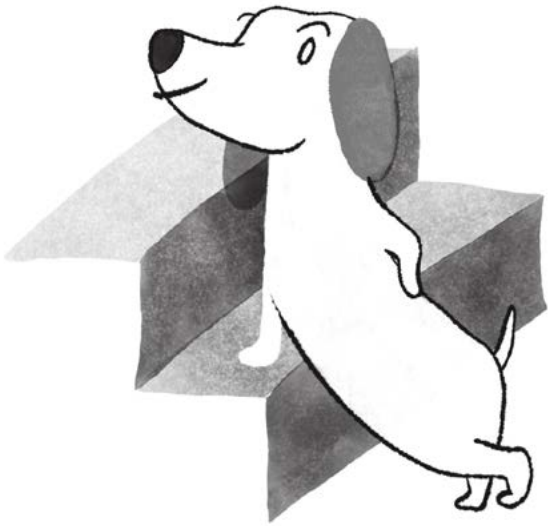
madmacx

Apple IT for [creative] professionals.

KNOWLEDGE BASE

OVER MALWARE



© MadMacX 2021 - www.madmacx.be

madmacx
Apple IT for [creative] professionals.

INHOUD

© MadMacX 2021 - www.madmacx.be

EEN MAC IS TOCH BESTAND TEGEN VIRUSSEN?

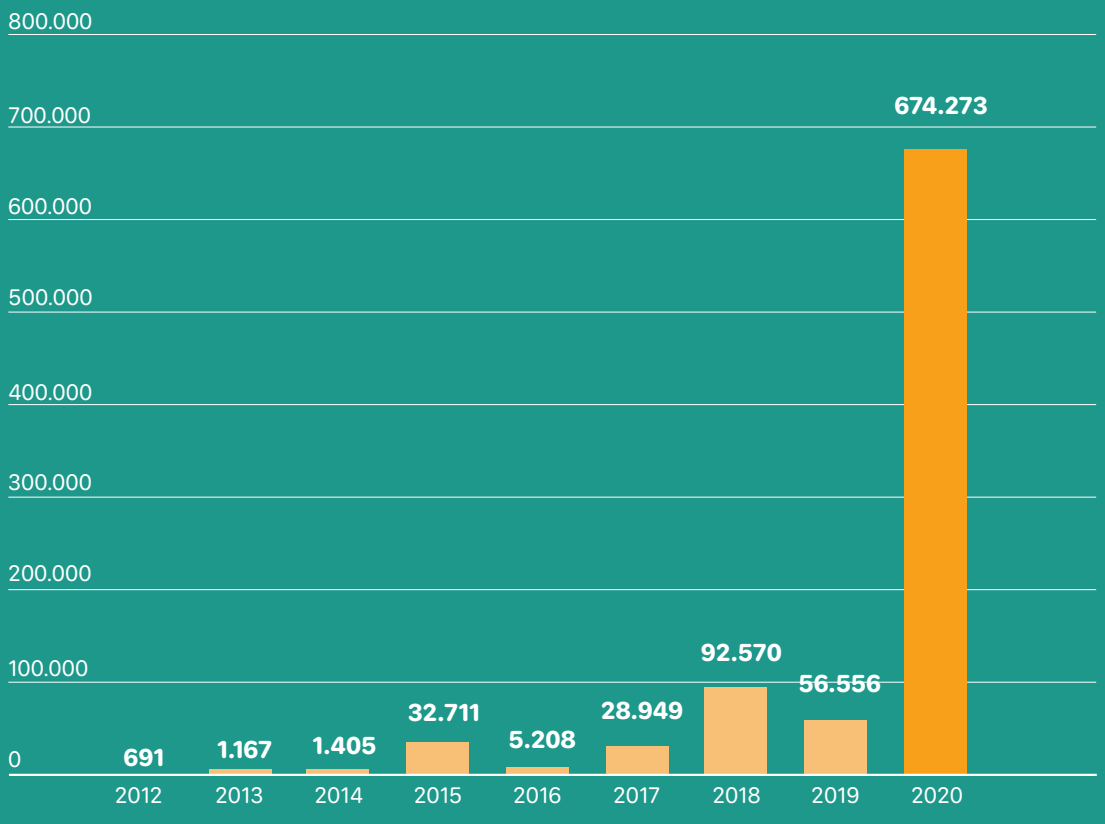
Tijd om de mythe te ontkrachten. Apple computers zijn gedurende vele decennia absoluut 'veilige' toestellen gebleken. Ze kregen daardoor een soort quasi onwrikbare reputatie. Maar in realiteit is dat eigenlijk al een hele tijd niet meer het geval.

Hoewel macOS van technische opbouw (we besparen u de details) nog steeds een stuk veiliger is dan pakweg Windows, betekent dat helemaal niet dat het daarom ook echt meer bescherming biedt.

De belangrijkste oorzaak voor die afbrokkelende veiligheid, is de altijd groeiende populariteit van Apple. Het aantal aanvallen op de Mac omgevingen van zowel particuliere als professionele gebruikers, is de laatste jaren enorm gestegen.

DE EVOLUTIE VAN MACOS MALWARE 2012-2020

In 2020 verlegde de focus van cybercriminelen zich naar macOS systemen.
Er werd dat jaar een gemiddelde van 1.847 bedreigingen per dag vastgesteld.



source: www.av-test.org

© MadMacX 2021 - www.madmacx.be

TOP

De toename van het aantal aanvallen op macOS systemen, leidt onvermijdelijk ook tot een sterke toename in het aantal geslaagde inbreuken. (De mobiele iOS systemen, zijn voorlopig nog redelijk ondoordringbaar voor de doorsnee hacker.

Maar je kan er prat op gaan dat deze een hoofdfocus worden in de toekomst. Die markt is qua omvang gewoon te verleidelijk voor malafide digitale goudzoekers.)

MALWARE OF VIRUS?

