Table of Contents

1. Introduction

Since the beginning of the COVID-19 crisis, security actors are unanimous: the number of cyber threats and attacks is increasing consistently.

On March 25th 2020 Hacknowledge decided to launch the free-of-charge « **Heath Crisis Solidarity Project**» addressed to the health sector in both Luxembourg and Switzerland.

The idea was to support IT teams during the pandemic crisis to prevent an IT disaster from occurring at the same time, as they face the already complicated current situation.

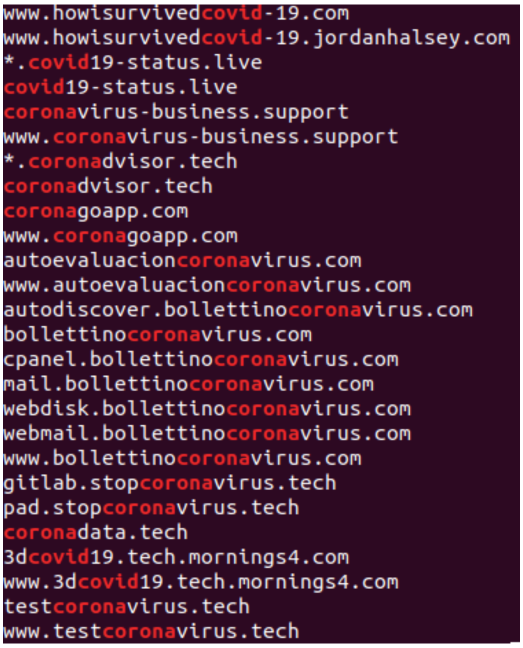
Due to a high demand and because solidarity is important in this crisis time, Hacknowledge has decided to expand the provided service to all actors engaged in the fight against COVID-19 and to make the present newsletter available to other sectors who also have to deal with a unusual situation due to COVID-19.

This provided service can be split in several parts such as:

- Better anticipate threats: a weekly newsletter to stay aware about active threats and campaigns (available to all sectors)
- better target corrective actions: easy-to-implement workarounds & quick-wins against recent weaknesses;
- Limit the risk exposure and attack surface: OSINT to identify your Internet exposure + simple service discovery scans (**NOT A VULN SCAN SENDING UNCONTROLLED DATA**) in order to identify the "shadow IT" and the services exposed requiring particular attention : **NO EXPLOITATION** in order to exclude any risk of service interruption;
- Allow you to focus on YOUR job **: SAVING LIVES** !

2. Active Campaign

- As any computer security expert knows, many new domain registrations using “covid-19”, “coronavirus”, "vaccine" have been registered in the last few days, which means that we can say that the delivery campaign of malware, phishing attacks, fraud, etc. will continue and even increase.
  We would like to emphasize this point and encourage you to actively communicate with end users by explaining that they must be particularly vigilant by clicking on a link related to the COVID-19.
  Some lists are publicly available on social media such as Twitter (not exhaustive – note that it does not mean that EVERY entries here are malicious) :



```
www.howisurvivedcovid-19.com
www.howisurvivedcovid-19.jordanhalsey.com
*.covid19-status.live
covid19-status.live
coronavirus-business.support
www.coronavirus-business.support
*.coronadvisor.tech
coronadvisor.tech
coronagoapp.com
www.coronagoapp.com
autoevaluacioncoronavirus.com
www.autoevaluacioncoronavirus.com
autodiscover.bollettinocoronavirus.com
bollettinocoronavirus.com
cpanel.bollettinocoronavirus.com
mail.bollettinocoronavirus.com
webdisk.bollettinocoronavirus.com
webmail.bollettinocoronavirus.com
www.bollettinocoronavirus.com
gitlab.stopcoronavirus.tech
pad.stopcoronavirus.tech
coronadata.tech
3dcovid19.tech.mornings4.com
www.3dcovid19.tech.mornings4.com
testcoronavirus.tech
www.testcoronavirus.tech
```

Figure 1: COVID-19 related DNS entries

- Active campaign targeting FRENCH users is actively spreading via twitter :
  The platform https://v-lert.com/ encourages people to download/install « valert.apk », a fake COVID-19 application containing ANUBIS (banking) malware.

  About Anubis :
  https://blog.trendmicro.com/trendlabs-security-intelligence/anubis-android-malware-returns-with-over-17000-samples/
  V-LERT apk Virtustotal results (note that some **important A.V solution do not detect this one** at the moment):
  https://www.virustotal.com/gui/file/6c90d561b580d6f1ae29998d4617567e7b45b91409322b687a65c98df6efacc2/detection

- COVID-19, Info Stealer and the Map of Threats is actively used to target Microsoft Windows users by delivering a malware using a fake coronavirus map viewer «Corona-virus-Map.com.exe ».
  Malware analysis on Virustotal :
  https://www.virustotal.com/gui/file/2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307/detection

  Right URL for coronavirus map from Johns Hopkins University is :
  https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

- Two zero-days are Targeting DrayTek Broadband CPE Devices are actively exploited "in the wild" by attacker. Note that an exploit for one of these unpatched issues was released on Monday 30th March 2020.
    1. Public disclosure : https://blog.netlab.360.com/two-zero-days-are-targeting-draytek-broadband-cpe-devices-en/
    2. Exploit : https://gist.github.com/0xsha/e7f59e9332b44d151039059bc98c554b
    3. Active attacks : https://www.securityweek.com/vulnerabilities-draytek-enterprise-routers-exploited-attacks

- Multiple vulnerabilities impacting the **D-Link DSL-2640B DSL gateway**:
    1. all vulnerabilities are (at least) applicable to the D-Link DSL-2640B (HW revision B2)
    2. all vulnerabilities apply to the latest available firmware (as of 27/03/2020)
    3. all vulnerabilities have been reported to D-Link
    4. we are not aware of any security fix released by D-Link
    5. as the device is EoL, following D-Link's policy, no fix may ever be available

Paper : https://raelize.com/posts/d-link-dsl-2640b-security-advisories/

- CVE-2019-10149 active campaign is running against unpatched systems
  Ref : https://nvd.nist.gov/vuln/detail/CVE-2019-10149

- Since COVID-19 enforces homeworking, attackers actively exploit **Zoom** to spread malware

Paper : https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/

- **[IMPORTANT]** Specific note to BGL customers :
  Few days ago Hacknowledge reported an active phishing/SMS campaign targeting BGL users.

