدود به ده جستجو کرده است و برای جستجوهای بیشتر نیاز است که در وب‌سایت ثبت‌نام کنند.

موتور جستجوی Zoomeye

موتور جستجوی Zoomeye یکی از قدرتمندترین موتورهای جستجوی آسیب‌پذیری چینی می‌باشد. در تصویر زیر خروجی جستجو وب‌سایت google.com آورده شده است. خروجی جستجو در چهار تب به کاربر نمایش داده می‌شود. Maps، Report، Result و Vulnerability که در تب آخر یا همان Vulnerability آسیب‌پذیری‌هایی مرتبط با هاست‌های وب‌سایت Google.com آورده شده است.

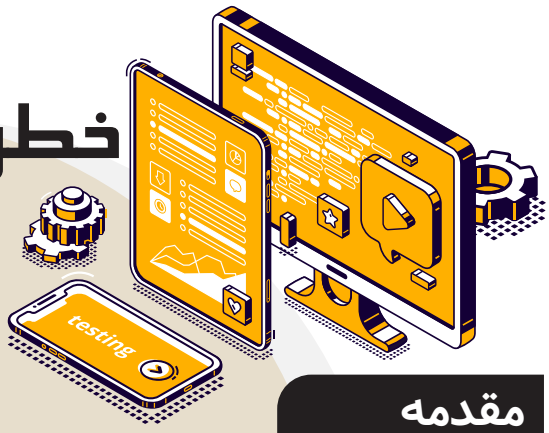


همچنین در صورت کلیک بر روی منوی Explore بخش statistics نمایش داده می‌شود که به‌صورت آماری، لیست دستگاه‌ها، سرویس‌ها، پروتکل‌ها و محصولاتی که بیشترین استفاده را در سطح شبکه اینترنت دارند نمایش می دهد.

این موتور جستجو نیز برای محققین حوزه امنیت سایبری طراحی‌شده است و می‌تواند اطلاعات بسیار مفیدی در اختیار آن‌ها قرار دهد. این ابزار توسط تیم Knownsec 404 هدایت می‌شود. Zoomeye بر اساس IPv4، IPv6 و دامنه‌های وب‌سایت‌ها به‌صورت پیوسته شبکه اینترنت را پویش می‌کند. سرویس‌ها و پروتکل‌ها را به‌صورت ۲۴ ساعته شناسایی می‌کند و درنهایت نقشه فضای مجازی کل شبکه را به‌صورت محلی یا جهانی تهیه می‌کند.

خطرات و تأمین امنیت API ها

تهیه و تدوین: سینا فقیری



مقدمه

Application Programming Interface یا به‌اختصار API ها، واسطهایی برای ارتباط دو اپلیکیشن باهم و استفاده از سرویس‌های یکدیگر هستند.
امروزه کاربرد API ها در موارد مختلفی همچون؛ اینترنت اشیا، خریدهای اینترنتی، سیستم‌های حمل‌ونقل و غیره باعث شده است تا در معرض خطراتی قرار بگیرند، چون می‌توانند حاوی اطلاعات حساسی مانند داده‌های حساس، اطلاعات شخصی و غیره باشند. نحوه محافظت از اطلاعاتی که در بین اپلیکیشن‌ها ردوبدل می‌شوند با توجه به نوع و اهمیت آن‌ها متفاوت است و برای هر داده باید رویکرد خاصی در نظر گرفته شود. برای مثال در بحث اینترنت اشیا، زمان خالی شدن یخچال و سفارش موارد جدید، شاید فهمیدن اطلاعات مواد خریداری‌شده زیاد مهم نباشد اما امکان دارد از اطلاعات محافظت نشده‌ای برای فهمیدن موقعیت مکانی شما استفاده شود.
در بحث تأمین امنیت و آشنایی با آسیب‌پذیری‌های رایج API ها به بررسی موارد مطرح‌شده توسط OWASP می‌پردازیم.

01 Broken Object Level Authorization

در این روش مهاجم شناسه منبع خود را با شناسه منبع متعلق به کاربر دیگری جایگزین می‌کند. با عدم بررسی صحیح مجوزها، مهاجم به‌راحتی به منابع موردنظر دسترسی پیدا می‌کند. این حمله با نام IDOR(insecure Direct Object Reference) نیز شناخته می‌شود.
به‌طور مثال فرض کنیم، یک لیست سِری از اطلاعات تعدادی محصول را در پایگاه داده خود نگهداری می‌کنیم که کاربران در پنل خود می‌توانند به این اطلاعات دسترسی پیدا کنند. حال مسئله این است که همه کاربران مجاز به دسترسی به همه محصولات نیستند؛ یا به‌طور مثال اجازه مشاهده بعضی از اطلاعات خاص یک محصول را ندارند؛ اما درعین‌حال محصولات دیگری نیز هستند که تمام دسترسی‌ها به آن توسط همه کاربران مجاز است. در این سناریو، محصولات و اطلاعات آن‌ها به‌صورت اشیائی در نظر گرفته می‌شوند که شامل یکسری قواعد خاص برای دسترسی به آن‌ها و همچنین یک شناسه برای هرکدام از آن‌ها هستند. در این صورت درخواست API برای خواندن یک محصول به‌صورت زیر است:

```
GET https://myproducts.com/products/32511
```

در این درخواست، شناسه منحصربه‌فرد محصول، شماره درخواست (۳۲۵۱۱) است.
حال مشکل اینجاست که با استفاده از شناسه‌های قابل پیش‌بینی و متوالی، امکان حملات brute-force با ابزارهای خاصی مانند burp-suite به‌وجود می‌آید

سناریوها

- API پارامترهایی را فراخوانی می‌کند که از ID منابع یا محصولات برای دسترسی به داده‌ها از طریق API استفاده کرده است.
- مهاجمان شناسه منبع خود را جایگزین یک شناسه منبع دیگر می‌کنند.
- بدون بررسی مجوزهای دسترسی، امکان فراخوانی را فراهم می‌کند.
- استفاده از شناسه‌های متوالی و قابل پیش‌بینی.

راه‌های جلوگیری

- مجوزها و سلسله‌مراتب دسترسی کاربران به هر بخش به‌درستی پیاده‌سازی شود.
- به شناسه‌های ارسالی clientها اعتماد نکرده و از شناسه‌های ذخیره‌شده در session object استفاده شود.
- برای دسترسی به پایگاه داده، مجوز دسترسی تعیین و پس از هر درخواست بررسی شود.
- از شناسه‌های تصادفی که حدس زدن آن‌ها مشکل است استفاده کنید. (UUIDs)
- برای دسترسی به تمام اشیاء (محصولات و موارد حساس)، یک فرایند احراز هویت وجود داشته باشد.

02 Broken User Authentication

مکانیزم‌های احراز هویت اغلب نادرست پیاده‌سازی می‌شوند. همین به مهاجمان اجازه می‌دهد تا با در دست گرفتن توکن‌های احراز هویت، هویت کاربری را به‌طور دائم یا موقت در دست بگیرند. با به خطر افتادن قابلیت یک سیستم برای شناسایی client ها یا user ها، امنیت کل API به خطر می‌افتد.

سناریوها

- API های محافظت نشده که داخلی در نظر گرفته‌شده‌اند. برای مثال API هایی که برای ارتباط بین اپلیکیشن‌های درون یک سازمان استفاده می‌شوند.
- احراز هویت و کلیدهای API رمزهای عبور ضعیف، متون ساده (plain text)، ترکیب hash ضعیف، استفاده از عبارات ساده و غیره، استفاده از گذرواژه‌های پیش‌فرض.
- احراز هویت آسیب‌پذیر در برابر حملات brute force
- قرار دادن شناسه‌ها و کلیدهای حساس در URL
- عدم اعتبارسنجی توکن‌ها
- JWT های بدون انقضا، یا امضا نشده

راه‌های جلوگیری

- تمام راه‌های موجود جهت احراز هویت کل APIها را بررسی کنید.
- APIها همچنین در هنگام مکانیزم reset password یا استفاده از لینک‌های یک‌بارمصرفی که در آن‌ها امکان احراز هویت به کاربر داده می‌شود نیز بایستی محافظت شوند.
- جهت ذخیره‌سازی رمز عبور، ایجاد توکن‌ها، احراز هویت چندمرحله‌ای، از روش‌های استاندارد و مطمئن استفاده نمایید.
- برای توکن‌های دسترسی چرخه حیات کوتاه تعیین کنید.
- برای فرایندهای احراز هویت از rate-limiting استفاده کنید و روش‌هایی همچون قفل شدن و بررسی رمزهای عبور ضعیف را پیاده‌سازی کنید.
- برای ارتباط با اپلیکیشن‌ها، احراز هویت قرار دهید تا بدانید از طرف چه کسی با شما ارتباط برقرارشده است.

03 Excessive Data Exposure

API ممکن است اطلاعاتی بیش از آنچه کاربر به‌طور قانونی به آن احتیاج دارد را با اتکا به فیلترینگ آن‌ها توسط کاربر در معرض دید قرار دهد، در این صورت مهاجمان با ربودن ارتباط، می‌توانند به‌کل اطلاعات API دسترسی داشته باشند.

برای مثال در یک سیستم نظارتی مبتنی بر اینترنت اشیا، مدیران می‌توانند کاربرانی با دسترسی‌های مختلف ایجاد کنند. یک مدیر، حسابی برای یک نگهبان ایجاد می‌کند به‌طوری‌که فقط به اطلاعات ساختمان‌های خاصی بر روی سایت دسترسی داشته باشد. با استفاده نگهبان از اپلیکیشن موبایل خود، دستور زیر برای فراخوانی API و نمایش اطلاعات مربوط به دوربین‌های موجود اجرا می‌شود:

```
Api/sites/111/cameras/
```

Response شامل لیستی با جزییات دوربین‌های موجود در قالب زیر است:

```
{"id":"xxx","live_access_token":"xxxx-bbbbb","bulding_id":"yyy"}
```

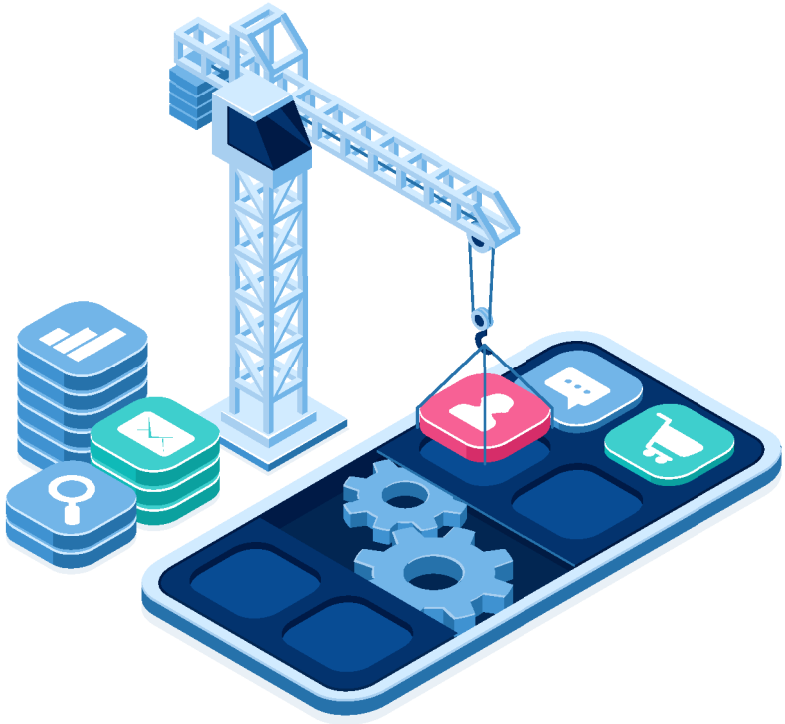
درحالی‌که در UI اپلیکیشن، فقط دوربین‌هایی را نشان می‌دهد که نگهبان به آن دسترسی دارد، اما response واقعی API شامل لیست تمامی دوربین‌های موجود در سایت است و نگهبان می‌تواند به سایر دوربین‌ها با تغییر ID دسترسی داشته باشد.

سناریوها

- API شیء داده را به شکلی که در پایگاه داده ذخیره‌شده است، هنگام فراخوانی، به‌طور کامل بازیابی می‌کند.
- اپلیکیشن client تمامی پاسخ‌ها را فیلتر و صرفاً اطلاعاتی که موردنیاز کاربر است به او نمایش می‌دهد.
- مهاجمان با فراخوانی API قادر به دستیابی به اطلاعات حساسی هستند که توسط رابط کاربری فیلتر شده است.

راه‌های جلوگیری

- فیلتر کردن داده‌ها در سمت client انجام نشود.
- با بررسی تمام response ها، پاسخ‌های API ها را با توجه به نیاز clientها، تنظیم کنید تا از محتوای آن‌ها مطمئن شوید. همچنین پاسخ‌های خطای مناسب تعریف کنید.
- طراحان backend باید قبل از در معرض دسترس قرار دادن هر داده از خود بپرسند که: مصرف‌کننده داده چه کسی است؟
- از متدهای عمومی به‌صورت to_json() و to_string() استفاده نکنید. در عوض properties هایی که لازم دارید را به‌صورت cherry-pick برگردانید.
- مکانیزمی برای بررسی همه response های برگشتی از API را به‌عنوان یک لایه امنیتی اضافه پیاده‌سازی کنید. به‌عنوان بخشی از این مکانیزم، قالب و محدودیت‌هایی برای تمامی متدهای Api شامل error ها تعریف شود.
- تمامی اطلاعات حساس و personally identifiable information (PII) را که اپلیکیشن ذخیره و با آن‌ها کار می‌کند را شناسایی نموده و تمام API Call ها در جهت اینکه آیا می‌تواند باعث بروز مشکل شود یا خیر؛ بررسی کنید.
- برای جلوگیری از نشت تصادفی داده‌ها، فرآیندی برای بررسی همه response ها اعمال کنید.



04 Lack of Resources & Rate Limiting

امکان محافظت از API در برابر حجم زیادی از درخواست‌ها یا پیلودها وجود ندارد. به‌این‌ترتیب مهاجمان با بهره‌گیری از این نقص و از طریق ارائه درخواست‌های پی‌درپی منجر به حملات منع دسترسی (DoS) و حملاتی مانند brute force می‌شوند.
به‌طور مثال، در یک صفحه قرار است لیستی از کاربران با محدودیت نمایش ۲۰۰ کاربر در هر صفحه‌نمایش داده شود. حال اگر مهاجم، پارامتر فراخوانی تعداد را از ۲۰۰ به ۲۰۰۰۰ تغییر دهد، باعث بروز مشکل در پایگاه داده می‌شود و در همین حال، API قادر به پاسخ و رسیدگی به درخواست‌ها نیست. این اتفاق نمونه‌ای از وقوع DoS است.

```
/api/users?page=1&size=200
```

سناریوها

- ارسال درخواست‌های بیش‌ازحد توان API توسط مهاجمان (overload the API)
- ارسال درخواست‌هایی با سرعتی بالاتر از سرعت پردازشAPI(clogging it up)
- ارسال Zip Bombs که فایل‌هایی هستند که باز کردن آن‌ها منابع زیادی از API را در اختیار گرفته و در آن اختلال ایجاد می‌کند.

راه‌های جلوگیری

- محدودیت‌های زمانی مناسبی را در جهت این‌که client در یک بازه زمانی مشخص چند بار می‌تواند API را فراخوانی کند، تعریف کنید.
- یک rate-limiting مناسب تعریف شود.
- میزان حجم payload را محدود کنید.
- برای container resource محدودیت تعیین کنید.
- نرخ فشرده‌سازی را بررسی کنید.
- با عبور از هر محدودیت، به client اطلاع‌رسانی کنید.
- اعتبارسنجی سمت سرور را برای بررسی کوئری‌ها و مواردی مانند کنترل تعداد رکوردهای برگشتی را انجام دهید.

05 Broken Function Level Authorization

سیاست‌های کنترل دسترسی پیچیده، با سلسله‌مراتب‌ها، نقش‌ها و گروه‌هایی با عدم تفکیک نامشخص بین توابع معمولی و توابع مدیریتی، موجب نقض Authorization می‌شود. با بهره‌برداری از این مشکل، مهاجمان می‌توانند به منابع کاربر یا توابع مدیریتی دسترسی پیدا کنند. در زمینه سلسله‌مراتب‌ها، نقش‌ها و گروه‌ها ابهاماتی باید پاسخ داده شود.

با بررسی یک مثال می‌توانیم به مفهوم این موضوع پی ببریم. در طی مراحل ثبت‌نام یک اپلیکیشن موبایل، فقط به کاربرانی که دعوت‌نامه دارند اجازه ثبت داده می‌شود. API هر دعوت‌نامه به شکل زیر است و response هر درخواست یک JSON شامل جزییات مربوط به دعوت ازجمله مشخصات و نقش کاربر است:

```
GET api/invites/{invite_guide}
```

یک مهاجم با duplicate کردن درخواست و تغییر endpoint و متد HTTP، درخواست را به‌صورت زیر درمی‌آورد.

```
POST api/invites/new
{"email":"user@mail.com","role":"admin"}
```

مهاجم با بهره‌برداری از این مشکل، می‌تواند برای خود دعوت‌نامه ایجاد کند.

سناریوها

- برخی از توابع و فایل‌های مدیریتی به‌عنوان API در معرض دسترسی قرار می‌گیرند.
- کاربران غیرمجاز بدون Authorization قادر به دسترسی به این توابع هستند.
- کاربران از طریق تغییر مقادیر در URL به مواردی که نباید دسترسی داشته باشند، دسترسی پیدا می‌کنند. به‌طور مثال با تغییر یک کلمه یا پارامتر و وجود نام‌گذاری قابل پیش‌بینی، بتوانند به لیست کلیه کاربران دسترسی پیدا کنند.

```
Api/users/v1/user/myinfo
Api/admins/v1/users/all
```

راه‌های جلوگیری

- به‌طور پیش‌فرض همه‌ی دسترسی‌ها را رد کنید.
- فقط به کاربران متعلق به گروه یا نقش موردنظر اجازه فعالیت داده شود.
- طراحی و ارزیابی دسترسی‌ها، سلسله‌مراتب‌ها و نقش‌ها به‌درستی انجام گیرد.

06 Mass Assignmet

داده‌هایی که توسط client تهیه‌شده‌اند، بدون استفاده از فیلترینگ مناسب ذخیره می‌شوند، در این خصوص مهاجمان می‌توانند ویژگی‌های object را حدس زده یا یک خصوصیت جدید را به درخواست‌های خود اضافه کند.
به‌طور مثال یک برنامه به کاربر اجازه می‌دهد اطلاعات پروفایل کاربری خود را ویرایش کند. در طی یک درخواست با استفاده از متد PUT به API، پاسخ زیر در قالب JSON دریافت می‌شود.

```
PUT /api/v1/users/me
{"user_name":"inons","age":24}
```

با تغییر متد HTTP به GET به‌طور مثال یک فیلد اضافی درباره میزان تراز اعتبار کاربر نیز نمایش داده می‌شود.

```
GET /api/v1/users/me
{"user_name":"inons","age":24,"credit_balance":10}.
```

مهاجم با دست‌کاری فیلد اعتبار و تغییر به مقدار دلخواه، درخواست بالا که با استفاده از متد PUT ارسال می‌شد را به شکل زیر تغییر می دهد و بدون هیچ پرداختی اعتبار خود را افزایش دهد.

```
{"user_name":"inons","age":24,"credit_balance":99999}.
```

سناریوها

- API بدون فیلتر و محدودیت با data structure های مختلف کار می‌کند.
- Payload های دریافتی به‌صورت کورکورانه تبدیل به object و ذخیره می‌شوند.
- مهاجمان با مشاهده درخواست‌های GET می‌توانند فیلدها را حدس بزنند.

راه‌های جلوگیری

- داده‌های ورودی و اشیا داخلی را به‌طور خودکار متصل نکنید.
- تمام پارامترها و payloadsهای مورد انتظار را به‌روشنی تعریف کنید.
- برای مواردی که از API بازیابی می‌شوند اما نباید ویرایش شوند، خاصیت readonly را در object schema برابر true قرار دهید.
- یک لیست سفید از مواردی که client می‌تواند تغییر دهد را ایجاد کنید. همچنین یک لیست سیاه برای مواردی که نباید دسترسی داشته باشند نیز تهیه کنید.
- در زمان طراحی، تعدادی pattern و schema و type از پیش تعیین‌شده برای درخواست‌ها در نظر گرفته و بعداً همه را در زمان اجرا اعمال کنید.