“ Mensen verwarren deze twee termen vaak.
Malware is een verzamelnaam voor malafide software. Terwijl ‘viraal’ slechts één manier is om het te verspreiden. Een app die zichzelf niet repliceert of andere computers niet infecteert, is geen virus, hoewel het nog steeds malware kan zijn.“

FOCUS OP MALWARE

Er zijn (nog) geen gevallen van zelf-replicerende virussen geregistreerd voor macOS. Maar in de praktijk vormen deze slechts een klein percentage van de malwarebedreigingen voor een modern besturingssysteem.

Precies om die reden zullen we het woord ‘virus’ in deze paper proberen te vermijden en het niet hebben over virussen in de strikte zin en definitie van het woord.

Dit document gaat over malware en dat is wel degelijk een bedreiging voor jou als Apple gebruiker.

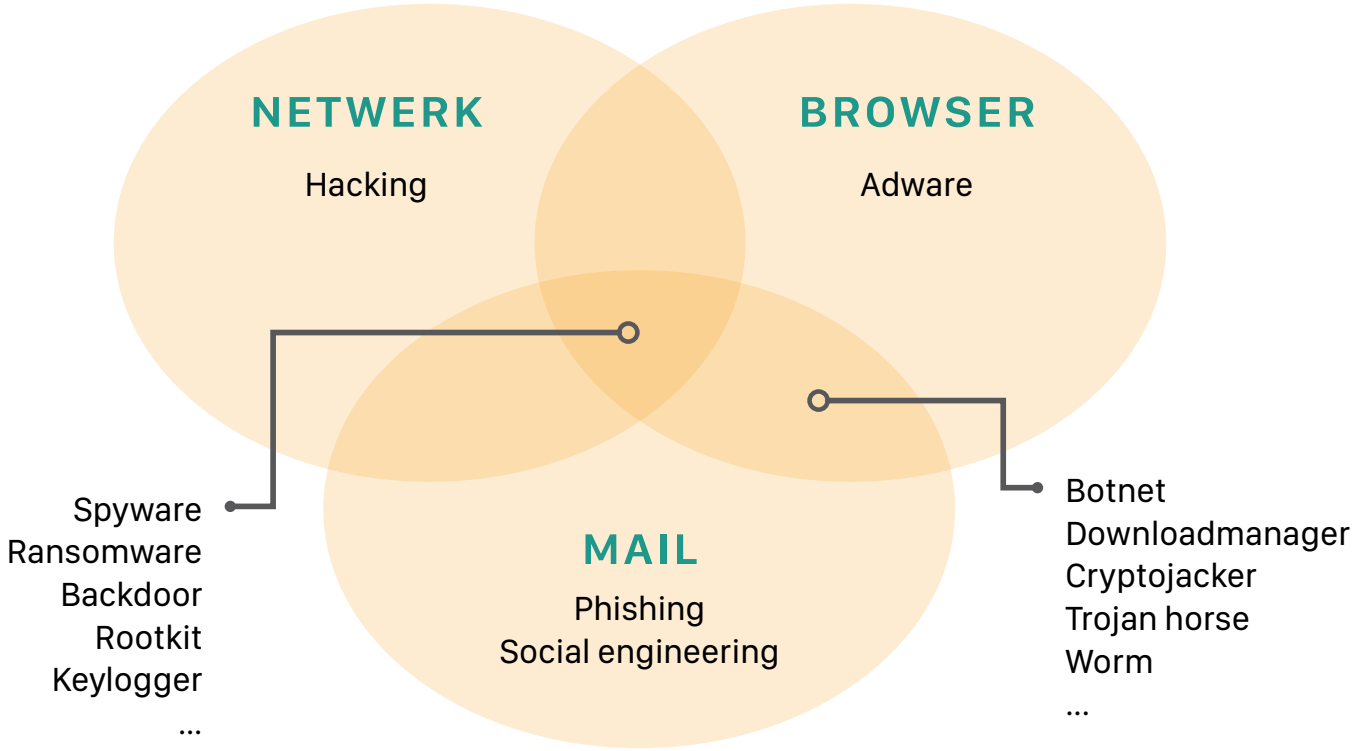
© MadMacX 2021 - www.madmacx.be

TOP

EEN SITUERING VAN MALWARE IN HET GEHEEL.

Er zijn zeer veel aspecten die invloed hebben op onze digitale levenssfeer (computers, netwerken, servers, mobiele toestellen, e.d.). Onder malafide invloeden verstaan we elke inbreuk of toepassing die de intentie heeft: a) je toestel over te nemen om acties aan te sturen die niet door jou gekend zijn of gevraagd werden; of b) je persoonlijke data te vangen en te misbruiken.

Een vereenvoudigde schets van de belangrijkste bedreigingen (the threat landscape).



MadMacX categoriseert deze bedreigingen op basis van hun ingangspunt (entry point): 1) browser, 2) mail (phishing) en 3) netwerk. Via één van deze 3 kanalen wordt het gros van de malafide digitale inbreuken gepleegd.

Malware wordt bij elk van deze entry points ingezet en verdient dus zeker een extra woordje uitleg (daarom ook deze paper). Voor een goed veiligheidsbeheer is het noodzakelijk om de drie entry points met de juiste bescherming af te dekken.

© MadMacX 2021 - www.madmacx.be

TOP

Helemaal veilig?

Zelfs met high level afdekking van de drie entry points **betaat er geen 100% security**. Er worden dagelijks nieuwe concepten rond security inbreuken bedacht. De deur staat dus in het beste geval op een kier, in het slechtste geval (zonder security tools, dus) staat de deur vaak wagewijd open.

Het is een race waarbij we als IT support partner via een juiste toolkit (combinatie van professionele oplossingen) de risico's zo klein mogelijk maken. We leggen bij elke professionele omgeving op dat vlak andere accenten, gebaseerd op de omkaderende netwerkinstellingen, de samenstelling van users en het type data.

SOCIAL ENGINEERING?

Voor de meeste vormen van cybercriminaliteit wordt tegewoordig flink gebruik gemaakt van Social Engineering*. Maar wat is dat nu precies? In de context van digitale veiligheid en informatica gaat het over het uitvoeren van misleidende of manipulatieve handelingen om individuen zover te krijgen confidentiële of persoonlijke informatie vrij te geven, die dan gebruikt wordt voor het stellen van fraudulente daden. Social Engineering heeft hier dus te maken met malafide intenties.

