Generalitat de Catalunya
Agència de Ciberseguretat de Catalunya

Butlletí de ciberseguretat

Situació COVID-19

Març 2020

ÍNDEX

01 Resum Executiu

Aquest comunicat va dirigit a **responsables i administradors TIC** i **professionals de l'àmbit de la ciberseguretat** perquè prenguin les mesures de verificació, contenció i erradicació que considerin adients en base a les recomanacions oferides, en relació a la situació creada per la COVID-19.

A mode de resum, el present comunicat recull les següents qüestions:

1. L'expansió mundial de la malaltia infecciosa COVID-19 ha generat una situació d'excepcionalitat que està sent aprofitada per actors cibercriminals.
2. Destaca l'impacte de ransomware a un dels principals laboratoris de proves de la COVID-19 de la República Txeca.
3. S'observa l'increment de campanyes de correus amb malware i de phishing o smishing relacionades amb la temàtica.
4. L'adopció massiva del teletreball de forma sobtada augmenta la superfície d'exposició fet que molt probablement també serà aprofitat pels cibercriminals.
5. Part d'aquesta activitat maliciosa ha arribat a Catalunya.
6. Aquest butlletí descriu les principals amenaces i recomana mesures a seguir vers les mateixes.

02 Descripció

L'expansió mundial de la malaltia infecciosa COVID-19 ha generat una situació d'excepcionalitat que està sent aprofitada per actors cibercriminals. Part d'aquesta ciber-activitat maliciosa arriba a Catalunya.

En l'àmbit digital, la situació creada per la COVID-19 té les següents característiques específiques:

- L'adopció majoritària i sobtada de diferents modalitats de teletreball.
- L'increment de l'atenció a missatges i canals digitals sobre aquesta malaltia, el virus que la causa i l'impacte dels mateixos.
- L'augment de criticitat dels serveis bàsics i essencials, amb especial èmfasi en serveis mèdics, de protecció civil i d'abastiment.

Les característiques de la situació excepcional actual estan sent aprofitades per diversos actors maliciosos per incrementar l'èxit de les seves campanyes. A l'àmbit internacional, destaquen el cas de suplantació de la OMS descrit anteriorment i, sobretot, l'impacte del desplegament de ransomware a un hospital de la República Txeca, que és, a més, un dels principals laboratoris de proves de la COVID-19 del país.

El següent llistat es un resum d'algunes de les principals amenaces i les seves categories identificades a nivell mundial en les últimes setmanes.

Tipologia d'amenaça	Campanyes	Exemples concrets
Indisponiblitat	Enviament de correus amb adjunts maliciosos de tipus ransomware	
	Distribució d'aplicacions mòbils que suposadament permeten fer un seguiment de l'evolució de la malaltia, però que en realitat segresten l'accés físic al terminal	https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware

Tipologia d'amenaça	Campanyes	Exemples concrets
Compromís del sistema	Enviament de correus impersonant organitzacions com la OMS (WHO en anglès) per distribuir RATs o programari maliciós amb el que llançar subsegüents atacs.	• GuLoader+FormBook • NanoCore RAT • HawkEye • Emotet. En aquest cas, aquest programari maliciós es conegut per habilitar atacs molt devastadors d'altres famílies de malware com Trickbot i Ryuk, relacionats durant el 2019 per estar darrere de milers d'atacs de ransomware al món i a Catalunya
	Distribució de mapes de seguiment d'infeccions del COVID-19 suposadament legítims, que fan servir dades descarregades en temps real des de la Universitat Johns Hopkins, tot i que en realitat aprofiten per instal·lar programari maliciós per prendre control sobre el sistema.	• AZORUlt • Loader distribuït per un actor cibercriminal en un fòrum underground: https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Tipologia d'amenaça	Campanyes	Exemples concrets
Frau	Per demanar diners i donacions	• Del "Department of Health": https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/ • Del "Centers of Dicease Control and Prevention" dels USA (CDC): https://www.bbc.com/news/technology-51838468

	Per llançar atacs de frau a través del compromís del correu corporatiu (BEC)	• https://www.bleepingcomputer.com/news/security/ancient-tortoise-bec-scammers-launch-coronavirus-themed-attack/

Tipologia d'amenaça	Campanyes	Exemples concrets
Robatori d'Informació	Campanyes de phishing impersonant organismes oficials per robar informació sensible.	Suplantació dels CDC de USA, de la OMS o del "HM Revenue and Customs" per aconseguir credencials de correu o dades financeres: https://www.bbc.com/news/technology-51838468
	Phishing utilitzat per actors molt avançats dirigits contra governs	És el cas de Mongòlia: https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
	Campanyes de smishing suplantant entitats financeres.	