07 Security Misconfiguration

پیکربندی نامناسب سرورهای API به مهاجمان امکان سوءاستفاده از آن‌ها را می‌دهد.
به‌طور مثال یک مهاجم پرونده.bash_history را در دایرکتوری ریشه سرور پیدا می‌کند که حاوی دستوراتی است که توسط تیم توسعه برای دسترسی به API استفاده‌شده است:

```
$ curl -X GET "https://api.server/endpoint/" -H "authorization: Basic Zm9vOmJhcg=="
```

همچنین مهاجم با استفاده از این اطلاعات (authorization: Basic Zm9vOmJhcg==) که برای احراز هویت جهت دسترسی به یک منبع استفاده‌شده است، می‌تواند سایر endpoint هایی که فقط توسط تیم توسعه استفاده می‌شود و در مستندات موجود نیست را نیز پیدا کند.

سناریوها

- سیستم‌های پچ نشده
- اسناد و دایرکتوری‌های محافظت نشده
- Image های امن سازی نشده
- TLS منسوخ‌شده یا دارای پیکربندی اشتباه
- به نمایش گذاشتن پنل‌های ذخیره‌سازی یا مدیریتی سرور
- نبود سیاست‌های اشتراک منابع متقابل (CORS)
- نبود header های امنیتی
- فعال بودن ویژگی‌های غیرضروری
- پیام‌های خطا که اطلاعات حساس را به نمایش می‌گذارند

راه‌های جلوگیری

- یک فرایند تکرارشونده قابل‌اطمینان را برای فرایند پچ قرار دهید.
- یک پروسه برای بررسی و به‌روزرسانی تنظیمات کل API قرار دهید. موارد بررسی باید شامل کلیه‌ی اجزای API و سرویس‌های ابری مانند مجوزهای دسترسی bucket S3 باشد.
- یک فرایند خودکار برای بررسی اثرات تنظیمات در همه بخش‌ها و محیط‌ها ایجاد شود.
- عیب‌یابی پیکربندی به‌صورت خودکار انجام شود.
- دسترسی‌های بخش مدیریت را محدود کنید.
- ویژگی‌های غیرضروری را غیرفعال کنید.
- برای جلوگیری از ارسال اطلاعات حساس به مهاجمان، همه خروجی‌ها، ازجمله خطاها را به شکل سفارشی تعریف کنید.

08 Injection

از حملات تزریق به‌عنوان یکی از انواع حملات موردعلاقه مهاجمان نام‌برده می‌شود. این حمله انواع مختلفی دارد ازجمله: OS، LDAP، noSql، sql. در طراحی APIها باید نسبت به این حملات امن‌سازی صورت گیرد. نظارت مداوم پس از پیاده‌سازی نیز برای اطمینان از امنیت کدها ضروری است.

سناریوها

- حملات injection، مانند Command Injection، NoSQL، SQL و غیره، هنگامی رخ می‌دهد که داده‌های مخرب به‌عنوان بخشی از یک پارامتر به مفسر ارسال می‌شود. داده‌های مخرب مهاجم می‌تواند مفسر را فریب دهد تا دستورات ناخواسته را اجرا کند یا بدون مجوز مناسب به داده‌ها اجازه دسترسی بدهد.

راه‌های جلوگیری

- هرگز به‌طور کامل به client های API اعتماد نکنید. اگرچه مورداستفاده داخلی باشد.
- کلیه‌ی داده‌های دریافتی اعتبارسنجی و فیلترینگ شوند.
- برای جلوگیری از نشت داده، خروجی‌ها را محدود کنید.
- تمام شکل‌های ممکن داده‌های ورودی از قبل تعریف و در زمان اجرا، اعمال شوند.

09 Improper asset management

مهاجمان با شناسایی نسخه‌های غیررسمی که به‌اندازه نسخه اصلی محافظت نشده‌اند مانند نسخه بتا یا نسخه‌های قدیمی، اقدام به انجام حملات خود می‌کنند.
به طور مثال یک شبکه اجتماعی از مکانیزم محدودکننده نرخ درخواست برای جلوگیری از حدس توکن‌های reset password با استفاده از حملات brute-force پیاده‌سازی کرده است.
این مکانیزم به عنوان بخشی از API در نظر گرفته نشده است و به عنوان یک کامپوننت بین کاربر و API با آدرس www.socialnetwork.com قرار گرفته شده است. اکنون یک محقق امنیتی نسخه بتای این API را که در آدرس www.mbasic.beta.socialnetwork.com میزبانی می‌شود را پیدا می‌کند که در این نسخه مکانیزم محدود کردن نرخ درخواست پیاده‌سازی نشده است و با استفاده از این ضعف پیاده‌سازی، توانسته توکن‌های بازیابی رمز عبور را brute-force کند و در نهایت قادر بوده با استفاده از توکن‌های شش رقمی بازیابی رمز عبور به دست آمده، گذرواژه کاربران سامانه را بازیابی و به حساب کاربری آن ها دسترسی پیدا کند.

سناریوها

- استفاده از نسخه‌های ناامن و قدیمی
- تلاش برای ایجاد سازگاری در جهت اجرای نسخه‌های قدیمی API
- با احراز هویت از طریق یک endpoint، مهاجم امکان دسترسی به endpoint ها و حتی منابع و محصولات نهایی دیگر را نیز دارد.

راه‌های جلوگیری

- به‌روز نگه‌داشتن، فهرست کلیه‌ی میزبان‌های API
- محدود کردن دسترسی به هر چیزی که نباید عمومی باشد.
- نسخه‌های مختلف از منابع دادهای مشترک استفاده نکنند.
- اقدامات کنترل‌کننده خارجی مانند استفاده از API firewall را استفاده کنید.
- از نسخه‌های قدیمی استفاده نکنید یا مشکلات امنیتی را در آن‌ها رفع کنید.
- احراز هویت دقیق، کنترل redirect ها و CORS ها را پیاده‌سازی کنید.

Insufficient Logging & Monitoring

10

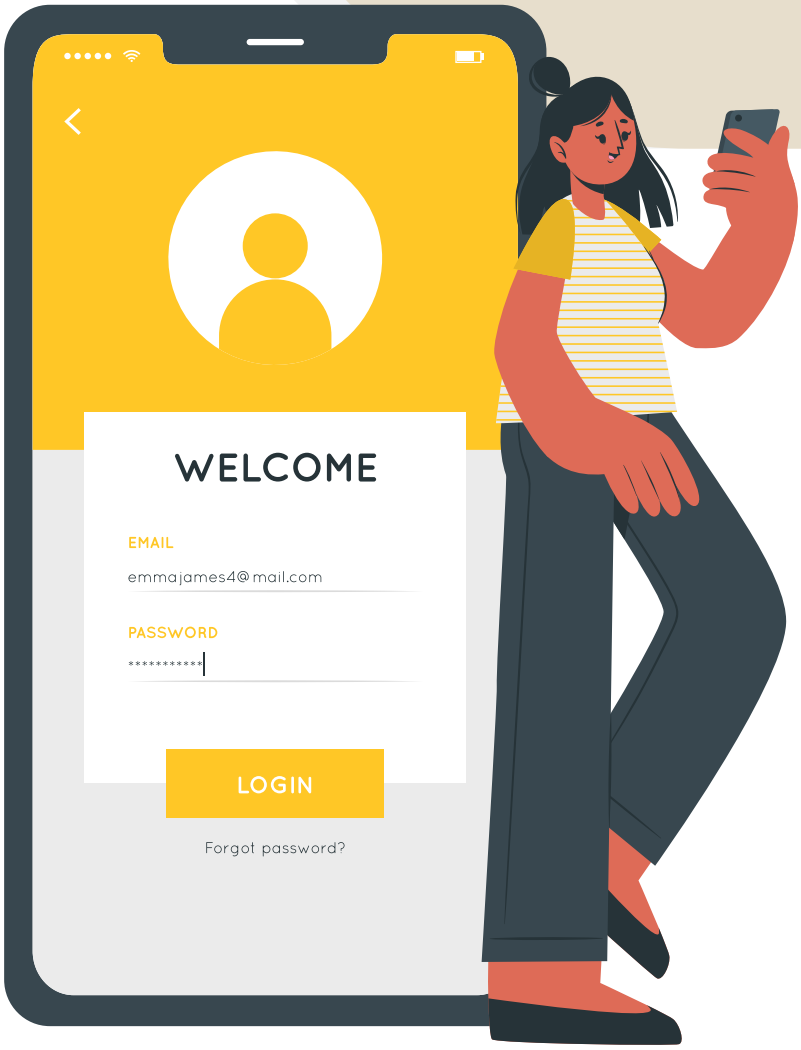
عدم توجه به log ها، مانیتورینگ و هشدار دهی، باعث سوءاستفاده مهاجمین می‌شود.
به‌طور مثال، یک پلتفرم اشتراک ویدیو موردحمله‌ی credential stuffing قرار گرفت. باوجود ورودهای ناموفق در طول حمله، هیچ هشداری داده نشد. بعدها برای رسیدگی به شکایت کاربران در این زمینه، گزارش‌های API موردبررسی قرارگرفته و حمله شناسایی شد و پس‌ازآن این شرکت با یک اعلام عمومی از کاربران خود خواست تا رمزهای عبور خود را تغییر دهند.

سناریوها

- کنترل لاگ‌ها به‌درستی تنظیم‌نشده و پیام‌های آن، جزییات کافی را ندارند.
- هشدارها به‌درستی طراحی نشده‌اند.
- عدم کنترل مستمر لاگ‌ها و نبود یکپارچگی در آن‌ها.
- عدم کنترل زیرساخت API ها.
- گزارش‌ها و لاگ‌ها در سیستم‌های امنیتی و مدیریت رویداد ثبت نمی‌شوند.

راه‌های جلوگیری

- مواردی مانند تلاش‌های ناموفق، دسترسی‌های غیرمجاز، تأیید اعتبار ورودی‌ها یا هرگونه اشکال در سیاست‌های امنیتی به‌عنوان گزارش ثبت شود.
- از لاگ‌ها همان‌طور که از اطلاعات حساس محافظت می‌شود، محافظت کنید.
- از فرمت و قالب لاگ‌ها از نظر وجود جزییات کافی مطمئن شوید تا ابزارهای دیگر نیز بتوانند از آن استفاده کنند.
- درج جزییات کافی برای شناسایی مهاجمان در لاگ‌ها
- عدم درج اطلاعات حساس در گزارش‌ها. اگر نیاز بود اطلاعاتی برای اشکال‌زدایی ثبت شود، تا حد امکان تغییر داده شود.
- سایر ابزارهای امنیتی و هشدارها را پیکربندی کنید. با این کار امکان اینکه زودتر فعالیت‌های مشکوک شناسایی و به آن‌ها پاسخ داده شود، به وجود می‌آید.



مقدمه‌ای بر تحلیل بدافزار و معرفی ابزارهای این حوزه

تهیه و تدوین: محمد ساروقی

مقدمه

«کامپیوتر من ویروس دارد!» تقریباً هرکسی که با هر نوع دستگاه هوشمند درگیر باشد این عبارت را گفته یا شنیده است. امروزه، به‌طور مکرر در مورد حملات ویروسی به ساختار فناوری اطلاعات در سرتاسر جهان اخبار مختلفی به گوش می‌رسد. برخی از این حملات، میلیون‌ها کاربر را در سرتاسر جهان تحت تأثیر قرار می‌دهند. در این مقاله بررسی می‌شود که اصطلاح ویروسی‌شدن دقیق و علمی نیست و فقط برای عنوان، یک مشکل در میان عامه مردم است. اصطلاح صحیح و علمی که در این باره مورداستفاده قرار می‌گیرد بدافزار است که ویروس‌ها یک گروه از بدافزارها می‌باشند.

بدافزار چیست؟

ازنظر لغوی بدافزار معادل کلمه Malware است که خود از عبارت Malicious Software اقتباس شده است. در حالت کلی به هرگونه ابزاری که توسط فرد مهاجم برای اجرای انگیزه‌های شوم مورداستفاده قرار گیرد، بدافزار می‌گویند. ازنظر فنی، یک نرم‌افزار یا یک بخشی از نرم‌افزار را که به دنبال اهداف خرابکارانه در یک ساختار باشد، نرم‌افزار مخرب یا بدافزار گویند.

بدافزارها از زمان به وجود آمدن نرم‌افزارها و دستگاه‌های محاسباتی وجود داشته‌اند اما در اوایل برای کاربران نگران‌کننده نبوده‌اند. بخش‌هایی مانند بانکداری، سازمان‌های مالی و دولت‌ها درگذشته بیشتر موردتوجه بدافزارها قرار می‌گرفتند اما چشم‌انداز بدافزارها باگذشت زمان به‌شدت تغییر کرد. پیش‌ازاین به نظر می‌رسید که باارزش‌ترین دارایی پول است اما اکنون باارزش‌ترین دارایی، داده‌ها و اطلاعات هستند و به هدف اصلی بدافزارها تبدیل‌شده‌اند. سازمان‌هایی که اطلاعات مربوط به افراد جامعه را در هر زمینه‌ای نگهداری می‌کنند، مسئول حفظ امنیت این داده‌ها هستند؛ بنابراین هیچ سازمانی در دنیا نمی‌تواند امنیت سایبری را قطعی بداند زیرا مهاجمان به دنبال دسترسی به باارزش‌ترین دارایی انسان‌ها هستند. امروزه، هیچ‌کس نمی‌تواند خود را از گزند بدافزارها در امان بداند. درگذشته حملات به‌طور مستقیم شامل یک شرکت یا یک نهاد دولتی بوده است اما امروزه حملات در سطح کاربران رشد کرده است. بدافزار تقریباً بخشی از هر حمله سایبری است که توسط مهاجمان انجام می‌شود. مهاجمان هر روز میلیون‌ها بدافزار جدید ارائه می‌کنند اما تعداد متخصصان امنیت که بر روی بدافزارها کار می‌کنند بسیار کمتر از تعداد موردنیاز برای مقابله با این بدافزارها هستند. در ادامه انواع بدافزارها به‌صورت مختصر توضیح داده می‌شوند و سپس به بررسی روش‌های تجزیه‌وتحلیل بدافزار خواهیم پرداخت و درنهایت ابزارهای مختلف را به‌صورت مختصر معرفی می‌کنیم.

انواع بدافزار

ویروس

اولین نوع بدافزار است که به‌عنوان تکثیر شونده توسط عامل انسانی شناخته می‌شود. همچنین به آن File Infector یا آلوده‌کننده فایل نیز گفته می‌شود. ویروس‌ها با آلوده کردن و قرار گرفتن در سایر پرونده‌های سالمِ موجود در سیستم، به بقای خود ادامه می‌دهند. برنامه‌های سالم در زمان اجرا، ویروس پیوست‌شده را نیز اجرا می‌کنند.

کرم

یک بدافزار است که می‌تواند در شبکه یا با استفاده از تجهیزات فیزیکی USB و غیره گسترش یابد و عملیات موردنظر مهاجم را اجرا کند. کرم‌ها به‌عنوان بدافزارهای خود تکثیر شونده شناخته می‌شوند.

درب‌پشتی

درب‌پشتی یک نقطه ورود غیرمجاز است که توسط آن مهاجم می‌تواند به سیستم قربانی وارد شود. به‌عنوان‌مثال، بدافزار می‌تواند یک پورت باز ایجاد کند که دارای دسترسی Shell است و مهاجم می‌تواند به آن دسترسی پیدا کند.

Trojan

یک نوع بدافزار است که به‌عنوان یک نرم‌افزار سالم شناخته می‌شود و با آگاهی کامل کاربر بر روی دستگاه قربانی نصب می‌شود اما کاربر از اهداف مخرب واقعی آن آگاهی ندارد.

Spyware

Spyware یا Info stealer یک جاسوس ابزار است که اطلاعات حساس سیستم را جاسوسی و به سرقت می‌برد. داده‌های هدف جاسوسی می‌تواند نام کاربری، رمزهای عبور، تصاویر و یا اسناد محرمانه باشند.

Key logger

نوعی نرم‌افزار جاسوسی است که می‌تواند کلیدهای فشار داده‌شده توسط کاربر را ضبط و برای مهاجم ارسال کند.

Botnet

یک شبکه ربات می‌باشد که شامل چندین دستگاه است که توسط بدافزار آلوده شده‌اند. بدافزارهایی که این شبکه ربات یا Botnet را تشکیل می‌دهند به‌عنوان یک گروه با یکدیگر همکاری می‌کنند و دستوراتی را که یک مهاجم از طریق سرور مرکزی ارسال می‌کند، اجرا می‌کنند. نمونه‌ای از نتایج اجرای شبکه Botnet اجرای حمله منع سرویس توزیع‌شده است.

دسترسی از راه دور (RAT)

یک بدافزار یا یک ویژگی از بدافزارها است که می‌تواند کنترل سیستم را به مهاجم بدهد. این ابزارها بسیار شبیه به برنامه‌های کنترل از راه دور هستند با این تفاوت که می‌توانند دسترسی‌های متفاوتی به سیستم قربانی داشته باشند. بدافزار RAT بدون هیچ‌گونه مجوزی به سیستم هدف متصل می‌شود.

Adware

با نام ابزارهای تبلیغاتی مزاحم، نوع متداول از بدافزارها هستند که معمولاً با آن روبرو هستیم اما هرگز متوجه حضور این برنامه‌ها نشده‌ایم. ابزارهای تبلیغاتی مزاحم همراه با دانلود نرم‌افزارها نصب می‌شوند. همه ابزارهای تبلیغاتی مخرب نیستند اما می‌توان آن را به‌عنوان زیرمجموعه از Trojan ها در نظر گرفت.

Rootkit

یک بدافزار یا ترکیبی از توابع بدافزاری همراه با یک برنامه دیگر است که هدف آن مخفی‌کردن فعالیت‌های خود یا بدافزار است. Rootkit بیشتر باهدف تغییر در عملکرد توابع سیستم و یا سرقت داده‌ها عمل می‌کند.

Banking malware

بدافزارهای بانکی با رهگیری و تغییر ارتباط مرورگر برای دریافت اطلاعات معاملات و اعتبارات بانکی کار می‌کند که هدف نهایی آن سرقت اطلاعت حساب‌های بانکی قربانی است.

Point-of-sale malware (POS)

این بدافزار دستگاه‌های POS را آلوده می‌کند. این دستگاه‌ها در اکثر مغازه‌ها، مراکز خرید و رستوران‌ها مورداستفاده می‌گیرند. عملکرد اصلی بدافزار POS شامل تلاش برای سرقت اطلاعات کارت‌های اعتباری از طریق نرم‌افزار POS است.

Ransomware

باج‌افزار از طریق رمزنگاری داده‌ها، پرونده‌ها و سایر منابع سیستم و در ازای آزادسازی این اطلاعات از قربانی خود باج‌خواهی می‌کند. در مقایسه با سایر انواع بدافزارها، طراحی باج‌افزارها برای هکرها آسان‌تر هستند اما بازیابی اطلاعات رمزنگاری‌شده توسط باج افزار سخت و دشوار است و رمزگشایی داده‌ها نیازمند کار بسیار است همچنین امکان از بین رفتن اطلاعات در روند رمزگشای بسیار بالا است.

Crypto miner

یکی از بدافزارهای جدید است که هیچ‌گونه آسیبی به اطلاعات قربانی نمی‌زند اما این بدافزار از منابع پردازشی سیستم قربانی برای استخراج رمز ارزها استفاده می‌کند.

Downloader

بدافزاری است که دیگر بدافزارها را بارگیری می‌کند. Botnets با دریافت دستور از سرور مرکزی، به‌عنوان دریافت‌کننده عمل می‌کنند و بدافزار دیگری را بارگیری می‌کنند. امروزه، بدافزارهای زیادی مبتنی بر پرونده‌های مایکروسافت آفیس به‌عنوان دریافت‌کننده عمل می‌کنند که درنتیجه بدافزارهای دیگر را بارگیری می‌کند. Emotet یک بدافزار معروف است که از یک دریافت‌کننده ماکرو مایکروسافت آفیس استفاده می‌کند.

Spammers

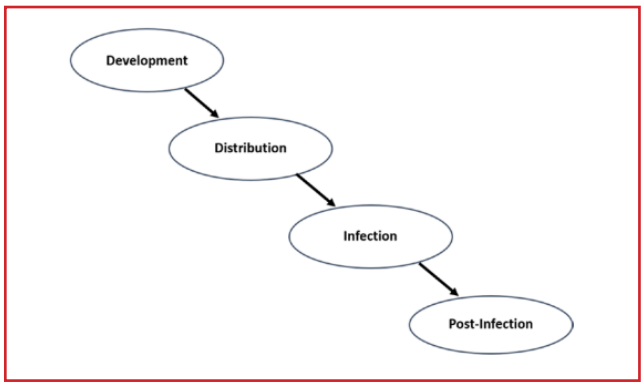
ایمیل‌های هرزنامه را با استفاده از دستگاه قربانی ارسال می‌کند. هرزنامه ممکن است حاوی ایمیل‌هایی که خود حامل پیوندهای وب‌سایت‌های مخرب هستند، باشند. این بدافزار ممکن است مخاطبین سرویس‌گیرنده‌های ایمیل مانند Microsoft outlook را که بر روی دستگاه قربانی نصب‌شده است بخواند و برای مخاطبین ایمیل‌های مخرب ارسال کند.