De realiteit van de hacker is, dat er vaak een eerste actieve handeling moet geïnitieerd worden door de hoofduser (voor jouw Mac, ben jij dat) om al dan niet rechtstreeks toegang te verlenen tot je toestel. Omdat je die toegang natuurlijk nooit zomaar met je volle verstand aan een wildvreemde zou geven, moet je op een of andere manier misleid worden om die stap te zetten. Daarom gaat elke zichzelf respecterende cybercrimineel op zoek naar de meest elegante manier om jou, via één van de drie hoofd-entry-points (mail, browser, netwerk), te verleiden het nodige te doen. Die hele misleidings- en verleidingsdans is Social Engineering.

De meest gebruikte strategie in dit domein zijn de phishing-berichten via mail, messenging apps of sms. Het betreft hier soms zeer persoonlijke berichten van onderschepte communicaties tussen familieleden of andere vertrouwensrelaties. De stap om op een verkeerde link te klikken is dan veel kleiner. Het aantal phishing-aanvallen en bijhorende slachtoffers stijgt de laatste maanden ook schrikwekkend.

**Niet te verwarren met Social Engineering in de context van de Sociale Wetenschappen, waar het hoofdoel niet draait om het ontfutselen van je gegevens, maar om het initiëren van grootschalige sociale (gedrags-)verandering en het reguleren van de maatschappelijke evolutie. Lange termijn manipulatie dus.*

© MadMacX 2021 - www.madmacx.be

TOP

DE VERSCHILLENDE TYPES MALWARE.

Een greep uit de belangrijkste categorieën van malware, met een klein woordje uitleg.

TYPE 1 - DOWNLOAD MANAGERS

Sommige sites die software-applicaties aanbieden, staan erop dat je hun 'eigen' downloadmanager gebruikt om de betreffende installer te downloaden. In sommige gevallen worden deze downloads dan vergezeld van 'bloatware' (=ongewenste software die invloed kan hebben op de werking van je toestel). Elke site die eist dat je hun downloadmanager gebruikt, kan je als malafide beschouwen. Dat is een rode vlag!

TYPE 2 - SPYWARE

De term 'spyware' is een verzamelnaam voor verschillende soorten malafide code, die allemaal één ding gemeen hebben: ze proberen sensitieve data te verzamelen. Dat kan bijvoorbeeld door ongemerkt foto's te maken met een webcam, of door informatie die je intypt op een website te onderscheppen. Deze gegevens worden dan op verschillende manieren tegen je gebruikt.

TYPE 3 - KEYLOGGER

Een veelgebruikt type spyware zijn 'keyloggers'. Eenmaal geïnstalleerd, registreren deze de toetsaanslagen die je typt en sturen deze in detail terug naar de server van de hacker. Zo achterhaalt die snoodaard je logingegevens als je je gebruikersnaam en paswoord ingeeft om ergens in te loggen. De weg ligt dan uiteraard volledig open om de betreffende account te manipuleren. Keyloggers zijn relatief zeldzaam in vergelijking met andere soorten malware, maar de schade die ze kunnen aanrichten is enorm.

TYPE 4 - BACKDOOR

Een 'backdoor' is een bewust ingebouwde (bv. door de oorspronkelijke ontwikkelaar als fail-safe) of onopzettelijk geprogrammeerde kwetsbaarheid in de code van een applicatie dat ongeautoriseerde toegang tot een systeem mogelijk maakt. Achterdeuren worden vaak uitgebuit door hackers om ongeoorloofde toegang te krijgen tot kritieke gegevens of om bestanden op een computer of mobiel apparaat te plaatsen. Ze komen verrassend vaak voor, zelfs in code die zo robuust is als iOS en macOS.

" Backdoors zijn het gevaarlijkste type malware-indringers. "

© MadMacX 2021 - www.madmacx.be

TOP

TYPE 5 - RANSOMWARE

Distributeurs van malware hebben veel verschillende doelen. Een belangrijk doel is geld verdienen. 'Ransomware' is daarbij een frequent voorkomende strategie. De naam verklaart deel van het opzet: **je data wordt gegijzeld en pas na betaling van losgeld weer vrijgegeven.**

Deze vorm van malware kreeg al de nodige aandacht in de media omwille van diens spectaculaire aard en vooral ook omwille van de zware financiële gevolgen.

Het is erg belangrijk dat, als je een ransomware-dreiging ontvangt, **je niet in paniek raakt** en twee keer nadenkt vooraleer contact op te nemen met de afzender. Door in te gaan op de vraag en proberen te voldoen aan de losgeldeis, markeer je jezelf als kwetsbaar.

Je vergroot daarbij de kans om in de toekomst het doelwit te worden van andere aanvallen.

In andere gevallen wordt er via mailverkeer beweerd dat er een ransomware aan de gang is, zonder dat er effectief versleutelingssoftware actief is binnen het netwerk.

Reden te meer om **eerst in detail na te gaan wat er precies aan de hand is en welke data al dan niet bedreigd wordt, en dus zeker niet te snel mee te gaan in de bewering.**

Dit soort blufwerk is onderdeel van de eerder besproken Social Engineering, waar ook Phishing een deel van uitmaakt.

" Ransomware versleutelt alle gegevens op de computer van het slachtoffer, waardoor deze onbruikbaar wordt.

Als het slachtoffer ermee instemt de kapers te betalen, ontvangen hij/zij een speciale code om de gegevens te ontgrendelen.

De recente macOS-aanval, KeRanger, eiste bijvoorbeeld dat gebruikers één Bitcoin betaalden om hun gegevens te herstellen."

© MadMacX 2021 - www.madmacx.be

TOP

MEER OVER RANSOMWARE.

Ransomware is een subcategorie van malware **waarbij onbetrouwbare software zichzelf op je computer nestelt en vervolgens bestanden ongevraagd versleutelt.**

Eens de ransomware geactiveerd is, krijg je twee duidelijke opties:

1. **nooit meer toegang krijgen tot de bestanden** op het gekaapte toestel, of
2. **losgeld betalen** om ze te decoderen.