  CIRCL was informed and the main domain in use was taken down (szontag.de).
  The malicious mail/SMS requires users to click on shortened URL https://da.gd that is a redirect to the malicious website https://webbanking.bgl.lu-fr-webbanking-login-bnp-paribas.szontag.de .

  We would like to ask you to be extremely careful when receiving a request from your bank, specifically in those times where attacks are growing, in case of suspicious, contact your bank using the classical channel instead of unknown one.

  Note that this advice should also be applied to other bank's users to protect against such attacks.

Newsletter #1 updates :

- **CVE-2020-0796** (SMB Ghost) updates : A PoC was released leading to DoS only, however, based on social media we are aware that several teams are actively working on reliable exploit that will be actively used within a few days by using patch diffing technique meaning that there is an emergency to apply the associated fix.

Publication and PoC : https://blog.zecops.com/vulnerabilities/vulnerability-reproduction-cve-2020-0796-poc

- **Type 1 Font Parsing RCE (Remote Code Execution Vulnerability) 0day** :
  CERT Europa released an updated version of the advisory on their website and no official fix is available at the moment.
  Note that workaround details are provided in this document.

  Paper : https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-017.pdf
  Micro Patch technical details: https://blog.0patch.com/2020/03/micropatching-unknown-0days-in-windows.html

- In case of having partners or remote workers in Asia, active campaign related to COVID-19 is still active for Hong-Kong based IOS and Android users:

Technical analysis about infection mechanisms and exploit-chain for both IOS and Android platforms:

https://documents.trendmicro.com/assets/Tech-Brief-Operation-Poisoned-News-Hong-Kong-Users-Targeted-with-Mobile-Malware-via-Local-News-Links.pdf

3. How to Protect: What We Recommend / Quick-Wins to Stay Safe

- Inform users about latest threats and ask them not to download and/or install any .apk/.exe file from website ;

- In case of using IOS or Android, always install Antivirus solution to limit risks – free software exist and, even if not perfect, can prevent on classical malware ;

- If you use ZOOM meeting plateform :
    1. Connect to Zoom via SSO if possible ;
    2. Activate the « waiting room » to validate who will join the meeting ;

- Validate that you do not expose useless management interface on the Internet / challenge your exposure ;

- Keep your infrastructure **up-to-date** including internally used applications, web browsers… ;

- Check your patch management policy to validate that all assets are covered ;

- Deploy **kb4551762** on Windows machines and apply « quick-wins » or « micro-patch » to mitigate the « Type 1 Font Parsing RCE » 0 day vulnerability on affected component ;

- If unsure about the authenticity of a website, don't proceed with any login procedures (if you already clicked) ;

- Implement double factor authentication when possible, specifically on exposed assets (VPN access…) ;

- Beware of COVID-19 related phishing schemes and fake alerts/health advisories ;

- Monitor :
    1. Remote access devices ;
    2. Abnormal network load peaks (data exfiltration) ;
    3. Suspicious credential sharing ;
    4. Mail gateway/spam alert and covid-19/coronavirus/vaccine URL accessing ;
    5. Log all remote access events ;

4. Latest « COVID-19 » Related Papers And Resources

Official papers

- Europol : https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic
- Thales Group covid-19/I.T security analysys (FR) : https://www.thalesgroup.com/fr/marches-specifiques/systemes-dinformation-critiques-et-cybersecurite/news/le-covid-19-une-nouvelle
- AUSCERT recommendation : https://www.auscert.org.au/blog/2020-03-16-covid-19-observations-osint-and-safety-recommendations

Some news from battlefield

- https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks
- https://www.zdnet.fr/actualites/un-hopital-tcheque-frappe-par-une-cyberattaque-en-pleine-epidemie-de-covid-19-39900659.htm
- https://www.zdnet.fr/actualites/l-ap-hp-visee-par-une-attaque-ddos-39901161.htm
- https://www.theverge.com/2020/3/25/21194417/namecheap-coronavirus-covid-19-domain-name-ban-registrar-abuse
- https://www.reuters.com/article/us-china-health-amazon-com/amazon-bars-one-million-products-for-false-coronavirus-claims-idUSKCN20L2ZH
- https://www.securityweek.com/hackers-target-two-unpatched-flaws-windows-adobe-type-manager-library

Additional Useful Resources

Online sandbox for malware analysis : https://medium.com/@su13ym4n/15-online-sandboxes-for-malware-analysis-f8885ecb8a35

Oracle's commitment to our customers and partners during the COVID-19 crisis (FAQ) : https://www.oracle.com/corporate/covid-19.html

Contacts

Bourbon Jean-Marie – Head of Offensive Security

Mail : jean-marie@hacknowledge.lu

Phone : (+352) 661 523 211

Barbara Terra – Sales Manager

Mail : barbara@hacknowledge.lu

Phone : (+352) 671 122 709