چرخه عملکرد بدافزار

در ابتدا هدف و انگیزه از حملات سایبری بیشتر مسائل مالی یا سرگرمی بوده است اما اکنون بیشتر هدف جاسوسی است که توسط مجرمان با بودجه و ساختار سازمان‌یافته اداره می‌شوند. در جنگ سایبری، بدافزارها به‌عنوان سلاح اصلی استفاده می‌شود و توانایی آسیب رساندن به هر هدفی در هر سطحی را دارند. بدافزارها مانند سایر نرم‌افزارها به‌صورت ماژولار نوشته‌شده‌اند. هرکدام از ماژول‌ها توسط سازندگان مختلف توسعه داده‌شده‌اند. عموماً، ماژول‌های یکسانی در بین خانواده‌های مختلف بدافزارها شناسایی می‌شوند که درنتیجه منجر به تسریع روند تجزیه‌وتحلیل بدافزار می‌شود.

همانند فرآیند تضمین کیفیت نرم‌افزار (QA)، بدافزار نیز مراحل آزمایش را طی می‌کند تا سازندگان مطمئن شوند مطابق انتظار عمل می‌کند. بسیاری از بدافزارها مانند نرم‌افزارهای معمولی خود را به‌روزرسانی می‌کنند. بدافزارهای نهایی معمولاً رمزگذاری، مبهم‌سازی و فشرده می‌شوند و سپس با استفاده از محصولات شناسایی بدافزار آزمایش می‌شوند تا اطمینان حاصل شود که بدافزار توسط محصولات امنیتی شناسایی نمی‌شود.

بدافزارها برای اهداف مختلفی بر اساس نیاز مهاجم ساخته می‌شوند. بدافزارها باید توزیع شوند تا پس از عبور از موانع امنیتی هدف، به سیستم موردنظر دسترسی پیدا کند اما دسترسی به سیستم موردنظر کافی نیست و می‌بایست از سامانه‌های دفاعی سیستم هدف در امان بماند و هدف را با موفقیت آلوده کند. آخرین مرحله چرخه حیات بدافزار انجام اهداف بعد از آلودگی هدف است. اهداف نهایی می‌تواند درآمدزایی، جاسوسی یا موارد دیگر باشد. در شکل ۱ مراحل چرخه عملکرد بدافزار نشان داده‌شده است.



شکل ۱- چرخه عملکرد بدافزار

ماهیت تطبیقی و فریبندگی بدافزارها

ویروس‌های رایانه‌ای (بدافزار) مانند ویروس‌ها و میکروب‌های واقعی در بدن انسان تکامل می‌یابند. آن‌ها با تغییر خود در محیط سازگار می‌شوند و در برابر دفاع ضد بدافزار مقاومت می‌کنند. تعدادی از بدافزارها، نرم‌افزارهای ضد بدافزار را بر روی سیستم شناسایی و روند شناسایی آن‌ها را دور خواهند زد. همچنین بدافزارها در صورت تشخیص حضور ضد بدافزارها در محیط، کیفیت و عملکرد واقعی خود را نشان نخواهند داد. در این حالت مقابله با بدافزارها و روند شناسایی بدافزار بسیار دشوار است.

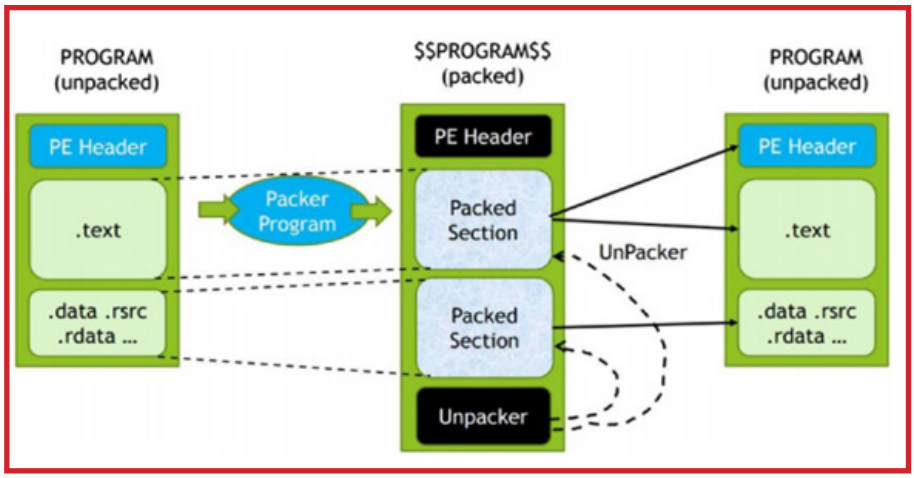
Packer بدافزارها

مهاجم از نسخه خام بدافزار برای حمله به هدف استفاده نمی‌کند. یکی از دلایل این امر به این صورت است که برنامه‌های ضد بدافزار با استفاده از امضای ثابت می‌توانند بدافزار را به‌راحتی شناسایی کنند. عامل دوم، حجم بالای بدافزار است که بارگذاری آن بر روی سیستم قربانی زمان‌بر است. برای جلوگیری از تشخیص زودهنگام برنامه‌های ضد بدافزار ابتدا مهاجم بدافزار را رمزگذاری، فشرده‌سازی و درنهایت Packer می‌کند. همان‌طور که برنامه‌های معمولی نیز نیاز به Packer برای جلوگیری از نشت اطلاعات برای رقبای خود دارند، بدافزار نیز رمزنگاری و Packer می‌شود.

بدافزارها از الگوریتم‌های رمزنگاری مانند RC۴، Xtea، AES و Base۶۴ استفاده می‌کنند همچنین برای فشرده‌سازی نیز از الگوریتم‌های LZSS، LZMA و APLib برای رمزنگاری و فشرده‌سازی بخش‌هایی از کُد و داده‌ی خود استفاده می‌کنند درحالی‌که به‌صورت یک فرآیند اجرا می‌شوند. در هنگام تجزیه‌وتحلیل و شناسایی بدافزار، این موارد به یک چالش تبدیل‌شده‌اند که محققان باید در ابتدا روند رمزنگاری و فشرده‌سازی را برطرف کرده سپس به تجزیه‌وتحلیل برنامه بپردازند.

اکثر برنامه نویسان بدافزار خود را درگیر مباحث مربوط به رمزنگاری و فشرده‌سازی نمی‌کنند و در عوض این وظیفه را به نرم‌افزار جداگانه آماده Packer واگذار می‌کنند که پرونده‌های اصلی بدافزار را دریافت و فایل رمزنگاری و فشرده‌شده را تحویل می‌دهد. نرم‌افزارهای Packer برنامه‌ای هستند که فایل‌های اجرایی را فشرده و رمزنگاری می‌کنند. فشرده‌سازی یک فایل اجرایی باعث کاهش اندازه و همچنین تغییر ظاهر فایل اجرایی می‌شود و محتوای برنامه را ناخوانا می‌کند که یک مزیت عمده برای بدافزارها محسوب می‌شود.

برنامه Packer یک فایل اجرایی PE را به‌عنوان ورودی می‌گیرد و یک فایل اجرایی PE جدید را که اکنون Packer شده است، تولید می‌کند. یک فایل PE قابل‌اجرا عمدتاً دارای دو جزء است: سرآیندها و بخش‌ها، بخش‌ها می‌توانند حاوی کُد، داده و منابع مورد نیاز برنامه باشند. بخش‌ها اجزای اصلی هستند که برای کاهش اندازه قابل‌اجرا نیاز به فشرده‌سازی دارند. برنامه Packer سرآیندها و بخش‌ها را از پرونده PE که Packer می‌کند می‌گیرد و سرآیندها و بخش‌های جدید را تولید می‌کند. سرآیندها و بخش‌های جدید برای تولید یک فایل اجرایی جدید باهم ترکیب می‌شوند که فشرده‌شده و فضای کمتری را بر روی حافظه سخت‌افزاری مصرف می‌کند که درعین‌حال داده‌های آن نیز مبهم است.



شکل ۲- فرایند Packer در بدافزارها

اکنون کد و داده‌ها در پرونده‌های اجرایی فشرده‌شده و تولیدشده است آیا هنگام اجرا به‌درستی اجرا می‌شود؟ اگر جواب مثبت است چگونه؟ هنگام ایجاد فایل اجرایی Packerشده جدید، یک نسخه سبک Packer که محل کُد و داده‌های فشرده‌شده را در پرونده Packerشده می‌داند در خود قرار می‌دهد که می‌تواند کُد و داده‌های فشرده‌شده را دریافت و کُد و داده‌های فشرده نشده را بازیابی کند. فرایند Packer در شکل ۲ نشان داده‌شده است.

یک تحلیلگر بدافزار با نمونه‌های مختلف بدافزار روبرو می‌شود. بدافزارهایی که توسط مهاجم Packer نشده باشند، بدافزارهایی که Packerشده باشند و یا یک بدافزار Packer نشده توسط تحلیلگر دیگری که برای تحلیل به او داده شود. اولین آزمایش در تحلیل بدافزار این است که متوجه شویم یک بدافزار Packer شده است یا نه که برخی از روش‌ها به‌صورت ایستا به کار گرفته می‌شوند این روش‌ها زمانی مورداستفاده قرار می‌گیرند که بتوان بدون اجرای بدافزار آن را تحلیل کرد. برخی از روش‌های دیگر نیز وجود دارند که می‌توانند تشخیص دهند که آیا بدافزار Packer شده است یا خیر که مجموعه این روش‌ها به تحلیل پویا معروف است. در ادامه یکی از روش‌های بررسی Packer بدافزار را به‌عنوان نمونه بررسی می‌کنیم.

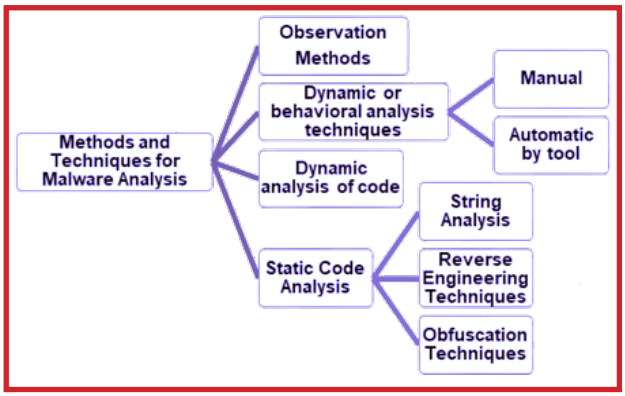
آنتروپی

آنتروپی یک معیار برای بررسی مقدار ابهام موجود در داده‌ها است. در این مسئله آنتروپی یک روش محبوب برای تشخیص رمزنگاری و فشرده‌سازی است زیرا پس از فشرده‌سازی و رمزنگاری داده‌ها درصد تصادفی بودن بالاتری دارند که منجر به مقدار آنتروپی بالاتر می‌شود. به بیان دیگر یک فایل اجرایی Packer نشده دارای ابهام کمتر است درنتیجه میزان تصادفی بودن آن کمتر است و نهایتاً میزان آنتروپی کمتری دارد. برای این منظور می‌توانیم از ابزار PEiD استفاده کنیم. در این برنامه میزان آنتروپی از عدد هشت محاسبه می‌شود که هرچقدر میزان آنتروپی به هشت نزدیک‌تر باشد احتمال این‌که بدافزار موردنظر Packer شده باشد، بیشتر است.

انواع تحلیل بدافزارها

روش‌های مختلف برای تحلیل بدافزار موجود است که در دو دسته کلی تشخیص یک بدافزار و تجزیه‌وتحلیل یک بدافزار دسته‌بندی می‌شوند. برای بررسی ابزارهای مختلفی موجود است که همان‌طور که در شکل ۳ نشان داده‌شده است در زیرمجموعه‌های مختلف دسته‌بندی می‌شوند. بدافزارها را می‌توان علاوه بر اجرا کردن بدون اجرا نیز تحلیل کرد. تحلیل ایستا، تجزیه‌وتحلیل یک بدافزار بدون اجرای آن می‌باشد که در مقابل تجزیه‌وتحلیل مبتنی بر اجرای بدافزار که به تحلیل پویا معروف است قرار دارد. شاید به نظر بیاید که در تحلیل بدافزار این دو روش کاملاً مجزا از یکدیگرند اما در حقیقت چنین نیست زیرا روند تجزیه‌وتحلیل یک بدافزار یک‌روند ترکیبی از دو تحلیل ایستا و پویا است.

تجزیه‌وتحلیل ایستا اولین قدم مفید در تحلیل یک نرم‌افزار مشکوک به بدافزار است اما در بسیاری از مواقع ممکن است نتوان به نتیجه مشخصی رسید. این‌زمانی است که باید از تجزیه‌وتحلیل پویا استفاده کرد. در تحلیل پویا نرم‌افزار اجرا می‌شود و رفتار آن زیر ذره‌بین ابزارهای مختلف بررسی می‌شوند اما قبل از اینکه سراغ تحلیل پویا برویم تحلیل استاتیک یک پیش‌نیاز ضروری است که به ما کمک می‌کند تا مقدمات و ابزارهای لازم برای تحلیل بدافزار را مهیا کنیم. برای مثال امکان دارد نیاز به برخی از چهارچوب‌های NET. باشد و یا ممکن است بدافزار موردنظر یک برنامه جاوا باشد که برای تجزیه‌وتحلیل برنامه‌های جاوا نیاز به Java Runtime Engine(JRE) است. تمام این اطلاعات پیش‌نیاز با استفاده از تجزیه‌وتحلیل ایستا به دست می‌آید.



شکل۳- تقسیم‌بندی ابزارها در تحلیل بدافزار

مهندسی معکوس (Reverse Engineering)

مهندسی معکوس فرآیند کشف اصول یک نرم‌افزار یا سخت‌افزار مانند معماری و ساختار داخلی آن است. سؤالی که باعث ایجاد زمینه‌ای بنام مهندسی معکوس می‌شود این است که برنامه چگونه کار می‌کند؟ بدیهی است که اگر مستندات نحوه عملکرد را داشته باشید که مراحل عملکرد یک برنامه را شرح داده باشد، کار بسیار ساده‌تر می‌شود اما در بدافزارها هیچ اسنادی وجود ندارد و شما باید روش دیگری برای یادگیری نحوه کار یک برنامه را پیدا کنید. زمانی که با یک بدافزار روبرو می‌شویم هیچ‌گونه اطلاعی از نحوه عملکرد داخلی آن نداریم پس برای کشف این روند از مهندسی معکوس استفاده می‌کنیم. دانستن خروجی اسمبلی برای نمونه کُدهای مختلف ممکن است به شما در کشف عملکرد اصلی بدافزار کمک کند. در مثال زیر یک نمونه کُد C++ برای سیستم‌عامل ویندوز X۸۶ در نظر می‌گیریم که یک مثال بسیار ساده از نحوه انجام مهندسی معکوس است:

```
int count = 0;
for (int i = 0; i < 10; ++i)
{
count++;
}
std:cout << count
```

اگر این برنامه ساده را در یک فایل اجرایی کامپایل کنیم کُد زیر را در Disassembler مشاهده خواهیم کرد:

```
004113DE loc_4113DE:
004113DE    mov     eax, [ebp14-h]
004113E1    add     eax, 1
004113E4    mov     [ebp14-h], eax
004113E7 loc_4113E7:
004113E7    cmp     [ebp14-h], 0Ah
004113EB    jge     short loc_4113F8
004113ED    mov     eax, [ebp8-]
004113F0    add     eax, 1
004113F3    mov     [ebp8-], eax
004113F6    jmp     short loc_4113DE
004113F8 loc_4113F8:
004113F8    mov     ecx, ds:?cout@std
004113FE    push    eax
00411400    call    ds:basic_ostream@operator<<(int)
00411404    xor     eax, eax
00411406    retn
```

همان‌طور که می‌بینید کُد برنامه به ساختار اسمبلی تبدیل می‌شود حال اگر این کُد را با استفاده از نسخه release کامپایل کنیم خروجی آن به چه صورت خواهد شد؟

```
00401000 main    proc near
00401000         mov     ecx, ds:?cout@std
00401006         push    0Ah
00401008         call    ds:basic_ostream@operator<<(int)
0040100E         xor     eax, eax
00401010         retn
00401010 main    endp
```

این قطعه کُد شبیه کُد قبلی نیست. این امر به‌دلیل نحوه بهینه‌سازی کُد اصلی است که ازنظر فنی حلقه For حذف‌شده است زیرا بهینه‌سازی تصمیم گرفته است که فقط مقدار نهایی متغیر را ذخیره کند و مقدار را به‌صورت مستقیم در خروجی قرار دهد. کامپایلرهایی که امروزه از آن‌ها استفاده می‌شود در بهینه‌سازی کُد، بسیار خوب عمل می‌کنند. به همین دلیل است که هنگام مهندسی معکوس به دنبال یافتن ایده‌ی کد اصلی بدافزار یا نرم‌افزار هستیم تا اینکه بتوان نحوه عملکرد کُد اصلی را درک کرد.

خطایاب‌ها (Debuggers)

درواقع خطایاب‌ها برنامه‌هایی هستند که قادرند برنامه‌ها را خط به خط اجرا کرده و خطاهای موجود در نرم‌افزار را دنبال نمایند. نحوه عملکرد آن‌ها هم بدین‌صورت است که ابتدا نقطه توقف (Break Point) در برنامه ایجاد و سپس آن را اجرا می‌نماید و هنگامی‌که برنامه به این نقطه رسید متوقف‌شده و کاربر می‌تواند مقدار یا عبارت متغیرها را در هنگام اجرا مشاهده نماید.
خطایاب‌ها به دودسته مُد کاربر (User) و مُد هسته (kernel) تقسیم‌بندی می‌شوند و می‌توان این‌گونه بیان نمود که مُد هسته بخشی از سیستم‌عامل است که می‌تواند برنامه‌های راه‌اندازی سیستم را مهندسی معکوس نماید. امروزه از روش‌های مختلف برای جلوگیری از اجرای درست فرآیند Debug در بدافزارها استفاده می‌شود که باعث ایجاد تأخیر زمانی در Debug سریع می‌شود.

جرم‌شناسی در حافظه

تجزیه‌وتحلیل حافظه یا تحلیل داده‌های فرار (Volatile) به تحلیل داده‌ها در حافظه موقت اشاره دارد. متخصصین، حافظه موقت را برای یافتن و ردیابی عوامل مخربی که اطلاعاتی بر روی دیسک سخت‌افزاری باقی نمی‌گذارند را بررسی می‌کنند. Dump حافظه، ذخیره‌ی داده‌های حافظه موقت سیستم در یک لحظه‌ی خاص است که می‌تواند حاوی اطلاعات ارزشمندی درباره وضعیت حافظه قبل و بعد از یک خرابی باشد. همچنین برای بررسی جزئیات در مورد دلایل آنچه اتفاق افتاده است، مورداستفاده قرار می‌گیرد.

جعبه شنی (Sandbox)

به‌منظور جلوگیری از آسیب‌رسیدن به سیستم‌عامل و نرم‌افزارهای موجود در آن، ابزاری طراحی‌شده است محیطی حفاظت‌شده را جهت اجرای نرم‌افزارهای مشکوک به داشتن ویروس یا هر کُد مخربی در سیستم‌عامل ایجاد می‌کند. این محیط امن که در برخی آنتی‌ویروس‌ها و بسته‌های امنیتی نیز مشاهده می‌شود، با نام سطل شنی یا همان Sandbox شناخته می‌شود. Sandbox با ایجاد یک محیط حفاظت‌شده مانع از دسترسی برنامه مشکوک اجراشده به بخش‌های حساس سیستم‌عامل به‌منظور تغییر دادن تنظیمات سیستم و نظارت بر پردازش‌ها می‌شود.

تحلیل پویا شبکه

در این روش با استفاده از بسته‌هایی که در شبکه جریان پیدا می‌کنند و بررسی عوامل مختلف از قبیل آدرس IP، شماره Port و نوع پروتکل و غیره می‌توان اطلاعات مفیدی از بدافزارها در اختیار قرار بگیرد. علاوه بر این، برای تحلیل وب‌سایت‌ها نیز می‌توان به‌صورت پویا عمل کرد و با استفاده از بسته‌های تبادل شده بین کلاینت و سرور به وجود بدافزارها پی برد.