In de praktijk staat de ransomware software gemiddeld 6 maanden passief op een toestel vooraleer die automatisch of via een externe trigger geactiveerd wordt. Daarmee worden bv. de gegarandeerde data-recuperatie termijnen (bv. 3 maanden) van cloud-opslagsystemen (zoals Dropbox, Onedrive, Google Drive, e.d.) omzeild.

Een goede bescherming tegen ransomware is de afhankelijkheid van je data te verkleinen door bv. een ontkoppeld en vooral gespreid data- en back-up-beheer. Zo kan je naar een back-up van een andere bron uitwijken als de data op je hoofdtoestel geblokkeerd werd.

© MadMacX 2021 - www.madmacx.be

TOP

TYPE 6 - CRYPTOJACKER

Een 'cryptojacker' kaapt de krachtbronnen van je Mac, zoals de CPU en het geheugen, om cryptovaluta te delven (Engels: mining). Crypto-currencies zoals Bitcoin worden 'gedolven' door computers die cryptografische puzzels oplossen. Naarmate er meer crypto-valuta in omloop komen, worden de puzzels complexer en hebben ze steeds meer krachtbronnen nodig. Gewetenloze crypto-miners trachten daarom de computers van andere mensen te gebruiken om hun verwerkingscapaciteit te maximaliseren. Door honderden of zelfs duizenden computers op deze manier in te zetten, kunnen hackers aanzienlijke hoeveelheden crypto-currency delven.

TYPE 7 - TROJAN HORSE

Een 'Trojaans paard', meestal afgekort tot 'Trojan', is een methode om malware op een computer te installeren door deze te verbergen of te vermommen als iets anders. Meestal neemt deze de vorm aan van een schijnbaar legitieme app die de gebruiker dan nietsvermoedend downloadt. Trojaanse programma's voeren allerlei geheime activiteiten uit, van het simpelweg kopiëren van bestanden tot complexe cyberaanvallen. Ze behoren eerder tot de familie van apps dan tot de software-categorie. Trojaanse paarden verbergen zich vaak in de 'eigen' downloadmanagers (zie Type 1) die door populaire downloadsites worden gebruikt.

TYPE 8 - BOTNET

Botnet verandert uw computer in een op afstand bediende spam-machine. Zo ben je mogelijk, zonder het te weten, één van die Facebook-bots die de politiek in een ander land probeert te destabiliseren. Botnet-netwerken bestaan soms uit miljoenen computers die - na de initiële infectie - soms lange tijd in slaapstand worden gehouden vooraleer ze worden geactiveerd voor de uitvoering/ondersteuning van een specifieke actie.

TYPE 9 - WORM

Een worm is een type malware dat zich snel van de ene computer naar de andere verspreidt. (een bekend voorbeeld is Koobface). Wanneer je de worm downloadt, verzamelt het details van je Facebook-vrienden en stuurt het hen schijnbaar persoonlijke berichten met daarin een link. Als de bestemmeling op de link klikt, krijgt deze een melding om de Adobe Flash Player up te daten. Bij instemming op deze vraag, wordt hun computer geïnfecteerd met de worm en krijgen ze gemanipuleerde advertenties (=adware) voorgeschoteld.

TYPE 10 - ROOTKIT

Een 'rootkit' is een verzameling hulpprogramma's, ontworpen om ongeautoriseerde toegang tot het root-account (de absolute kern van de systeeminstellingen) van een computer te krijgen. Zodra ze toegang hebben tot deze root, kunnen hackers letterlijk alles installeren op of toegang krijgen tot alle gegevens van het toestel. Normaal vereist dit soort ongeautoriseerde toegang zeer geavanceerde code en technieken. In 2017 werd echter ontdekt dat macOS High Sierra een kwetsbaarheid had die toegang tot de root bood door simpelweg het woord 'root' als gebruikersnaam in te voeren, zonder wachtwoord. Apple heeft de fout destijds snel rechtgezet met een update, maar dus wel degelijk na de feiten.

© MadMacX 2021 - www.madmacx.be

TOP

Nog enkele andere types onwenselijke software.

Type 11 - PUA/PUP
[Potentially Unwanted Applications or Programs]

'Potentieel ongewenste programma's (PUP) of toepassingen' (PUA) worden onbedoeld gedownload. Ze worden meestal verstopt in een wrapper (Engels voor verpakking) met een andere applicatie die de gebruiker wél bewust wilde downloaden. Deze wrappers worden soms samengesteld door downloadmanagers (zie Type 1) van sites die gratis software aanbieden. De PUP/PUA zelf is meestal een vorm van adware of spyware.

" 20% van alle Macs ter wereld is geïnfecteerd door PUP's – Potentially Unwanted Programs."

Sergei Shevchenko van Sophos – één van 's werelds grote security spelers op de digitale markt – vermeldde tijdens zijn toespraak op de Objective by the Sea-beveiligingsconferentie in 2019, **dat er bij 16% van hun klanten een effectieve PUA werd geblokkeerd.**

Daarnaast moest er bij slechts 1,06% van hun klanten een preventieve interventie rond macOS-malware infectie uitgevoerd worden.

De PUA's vormen dus een substantieel segment van de digitale security dreigingen.

© MadMacX 2021 - www.madmacx.be

TOP

TYPE 12 - BROWSERINFECTIES

Een groot deel van ons computergebruik speelt zich af in een webbrowser. Dat gedrag wordt daarom ook specifiek getarget. Browser-gebaseerde malware is de afgelopen jaren sterk toegenomen. Browserinfecties infiltreren de webbrowsers (Safari, Chrome, Firefox, e.d.) die op je Mac zijn geïnstalleerd. Dat gebeurt meestal wanneer je iets downloadt dat werd geïnfecteerd met malware. Browser-kapers verstoppen zich vaak in valse Flash-updaters of in browserextensies.

De nadruk ligt hier vooral op het manipuleren van de inhoud die de browser weergeeft, of het kapen van de functionaliteiten ervan, waaronder je startpagina, zoekfuncties, browser- en zoekgeschiedenis. Zo kunnen kapers op termijn aan zeer gevoelige private data geraken, met alle gevolgen vandien.