Aquestes amenaces aprofiten majoritàriament els següents vectors d'atac:

- **Correus o SMS temàtics** en que es suplanta la identitat emissora. Aquest tipus de missatges persegueix majoritàriament l'obtenció de credencials mitjançant portals fraudulents de phishing i/o el desplegament de malware als equips de les víctimes.
- Correus amb documents que **instal·len programari maliciós**. S'envien correus amb documents que suposadament contenen informació sobre com actuar davant la malaltia, però que executen malware un cop oberts.
- Programari maliciós fent-se passar per programes que donen **dades en temps real** de l'expansió de la malaltia. S'utilitza la curiositat de l'usuari per aconseguir que executi programes que prendran el control de la màquina, podent robar dades dels usuaris o instal·lar ransomware als equips.

- La relaxació dels protocols de seguretat i l'obertura d'accessos a serveis des de internet per a facilitar el teletreball.

A **l'àmbit de la Generalitat Catalunya** s'ha pogut identificar dues campanyes malicioses que intenten explotar les preocupacions sobre el brot de COVID-19 per als seus propis fins criminals, i que estan actuant a nivell internacional. Les campanyes observades son en anglès:

- Destaca la campanya que està falsificant el domini de l'Organització Mundial de la Salut. El correu electrònic ofereix una "Actualització de Coronavirus" i conté un arxiu adjunt comprimit que inclou un executable capaç de descarregar Formbook, un programari maliciós amb la capacitat de robar informació i descarregar altres programes.
- La segona campanya a destacar utilitza correus amb el tema 'Problema d'assessorament a el client de Coronavirus' i ha adjuntat un arxiu PDF que pot executar i descarregar el malware Lokibot, un troià que crea una porta del darrere en els sistemes de Windows per robar informació confidencial de les víctimes.

03 Mesures i recomanacions

En front a l'arribada de missatges no sol·licitats, ja sigui via xarxes socials, SMSs o correus, es recomana **avisar els usuaris** per tal que es desconfiï d'aquests i per a què, per norma general, la informació s'obtingui a través de **canals de confiança**, tant d'organismes governamentals oficials com de mitjans periodístics o d'especialistes coneguts. Es recomana els següents portals a tall d'exemple:

- Entrada sobre el nou coronavirus al Canal Salut del Departament de Salut de la Generalitat de Catalunya: http://canalsalut.gencat.cat/ca/salut-a-z/c/coronavirus-2019-ncov/
- Entrada sobre el brot de la malaltia COVID-19 al portal de la OMS (WHO, en anglès): https://www.who.int/emergencies/diseases/novel-coronavirus-2019 (disponible en 6 idiomes, inclòs el castellà).

Pel que fa a l'adopció de modalitats de teletreball, l'Agència de Ciberseguretat de Catalunya recomana realitzar, sempre que sigui possible, una **transició ordenada que mantingui els estàndards de seguretat de l'organització**. Més enllà de les normes aplicables, tals com les descrites al document "Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball", adreçat als treballadors de la Generalitat de Catalunya i el seu Sector Públic, es recomana a responsables i administradors TIC i professionals de l'àmbit de la ciberseguretat seguir les mesures següents:

- Mantenir actualitzats els sistemes VPN, l'equipament d'infraestructura de xarxa i els equips utilitzats per al treball en remot.
- Assegurar la traçabilitat dels mecanismes establerts per a oferir connexió des de l'exterior i la vinculació d'aquests mecanismes amb els sistemes de protecció de l'organització (p.e. vinculació amb solucions IPS de l'organització).
- Implementar l'ús de mecanismes d'autenticació multi-factor (MFA) als serveis exposats a Internet i dissenyats per l'ús intern (VPNs i servei de correu inclosos).
- Implementar mecanismes per a assegurar que es compleixen les polítiques de renovació de credencials i, en cas d'utilitzar paraules de pas, que aquestes siguin robustes. Especialment en els serveis exposats a Internet i dissenyats per a l'ús intern (VPNs i servei de correu inclosos).
- Avaluar les limitacions de la infraestructura d'accés remot i establir mecanismes de gestió de la demanda que es considerin adients.
- Establir mecanismes i normes que regulin l'ús de dispositius no corporatius (BYOD) i mecanismes que n'assegurin el compliment, allí on estigui autoritzat. Recordem que les normes de la Generalitat de Catalunya únicament admenten l'ús de BYOD connectant contra la extranet.
- Tal com s'ha mencionat anteriorment, notificar al personal l'increment de campanyes malicioses que persegueixen obtenir accés a les xarxes corporatives mitjançant el compromís de credencials o del sistema utilitzat en remot.

04 Referències

Agència de Ciberseguretat de Catalunya: Normes de ciberseguretat per a la prestació de serveis en la modalitat de teletreball, adreçat als treballadors de la Generalitat de Catalunya i el seu Sector Públic
https://ciberseguretat.gencat.cat/ca/detalls/noticia/Normes-de-ciberseguretat-per-a-la-prestacio-de-serveis-en-la-modalitat-de-teletreball

WHO: Beware of criminals pretending to be WHO
https://www.who.int/about/communications/cyber-security

ZDnet: Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak
https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/