معرفی ابزارهای تجزیه‌وتحلیل

تحلیلگران بدافزار از ابزارهای تجزیه‌وتحلیل بدافزار برای تشخیص به‌موقع، محافظت و پیش‌بینی حملات استفاده می‌کنند. ابزارهای متن‌باز اولین انتخاب تحلیلگران بدافزار هستند. توزیع بدافزارها امروزه به یک تجارت تبدیل‌شده است که محققان با استفاده از ابزارهای تشخیص، انواع عوامل مخرب را بررسی، شناسایی و کنترل می‌کنند. با رشد پیچیدگی‌های انواع بدافزارها، بررسی آن‌ها نیز سخت‌تر شده است که این وظیفه محققان امنیتی است که از روش مناسب و همچنین ابزار مناسب برای تجزیه‌وتحلیل بدافزارهای خاص استفاده کنند. در ادامه برخی از ابزارهای متن‌باز و رایگان در انواع تجزیه‌وتحلیل‌ها معرفی‌شده‌اند که می‌توانند برای متخصصین حوزه تحلیل بدافزار مفید باشد.

ابزارهای تشخیص	
AnalyzePE	Wrapper برای انواع ابزارها و گزارش در مورد فایل‌های PE ویندوز
Chkrootkit	اسکنر Rootkit لینوکس
Detect-It-Easy	نرم‌افزاری برای تشخیص نوع پرونده
hashdeep	محاسبه انواع Hash با الگوریتم‌های مختلف
Loki	اسکنر مبتنی بر میزبان برای IOCs
MASTIFF	یک چهارچوب تحلیل استاتیک
MultiScanner	یک چارچوب تجزیه‌وتحلیل/ تجزیه‌وتحلیل فایل‌های ماژولار
Nsrllookup	ابزاری برای جستجو رشته Hash در پایگاه داده مرجع نرم‌افزار NIST است.
PEV	یک مجموعه ابزار چندمنظوره برای کار با پرونده‌های PE، ارائه ابزارهای تجزیه‌وتحلیل باینری
Yara	ابزار تطبیق الگو برای تحلیلگران
Rootkit Hunter	تشخیص Rootkit در لینوکس
Totallhash.py	یک برنامه پایتون برای جستجو در پایگاه داده TotalHash.cymru.com
TrID	شناسایی نوع فایل
RDG Packer Detector	شناسایی نوع Packer تکنیک‌های مبهم‌سازی
Detect-It-Easy	نرم‌افزاری برای تشخیص نوع پرونده

ابزارهای جرم‌شناسی یا Forensic حافظه

DAMM	تجزیه‌وتحلیل تفاضلی در حافظه، بر اساس نوسانات ایجادشده
FindAES	کلیدهای رمزنگاری AES را در حافظه پیدا می‌کند.
Rekall	یک چهارچوب تجزیه‌وتحلیل حافظه
Volatility	یک چهارچوب پیشرفته Forensics حافظه
evolve	رابط وب برای چهارچوب Forensics حافظه متغیر
Muninn	اسکریپتی برای خودکارسازی بخش‌های تجزیه‌وتحلیل با استفاده از نوسانات و ایجاد یک گزارش خوانا برای کاربر
TotalRecall	اسکریپت مبتنی بر نوسانات برای خودکارسازی مراحل مختلف تجزیه‌وتحلیل بدافزار
WinDbg	رفع اشکال در هسته برای سیستم‌های ویندوز

ابزارهای تجزیه‌وتحلیل بسته‌ها در شبکه

Network Miner	یک ابزار تجزیه‌وتحلیل Forensic شبکه برای سیستم‌عامل ویندوز
PacketTotal	موتور آنلاین برای تجزیه‌وتحلیل پرونده‌های pcap. و مصورسازی ترافیک داخلی برای تجزیه‌وتحلیل بدافزار و پاسخ به حوادث
NetworkTotal	تجزیه‌وتحلیل آنلاین پرونده‌های pcap. برای شناسایی بدافزارها
Wireshark	تجزیه‌وتحلیل پروتکل‌های شبکه

Sandbox و اسکنرهای آنلاین

AndroTotal	تجزیه‌وتحلیل آنلاین APK توسط چندین برنامه ضدویروس تلفن همراه
AVCaesar	مخزن اسکنر و بدافزار آنلاین
Cuckoo Sandbox	Sandbox و سیستم تجزیه‌وتحلیل خودکار متن‌باز
DeepViz	تجزیه‌وتحلیل فایل‌ها با فرمت‌های مختلف برای طبقه‌بندی در کلاس‌های مختلف یادگیری ماشین
Document Analyzer	تجزیه‌وتحلیل فایل DOC و PDF
File Analyzer	تحلیل پویا و رایگان فایل PE
Hybrid Analysis	ابزار تجزیه‌وتحلیل بدافزار آنلاین
Joe Sandbox	تجزیه‌وتحلیل بدافزار بصورت عمیق
Jotti	انتی‌ویروس آنلاین
Malwr	تجزیه‌وتحلیل رایگان با یک نمونه Cuckoo sandbox آنلاین
Metadefender.com	یک پرونده، Hash برنامه یا آدرس IP را برای بدافزار اسکن کنید.
NVISO ApkScan	تجزیه‌وتحلیل پویا APK
SEE	" Sandboxed Execution Environment " یک چهارچوب برای ساخت اتوماسیون ارزیابی در یک محیط امن
VirusTotal	تجزیه‌وتحلیل آنلاین بدافزارها و URL
APK Analyzer	تجزیه‌وتحلیل پویا APK
Cryptam	بررسی اسناد مشکوک office
Comodo Valkyrie	یک سیستم بررسی و ارزیابی فایل با استفاده از چندین نوع تحلیل مختلف در زمان اجرا و بررسی صدها ویژگی از یک برنامه
detux	Sandbox برای تجزیه‌وتحلیل ترافیک بدافزارهای لینوکسی و ثبت IOC ایجادشده
DRAKVUF	سیستم تجزیه‌وتحلیل بدافزار پویا
firmware.re	UNPACKS، اسکن و تجزیه‌وتحلیل بسته‌های FIRMWARE
IRMA	یک سیستم تجزیه‌وتحلیل غیرهمزمان و قابل شخصی‌سازی برای پرونده‌های مشکوک
Limon	Sandbox برای تجزیه‌وتحلیل بدافزار لینوکس
Malheur	تجزیه‌وتحلیل خودکار رفتار بدافزار توسط Sandbox

Sandbox و اسکنرهای آنلاین

MASTIFF Online	آنالیز بدافزار ایستا آنلاین
NoDistribute	پرونده‌ها را با بیش از ۳۵ ضد ویروس اسکن می‌کند.
NetworkTotal	تجزیه‌وتحلیل آنلاین پرونده‌های pcap. برای شناسایی بدافزارها
PDF Examiner	تجزیه‌وتحلیل پرونده‌های مشکوک PDF
URL Analyzer	تجزیه‌وتحلیل پویا از طریق URL

ابزارهای تجزیه‌وتحلیل وب‌سایت‌ها

Desenmascara.me	ابزاری برای بازیابی فراداده از وب‌سایت‌ها
dnstwist	موتور جایگزینی نام دامنه برای تشخیص typo squatting، فیشینگ و جاسوسی
IPinfo	با جستجو منابع آنلاین اطلاعات مربوط به IP یا دامنه را جمع‌آوری می‌کند.
Java IDX Parser	تجزیه فایل‌های حافظه پنهان Java IDX
jsunpack-n	Unpacker جاوا اسکریپت که از قابلیت‌های مرورگر تقلید می‌کند.
Machinae	ابزار OSINT برای جمع‌آوری اطلاعات درباره IP، URL و یا Hash محاسبه‌شده
RABCDAsm	ActionScript Bytecode Disassembler
Spidermonkey	موتور جاوا اسکریپت Mozilla، برای رفع خطا JS مخرب
TekDefense Automator	ابزار OSINT برای جمع‌آوری اطلاعات درباره IP، URL و یا Hash محاسبه‌شده
Dig	ابزاری برای جمع‌آوری اطلاعات DNS
Firebug	افزونه فایرفاکس برای توسعه وب
Java Decompiler	برنامه‌های جاوا را دوباره کامپایل و بازرسی می‌کند.
JSDetox	ابزار تجزیه‌وتحلیل بدافزار جاوا اسکریپت
Krakatau	Java decompiler, assembler, and disassembler
Malzilla	تجزیه‌وتحلیل صفحات وب مخرب
SenderBase	IP، دامنه یا مالک شبکه را جستجو می‌کند.
swftools	Adobe Flash decompiler
xxxswf	ابزار تجزیه‌وتحلیل برای فایل‌های Flash

ابزارهای خطایابی و مهندسی معکوس

angr	چارچوب تجزیه‌وتحلیل باینری Platform-agnostic
BARF	تحلیل باینری متن‌باز و چارچوب مهندسی معکوس
Capstone	چارچوب جداسازی بخش‌ها برای تجزیه‌وتحلیل باینری و مهندسی معکوس
dnSpy	ویرایشگر اسمبلی .NET، تجزیه‌کننده و خطایابی
Fibratus	ابزار کاوش و ردیابی هسته ویندوز
GEF	ویژگی‌های بهبودیافته GDB برای استفاده در مهندسی معکوس
IDA Pro	Disassembler و خطایابی ویندوز
ltrace	ابزار تجزیه‌وتحلیل پویا برای فایل‌های اجرایی لینوکس
OllyDbg	خطایاب برای فایل‌های اجرایی ویندوز
PEDA	«Python Exploit Development Assistance» برای GDB
plasma	جداسازی تعاملی برای ARM/MIPS/X86
Process Monitor	ابزار نظارت پیشرفته برای برنامه‌های ویندوز
Rdare2	چارچوب مهندسی معکوس
SMRT	Sublime Malware Research Tool، افزونه‌ای برای Sublime Text 3 با تمرکز بر تجزیه‌وتحلیل بدافزار.
Triton	یک چارچوب تحلیل باینری پویا
Vivisect	ابزار پایتون برای تجزیه‌وتحلیل بدافزار
bamfdetect	اطلاعات خاص را از Bots و بدافزارها شناسایی و استخراج می‌کند.
binnavi	محیط برنامه‌نویسی تجزیه‌وتحلیل باینری برای مهندسی معکوس
codebro	یک مرورگر کُد مبتنی بر وب با امکان تجزیه‌وتحلیل کُدهای پایه
Evan's Debugger (EDB)	رفع اشکال ماژولار با رابط کاربری گرافیکی Qt

ابزارهای خطایابی و مهندسی معکوس

GDB	خطایابی GNU
hackers-grep	برنامه‌ای برای جستجو رشته‌ها در اجراهای PE
Immunity Debugger	خطایابی برای تجزیه‌وتحلیل بدافزار
objdump	ابزار تجزیه‌وتحلیل استاتیک برای باینری لینوکس
PANDA	چارچوبی برای تجزیه‌وتحلیل پویا معماری
pestudio	ابزار تجزیه‌وتحلیل استاتیک برای برنامه‌های اجرایی ویندوز
PPEE (puppy)	بازرسی از پرونده‌های PE
Pyew	یک ابزار پایتون برای تجزیه‌وتحلیل بدافزار
ROPMEMU	چارچوبی برای تجزیه‌وتحلیل، تشریح و مقابله با حملات استفاده مجدد از کد
strace	ابزار تجزیه‌وتحلیل پویا برای فایل اجرایی لینوکس
Udis86	جداساز کتابخانه‌ها و ابزارها
X64dbg	خطایاب برای ویندوز

معرفی ابزار

MASSCAN

گردآوری: محمد حبیبی

معرفی ابزار Masscan

در این بخش سعی داریم یکی از ابزارهای پویش شبکه با نام Masscan را معرفی کنیم. ابزارهای زیادی برای پویش شبکه به‌صورت متن‌باز یا تجاری عرضه‌شده‌اند که می‌توان گفت یکی از قدرتمندترین آن‌ها ابزار Nmap است که به‌صورت رایگان و متن‌باز عرضه‌شده است و یکی از پراستفاده‌ترین و شناخته‌شده‌ترین ابزارها به‌حساب می‌آید. ابزار Masscan توسط آقای Robert David Graham نوشته‌شده است و در گیتهاب شخصی ایشان قابل دانلود است. ابزار Masscan عملکرد مشابهی با Nmap دارد با این تفاوت که می‌تواند بسیار سریع‌تر عمل کند. گفته‌شده است این ابزار می‌تواند کل شبکه اینترنت را در کمتر از شش دقیقه اسکن کند و با سرعتی برابر با ۱۰ میلیون بسته در ثانیه عمل کند. اگر شما با Nmap آشنایی داشته باشید یادگیری نحوه استفاده از Masscan کار دشواری نیست.

نحوه نصب Masscan

ابزار Masscan از طریق لینک زیر قابل‌دسترس است:
https://github.com/robertdavidgraham/masscan

- نصب بر روی سیستم‌عامل‌های مبتنی بر Debian/Ubuntu
برای نصب این ابزار بر روی سیستم‌عامل‌های لینوکس مبتنی بر Debian/Ubuntu فرامین زیر را اجرا کنید:

```
$ sudo apt-get install gcc git libpcap-dev
$ git clone https://github.com/robertdavidgraham/masscan
$ cd masscan
$ make
```

همچنین برای سریع انجام شدن مراحل نصب به‌صورت multithread می‌توان make را با j– به شکل زیر فراخوانی کرد: (برای سیستم‌عامل FreeBSD از دستور gmake استفاده شود)

```
$ make –j
```

برای نصب ابزار بر روی ویندوز می‌توان از پروژه masscan موجود در آدرس زیر استفاده کرد که با استفاده از Visual Studio 2010 نوشته‌شده است:
https://github.com/robertdavidgraham/masscan/tree/master/vs10

سپس می‌توان با استفاده از کامپایلر MinGW و دستور make یک نسخه قابل‌اجرا از این پروژه تهیه کرد.
- بررسی نسخه نصب‌شده
پس از نصب می‌توان برای تست موفقیت‌آمیز بودن نصب ابزار، از فرمان زیر استفاده کرد:

```
$ make regress
```

نحوه استفاده از ابزار

پس از نصب ابزار به‌صورت پیش‌فرض نسخه اجرایی Masscan در دایرکتوری bin در مسیر نصب قرار می‌گیرد، در زیر یک نمونه از پویش توسط این ابزار آورده شده است:

```
masscan –p22, 50-100 10.0.0.0/8
```

خروجی اجرای ابزار در نمونه‌ی فوق، پویش پورت‌های 22 و پورت‌های محدوده 50 تا 100 بر روی زیر شبکه 10.x.x.xمی‌باشد. خروجی به شکل پیش‌فرض در محیط ترمینال CMD چاپ می‌شود.

نحوه ذخیره خروجی ابزار

به‌صورت کلی خروجی ابزار می‌تواند در پنج قالب زیر باشد:

1 . XML

این فرمت به نسبت فایل‌های بزرگی را در قالب XML ایجاد می‌کند اما خواندن اطلاعات ممکن است بعداً آسان‌تر باشد. برای ذخیره خروجی در این فرمت، در انتهای فراخوانی از عبارت
" <-ox<filename>"یا -output-format xml و سپس نام فایل خروجی استفاده شود. به‌عنوان‌مثال:

```
masscan -p22, 50-100 10.0.0.0/8 –oX OutputFileName
```

2 . Binary

این فرمت، فرمت پیش‌فرض برای خروجی است. این فایل‌ها کم‌حجم هستند ولی برای خواندن آن‌ها نیاز است از فرمان readscan- استفاده شود.
به عنوان‌مثال می‌توان از readscan- همراه oX استفاده شود تا پس از خوانده شدن خروجی آن به فرمت XML ذخیره شود.

3 . Greapable

خروجی این فرمت شبیه به خروجی oG- در ابزار Nmap می‌باشد. برای تولید این نوع خروجی از عبارت oG- استفاده می‌شود. این خروجی به‌سادگی می‌تواند توسط ابزارهای خط فرمان استفاده شود.

4 . Json

با استفاده از عبارت oJ- خروجی ابزار در فرمت Json ذخیره می‌شود.

5 . List

این فرمت به شکل لیستی از میزبان‌ها است که برای هر میزبان پورت‌ها آورده شده است.

مشخص‌کردن هدف	
توضیحات	دستور
پویش یک میزبان	masscan 10.0.0.1
پویش دو رنج شبکه	masscan 192.168.1.0/24 10.0.0.0/24
حذف IP های موجود در یک فایل از محدوده پویش	masscan 10.0.0.1/24 --excludeFile <file>
حذف یک آدرس IP از محدوده پویش	masscan 180.215.0.0/16 --exclude=180.215.122.120

مشخص‌کردن پورت	
توضیحات	دستور
پویش پورت 80	masscan 10.0.0.1 -p 80
پویش تمامی پورت‌ها	masscan 10.0.0.1 -p 0-65535
پویش پورت‌های 80 و 443	masscan 10.0.0.1 -p 80,443
پویش UDP پورت 53	masscan 10.0.0.1 -pU 53

زمان‌بندی و کارایی	
توضیحات	دستور
انجام پویش به‌صورت آفلاین، ترافیکی ارسال نمی‌شود ولی زمان انجام پویش تخمین زده می‌شود.	masscan 0.0.0.0/24 --offline
با استفاده از پارامتر rate مشخص می‌کند که ابزار در هر ثانیه 10000 پکت ارسال کند.	masscan 10.0.0.1/24 --rate 10000
خواندن بنر پورت‌های مشخص‌شده (پروتکل‌های محدود)	masscan 10.0.0.1 --banners
تعیین یک IP برای Masscan (هنگام خواندن بنر پورت‌ها حتماً نیاز است استفاده شود.)	masscan 10.0.0.1 --source-ip 192.168.1.200
پویش شامل یک Ping می‌شود.	masscan 10.0.0.1 --ping
تغییر user agent پیش‌فرض به مقدار تعیین‌شده	masscan 10.0.0.1 --http-user-agent <user-agent>
فقط پورت‌هایی با وضعیت Open گزارش می‌شوند.	masscan 10.0.0.1 --open-only
پکت‌های ارسالی در قالب pcap ذخیره می‌شوند.	masscan 10.0.0.1 --pcap <filename>
پکت‌های ارسالی در ترمینال/CMD نمایش داده می‌شوند. هنگام ارسال پکت‌هایی با تعداد بالا پیشنهاد نمی‌شود.	masscan 10.0.0.1 --packet-trace

خروجی ابزار	
توضیحات	دستور
ذخیره خروجی با فرمت binary	massscan10.1.1.1/24 -p 80 -oB <filename>
ذخیره خروجی با فرمت XML	massscan 10.1.1.1/24 -p 80 -oX<filename>
ذخیره خروجی با فرمت محدود(grepable)	massscan 10.1.1.1/24 -p 80 -oG <filename>
ذخیره خروجی با فرمت JSON	massscan 10.1.1.1/24 -p 80 -oJ <filename>
ذخیره خروجی با فرمت list	massscan 10.1.1.1/24 -p 80 -oL <filename>
خواندن خروجی ابزار که به فرمت باینری ذخیره‌شده است.	masscan --readscan bin-test.scan
خواندن خروجی ابزار با فرمت باینری و تبدیل و ذخیره آن در قالب XML.	masscan --readscan bin-test.scan -oX bin-test.xml

چند نمونه کامل از پویش‌های Masscan

پویش سریع برای پورت‌های باز در یک رنج شبکه

```
masscan 10.1.1.1/24 -p 65535-0 --rate 1000000 --open-only --http-user-agent \
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0"\
 -oL "output.txt"
```

پویش سریع پورت‌های 80 و 443 برای سه میزبان

```
masscan <target1> <target2> <target3> -p 80,433 --rate 100000 --banners
--open-only--http-user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0)
Gecko/20100101 Firefox/67.0"--source-ip 192.168.100.200 -oL "output.txt"
```

پویش 20 پورت کاربردی (موجود در TOP 20) برای یک میزبان

```
masscan <target> -p 21,22,23,25,53,80,110,111,135,139,143,443,445,993,995,1723,3306,3389,
5900,8080\
--http-user-agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101
Firefox/67.0"\
--rate 100000 --oL "output.txt"
```

اسکن کل شبکه اینترنت (IPv4)

```
masscan 0/0.0.0.0 -p65535-0  --rate 100000 --oL "output.txt"
```