De meest bekende, recente malware-aanvallen manifesteerden zich in vorm van browser-kapers zoals: Time Search Now, Booking app, Tapsnake, Pitch of Case, Search Quick, ...

“ Sorry, we hebben je advertenties gestolen.

Wist je dat browserinfecties de reguliere advertenties kunnen vervangen om andere dingen te promoten?
De grootste bedreiging?
Gebruikers realiseren zich vaak niet dat ze al zijn gehackt. ”

TYPE 13 - “ZERO DAY” KWETSBAARHEID

Een zero day-kwetsbaarheid is een zwak punt in een stuk code, waaronder bv. die van besturingssystemen zoals macOS waarvan de producent zelf niet op de hoogte is. De producent kreeg dus ook nog geen kans om deze fout te remediëren (patchen, in het jargon).

Hackers misbruiken zo’n kwetsbaarheid om kwaadaardige code te injecteren, gegevens te stelen of andere problemen voor gebruikers te veroorzaken. Voorwaarde is dat het zwakke punt wordt ontdekt. Maar hackers gaan er doelbewust naar op zoek bij elk nieuw gelanceerd systeem en elke nieuwe update.

Niet elke zero-day-kwetsbaarheid leidt tot hacking van de broncode. Vaak worden ze ontdekt door ‘White Hats’ (=bonafide hackers) die de producent vervolgens op de hoogte stellen of het euvel openbaar maken. De producent lanceert dan meestal zo snel mogelijk een patch via een update van het besturingssysteem.

“Zero-day-kwetsbaarheid moet nog worden opgelost in een huidige versie van een besturingssysteem.”

Een recent voorbeeld van een zero-day kwetsbaarheid is BuggyCow. Dit zwakke punt werd ontdekt door het Project Zero-team van onderzoekers van Google. Het betrof een kwetsbaarheid in de code van Apple, waardoor een stukje malware - met normaal beperkte privileges - toegang kreeg tot delen van macOS die gereserveerd zijn voor programma’s met veel grotere privileges.

Deze kwetsbaarheid had impact op de manier waarop apps opslagruimte gebruiken als virtueel geheugen en op de mogelijkheid om het virtuele geheugen voor meerdere processen tegelijk toegankelijk te maken.

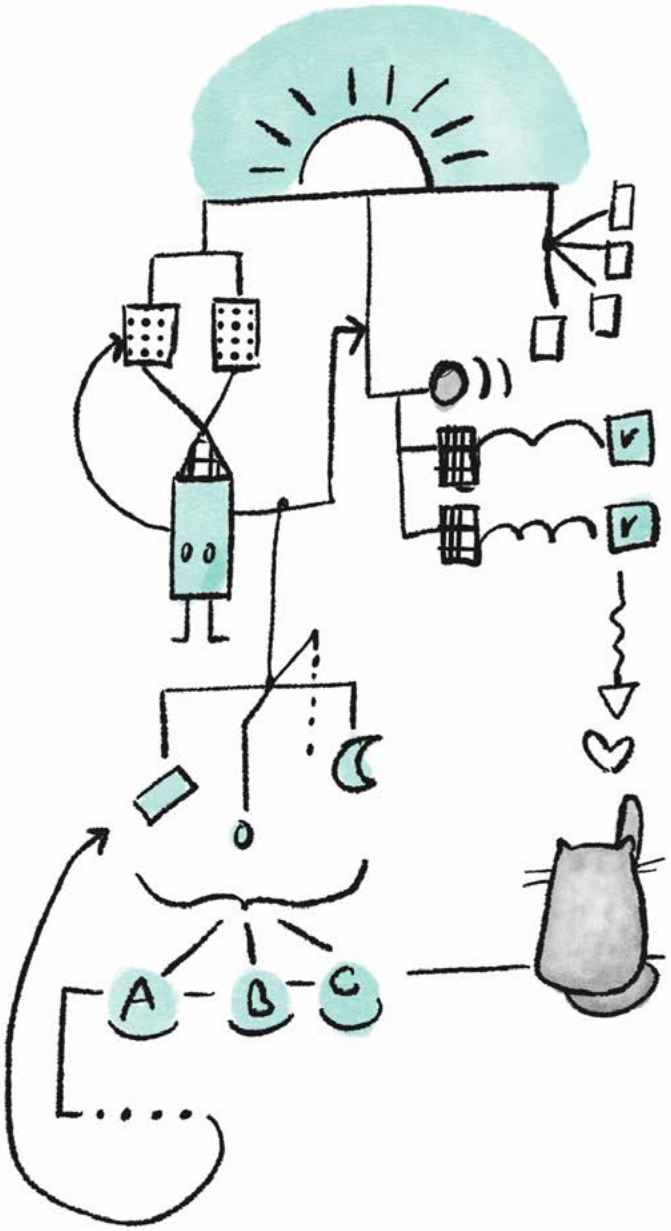
© MadMacX 2021 - www.madmacx.be

TOP

Een bug in het geheugenbeheer van macOS stond vrijblijvend toe een regulier bestandssysteem te ontkoppelen en opnieuw te koppelen – en dus 'vervangen' – met andere code, die de hacker meer rechten op je toestel gaf.

Eenvoudiger gezegd, jouw computer kon door iemand anders als server worden gebruikt. Onder andere voor criminele activiteiten.

Apple kreeg in 2019 kritiek omdat het niet snel genoeg handelde na meldingen door o.a. het Project Zero-team van Google.



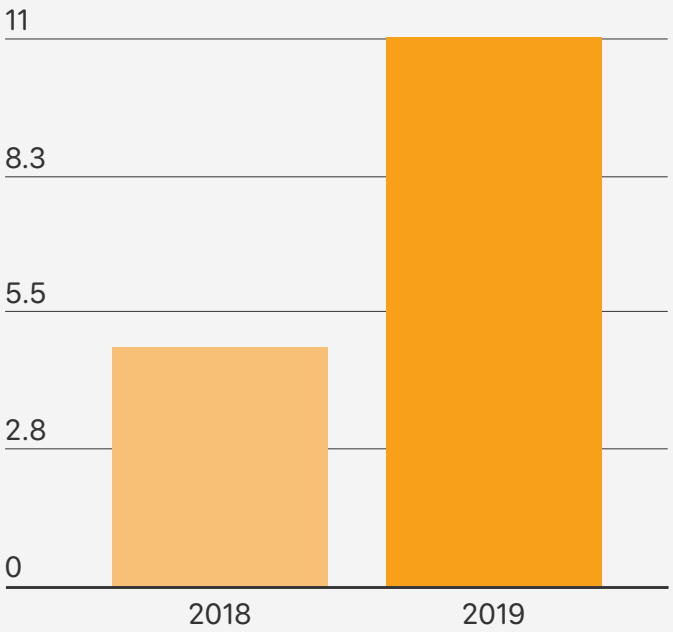
© MadMacX 2021 - www.madmacx.be

TOP

DE HARDE CIJFERS OMTRENT MALWARE OP MAC.

- **43%** van de cyberaanvallen is gericht op kleine bedrijven – 1 > 50 mensen
- **47%** van de kleine bedrijven had het afgelopen jaar te maken met cyberaanvallen, **44%** daarvan werd twee tot vier keer aangevallen.
- **70%** van de kleine bedrijven is niet voorbereid op een cyberaanval.
- **3 op de 4** kleine bedrijven zegt niet voldoende personeel te hebben om IT-beveiliging aan te pakken.
- **In 2018** kostten cyberaanvallen kleine bedrijven **gemiddeld $ 34.604**.
- **60%** van de kleine bedrijven gaat binnen zes maanden na een cyberaanval failliet.
- **69%** van kleine bedrijven hanteert geen strikte veiligheidsprotocollen.
- **16%** van kleine bedrijven zegt dat ze hun houding tegenover digitale veiligheid pas herbekeken na een cyberaanval.

De evolutie van detecties van inbreuken per Mac-toestel volgens Malwarebytes in 2018 en 2019.



source: www.malwarebytes.com

Kleine bedrijven maken zich het meest zorgen over de beveiliging van volgende klantgegevens:

- **66%** Consumentengegevens
- **49%** Intellectuele eigendom
- **46%** Credit- of debetkaartgegevens van klanten
- **26%** Financiële informatie
- **8%** Personeelsdossiers
- **5%** Zakelijke correspondentie
- **1%** Andere

Kleine bedrijven hebben met volgende soorten cyberaanvallen te maken:

- **49%** Web-based / Browser
- **43%** Phishing / Social Engineering
- **35%** Reguliere Malware
- **26%** SQL injectie
- **25%** Gecompromitteerde / gestolen toestellen
- **21%** Denial-Of-Service (DOS) aanvallen
- **14%** Geavanceerde Malware / zero day attacks
- **13%** Malafide medewerker
- **11%** Cross-site scripting (XSS)
- **2%** Ransomware (data-gijzeling)
- **1%** Andere

Malware wordt in quasi alle bovenstaande gevallen ingezet om de aanval uit te voeren of te faciliteren.

© MadMacX 2021 - www.madmacx.be

TOP

MEEST VOORKOMENDE MALWARE OP MAC.

Een lijst van de meestvoorkomende malware op Mac (2020), vastgesteld door Malwarebytes.

- **80.65%** OSX.Generic.Suspicious
- **13.19%** OSX.FakeFileOpener
- **1.96%** OSX.ThiefQuest
- **1.37%** OSX.BirdMiner
- **1.05%** OSX.SearchAwesome
- **0.74%** OSX.FakeAV
- **0.22%** OSX.Honkbox
- **0.15%** OSX.Dummy
- **0.1%** OSX.Adwind
- **0.1%** OSX.KeRanger

Enkele details, per type:

Generic.Suspicious

Goed voor meer dan 80% van de gevallen. Dit is echter geen specifiek geval van malware maar een verzamelterm, gebruikt door Malwarebytes, voor alle detecties die als verdacht of gevaarlijk worden beschouwd, maar (nog) niet aan een specifieke, gekende malware-categorie toe te wijzen zijn.

FakeFileOpener

Malwarebytes gebruikt de naam FakeFileOpener om apps te beschrijven die reclame maken voor PUP's (potentieel ongewenste programma's). Dit zijn meestal programma's die beweren systeemoptimalisatie te bieden.

Enkele voorbeelden:

1. Er verschijnt een pop-up waarin wordt gemeld dat je geen software hebt om een bepaalde app te openen. Je krijgt daarbij 'advies' over waar je de nodige software op het internet kan vinden. Niet op ingaan dus!

2. Of je krijgt een waarschuwing dat je toestel werd geïnfecteerd met een aantal virussen, vergezeld van de uitnodiging een app te gebruiken zoals Advanced Mac Cleaner, Mac Adware Remover of Mac Space Reviver, om dat op te lossen.

© MadMacX 2021 - www.madmacx.be

TOP

ThiefQuest (aka EvilQuest)

ThiefQuest installeerde zich op Mac-toestellen via een Russisch torrent-forum (je weet wel, die fora waar mensen illegaal films downloaden). Het stak de kop op in juni 2020. Aanvankelijk werd gedacht dat het om het eerste geval van Mac-ransomware ging sinds 2017, maar het bleek niet als ransomware te werken. De software versleutelde wel degelijk de bestanden, maar er was geen manier om te bewijzen dat er effectief losgeld werd betaald of om de bestanden terug te ontgrendelen. Het doel van ThiefQuest was dus niet om losgeld af te persen, maar om gegevens los te peuteren. Deze malware, bekend als 'Wiper'-malware, was de eerste in zijn soort op Mac.

BirdMiner

BirdMiner is een crypto-miner (zie Type 6) die wordt uitgevoerd op macOS-systemen, meer bepaald in een Linux-emulator (een soort ongewenst gecreëerde, afgeschermde bubbel die steunt op de Apple Linux opbouw en eigenlijk werkcapaciteit leent/steelt van het toestel in kwestie). Gebruikers van getroffen systemen ervaren een hoog CPU-gebruik, dat stopt zodra de malware merkt dat de Activity Monitor geactiveerd wordt. (Dit laatste is een ingebouwde macOS app waarmee je o.a. het geheugen- en processorgebruik van je Mac kan bekijken en beheren.) De malware kan zich dus slim blijven verbergen voor manuele controles via de Activity Monitor.