OLLYDBG

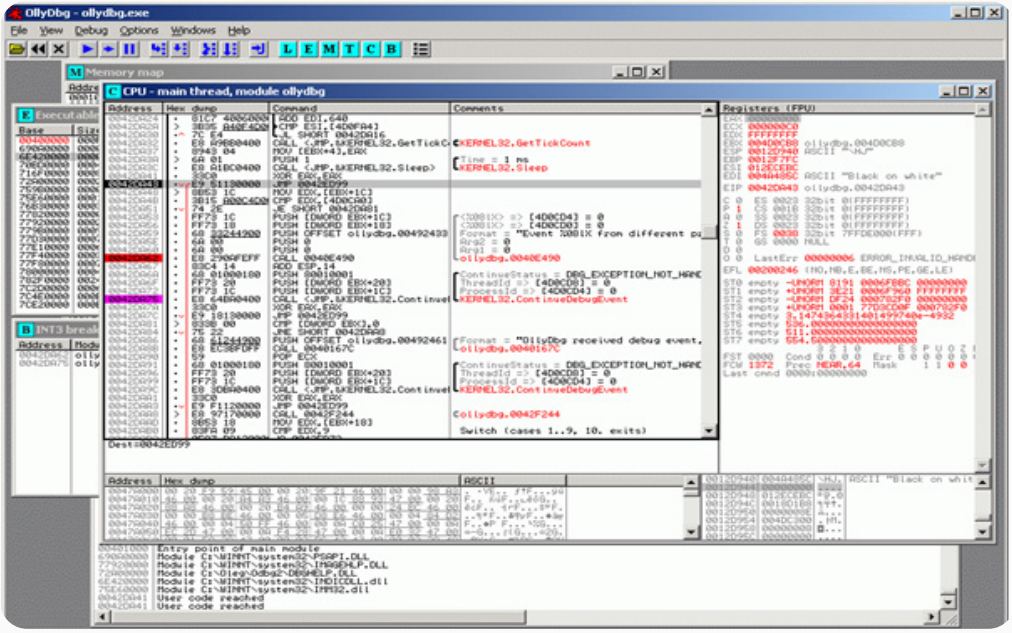
تهیه و تدوین: محمد ساروقی

مقدمه

OllyDbg یک Debugger است که تأکید بر تحلیل باینری دارد و برای برنامه‌های ویندوز مورداستفاده قرار می‌گیرد. زمانی که کُد اصلی برنامه در دسترس نیست از این نرم‌افزار برای تحلیل روند برنامه استفاده می‌شود و در تحلیل بدافزارها نیز از این برنامه استفاده می‌شود. از ویژگی‌های مثبت این برنامه می‌توان از رابط گرافیکی، رایگان بودن، داشتن Disassembler قدرتمند، قابلیت تشخیص مبدأ و مقصد توابع، دستورات پرش و مقصد پرش و غیره نام برد که کار را برای روند مهندسی معکوس آسان می‌کند. اگر بخواهیم در بخش‌های خاصی از روند اجرای برنامه‌ی مورد تحلیل، توقف ایجاد کنیم تا بتوانیم مقادیر حافظه یا ثبات‌ها را ببینیم و مورد تجزیه‌وتحلیل قرار دهیم از قابلیت نقطه توقف (Break Point) استفاده می‌کنیم که برنامه به‌محض اینکه به این نقطه برسد متوقف می‌شود. در شکل ۱ محیط کار نشان داده‌شده است.

Ollydbg این قابلیت را دارد که هم فایل‌های اجرایی (.exe) و هم فایل برنامه با پسوند dll. را اجرا کند. برای اجرای فایل موردنظر خود در Olldbg تنها کافی است فایل موردنظر را از گزینه Open در منوی File انتخاب کنید سپس این برنامه توسط Olldbg اجراشده و یک Debugger به روند آن اختصاص داده می‌شود تا بتواند فایل موردنظر را مورد تحلیل و بررسی قراردهد. برای باز کردن فایل با پسوند dll. باید مطابق روند اجرای فایل‌های exe. عمل کرد، فقط برای اجرای این فایل یک برنامه کمکی به نام LOADDLL.EXE در اختیار دارد که با اجرا و سپس واردکردن فایل موردنظر یک Debugger به فایل با پسوند dll. اختصاص داده می‌شود.

در Ollydbg می‌توانید با چسباندن Debugger به یک پروسه در حال اجرا در سیستم به روند اجرا دسترسی پیدا کنید و روند اجرای برنامه را تجزیه‌وتحلیل کنید. در این حالت می‌بایست Process ID و Thread ID برنامه موردنظر را در اختیار داشته باشید که بتوانید جریان مربوط به پروسه اجرای این برنامه را کشف کنید و درنهایت عملکرد آن را مورد تجزیه‌وتحلیل قرار دهید. این روش از طریق منوی فایل و گزینه attach اجرا می‌شود.



شکل ۱- محیط کار OllDbg

همان‌طور که در شکل ۱ نشان داده‌شد، در برنامه چهار بخش اصلی وجود دارد:

- Disassembler

کُدهای Debug شده برنامه را نمایش می‌دهد که همان کُدهای اسمبلی اقتباس‌شده از کُدهای حافظه فایل اجرایی است که بر روی RAM قرارگرفته‌اند. درصورتی‌که تحلیلگر تصمیم به ایجاد تغییر در کُد اجرایی برنامه بگیرد با ایجاد تغییرات در این بخش تغییرات موردنظر خود را اجرا می‌کند.

- Register

در این بخش رجیستری‌های برنامه قابل‌مشاهده است. هنگامی‌که یک کُد Debug می‌شود، این مقادیر تغییر می‌کنند.

- Stack

از طریق این بخش می‌توان وضعیت فعلی Stack داخل حافظه که مربوط به Thread است را مشاهده کرد.

- Memory dump

در این بخش حافظه اختصاص داده‌شده به پروسه برنامه اجرا می‌شود که مقادیر آن همان مقادیر باینری داخل فایل اجرایی برنامه است که موقعیت آن را بر روی حافظه می‌توان مشاهده کرد و یا تغییر داد.

ردیابی (Trace)

ردیابی ابزاری قدرتمند در روش‌های Debug است که جزئیات اجراها را ثبت می‌کند. Ollydbg سه نوع ردیابی را پشتیبانی می‌کند:

- Standard Back

زمانی که از پنجره‌ی disassembler با دو گزینه trace-over و trace-into استفاده می‌کنید تمام وقایع ثبت می‌شود و می‌توانید با استفاده از دو کلید + و – به مرحله بعد و قبل بروید. این روش برای محدوده مشخصی از کُد استفاده می‌شود، قبلاً برنامه را متوقف کرده‌اید و نمی‌توان مسیر دیگری از برنامه را اجرا کنید، نکته‌ی دیگر این است که فقط بخش محدودی را اجرا کرده است تا به نقطه شکست برسد که در این نوع ردیابی محدودیت اجرای حجمِ محدودی از برنامه را دارد.

- Call Stack

در Ollydbg برای مشاهده مسیر اجرای برنامه و توابع مختلف آن از Call stack استفاده می‌شود. برای دسترسی به Call Stack از منوی اصلی View >> Call Stack را انتخاب کنید؛ که پنجره‌ای از فراخوانی‌ها تا اولین نقطه شکست که برنامه اجراشده است را نمایش می‌دهد و دسترسی به توابعی که تا به حال اجراشده‌اند را دارید.

- Run Trace

در این روش ردیابی با اجرای برنامه، دستوراتِ اجراشده و تغییرات صورت گرفته در Register و Flag نشان داده می‌شود. Run trace اولین بار در OllyDbg معرفی شد. این تکنیک بسیار ساده است به این صورت که کُد قدم‌به‌قدم اجرا می‌شود، در اجرای هر دستور به همراه رجیستری‌ها و پرچم‌ها در پروتکل Debugger در یک بافر دایره‌ای ذخیره می‌شود، درصورتی‌که روند با خطا مواجه شود می‌توان با استفاده از برگشت به عقب، می‌تواند یک دستور یا صدها و یا هزاران دستور به عقب برگردد و شرطی را که منجر به خطا شده است بررسی کند. در Ollydbg 1.06 به‌طور واضحی امکانات ردیابی بهبودیافته است. برای مثال اصلاح رجیستری‌ها و پیام‌ها و عملگرهای توابع شناخته‌شده را نگهداری می‌کند. در ادامه کلیدهای میانبری که در OllyDbg می‌تواند برای کاربران مفید واقع شود، در جداول ۱، ۲ و ۳ ارائه‌شده است.

جدول ۱- میانبرها در پنجره‌های خاص و نحوه عملکرد

میانبر	دستور در منو	پنجره	تابع
Ctrl+E	Binary | Edit	Disassembler, Stack Dump	حافظه را به‌صورت رشته باینری، ASCII یا UNICODE ویرایش کنید.
Alt+BkSp	Undo selection Undo	Disassembler, Dump Registers	واگرد تغییرات
F9	Debug | Run	Main	اجرای برنامه
F4	Breakpoint | Run to selection	Disassembler	اجرای بخش انتخاب‌شده
Ctrl+F9	Debug | Execute till return	Main	اجرا کردن تا بازگشت
Alt+F9	Debug | Execute till user code	Main	اجرا کردن تا کُد کاربر
F2	Breakpoint | Toggle Toggle breakpoint	Disassembler Names, Source	ایجاد/بازنشانی نقطه توقف INT3
Shift+F2	Breakpoint | Conditional Conditional breakpoint	Disassembler Names, Source	ایجاد/ویرایش نقطه توقف مشروط INT3
Shift+F4	Breakpoint | Conditional log/Conditional log breakpoint	Disassembler Names, Source	Set/Edit نقطه توقف ورود به‌شرط (logs مربوط به پنجره Log)
Space	Disable Enable	Breakpoints	نقطه توقف INT3 را به‌طور موقت غیرفعال کنید / بازیابی کنید
-	Breakpoint | Memory, on access Breakpoint | Memory,onwrite	Disassembler Names, Source	تنظیم نقطه توقف حافظه (فقط یک مورد مجاز است)
-	Dump Breakpoint | Remove memory breakpoint	Disassembler, Dump	حذف نقطه توقف حافظه

جدول ۱- میانبرها در پنجره‌های خاص و نحوه عملکرد (ادامه)

-	Breakpoint | Hardware (انتخاب نوع و اندازه)	Disassembler, Dump	ایجاد یک نقطه توقف حافظه (only ۲۰۰۰/ME/NT)
-	-	Main	حذف نقطه توقف سخت‌افزار
F2	مجموع شکستن دسترسی	Memory	تنظیم یک توقف single-short به بلوک حافظه (فقط ۲۰۰۰ / NT)
-	Events	Options	ایجاد یک توقف بر روی ماژول، debug string، Thread
-	New origin here	Disassembler	تنظیم مبدأ جدید
Ctrl+N	Search for | Name (label) View names	Disassembler, Dump Modules	نمایش لیست تمام اسامی نمادین
Ctrl+F1	Help on symbolic name	Disassembler, Names	راهنمای حساس به محتوا (به پرونده help نیاز دارد)
Ctrl+R	Find references to | Command Find references	Disassembler Dump	انتخاب همه منابع مرتبط در محدوده آدرس تعیین‌شده
-	Find references to | Constant Search for | All constants	Disassembler	همه ارجاعات در کُد به مقادیر ثابت مشخص شود.
Ctrl+L	Search Search nex	Memory	جستجوی حافظه اختصاص‌یافته
Ctrl+G	Go to | Expression Go to expression	-	ارجاع به آدرس یا مقدار خاص
Minus	Go to | Previous	Disassembler	ارجاع به آدرس قبلی/ run trace
Plus	Go to | Next	Disassembler	ارجاع به آدرس بعدی/ run trace

جدول ۱- میانبرها در پنجره‌های خاص و نحوه عملکرد (ادامه)

به روال قبلی رفتن	Disassembler	Go to | Previous procedure	Ctrl+Minus
به روال بعد رفتن	Disassembler	Go to | Next procedure	Ctrl+Plus
مشاهده فایل اجرایی	Disassembler, Dump, Modules	View | Executable file	-
کپی کردن تغییرات بر روی فایل اجرایی	Disassembler	Copy to executable file	-
تجزیه‌وتحلیل کُد اجرایی	Disassembler	Analysis | Analyse code	Ctrl+A
اسکن پرونده‌های Object و کتابخانه‌های آن	Disassembler	Scan object files	Ctrl+O
مشاهده منابع	Modules, Memory	View all resources View resource strings	Ctrl+R
تعلیق یا ازسر گرفتن یک Thread	Threads	Suspend Resume	-
نمایش آدرس‌های مرتبط	Disassembler, Dump, Stack	Doubleclick address	Ctrl+L
کپی	Most of windows	Copy to clipboard	Ctrl+C

جدول ۲- میانبرهای سراسری که اغلب استفاده می‌شوند.

میانبر	عملکرد
Ctrl+F2	Restart program
Alt+F2	Close program
F3	Open new program
F5	Maximize/restore active window
Alt+F5	Make OllyDbg topmost
F7	Step into (entering functions)
Ctrl+F7	Animate into (entering functions)
F8	Step over (executing function calls at once)
Ctrl+F8	Animate over (executing function calls at once)
Ctrl+F8	Run
Shift+F9	Pass exception to standard handler and run
Ctrl+F9	Execute till return
Alt+F9	Execute till user code
Ctrl+F11	Trace into
F12	Pause

جدول ۲- میانبرهای سراسری که اغلب استفاده می‌شوند. (ادامه)

Trace over	Ctrl+F12
Open Breakpoints window	Alt+B
Open CPU window	Alt+C
Open Modules window	Alt+E
Open Log window	Alt+L
Open Memory window	Alt+M
Open Options dialog	Alt+O
Set condition to pause Run trace	Ctrl+T
Close OllyDbg	Alt+X

جدول ۳- میانبرهای Disassembler که اغلب استفاده می‌شوند.

عملکرد	میانبر
Toggle breakpoint	Ctrl+F2
Set conditional breakpoint	Alt+F2
Run to selection	F3
Go to previous reference	F5
Go to next reference	Alt+F5
Analyse code	F7

جدول ۳- میانبرهای Disassembler که اغلب استفاده می‌شوند. (ادامه)

Start binary search	Ctrl+B
Copy selection to clipboard	Ctrl+C
Edit selection in binary format	Ctrl+E
Search for a command	Ctrl+F
Follow expression	Ctrl+G
Show list of jumps to selected line	Ctrl+J
View call tree	Ctrl+K
Repeat last search	Ctrl+L
Open list of labels (names)	Ctrl+N
Scan object files	Ctrl+O
Find references to selected command	Ctrl+R
Search for a sequence of commands	Ctrl+S
Origin	Asterisk (*)
Follow jump or call	Enter
Go to next location/next run trace item	Plus (+)
Go to previous location/previous run trace item	Minus (-)
Assemble	Space

دفترچه ◆ تقلب

IDAPRO CheatSheat

گردآوری: پرستو مجیدی

عملگرها

Offset (data segment)	O
Offset (current segment)	Ctrl + o
Offset by (any segment)	Alt + r
Offset (user-defined)	Ctrl + r
Offset(struct)	T
Number	#
Hexadecimal	Q
Decimal	H
Binary	B
Character	R
Segment	S
Enum member	M
Stack variable	K
Change sign	_ (Underscore)
Bitwise negate	~
Manual	Alt + F1

توضیحات

Enter comments	:
Enter repeatable comment	;
Enter anterior lines	Ins
Enter posterior lines	Shift + Ins
Insert predefined comment	Shift +F1

جستجو

Next code	Alt + c
Next data	Ctrl + d
Next explored	Ctrl + a
Next unexplored	Ctrl + u
Immediate value	Alt + i
Next Immediate value	Ctrl + i
Text	Alt + t
Next text	Ctrl +t
Sequence of bytes	Alt + b
Next sequence of bytes	Ctrl + b

توابع

Create function	P
Edit function	Alt+p
Set function end	E
Stack variables	Ctrl + p
Change stack pointer	Alt+k
Rename register	V
Set function type	Y

عملیات بر روی فایل	Parse C header file	Ctrl + F9
	Create ASM file	Alt + F10
	Save	Ctrl + W
دیباگر	Add breakpoint	F2
	Start process	F9
	Terminate process	Ctrl+F2
	Step into	F7
	Step over	F8
	Run until return	Ctrl+F7
	Run to cursor	F4
	Breakpoint list	Ctrl+alt+b
	Delete watch	Del
	Stack trace	Ctrl+alt+s
نمایش پنجره‌های مختلف IDA	Local type	Shift+F1
	Functions	Shift+F3
	Name	Shift+F4
	Signatures	Shift+F5
	Segments	Shift+F7
	Segment registers	Shift+F8
	Structures	Shift+F9
	Enumerations	Shift+F10
	Type libraries	Shift+F11
	Strings	Shift+F12

ویرایش

Copy	Ctrl + C
Begin selection	Alt + L
Manual instruction	Alt + F2
Code	C
Data	D
Struct variable	Alt + q
Asci string	a
Array	Num *
Undefined	u
rename	n

کار با metadata

Pull all metadata	F12
Push all metadata	Ctrl+F12
View all metadata	Alt+F12

انواع Jump

Jump to operand	ENTER
Jump in a new window	Alt + enter
Jump to previous position	Esc
Jump to next position	Ctrl + enter
Jump to address	G
Jump by name	Ctrl + L
Jump to function	Crtl + p
Jump to pseudocode	Tab
Jump to segment	Ctrl+ s
Jump to segment register	Ctrl + g
Jump to problem	Ctrl + q
Jump to xref to operand	X
Jump to entry point	Ctrl + e
Jump to marked position	Ctrl + m

کار با Segmentها

Edit segment	Alt + s
Change segment register value	Alt + g

ترسیم نمودار از روند اجرایی برنامه

Flow chart	F12
Function calls	Ctrl + F12

سایر موارد

Calculator	?
Windows list (next)	Ctrl + tab
Switch to windows #1..9	Alt + 1..9
Close window	Alt + F3
Script command	Shift + F2
Exit	Alt + x

معرفی دوره

تهیه و تدوین: هادی گلباغی

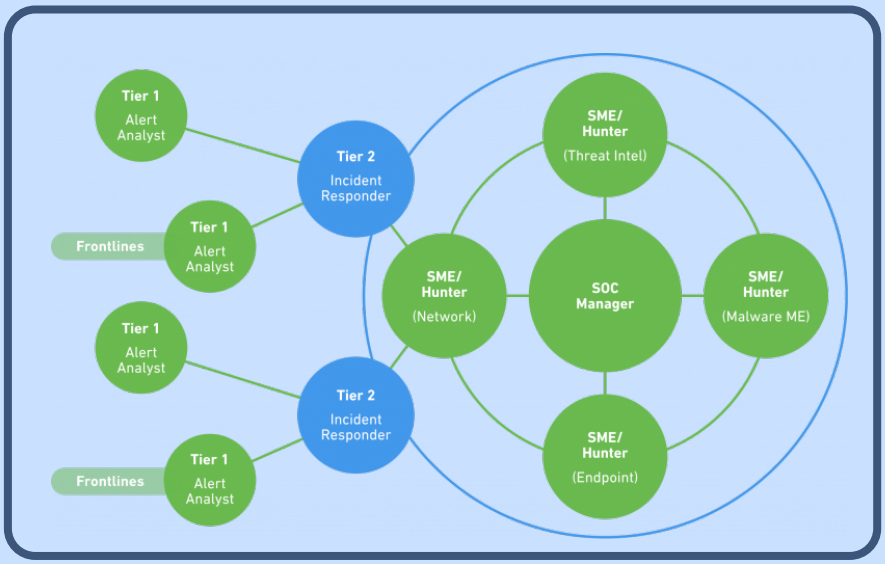
مقدمه

مرکز The International Council of Electronic Commerce Consultants (EC-Council) با آدرس www.eccouncil.org دارای دوره‌های آموزشی و مدارک معتبری در حوزه‌های مختلف تکنولوژی شامل امنیت سایبری است. دوره‌هاي اين مرکز مبتنی بر نیازهاي کسب و کار بوده و با روش‌هاي فني و مبتنی بر کسب مهارت طراحي شده‌اند. این مرکز دارای دوره‌های مختلفی نظیر LPT، ECSA، CHFI، CEH و غیره بوده که علاوه بر گواهی‌نامه و مدرک معتبری که دارند، بسیار کاربردی و مهارت‌محور نیز هستند. EC-Council تا زمان نوشتار این مطلب دارای بیش از ۲۳۷ هزار فراگیر دوره‌ها از ۱۴۵ کشور دنیا بوده است. این مرکز در سال‌های اخیر دوره‌های بسیار خوبی در حوزه امنیت سایبری برگزار کرده است که به یکی از مراجع مهم و اصلی برای برگزاری دوره‌های امنیتی و اخذ گواهی‌نامه‌های امنیتی در دنیا بدل شده است. در این مطلب به معرفی دوره CERTIFIED SOC ANALYST (CSA) پرداخته‌ایم.