SearchAwesome

SearchAwesome is een soort adware dat zich richt op macOS-systemen. Deze malware werd voor het eerst in 2018 gedetecteerd en kan versleuteld webverkeer onderscheppen. In de praktijk worden er dan alternatieve advertenties geïnjecteerd in de webpagina's die je te zien krijgt. Het kan lang duren voor je door hebt dat je toestel geïnfecteerd werd omdat adware de basiswerking van je toestel meestal niet aantast. Het vervangt gewoon de officieel gepushte irritante reclame door een andere, illegaal gepushte, reclame. Hoe dan ook staat de deur hiermee weer een beetje meer open voor andere inbreuken.

FakeAV

FakeAV of 'Fake Anti Virus' is opniew een verzamelnaam voor elk type kwaadaardige software dat pretendeert antivirus voor macOS te bieden. De uiteindelijke infectie van het toestel kan zich in alle malware categorieën manifesteren.

Honkbox

Honkbox is nog een cryptominer die qua uitvoering en implementatie grotendeels vergelijkbaar is met OSX. BirdMiner.

Dummy

Dummy is een shellscript (= klein programma of lijstje van instructies) gericht op macOS-systemen. Het script creëert een 'backdoor' (zie Type 4) of achterpoortje door een uitgaande verbinding te maken met een extern IP-adres 185.243.115.230. Dit IP adres is een adres van een computer op het internet en achter dit IP adres schuilt een kwaadaardige server. Eens deze connectie werd gemaakt, heeft de hacker toegang tot de getroffen Mac. Deze malware werd verspreid op crypto-mining-chatgroepen door users die zich voordeden als beheerders.

AdWind

Adwind is een platformonafhankelijke (=niet exclusief Mac dus) 'backdoor' (zie Type 4) malware. Het is ontwikkeld in Java (open source programmeertaal) en beoogt eveneens externe toegang tot andermans systeem te realiseren. Een belangrijk symptoom is de actieve webcam, ook al ben je die zelf niet aan het gebruiken. Bij onderzoek valt er ook een schijnbaar willekeurig plist-bestand te detecteren in de LaunchAgents-map (een belangrijke systeemmap op je Mac). Deze malware werd per e-mail verspreid als een JAR (Java ARchive) bijlage. Adwind doet via de 'backdoor' tal van zaken, zoals het automatisch downloaden en uitvoeren van nieuwe malafide bestanden, het doorvoeren van externe opdrachten en het verzenden van gegevens van het geïnfecteerde systeem naar een server die wordt beheerd door de hacker(s).

© MadMacX 2021 - www.madmacx.be

TOP

KeRanger

KeRanger is momenteel een uitgefaseerde ransomware, omdat deze op het moment van dit schrijven niet langer in staat is om bestanden te versleutelen.

Toch duikt de malware nog af en toe op omdat een kleine groep hackers periodiek wil testen of het nog wel wordt gedetecteerd door de meest courante malware scanners.

Mocht dat niet meer zo zijn, wordt het opnieuw een interessant vehikel om nieuwe malware-functies aan te koppelen. Work in progress dus.

Ransomware had lange tijd geen effect op Mac-gebruikers maar met het verschijnen van KeRanger in maart 2016 kwam daar verandering in.

Claud Xiao en Jin Chen van Palo Alto Network leggen uit hoe KeRanger werkt: "De KeRanger-toepassing was ondertekend met een geldig ontwikkelingscertificaat voor Mac-apps. Het werd samen met een versie van een stukje legitieme software verspreid: de Transmission torrent-client (Transmission Project). Daarmee kon het de Gatekeeper-bescherming van Apple omzeilen. Als een gebruiker onwetend de geïnfecteerde apps installeert, wordt een er een bijgevoegde actie gelanceerd op het systeem.

KeRanger wacht vervolgens drie dagen voordat het verbinding maakt met 'command and control (C2) servers' via het Tor-anonimiseringsnetwerk. De malware begint vervolgens gegevensbestanden te versleutelen om aansluitend één bitcoin (ongeveer $400 op dat moment) van de slachtoffers te eisen - te betalen aan een specifiek adres - om hun bestanden ontgrendeld te zien.

Transmission is sindsdien aangepast; Palo Alto Networks heeft de URL-filtering en Threat Prevention bijgewerkt; en Apple heeft ook de nodige systeemingrepen doorgevoerd. Dit gebeurde allemaal nà dat talloze ongelukkige gebruikers het slachtoffer van de ransomware werden.

KeRanger blijkt nog altijd in actieve ontwikkeling en uitbreiding. De malware beoogt nu naar verluidt ook om Time Machine-back-upbestanden te versleutelen. Zo wordt er verhinderd dat slachtoffers hun bestanden kunnen herstellen via back-upgegevens.

© MadMacX 2021 - www.madmacx.be

TOP

HOE KUNNEN WE MALWARE AANPAKKEN?

Security is een vraagstuk van groeiende complexiteit dat vooral met bewustwording te maken heeft. Er is een 'nieuw normaal' in het digitale landschap en veel gebruikers zijn nog niet doordrongen van de omvang en alomaanwezigheid van de bedreigingen. We kunnen het geheel natuurlijk door slimme tooling en infrastructuur ondersteunen maar geen enkele oplossing kan sluitend zijn als de gebruiker zijn gedrag niet aanpast. Hieronder een overzicht van de ingrepen waar je zelf grotendeels impact op hebt.

- **Houd je macOS up-to-date**

Installeer de beveiligingsupdates van macOS altijd vanaf dat ze door Apple beschikbaar gesteld worden. Zo zorgt Apple deels zelf voor de beveiliging van het macOS systeem. Door updates te negeren bied je potentiële malware de kans om jouw Mac te infecteren.