EC-Council
Hacker are here. Where are you?

معرفی

دوره Certified SOC Analyst (CSA) اولین گام برای یادگیری اصول Security Operations Center یا SOC است. در این دوره ابتدا درخصوص مرکز عملیات امنیت SOC و اصول آن توضیحاتی داده می‌شود. SOC به طور کلی زیرساختی است که یک تیم امنیت سایبری که مسئولیت نظارت و بررسی امنیتی یک سازمان را بر عهده دارند، در خود جای می‌دهد. هدف تیم SOC، تحلیل، بررسی و اقدام متناسب در واکنش به رخدادهای امنیت سایبری براساس راهکارهایی موجود می‌باشد. در زیر ساختار یک SOC نشان داده شده است.



CSA یک برنامه و دوره آموزشی و اعتبارسنجی است که به داوطلبان و فراگیران آن در زمینه یادگیری مهارت‌های به‌روز و کارآمد از طرف متخصصین باتجربه‌تر، کمک می‌کند. تمرکز این دوره بر روی ایجاد یک بستر و فرصت شغلی جدید از طریق یادگیری سطوح پیشرفته‌ای از مهارت برای ورود به تیم‌های SOC است. در این دوره که به‌صورت فشرده برگزار می‌شود هدف اصلی پوشش اصول و اقدامات ممکن در SOC، کسب دانش لازم برای تحلیل و بررسی و مدیریت لاگ‌ها، استقرار SIEM، شناسایی تهدیدات به صورت پیشرفته و اقدام و پاسخ متناسب به تهدیدات است. همچنین داوطلبان می‌آموزند که به چه شکل فرآیند مختلف SOC را مدیریت کنند و در زمان‌های مختلف به چه صورت با تیم‌های آبی، قرمز و CSIRT همکاری کنند.

سرفصل‌ها

- مفاهیم و اصول اولیه در SOC
- اقدامات امنیتی و مدیریت آنها
- درک عمیق تهدیدات و حملات سایبری
- رخدادها، تهدیدات و بررسی لاگ‌ها
- شناسایی حملات و رخدادها به وسیله SIEM
- تشخیص تهدیدات و حملات پیشرفته به وسیله ابزارهای هوشمند تشخیص تهدیدات
- واکنش و اقدام در مقابل رخدادها و حوادث امنیتی

مخاطبان

- تحلیلگران SOC (لایه ۱ و لایه ۲)
- مهندسین و مدیران شبکه و امنیت
- تحلیلگران، اپراتورها، تکنسین‌ها و متخصصین امنیت شبکه
- تحلیلگران امنیت سایبری
- علاقه‌مندان ورود به تیم‌های SOC

در این دوره چه نکاتی آموخته خواهند شد؟

- کسب دانش درخصوص فرآیندها، روال‌ها، تکنولوژی‌ها و جریان‌های کاری در SOC
- کسب دانش و مهارت عمیق‌تر درخصوص تهدیدات امنیتی، حملات، آسیب‌پذیری‌ها و رفتار مهاجمین و نفوذگران
- کسب مهارت برای شناسایی ابزارها، تاکتیک‌ها و روال‌های مورد استفاده مهاجمین در حملات
- توانایی مانیتورینگ و تحلیل لاگ‌ها در بسترها و تکنولوژی‌های مختلف مانند IPS، IDS، سرورها و غیره
- کسب مهارت برای متمرکز کردن فرآیند مدیریت لاگ‌ها (CLM)
- توانایی در جمع‌آوری اطلاعات درخصوص رخدادهای امنیتی و مدیریت رویدادها
- کسب مهارت برای استقرار و مدیریت راهکارهای SIEM مانند ELK، OSSIM، AlienVault، Splunk و غیره
- توانایی در ارائه گزارش درخصوص رخدادها، تهدیدات و حملات و آماده‌سازی مستندهایی در خصوص اقدامات صورت گرفته

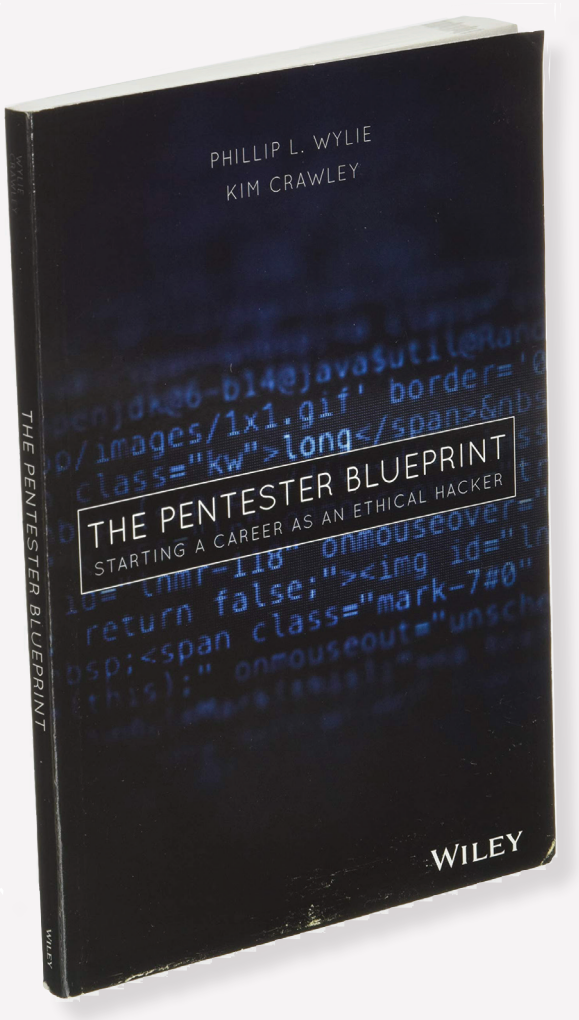
لینک دوره

معرفی کتاب

The Pentester BluePrint:
Starting a Career as an Ethical Hacker 1st Edition

تهیه و تدوین: هادی گلباغی

نام کتاب:	The Pentester BluePrint
نویسندگان:	Kim Crawley, Phillip L. Wylie
زبان:	انگلیسی
تعداد صفحات:	192
ناشر و سال انتشار:	Wiley; 1st Edition (November 2020 ,6)



معرفی کتاب

کتاب The Pentester BluePrint راهنمای شما برای حرکت در مسیر تبدیل‌شدن به یک ارزیاب امنیتی و کارشناس تست نفوذ است و فرصت ورود به دنیای هکرهای کلاه‌سفید را فراهم می‌کند. نویسندگان این کتاب سعی دارند مباحث ضروری و مهم برای درک چگونگی ایجاد مهارت به‌منظور شناسایی آسیب‌پذیری‌های سیستم، شبکه و برنامه‌ها را فراهم کنند و راهنمای این مسیر به شکلی اصولی و پیشرفته باشند.
خوانندگان این کتاب قوانین و اصول یک تست نفوذ استاندارد را می‌آموزند و همچنین این مسئله که تست نفوذ شامل چه اموری بوده و برای شروع این فعالیت چه دانش و مهارت‌هایی نیاز است فراگرفته شود. همچنین چگونه باید یک نقشه راه برای ارزیابی میزان مهارت فعلی و شناسایی منابع و ابزارهایی که برای رشد مهارت و دانش شما ضروری است، نیز ارائه خواهد شد و درنهایت به‌عنوان یک ارزیاب امنیتی به چه شکل از ابزارها، شبکه‌های اجتماعی تخصصی و موتورهای جستجو برای کشف و شناسایی آسیب‌پذیری‌ها می‌بایستی استفاده کرد.
در این کتاب از ارائه نکات غیرضروری و روش‌ها و تکنیک‌های قدیمی و منسوخ پرهیز شده و سعی بر این بوده که تکنیک‌های مفید و استراتژی‌ها و توصیه‌های عملی و کاربردی ارائه شود تا از به هدر رفتن زمان یک ارزیاب امنیتی جلوگیری کند و فرآیند تست نفوذ را به نسبت خودکار نماید.

در این کتاب چه مواردی آموخته می‌شوند؟

- دانش‌ها و مهارتی‌های پیش‌نیاز مانند اطلاعاتی در خصوص سیستم‌عامل، شبکه و امنیت سیستم‌ها
- اصول اولیه تست نفوذ و ارزیابی امنیتی
- بررسی ذهنیت هکر شدن و توسعه مهارت‌های یک هکر
- چگونگی یافتن منابع آموزشی مناسب شامل دروس دانشگاهی، دوره‌های آموزشی و مطالعه خودآموز
- معرفی مدارک و گواهینامه‌های مفید و کاربردی برای یک کارشناس تست نفوذ و ارزیاب امنیتی
- چگونگی کسب تجربه در حوزه تست نفوذ شامل ایجاد آزمایشگاه، CTF ها و فعالیت‌های باگ‌بانتی

این کتاب مناسب چه کسانی است؟

- تیم‌های تخصصی حوزه فناوری اطلاعات
- محققین و متخصصین حوزه امنیت سایبری
- کارشناس تست نفوذ و ارزیاب‌های امنیتی
- علاقه‌مندان به یادگیری اصول ارزیابی امنیتی و تست نفوذ

سرفصل‌های کتاب:

1. **What is a Pentester?**
2. **Prerequisite Skills**
3. **Education of a Hacker**
4. **Education Resources**
5. **Building a Pentesting Lab**
6. **Certifications and Degrees**
7. **Developing a Plan**
8. **Gaining Experience**
9. **Getting Employed as a Pentester**

لینک کتاب

مقاله‌های تحقیقاتی

بررسی آخرین گزارش آزمایشگاه تهدیدات مک‌آفی و کسپرسکی

تهیه و تدوین: سینا فقیری

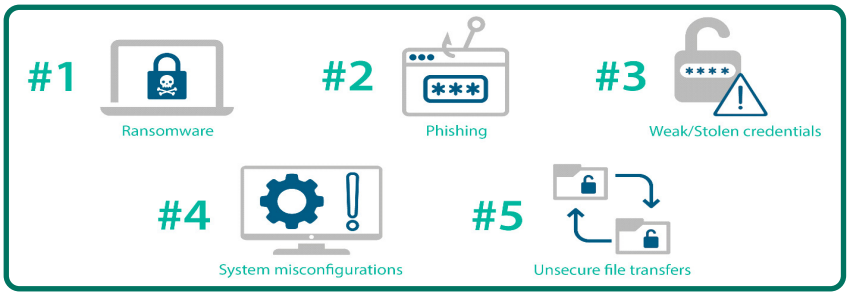
مقدمه

در سالی که گذشت با گروه‌های جدیدی از مهاجمین سایبری روبرو بودیم که از شرایط پیش‌آمده به دلیل همه‌گیری کرونا نهایت سوءاستفاده را کرده‌اند به شکلی که نرخ حملات و نفوذها با رشد قابل‌توجهی مواجه بوده است. یکی از مهم‌ترین عوامل رشد این حملات، درواقع دورکاری و انجام امورات در حوزه‌های مختلف به‌صورت مجازی بوده است. به نظر می‌رسد با توجه به گزارشات، نفوذگران هر کاری را برای سوءاستفاده از این شرایط انجام داده‌اند.

طبق گزارش آزمایشگاه تهدیدات مک‌آفی، در سه‌ماهه دوم سال ۲۰۲۰، فضای سایبری شاهد افزایش حدوداً ۶۰۰ درصدی تهدیدات ناشی از تأثیرات ویروس کرونا به نسبت سه‌ماهه اول بوده است و در کل به نسبت سال گذشته در سایه این همه‌گیری کرونا، حملات سایبری افزایش ۳۰ درصدی داشته است.

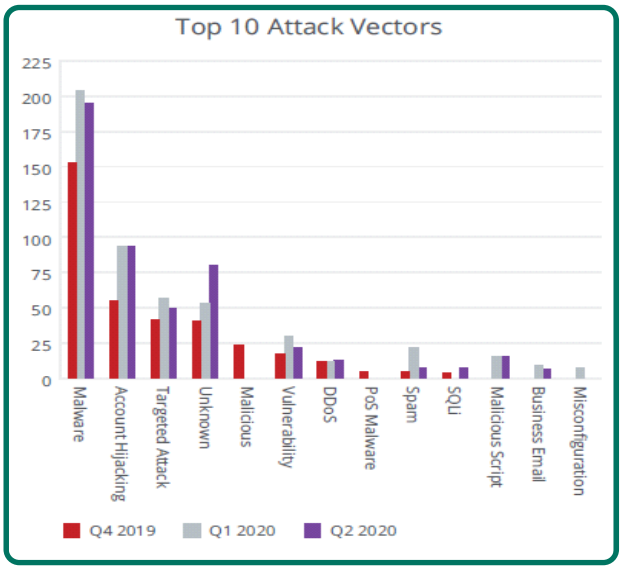
پس از سه‌ماهه اول سال ۲۰۲۰ که جهان درگیر این بیماری همه‌گیر شد، دانشگاه‌ها، مدارس، سازمان‌ها و شرکت‌ها شاهد یک سطح بی‌سابقه از فعالیت کارمندان به‌صورت دورکاری بودند و امنیت سایبری نیز با خواسته‌های جدید، به چالش کشیده شد.

خرابکاران با استفاده از روش‌های پیشرفته، مدارس، دولت‌ها، مشاغل و نیروهای کاری که هنوز با چالش‌ها و محدودیت‌های مربوط به بیماری کرونا و آسیب‌پذیری‌های مربوط به امنیت این بسترها و پهنای باند روبرو است را مجدداً مورد هدف قراردادند. در این سال ۶۲ درصد سازمان‌های جهان نفوذ و حملات سایبری جدی را تجربه کردند. در شکل ۱ پنج تهدید پرشمار در سال ۲۰۲۰ نشان داده‌شده است.



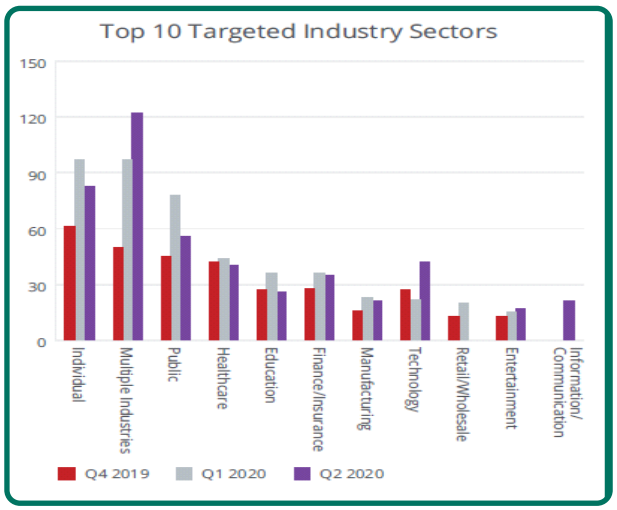
شکل۱. پنج تهدید امنیتی پرشمار در سال ۲۰۲۰

در شکل ۲ بردار حملات برای ۱۰ مورد که بیشترین نرخ رخداد را داشته‌اند، نشان داده‌شده است. به‌طورکلی در سه‌ماهه دوم سال ۲۰۲۰، حملات بدافزاری بیشترین موارد ثبت‌شده یعنی ۳۵ درصد از موارد گزارش‌شده را شامل می‌شود. همچنین حملات Account Hijacking در کل ۱۷ درصد و حملات هدف‌دار ۹ درصد از کل موارد را شامل می‌شود.



شکل ۲. بردار حملات ۱۰ مورد دارای بیشترین نرخ رخداد

حوادث امنیتی شناسایی‌شده در سه‌ماهه دوم سال ۲۰۲۰ با هدف قراردادن حوزه علم و فناوری ۹۱ درصد و در حوزه‌های صنایع ۲۵ درصد افزایش را به نسبت سه‌ماهه اول همین سال تجربه کرده‌اند. در شکل ۳ این آمار نشان داده‌شده است.



شکل ۳. بردار حملات ۱۰ مورد دارای بیشترین نرخ رخداد در حوزه‌های مختلف

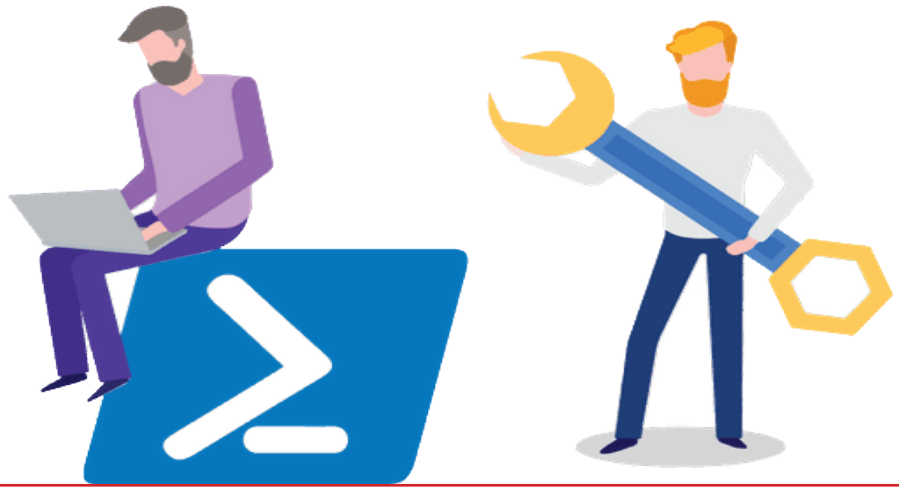
بر اساس گزارش آزمایشگاه‌های مک‌آفی، آمار تهدیدات و حملات بدافزاری در سه‌ماهه دوم سال ۲۰۲۰ افزایش قابل‌توجهی داشته است. در این بازه زمانی برای حملات بدافزاری ۴۱۹ تهدید در هر دقیقه مشاهده شده است که به‌طورکلی نسبت به سه‌ماهه قبل از آن، ۱۲ درصد افزایش داشته است. بدافزارهای جدید پاورشل نسبت به سه‌ماهه قبل از آن ۱۱۷ درصد، بدافزارهای جدید موبایلی ۱۵ درصد، بدافزارهای جدید حوزه اینترنت اشیاء ۷ درصد، بدافزارهای جدید لینوکسی ۲۲ درصد، بدافزارهای جدید مجموعه آفیس ۱۰۳ درصد و بدافزارهای جدید استخراج‌کننده رمز ارز ۲۵ درصد افزایش داشته‌اند.
در شکل‌های زیر آمار هر دسته بدافزاری در شش‌ماهه آخر ۲۰۱۹ و مقایسه آن با شش‌ماهه اول ۲۰۲۰ نشان داده‌شده‌اند.

نکته قابل‌توجه در خصوص آمار مربوط به حملات بدافزاری مربوط به دسته‌های بدافزارهای جدید پاورشل، بدافزارهای جدید مجموعه آفیس، بدافزارهای جدید موبایلی و بدافزارهای جدید استخراج‌کننده رمز ارز است که رشد چشم‌گیری را در این بازه زمانی داشته‌اند. در ادامه بررسی‌هایی برای این دسته‌ها خواهیم داشت.

بدافزارهای پاورشل

برای آلوده‌سازی و تکثیر بیشتر بدافزارها، مهاجمان سعی می‌کنند از ابزارهایی که به‌صورت پیش‌فرض بر روی سیستم قربانیان هدف وجود دارند، استفاده کنند. این عمل که با نام Living Off The Land شناخته می‌شود، به آن‌ها این امکان را می‌دهد که تهدیدات را با فرآیندهای روتین و مدیریتی سیستم ترکیب کرده و از ابزارهای موجود در سیستم بهره ببرند و سعی بر این باشد که آثار کمتری به‌جا گذاشته و دیرتر شناسایی شوند. ازآنجاکه مایکروسافت پاورشل به‌صورت پیش‌فرض بر روی سیستم‌عامل‌های ویندوزی نصب‌شده است، گزینه‌ای ایده‌آل برای مهاجمان است.

بدافزارهای fileless دسته‌ای از بدافزارها هستند که با روش‌هایی مانند جاسازی کد مخرب در اسکریپت‌ها و یا بارگذاری بدافزار در حافظه، بدون نوشتن در دیسک و داشتن فایل، رخ می‌دهند. به دلیل اینکه پاورشل می‌تواند یک اسکریپت را مستقیماً در حافظه اجرا کند، بنابراین به شکل گسترده‌ای برای انجام حملات بدافزاری fileless استفاده می‌شود. ازآنجاکه فایلی هرگز در هارددیسک کپی نمی‌شود، عبور از ابزارهای امنیتی که با بررسی ورودی‌ها و خروجی‌ها تهدیدات را تشخیص می‌دهند تا حدی آسان می‌شود. ممکن است کاربر فکر کند که چون سیاست‌های اجرای پاورشل بر روی سیستم خود را محدود کرده تا اسکریپت‌ها نتوانند اجرا شوند، از آلودگی به بدافزارهای fileless محافظت‌شده است اما مهاجمان می‌توانند به‌راحتی این سیاست‌ها را دور بزنند. به‌عنوان نمونه برای این دسته از بدافزارها می‌توان از Trojan.Kotver، JS.Downloader و W۹۷M.Downloader نام برد که درمجموع ۱۶ درصد از آلودگی‌های بدافزارهای پاورشل را در این بازه زمانی به خود اختصاص داده‌اند.



ماکروهای مجموعه آفیس

استفاده از ماکروها ابزار و روشی قدرتمند برای خودکارسازی روال و فعالیت‌های معمول در مجموعه مایکروسافت آفیس هستند و می‌توانند باعث بهره‌وری بیشتر و صرفه‌جویی در زمان شوند. به بیان ساده‌تر، ماکروها مجموعه‌ای از فرمان‌ها، کلیدها و یا کلیك‌های ماوس هستند که می‌توان آن را ذخیره کرد و به‌صورت یک ساختار دستوری درآورد که به‌صورت مکرر هر زمان که خواسته شد، اجرا گردد. در حقیقت اگر یک کاربر مجبور است به‌طور مداوم فعالیت‌ها و کارهایی تکراری و معین را در نرم‌افزارهای مجموعه آفیس مانند Word یا Excel انجام دهد، می‌تواند با پیاده‌سازی، ترکیب و ذخیره مراحل کار در یك ماکرو و سپس اجرای آن با کلیك بر روی یك آیکون و یا فشردن ترکیبی از کلیدها، حجم کار را سبك کرده و این فرآیند تا حدی خودکار شود. نکته قابل‌توجه این است که مهاجمین از همین قابلیت سوءاستفاده کرده و از ماکروها برای آلوده کردن سیستم قربانیان استفاده می‌کنند.

ماکروها به‌صورت الحاق در فایل‌های مجموعه آفیس ایجاد می‌شوند. باید دقت کرد که به‌طور مثال یک فایل Word حاوی ماکرو تفاوتی با فایل بدون ماکرو ندارد و به‌محض اجرای فایل، پیامی به کاربر نشان داده‌شده که فعال‌سازی اجرای ماکرو را درخواست می‌کند و در صورت فعال‌سازی، ماکرو اجرا خواهد شد. فایل‌های مجموعه آفیس به دلیل اینکه به‌صورت روتین توسط کاربران مورداستفاده هستند این بستر را برای مهاجمین فراهم کرده که بتوانند فایل‌های آلوده به ماکرو را از روش‌های مختلف برای قربانیان ارسال کرده یا آن‌ها را ترغیب به دانلود این فایل‌ها کنند و در اغلب موارد به دلیل عدم وجود آموزش صحیح به کاربران، فایل اجراشده و ماکرو نیز فعال‌سازی می‌شود!!!

البته باید گفت که در سال‌های گذشته استفاده از ماکروها برای آلوده‌سازی بسیار رایج‌تر بود به این دلیل که تنظیمات مربوط به اجرای ماکرو در مجموعه آفیس به‌صورت پیش‌فرض فعال بود و به‌محض اجرای فایل، ماکرو به‌طور خودکار اجرا می‌شد. در نسخه‌های اخیر مجموعه آفیس، اجرای ماکروها به‌طور پیش‌فرض غیرفعال است و در صورت وجود ماکرو در فایل، از کاربر درخواست فعال‌سازی اجرای ماکرو خواهد شد و این یعنی نویسندگان بدافزار باید کاربران را متقاعد کنند که اجرای ماکروها را فعال کنند تا بدافزار آن‌ها اجرا شود. به‌عنوان‌مثال دو نمونه از ماکروهای مخرب با نام‌های Virus:W32/Concept و Me-lissa.Macro.Virus وجود داشته‌اند و در چند سال گذشته از دو ماکروی W97M.Melissa.ac و W97M.Marker بیشترین استفاده‌شده است.

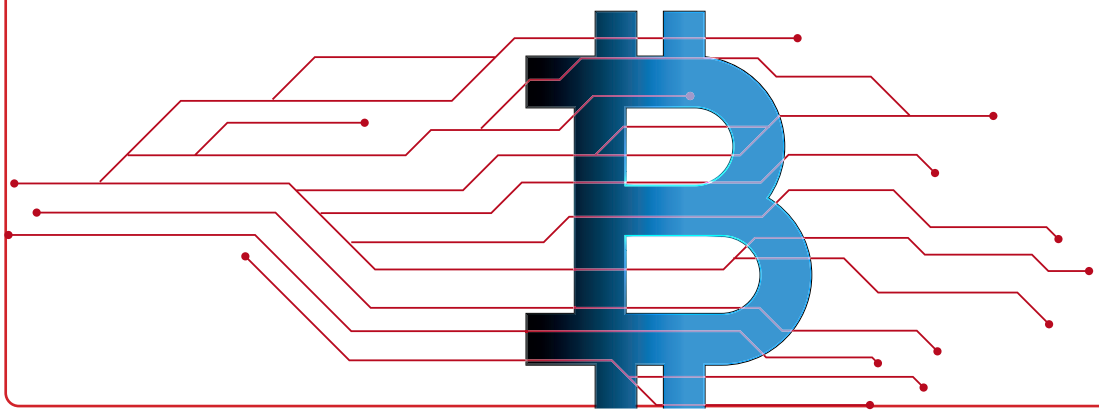
بدافزارهای استخراج‌کننده رمز ارز

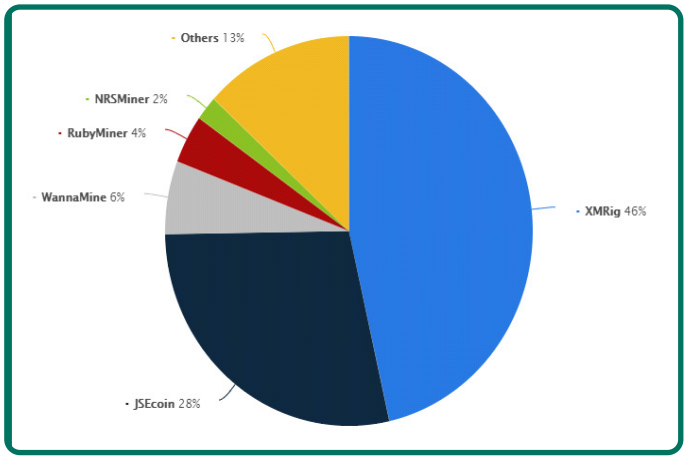
مجرمان اینترنتی همیشه به دنبال راه‌های جدیدی برای کسب درآمد هستند. با گسترش ارزهای دیجیتال، مجرمان فرصتی منحصربه‌فرد برای بهره‌بردن از منابع، پهنای باند و قدرت سخت‌افزار قربانیان استخراج رمز ارزها برای خود فراهم دیده‌اند. افزایش بسیار زیاد قیمت رمز ارزهایی مانند بیت‌کوین نیز در ترغیب مجرمان سایبری برای استخراج، بی‌تأثیر نبوده است.

با بررسی این نوع بدافزارها مشخص می‌شود که شروع این حملات ممکن است از طریق یکی از روش‌های زیر باشد:

- ایمیل‌هایی با پیوست‌های آلوده یا حاوی لینک‌هایی به این بدافزارها
- وب‌سایت‌هایی که از کیت‌های مخربی استفاده می‌کنند که سعی دارند با سوءاستفاده از آسیب‌پذیری‌های مرورگر، بدافزار استخراج‌کننده رمز ارز را بر روی سیستم قربانی نصب و اجرا کنند.
- وب‌سایت‌هایی که وقتی کاربر در حال بازدید از آن‌ها است با اجرای اسکریپت‌هایی از قدرت پردازنده سیستم قربانی برای استخراج رمز ارز بهره می‌برند.

برای نمونه می‌توان از Wannamine، JSEcoin، XMRig و RubyMiner به‌عنوان بدافزارهای استخراج رمز ارز نام برد و در شکل ۴ آمار بیشترین تکثیر این دسته بدافزارها در سال ۲۰۲۰ نشان داده‌شده است.

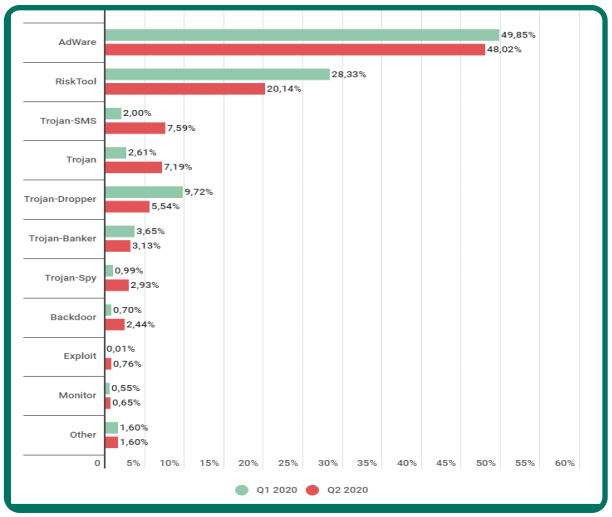




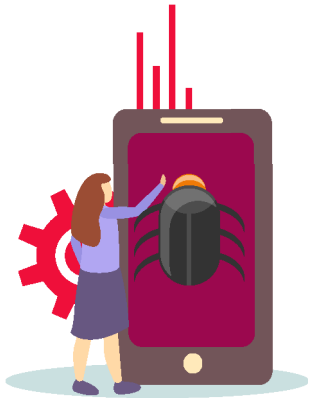
شکل ۴. بیشترین آلودگی بدافزارهای استخراج‌کننده رمز ارز در سال ۲۰۲۰

بدافزارهای موبایلی

همان‌طور که از نام آن‌ها پیداست، بدافزارهای موبایلی اپلیکیشن‌های مخربی هستند که به‌طور خاص سیستم‌عامل‌های تلفن‌های همراه را هدف قرار می‌دهند. در سالیان اخیر انواع مختلفی از بدافزارهای موبایلی و روش‌های مختلفی از توزیع و آلودگی به‌وجود آمده‌اند. برای بخش وسیعی از مردم که از تلفن‌های هوشمند استفاده می‌کنند و شرکت‌ها و سازمان‌هایی که برای انجام امور خود به اپلیکیشن‌های موبایلی وابسته هستند، این دسته بدافزارها یک تهدید بسیار جدی است. در حال حاضر، حجم تهدیدات اپلیکیشن‌های تلفن همراه به نسبت تهدیداتی که برای سیستم‌های دیگر بوده، کمتر است اما این تهدیدات به شکل بسیار گسترده‌ای در حال رشد هستند و مخاطرات بدافزارهای موبایلی در چند سال اخیر افزایش چشم‌گیری داشته است. طبق گزارشات آزمایشگاه تهدیدات کسپرسکی در این بازه زمانی بیشترین حملات موبایلی از طریق تبلیغ‌افزارها، RiskTools و TrojanSMS صورت می‌گیرد. در شکل ۵ لیست بیشترین حملات حوزه دستگاه‌های تلفن همراه در سه‌ماهه اول و دوم سال ۲۰۲۰ نمایش داده‌شده است. همچنین بیشترین آلودگی بدافزارهای موبایلی برای نمونه‌های مختلف در شکل ۶ نشان داده‌شده است.



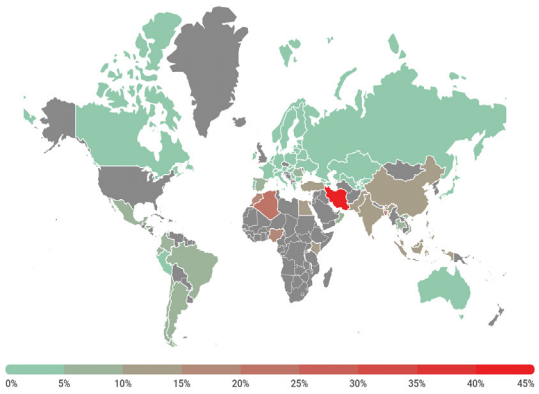
شکل ۵. بیشترین حملات حوزه دستگاه‌های تلفن همراه
در سه‌ماهه اول و دوم سال ۲۰۲۰



	Verdict	%*
1	DangerousObject.Multi.Generic	40.29
2	Trojan.AndroidOS.Boogr.gsh	9.02
3	DangerousObject.AndroidOS.GenericML	6.17
4	Trojan-Downloader.AndroidOS.Necro.d	4.86
5	Trojan-Dropper.AndroidOS.Hqwar.cf	3.63
6	Trojan.AndroidOS.Hiddad.fi	3.19
7	Trojan-Downloader.AndroidOS.Helper.a	2.84
8	Trojan-Downloader.AndroidOS.Agent.hy	2.64
9	Trojan.AndroidOS.Agent.vz	2.32
10	Trojan-Downloader.AndroidOS.Agent.ik	2.06

شکل ۶. ده نمونه بدافزار موبایلی با بیشترین نرخ آلودگی در سه‌ماهه اول و دوم سال ۲۰۲۰

همچنین در شکل ۷، جدول بیشترین کشورهای مورد هدف تهدیدات حملات موبایل نشان داده‌شده است. طبق این آمار، ایران در این بازه زمانی دارای بیشترین نرخ تهدیدات موبایلی بوده‌است که این امر نیاز به توجه جدی در این حوزه را در کشورمان طلب می‌کند.



kaspersky

	Country*	%**
1	Iran	43.62
2	Algeria	21.97
3	Bangladesh	19.30
4	Morocco	17.57
5	Nigeria	15.12
6	India	13.54
7	Saudi Arabia	13.52
8	Kenya	12.61
9	Indonesia	12.17
10	Pakistan	12.16

شکل ۷. بردار بیشترین کشورهای هدف حملات بدافزارهای موبایل

حمله فیشینگ به مایکروسافت آفیس با میزبانی

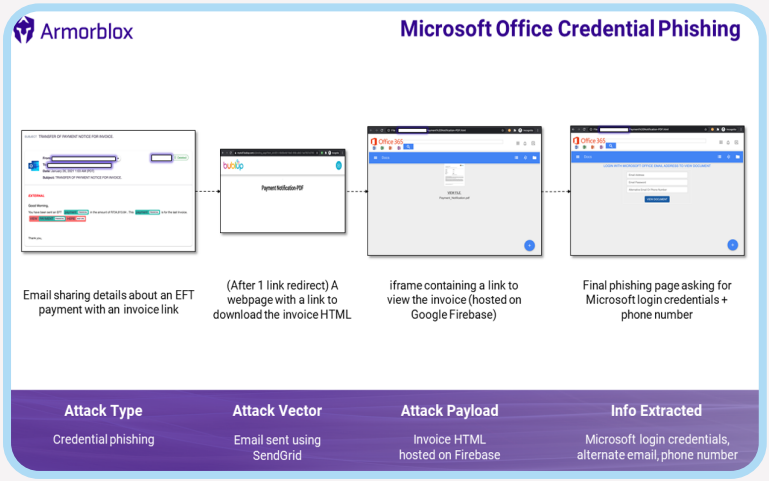
تهیه و تدوین: پرستو مجیدی

مقدمه

در این مطلب Blox Tale نگاهی به یک کلاه‌برداری هدفمند در ایمیل خواهد داشت و به‌طور خلاصه روند انجام حمله را توضیح می‌دهد. همچنین نکات و توصیه‌هایی را برای محافظت در برابر چنین حملاتی ارائه می‌دهد. تمرکز بر روی حمله‌ای خواهد بود که وانمود می‌کند اطلاعات مربوط به پرداخت EFT یا Electronic Funds Transfer را با پیوندی برای بارگیری فاکتور HTML به اشتراک می‌گذارد. با باز کردن HTML صفحه‌ای با عنوان Microsoft Office بارگیری می‌شود که در فایربیس گوگل (Google Firebase) میزبانی می‌شود. در صفحه نهایی فیشینگ، اطلاعات ورود قربانیان مایکروسافت شامل آدرس ایمیل، ایمیل پشتیبان و گذرواژه شماره تلفن قربانیان استخراج می‌شود.

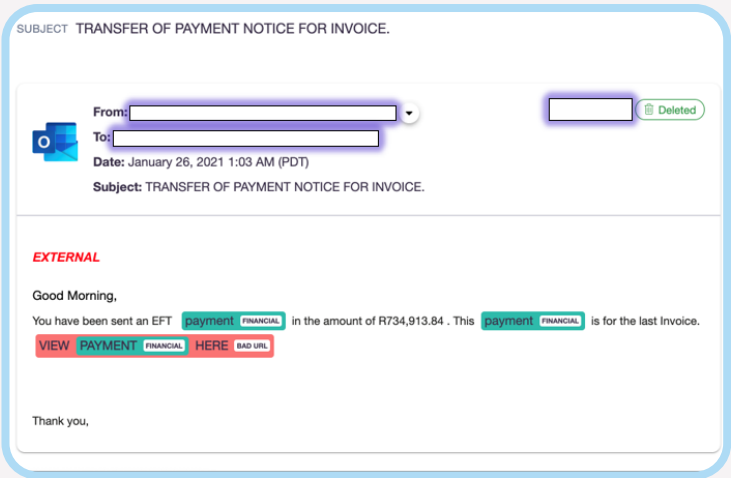
Org mailboxes = ~20000
Email security bypass = EOP/Microsoft defender for office 365
Techniques used = social engineering / link redirect / html hosted on google firebase / brand impersonation

این حمله هدفمند بر بستر ایمیل، کنترل‌های امنیتی ایمیل Microsoft را دور زده است. مایکروسافت سطح اطمینان هرزنامه Spam Confidence Level (SCL) of 1 را به این ایمیل‌ها اختصاص داده است، به این معنی که مایکروسافت ایمیل را مشکوک تشخیص نداده است و آن را به صندوق‌های ورودی کاربر نهایی تحویل می‌دهد. در شکل ۱ ساختار کلی این حمله نشان داده‌شده است.



شکل ۱: ساختار کلی حمله فیشینگ انجام‌شده

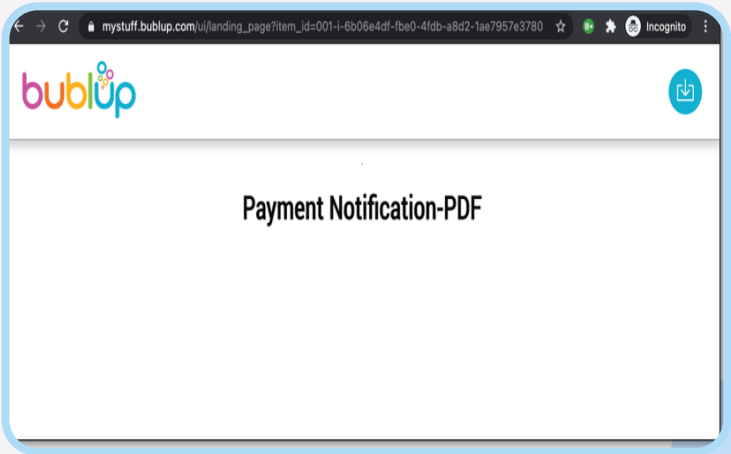
تیم تحقیقاتی Armorblox در یک خبر، یک حمله با نام مستعار «فاکتور» در محیط کاربری یکی از مشتری‌هایش را مشاهده کرده است. این ایمیل با عنوان «اخطار پرداخت برای فاکتور» است و قربانیان را در مورد پرداخت EFT مطلع می‌کند. این ایمیل شامل لینکی برای نمایش فاکتور است. در شکل ۲ این ایمیل نشان داده‌شده است.