Veel mensen stellen die updates uit om hun oude software operationeel te houden, maar werken hierdoor dus op een uitgefaseerd en dus minder veilige macOS. De deur staat dan open voor inbreuken op je systeem

- **Gebruik sterke paswoorden**

Het lijkt een no-brainer in het huidige security landschap. Cijfers en ervaring wijzen echter uit dat dit één van de meest voorkomende nalatigheden blijft, met zware data-, privacy- en beveiligingsproblemen tot gevolg. Gebruik nooit hetzelfde paswoord op verschillende diensten of websites en gebruik geen paswoorden waarin je persoonlijke informatie verschuilt. (zoals bijv: naamvanmijnhond123). Of nog beter: beheer je paswoorden via een slimme digitale paswoord-kluis.

- **Beveilig je netwerk**

Onze toestellen verbinden allemaal met het internet, of we nu thuis of op kantoor werken. Daarom is het zeer belangrijk dat ook deze netwerken goed beveiligd zijn. Een sterk WiFi-paswoord is daarbij het absolute minimum maar een goed geconfigureerde firewall is eigenlijk geen overbodige luxe. Ook voor kleine ondernemingen of eenmanszaken.

- **Veilig downloaden**

Download en installeer enkel software waarvan je zeker weet dat deze veilig is. Dit is één van de moeilijkst op te volgen aspecten. Hackers simuleren namelijk vaak op zeer schalkse wijze de vertrouwde software-platformen - zoals die van Adobe of Paypal - om hun malafide software op te dringen. Download je software dus enkel en alleen via de App Store van Apple.

- **Installeer goede anti-malware software**

Hoewel een Apple toestel by design een stuk veiliger is dan Windows en zelf al een hoop anti-malware maatregelen treft, is Apple in geen geval een cybersecurity bedrijf. Het is daarom belangrijk om de beveiliging nog flink op te krikken met extra lagen beveiliging.

.

© MadMacX 2021 - www.madmacx.be

TOP

- **Klik niet zomaar op links uit een email**

Phishing is helemaal in. Het is de meest voorkomende inbreuk op cybersecurity. Het betreft mails die vaak zeer goed gemaskeerd zijn als komende van een betrouwbare service of leverancier (bv. Paypal of Bpost). Door nietsvermoedend op de links in deze mails te klikken, geef je persoonlijke informatie vrij, waaronder vaak ook kredietkaartgegevens. Kijk steeds met extra aandacht naar het emailadres van de afzender om het kaf van het koren te scheiden.

- **Zorg dat je veilig surft via je browser**

Het internet is een allegaartje, dus waakzaamheid is cruciaal. Klik niet zomaar op links van minder bekende websites en geloof zeker niet alles wat je leest. Hackers spelen vaak in op emoties, om je snel naar een malafide website te leiden of om ervoor te zorgen dat je een onkuis bestand installeert, met alle gevolgen vandien.

- **Zorg voor een back-up van je data**

Dit advies valt nog vaak in dovemansoren, maar we kunnen het niet genoeg herhalen: neem back-ups van je data! We krijgen nog wekelijks de vraag om data te recupereren van schijven of toestellen, waar geen back-up van bestaat. Als dat al lukt, is het vaak een zeer kostelijke zaak.

Slimme data-opslag en bijhorende back-ups blijven de beste vorm van data-bescherming. Een goede back-up kan vaak zelfs een ransomware-aanval remediëren. Niemand wil de foto's van zijn kinderen of huwelijk zien verdwijnen óf daar een grote som geld voor neertellen om deze terug beschikbaar te krijgen.

madmacx
Apple IT for [creative] professionals.

Als Apple IT expert, beheert MadMacX zowat alle aspecten van de digitale levenssfeer van kleine ondernemingen.

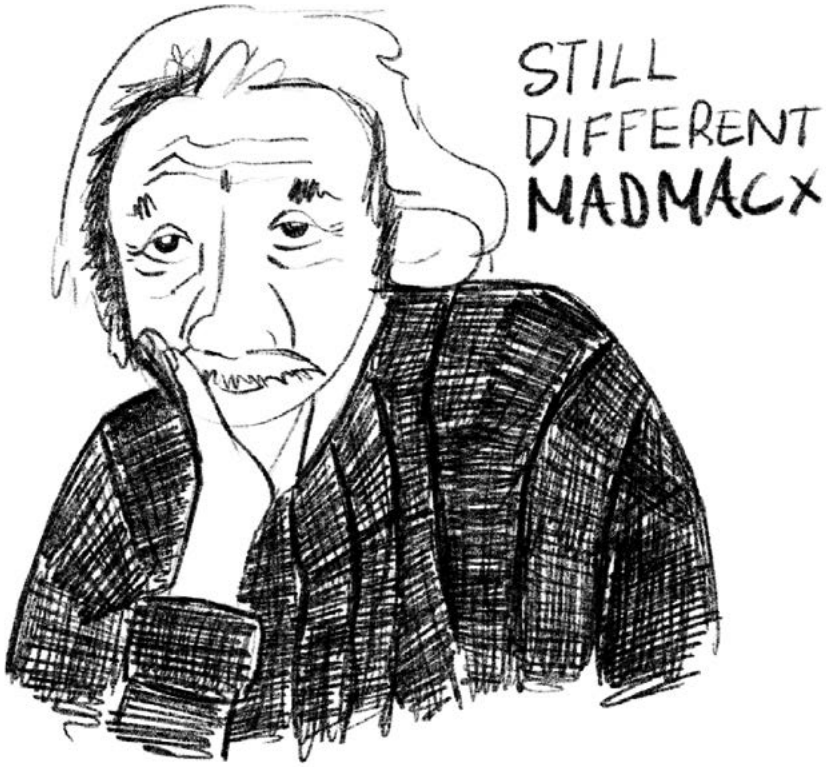
Onze aandacht gaat vooral naar het verhogen van productiviteit; slim data & back-up beheer; en gelaagde security.
Elke omgeving heeft andere noden.

Vraag vrijblijvend advies voor de optimalisering van jouw infrastructuur.

www.MadMacX.be
Broederminstraat 7B
2018 AntwerpEN

vision@madmacx.be
03 376 79 99

TOP



madmacx

Apple IT for [creative] professionals.

MADMACX.BE
BROEDERMINSTRAAT 7B
2018 ANTWERPEN

VISION@MADMACX.BE
03 376 79 99

© MadMacX 2021 - www.madmacx.be