شکل ۲: ایمیل ارسالی برای قربانیان

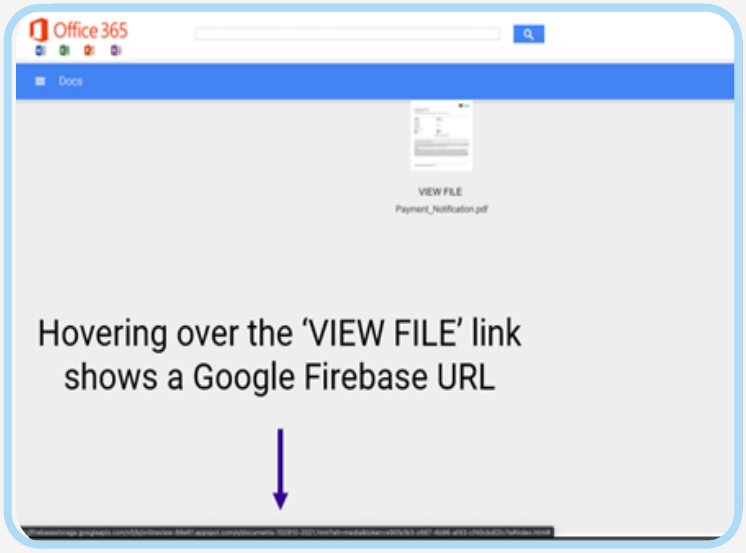
بررسی حمله

در این حمله با کلیک بر روی لینک موجود در ایمیل، کاربر به دامنه mystuff [.] Bublup [.] Com هدایت می‌شود، سپس تغییر مسیر به دامنه nam02[.]safelinks[.]protection[.]outlook[.]com' انجام می‌شود که نشان می‌دهد حتی اگر لینک هم مخرب باشد بازهم توسط کنترل‌های امنیتی محلی Microsoft بازنویسی می‌شود. صفحه‌ای که کاربر به آن هدایت می‌شود را در شکل ۳ می‌توان مشاهده کرد. در بالای این صفحه یک آیکون در سمت راست برای دانلود فاکتور پرداختی وجود دارد که در ایمیل به آن اشاره شده است



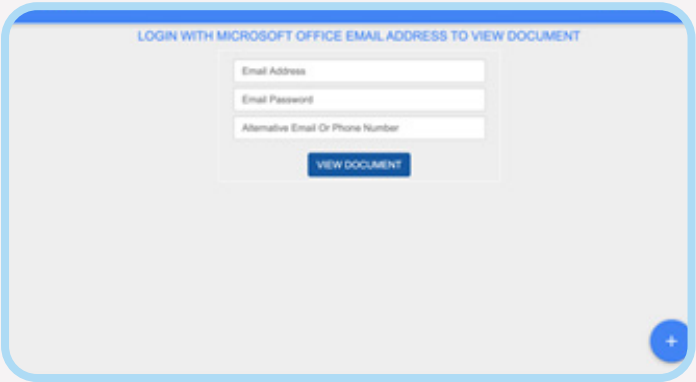
شکل ۳: صفحه‌ای که کاربر برای دانلود فاکتور به آن هدایت می‌شود.

نام فایل دانلود شده حاوی کلمه PDF در خود است اما در واقع یک فایل HTML است. پس از باز شدن فایل HTML یک تگ IFRAME با عنوان office 365 در آن نمایش داده می‌شود. همان‌طور که در شکل ٤ مشاهده می‌کنید، چون این صفحه HTML در فایربیس گوگل میزبانی می‌شود، URL های معتبری مانند فایربیس، افراد (و فناوری‌های امنیتی ایمیل) را گمراه می‌کنند و تصور می‌کنند فاکتور معتبر و مربوط به office 365 است.



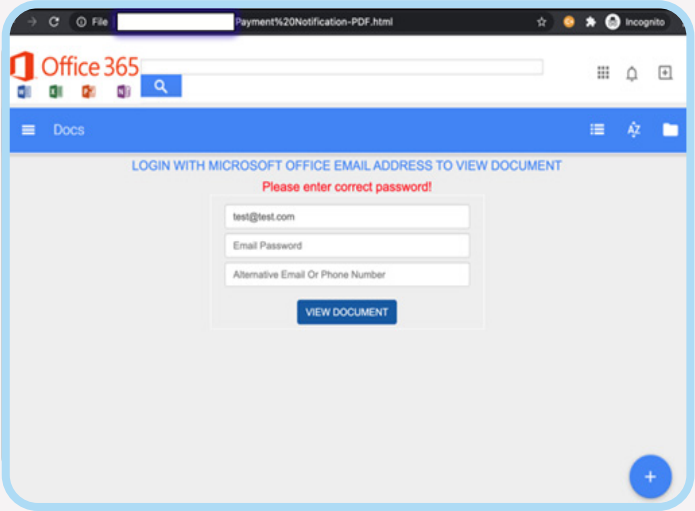
شکل ٤: صفحه حاوی لینک دانلود فاکتور

با کلیک بر روی تصویر کوچک یا پیوند VIEW FILE به صفحه فیشینگ نهایی منتقل می‌شوید که از قربانیان می‌خواهد با اطلاعات احراز هویت خود، وارد سیستم شوند، درنتیجه این صفحه فیشینگ، اطلاعات کاربران شامل آدرس ایمیل، گذرواژه و ایمیل پشتیبان یا شماره تلفن مرتبط با حساب‌های Microsoft قربانیان را به سرقت می‌برد. شماره تلفن و ایمیل پشتیبان برای کاربرانی استفاده‌شده است که احراز هویت دومرحله‌ای 2FA یا ایمیل پشتیبان در حساب کاربری مایکروسافت خود را فعال کرده‌اند.



شکل ٥: صفحه فیشینگ مربوط به دریافت اطلاعات قربانی

با واردکردن اطلاعات نادرست در این فرم، یک پیغام خطا نشان داده می‌شود و از کاربر می‌خواهد اطلاعات صحیح را وارد کند. این مورد ممکن است به مکانیزم اعتبارسنجی سمت سرور اشاره داشته باشد که صحت جزئیات واردشده را بررسی می‌کند. مهاجمان ممکن است به دنبال سرقت هرچه بیشتر آدرس‌های ایمیل و رمزهای عبور باشند و پیغام خطا بدون توجه به جزئیات واردشده، همچنان ظاهر شود.



شکل ٦: صفحه مربوط نشان دادن پیغام خطا پس از ورود اطلاعات نادرست توسط قربانی

خلاصه تکنیک‌های مورد استفاده

این حمله از طیف وسیعی از روش‌ها و تکنیک‌ها برای عبور از فیلترهای امنیتی سرور ایمیل و اینکه برای کاربران نهایی قابل‌تشخیص نباشد، استفاده کرده است. در ادامه چند تکنیک به‌کاررفته بررسی می‌شود:

از SendGrid برای احراز هویت استفاده می‌شود:

ایمیل جعلی با یک آدرس جیمیل شخصی از طریق سرویس SendGrid ارسال‌شده است که این کار منجر به دور زدن سیستم‌های اعتبارسنجی ایمیل نظیر DKIM، SPF و DMARC می‌شود.

مهندسی اجتماعی:

در این حمله از تکنیک‌های مختلف مهندسی اجتماعی برای فریب کاربر استفاده‌شده است.

جعل هویت تجاری:

صفحه فیشینگ نهایی طراحی‌شده یک پورتال Office 365 را جعل می‌کند و در صفحه اصلی آن از لوگوهای تجاری مایکروسافت استفاده‌شده است. همچنین برای مشاهده یک سند فاکتور، به اطلاعات حساب کاربری مایکروسافت نیاز است که این مورد در ذهن بیشتر قربانیان منطقی به نظر می‌رسد، زیرا آن‌ها هر روز اسناد، فایل‌ها و سخنرانی‌هایی را از همکاران دریافت می‌کنند که دقیقه مشابه همین روال جعلی است.

میزبانی فایبربیس گوگل:

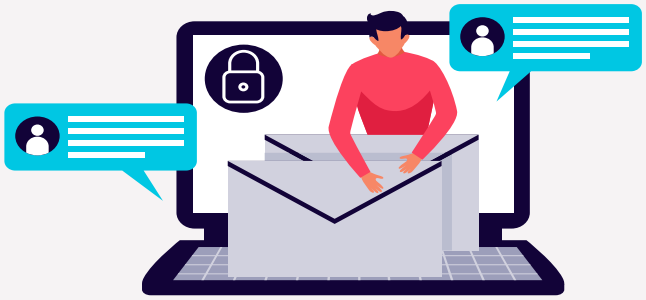
فاکتور نهایی در فایبربیس گوگل میزبانی می‌شود. قاعدتاً چنین میزبانی اطمینان کافی را ایجاد می‌کند و ایمیل با این آدرس، قادر است از فیلترهای امنیتی عبور کند.

لینک برای تغییر مسیر کاربر:

پیچیدگی فرآیند حمله و تغییر مسیرهای متفاوت، یکی از تکنیک‌هایی است که برای فریب ابزارهای امنیتی که لینک‌ها را ردیابی می‌کنند و به دنبال صفحات جعلی ثبت‌نام می‌گردند، استفاده‌شده است.

در انتهای این مطلب، توصیه‌هایی برای افراد یا سازمان‌هایی که به دنبال محافظت از خود در برابر این نوع حملات ایمیل هدفمند هستند، آورده شده است:

۱. امنیت ایمیل خود را با کنترل‌های اضافی تقویت کنید.



۲. به روش‌های مختلف مهندسی اجتماعی دقت داشته باشید.

۳. از احراز هویت دومرحله‌ای و ابزارهای مدیریت رمز عبور استفاده کنید.

امنیت اطلاعات

توصیه‌های مهم در زمینه امنیت سایبری برای کاربران

گردآوری: نازیلا خسروی

مقدمه

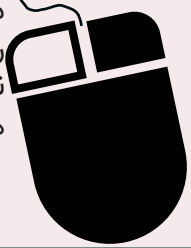
وابستگی روزافزون و ناگریز امورات ما به اینترنت و فضای مجازی موجب افزایش چشمگیر استفاده از این بستر شده است، تعداد کاربران هرلحظه در حال افزایش است و در حال حاضر طیف گسترده‌ای از اقشار جامعه کاربر اینترنت هستند.

واقعیت امر به این صورت است که امروزه اینترنت به فضایی مملو از لینک‌های مخرب، بدافزارهایی همچون تروجان‌ها، ویروس‌ها و باج افزارها تبدیل‌شده است و کاربران بیش‌ازپیش در معرض خطر و آسیب هستند. وقتی یک کلیک ممکن است هزینه‌های زیاد و مختلفی داشته باشد پس کاربران بیش از هر زمان دیگری به امنیت نیاز دارند و ملزم هستند به نکات امنیتی توجه بیشتری داشته باشند.

در این مقاله ۱۰ توصیه مهم و رایج امنیت سایبری آورده شده است تا کاربران بتوانند آنلاین بمانند و ایمن باشند.

① کلیک کردن بدون فکر، بی‌ملاحظگی است.

فقط به این دلیل که می‌توانید کلیک کنید، به این معنی نیست که باید کلیک کنید. لینک‌های مخرب می‌توانند از چند طریق مختلف آسیب برسانند، بنابراین حتماً لینک‌های دریافتی خود را بازبینی کرده و اطمینان حاصل کنید که آن‌ها از طرف فرستندگان معتمد هستند. همواره در نظر داشته باشید باز کردن هر لینکی بدون فکر کردن، می‌تواند با هزینه سنگینی برای شما همراه باشد.



② از احراز هویت دو مرحله‌ای استفاده کنید.

داشتن یک رمز ورودِ امن بسیار مهم است، اما احراز هویت دو یا چند مرحله‌ای ضروری‌تر است. این روش دو لایه اقدامات امنیتی را ارائه می‌دهد، بنابراین اگر یک مهاجم یا نفوذگر بتواند رمز ورود شما را با روش‌های مختلف به دست آورد و یا به‌دقت حدس بزند، هنوز یک اقدام امنیتی اضافی و محکم برای عدم دسترسی به حساب کاربری شما وجود دارد.

3 مراقب کلاه‌برداری فیشینگ باشید.

حملات فیشینگ از بزرگ‌ترین تهدیدهای امنیت سایبری هستند، ازاین‌جهت که تحقق آن‌ها بسیار آسان است. در این حمله فرد نفوذگر در جایگاه شخصی است که کاربر قربانی ممکن است فریب او را بخورد، لینک مخرب دریافتی را باز کند و اطلاعات مهم خود را فاش کند یا یک نرم‌افزار مخرب را نصب کند و سیستم خود را به بدافزار آلوده کند. عمده‌ترین راه حملات فیشینگ، ایمیل‌های جعلی است که روزانه بیش از ۳ میلیارد از آن‌ها ارسال می‌شود پس بهترین راه مراقبت در مرحله‌ی اول، پرهیز از باز کردن ایمیل‌هایی با فرستنده‌ی ناآشنا است. هر اطلاعات مشکوک در ایمیل یا فرستنده باید شما را حساس کند. گرچه فیشینگ روش‌ها و بسترهای مختلفی را دربرمی‌گیرد و همواره باید به این تله‌گذاری‌ها و فریب قربانیان با تکنیک‌های مختلف توجه داشته باشیم.

4 پیگیر ردپای دیجیتال خود باشید.

وقتی حساب‌های کاربری خود را مانیتور و کنترل می‌کنید می‌توانید از فعالیت‌های مشکوک مطلع شوید. آیا شما هر سایتی را که در آن حساب کاربری آنلاین دارید و اطلاعات خود را در آن ذخیره کرده‌اید، همیشه به خاطر دارید؟

سایت‌هایی که اطلاعات کارت‌بانکی خود را برای پرداخت‌های آنلاین وارد کرده‌اید؟

پیگیر ردپای دیجیتال بودن مسئله‌ی حائز اهمیتی است مخصوصاً در رسانه‌های اجتماعی و حساب‌های کاربری که استفاده نمی‌کنید.

5 با به‌روزرسانی‌ها همراه باشید.

اگر اعلان‌های به‌روزرسانی نرم‌افزار برای شما آزاردهنده است و همواره به فکر خاموش کردن آن‌ها می‌باشید، بدانید که تنها نیستید. با کشف نقص‌های امنیتی، وصله‌های نرم‌افزاری منتشر می‌شوند که شما برای حفظ امنیت اطلاعات و سیستم خود ملزوم به دریافت و نصب آن‌ها می‌باشید. با این کار خود را کمتر در معرض آسیب‌پذیری قرار می‌دهید و مصونیت بیشتری در برابر بدافزارها و آلودگی‌ها خواهید داشت.

6 ایمن متصل شوید.

نکات مربوط به امنیت سایبری توسط متخصصین این حوزه به‌روشنی بیان و ارائه‌شده است و به‌راحتی در دسترس همگان قرار دارد؛ اما هنوز بسیاری از کاربران این توصیه‌ها را جدی نمی‌گیرند و از آن پیروی نمی‌کنند. هرکسی در زمانی ممکن است وسوسه شود که از طریق کانکشن ناامن و عموماً رایگان به اینترنت متصل شود اما وقتی عواقب آن را بسنجد و به پیامدهای آن واقف باشد، قطعاً متوجه خواهد شد که ارزش ندارد و از این فکر خود منصرف می‌شود. در صورت امکان فقط از طریق شبکه‌های خصوصی و امنِ شناخته‌شده متصل شوید، علی‌الخصوص در مواقع مدیریت اطلاعات حساس که چالش برای آنها میتواند اثرات زیان‌باری داشته باشد.

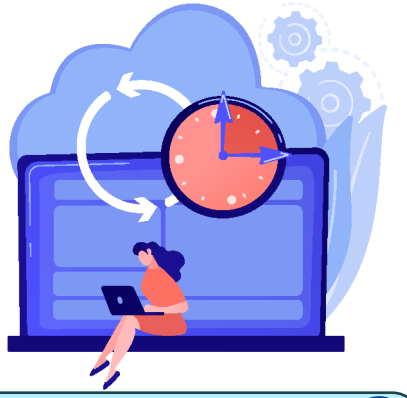
7 دستگاه تلفن همراه خود را ایمن کنید.

امنیت و ایمن‌سازی تنها به کامپیوترهای شخصی ختم نمی‌شود. امنیت حضور خود در فضای سایبری را از طریق دستگاه‌های تلفن همراه نیز تأمین کنید. از گذرواژه‌ها و راهکارهای بیومتریک قوی استفاده کنید. اطمینان حاصل کنید که بلوتوث خود را خاموش می‌کنید و به‌طور خودکار به هیچ دستگاه Wi-Fi عمومی متصل نمی‌شوید. با احتیاط و با دقت دانلود کنید!

8 مراقب مهندسی اجتماعی باشید.

وقتی مهاجمین و نفوذگران نتوانند یک آسیب‌پذیری امنیتی شناسایی کنند، به روش‌های دیگر حملات سایبری روی می‌آورند. مهندسی اجتماعی! یک نوع حمله به ذهن کاربر، نه به دستگاه و سیستم، که بر مبنای اصول روانشناسی است. مجرمان اینترنتی برای دسترسی به سیستم و اطلاعات کاربران راه‌های خلاقانه‌ای ارائه می‌کنند. به‌ویژه با اطلاعاتی که به‌صورت آنلاین و از طریق رسانه‌های اجتماعی در دسترس عموم است. گاهی حتی از طریق حربه‌هایی از مسیر مسائل اعتقادی، قومیتی و مذهبی این جمع‌آوری اطلاعات و فریب صورت می‌گیرد. باید توجه داشت در مهندسی اجتماعی مهاجم با قرار دادن قربانی در شرایط روحی-روانی خاص مانند هیجان، اضطراب، ترس، مسائل عاطفی و غیره، او را از حالت پایدار عقلانی و منطقی دور کرده و تصمیم‌گیری فرد در این شرایط خاص ممکن است کاملاً منطقی نباشد و اطلاعاتی حساس از قربانی به‌دست آورد.

9 از اطلاعات خود نسخه پشتیبان تهیه کنید.



این روزها تأمین و تهیه فضای ذخیره‌سازی همراه با هزینه زیادی نیست؛ یعنی بهانه‌ای برای نداشتن نسخه پشتیبان از اطلاعات مهم وجود ندارد. پشتیبان‌گیری می‌تواند بر بستر یک حافظه فیزیکی مانند فلش دیسک یا هارد اکسترنال یا در فضای اَبری باشد. به یاد داشته باشید تهدیدات مخرب و مهاجمین همیشه نمی‌خواهند داده‌ها و اطلاعات شما را سرقت کنند.

گاهی اوقات هدف آن‌ها رمزگذاری یا پاک کردن اطلاعات است، برای اخاذی و گرفتن باج! پس چه‌بهتر که یک نسخه پشتیبان از داده‌های مهم و حساس خود داشته باشید.

10 شما روئین‌تن نیستید!

مضرترین تصوری که هر کاربر اینترنت می‌تواند داشته باشد این است که «برای من اتفاق نخواهد افتاد» یا «من از وب‌سایت‌های ناامن بازدید نمی‌کنم»، «اطلاعات من بدرد کسی نمی‌خورد»!!! مجرمان اینترنتی هیچ تبعیضی در هدف قرار دادن کاربران قائل نیستند. مراقب باشید و احتیاط کنید. تمام اشتباهات با "ctrl + Z" قابل بازگشت نیستند.

درنهایت باید توجه داشت که قطعاً این موارد تنها نکات و توصیه‌های امنیتی در فضای سایبری نیستند اما تکنیک‌های ساده‌ای هستند که می‌توانند کمک زیادی به جلوگیری از رخ دادن یک فاجعه کنند و تا حدی امنیت کاربران را افزایش دهند.

توصیه‌های امنیتی فناوری اطلاعات برای
کاربران یک سازمان
دانشگاه کردستان
University of Kurdistan
تغییر کلمه عبور پیش‌فرض سامانه‌ها و تغییر دوره‌ای آن
انتخاب کلمه عبور مناسب با حداقل ۸ کاراکتر شامل ترکیبی از اعداد، حروف کوچک، بزرگ و نمادهای مختلف
به‌روزرسانی نرم‌افزارها و استفاده از نسخه‌های جدید سیستم‌عامل مانند ویندوز ۱۰
تهیه نسخه پشتیبان از اطلاعات حساس و فایل‌ها
بررسی امنیت فیزیکی سیستم و درگاههای کامپیوتر خود جهت اطمینان از عدم اتصال سخت‌افزار اضافی
VPN
در اختیار قرار ندادن اکانت VPN سازمان به دیگران
غیرفعال کردن پروتکل RDP بر روی سیستم‌عامل ویندوز
استفاده از قفل صفحه در صورت عدم حضور در پشت سیستم
در اختیار قرار ندادن اطلاعات حساس مانند نام کاربری و کلمه عبور ایمیل و حساب کاربری سامانه‌های مختلف
عدم دانلود و اجرای پیوست و لینک‌های ارسالی در ایمیل‌ها در صورت غیرمطمئن بودن فرستنده
عدم فعال‌سازی گزینه اجرای ماکروها در فایل‌های مجموعه آفیس
خاموش کردن کامپیوتر خود هنگام ترک محیط کار
استفاده از انتی‌ویروس و به‌روزسانی مداوم آن
2FA
رعایت نکات امنیتی در شبکه‌های اجتماعی و پیام‌رسان‌ها و فعال کردن احراز هویت دو مرحله‌ای (2FA)
CERT.UOK.AC.IR

مرکز آپا دانشگاه کردستان

www.cert.uok.ac.ir